STRATEGIC PLAN & MARKET ANALYSIS:

Enterprise Approach to Zero Trust

Florida Digital

Florida Digital Service
2555 Shumard Oak Blvd • Tallahassee, FL 32399
www.digital.fl.gov

Executive Summary

The Florida Digital Service (FLDS), pursuant to section (s.) 282.0051 and s. 282.318, Florida Statutes (F.S.), conducted a market analysis and developed a strategic proposal to achieve a Zero Trust Architecture (ZTA) and framework across the state enterprise. The Zero Trust strategic initiative is a holistic redesign of the state's digital architecture. ZTA will modernize Florida's cybersecurity infrastructure, including hardware, software, network components, cloud resources, and other information technology resources, ensure the protection of digital assets, including sensitive citizen data, sustain critical public services, and reinforce public trust in government operations. This architectural transformation enhances the traditional perimeter-based defenses to establish a proactive security model built on continuous verification, least privilege access, and granular controls across all digital assets.

The Imperative for Zero Trust

The increasing frequency and severity of cyber threats have exposed vulnerabilities in traditional security models, prompting the need for a resilient and adaptive approach. The Zero Trust framework emphasizes a "never trust, always verify" philosophy, treating every user, device, and network as untrusted until authenticated and authorized. This paradigm directly aligns with Florida's strategic objectives to modernize legacy systems, enhance interoperability among state agencies, and create a secure, scalable digital environment.

Strategic Objectives

The Zero Trust Architecture is grounded in five foundational Strategic Objectives, designed to comprehensively secure digital environments while enhancing operational efficiency and resilience:

1. **Establish a Federated Identity and Access Management (IAM) Framework**
   Identity management ensures that every user, device, and application accessing state resources is verified. A standardized, federated IAM framework reduces silos and enhances collaboration among agencies. Florida ensures secure access to sensitive information by adopting Multi-Factor Authentication (MFA) and continuous authentication. This strengthens security, aligns identity processes with real-time risk analytics, and ensures trust is continuously verified.

2. **Secure All Endpoint Devices**
   Endpoint devices are critical entry points for accessing state resources. Florida must enforce endpoint security policies, including real-time asset discovery, compliance checks, and continuous monitoring. Unified endpoint management (UEM) tools and Artificial Intelligence/Machine Learning (AI/ML)-driven threat detection mitigates risks associated with managed, unmanaged, and BYOD devices, ensuring all endpoints meet stringent security baselines.

3. **Enable Secure Network Access**
   Networks serve as conduits for data and resources. Secure network access requires continuous authentication, segmentation, Software Defined Perimeters (SDPs), and Secure Access Service Edge (SASE) capabilities. Implementing micro-segmentation and migrating to hybrid cloud environments enhances network resilience. Florida can streamline secure connectivity for distributed resources by integrating SASE, which combines network security functions with wide-area network capabilities. Continuous monitoring and analytics reinforce ZTA by ensuring that anomalies are detected early.

4. **Achieve Application-Level Visibility and Management**

   Applications must be continuously monitored for vulnerabilities. Florida will onboard applications into the Zero Trust framework, define clear access policies, and adopt secure software development practices. Progress in application visibility and management is enhanced by the development of a data catalog and Zero Trust Identity and Access Management (IAM) framework. However, these initiatives are designed to proceed in parallel with phased integration points. Standardized, centrally governed permissions, implemented either through a shared service or federated framework, along with regular vulnerability management, will ensure applications align with Zero Trust, minimizing risks and enhancing resilience.

5. **Treat Data as the New Perimeter**

   Data protection is central to Zero Trust. Continuous data discovery, tagging, and classification enable granular access controls. By incorporating Data Security Posture Management (DSPM), Florida can achieve real-time insights into data risks and compliance gaps across cloud and on-premises environments. Encryption and Data Loss Prevention (DLP) tools further safeguard data throughout its lifecycle, ensuring compliance and reducing exposure risks. This approach positions data as the focal point of security efforts, enhancing visibility and protection against unauthorized access.

Proposed Implementation Roadmap

The Zero Trust strategy will be executed through a phased approach:

- **Phase 1: Planning**
  Establishing objectives, stakeholder alignment, and foundational assessments.
- **Phase 2: Baselining**
  Evaluating current capabilities and identifying gaps.
- **Phase 3: Strategizing**
  Developing detailed roadmaps and prioritizing high-impact use cases.
- **Phase 4: Testing**
  Piloting proof-of-concept initiatives to refine strategies.
- **Phase 5: Scaling and Optimization**
  Expanding implementation across agencies while continuously improving processes.

Conclusion

Florida positions itself as a leader in cybersecurity resilience, protecting its critical infrastructure, safeguarding digital assets, including sensitive information related to citizens, and enabling a secure, interconnected digital government by adopting a Zero Trust framework. This strategy reflects a commitment to leveraging modern technology, fostering collaboration among state agencies, and embedding security into the foundation of public service operations.

Table of Contents

Introduction

Digital security has emerged as a paramount concern because of increasingly interconnected digital environments. The rapid expansion of digital technologies, combined with the rise of sophisticated cyber threats, has placed unprecedented pressure on traditional security frameworks. Florida's statutory requirements, outlined in s. 282.0051, F.S. and s. 282.318, F.S., mandate that the state take a proactive approach to protecting public systems and digital assets, including sensitive information related to citizens. Traditional security models that rely on perimeter defenses are no longer adequate to mitigate modern threats. The perimeter-based approach is built on the assumption that threats originate primarily from outside the network and fails to address the evolving tactics of attackers who now exploit vulnerabilities both inside and outside the perimeter. Perimeter-based defenses have been proven inadequate against increasingly sophisticated cyber-attack methods, including social engineering, zero-day exploits, and supply chain compromises. The advancement of attack methods necessitates the adoption of a security strategy that aligns with public policy objectives, including cost efficiency, public trust, and enhanced services reliability.

The Zero Trust Paradigm

Zero Trust has emerged as a cornerstone for broad-spectrum transformation across IT systems, operational workflows, and organizational culture. This transformation contributes to enhanced governance, improved system resilience, and a more cohesive IT infrastructure by bridging advanced security with IT operations. These outcomes align with strategic objectives that prioritize both innovation and efficiency across Florida's digital ecosystem. This change facilitates a reevaluation of foundational IT strategies and links security imperatives to broader goals of efficiency and innovation. ZTA fosters a cohesive approach that aligns technical innovations with strategic objectives by embedding security into every layer of IT infrastructure. Adopting ZTA will fortify Florida’s security posture and redefine the state’s IT infrastructure to align with the multifaceted demands of a digital-first government.

Architectural Modernization

The foundational principles of Zero Trust necessitate a reevaluation of traditional IT architectures. ZTA prioritizes the enhancement of interoperability, the systematic migration to cloud-native environments, and the strategic decommissioning of legacy systems. This architectural reassessment equips Florida with the ability to harness innovative technologies, optimize operational efficiencies, and ensure seamless interagency integration while addressing scalability and adaptability requirements. A Zero Trust approach supports robust infrastructure design by embedding security directly into the architecture, rather than treating it as an add-on. Infrastructure integration ensures that foundational improvements support subsequent process modernization efforts, creating an ecosystem where secure architectural and operational efficiency work together to address evolving governance and technological demands.

Operational Efficiency

The implementation of Zero Trust fosters systemic advancements in operational efficiency by institutionalizing standardized processes in critical areas such as identity lifecycle management, data governance, and incident response. Automation and orchestration streamline repetitive, high-volume tasks, redirecting human resources toward strategic, value-driven initiatives. Concurrently, real-time analytics augment the state's capacity for data-driven decision-making, enabling responsive and predictive operational agility that aligns IT functionalities with overarching governance objectives. Beyond efficiency gains, Zero Trust principles integrate visibility and control at every layer of the IT environment. Real-time monitoring and dynamic access controls ensure that operations remain resilient even under adverse conditions. Utilization of telemetry and analytics tools provides actionable insights into system performance and user behavior, enabling continuous optimization of both security and operational workflows.

Enhancing Cross-Agency Collaboration

Modernization happens faster and more effectively through cross-agency collaboration, where standardized processes and shared platforms reduce redundancies and foster seamless interconnectivity. For example, the MyFloridaNetwork system provides a unified communication network that enhances connectivity and information sharing. Federated identity management (FIM) systems, interconnected across agencies to enable enterprise-wide visibility, and interoperable data-sharing platforms would further enhance decision-making by providing agencies with real-time access to critical information, improving response times, and enabling more effective public service delivery. These collaborative efforts result in a more agile and cohesive state IT ecosystem that supports faster service delivery and enhanced user experiences.

Cultural Transformation

Adopting Zero Trust paradigms mandates a profound cultural shift from legacy constructs of implicit trust to a philosophy centered on perpetual verification and contextual adaptability. This shift transcends technical implementation, fostering interdisciplinary collaboration among IT professionals, policy architects, and operational stakeholders. Training and development programs empower employees to embrace Zero Trust principles, equipping them with the skills and knowledge to navigate an evolving threat landscape. These programs could include partnerships with local universities for advanced certification courses, practical exercises such as simulated threat scenarios, and specialized training in areas like advanced threat detection and secure coding practices. Leadership plays a critical role in driving this shift, ensuring alignment between technical objectives and organizational values through clear communication and stakeholder engagement.

Leadership in Digital Governance

Florida's journey toward Zero Trust exemplifies how a strategic approach to digital security can drive broader IT transformation. Linking security frameworks mitigates vulnerabilities and establishes an environment for sustained technological advancements. ZTA plays a critical role in enabling scalable, resilient systems that support Florida's mission to deliver reliable and efficient public services. By reimagining processes, architectures, and cultures through the lens of Zero Trust, the state creates an environment that is secure, adaptive, and poised for future innovations. This holistic transformation enhances Florida's capacity to deliver reliable, efficient, and secure services to its citizens, visitors, and communities.

Florida: Current State of Digital Security Resilience in Government Operations

Inadequate digital security resilience is a critical issue within government operations. This deficiency exists in an environment of extensive cyber exposure, the presence of advanced and persistent adversaries, and lack of adaptive and automated threat response. The State of Florida encounters intricate and far-reaching challenges in ensuring robust digital security across various governmental functions. These challenges impact all facets of state operations and create vulnerabilities that potentially undermine the delivery of public services and compromise the security of digital assets, including sensitive information related to citizens.

According to the FBI's Internet Crime Complaint Center (IC3) 2023 annual report[1], government facilities rank as the third most targeted critical infrastructure sector by ransomware attacks. The FLDS has established initiatives that address escalating threats, including the State Cybersecurity Operations Center (CSOC), which provides digital security to state agencies, and a whole-of-state-cyber grant program[2]. These investments are aimed at strengthening cyber resilience and fostering a coordinated approach to digital security challenges.

In addition, FLDS has implemented standards and processes, including NIST-based risk assessment frameworks and state-defined security protocols, to assess state agency digital security risks and determine appropriate security measures. These efforts include adopting standards to mitigate risks and safeguard digital assets, ensuring the availability, confidentiality, and integrity of information technology resources. Collectively, these initiatives highlight Florida's commitment to addressing the pervasive challenges in digital security while laying a foundation for a more resilient digital future.

[1] Nextgov. (2024). *Government facilities were third-largest ransomware target in 2023, FBI says.*

[2] Florida League of Cities. (2022). Florida Digital Service digital security operations.

Adversaries targeting Florida have grown increasingly sophisticated, using advanced techniques such as social engineering, ransomware, supply chain attacks, and multi-stage malware campaigns. These adversaries are adept at identifying and exploiting vulnerabilities within government systems, which they then leverage to compromise critical infrastructure, exfiltrate digital assets, including sensitive information related to citizens, and disrupt the delivery of essential services. Traditional security mechanisms are proving insufficient in the face of these persistent threats, necessitating a fundamental rethinking of the state's digital security posture. The ability to preempt, detect, and neutralize these advanced threat actors is imperative to maintain the integrity and continuity of state operations.

The existing cybersecurity decision-making workflows lack agility due to procedural inefficiencies and unclear role responsibilities, thereby constraining the state's ability to respond effectively to cyber incidents. This data-to-decision latency limits the capacity to implement timely mitigation and containment strategies, potentially resulting in extended system downtimes, delayed recovery, and ineffective incident management, all of which can severely impact citizens relying on the uninterrupted availability of state services. Enhancing the velocity and accuracy of data analysis and decision-making processes is crucial to ensure effective and agile responses to digital security incidents.

Given these broad deficiencies, it is evident that a strategic transformation is required to bolster resilience against persistent and evolving cyber threats. These operational challenges can be contextualized within a notional Cyber Attack Process.

Need For Change: A Notional Cyber Attack Process

The visualization above provides an overview of the cyber-attack process through distinct stages to demonstrate the pathways that an adversary might take to compromise operations. Understanding this sequence is critical to enhancing Florida's preparedness against cyber threats and ensuring the resilience of its systems and services. Traditional methods of digital security often struggle to prevent cyberattacks due to their reliance on perimeter-based defenses, which assume that threats originate outside the network. Once an attacker breaches the perimeter, these methods offer limited visibility and control over internal systems, allowing adversaries to move laterally and exploit vulnerabilities with minimal detection. Attackers continuously develop new tactics to exploit increasingly complex digital ecosystems. As a result, conventional processes are insufficient in addressing the dynamic nature of modern cyber threats.

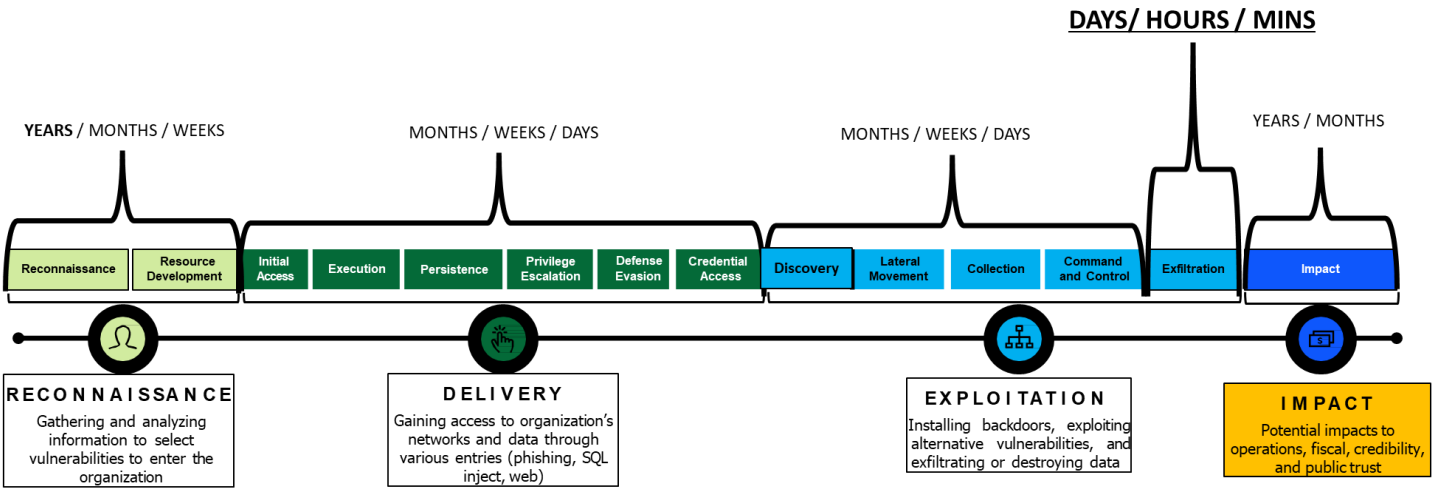


Figure: Cyber Attack Process

Stages of the Cyber Attack Process

The sequence of events in the cyber-attack process, as illustrated in the diagram on page 10, provides a view of how adversaries progress through an attack.

- **Reconnaissance:** In the initial stage, adversaries gather information about their target. This phase involves identifying potential vulnerabilities, researching public-facing systems, and harvesting data that can be used for crafting an attack. Reconnaissance can occur over weeks or months, because adversaries often take time to gather detailed information to increase the chances of a successful attack.

- **Delivery:** After reconnaissance, the adversary attempts to deliver a malicious payload. This could involve phishing emails, malicious links, or file attachments designed to trick users into downloading or executing malware. The delivery phase often unfolds in a matter of hours or days, depending on how quickly the adversary can exploit opportunities created by their reconnaissance efforts.

- **Exploitation:** Once the payload is delivered, it seeks to exploit system vulnerabilities. The payload seeks to exploit system vulnerabilities upon delivery. Exploitation typically involves leveraging software flaws or misconfigurations to gain unauthorized access to systems or networks. This phase can occur almost instantaneously upon delivery if the payload successfully interacts with a vulnerability, although in some cases, it may take days as attackers probe for weaknesses.

- **Installation:** Following exploitation, adversaries install malware or other malicious tools to establish persistent access. The installation process can take minutes or hours, as adversaries work to embed files or scripts that evade detection. The speed of installation often depends on the sophistication of the tools and the complexity of the target system.

- **Command and Control (C2):** In this phase, the adversary establishes a communication channel with the compromised system. This stage can begin within minutes of installation and may persist over days, weeks, or even months as the adversary maintains remote control to execute further actions.

- **Impact:** Finally, the adversary achieves their ultimate objective, which could include stealing sensitive data, including medical and personally identifiable information (PII) pertaining to citizens, disrupting critical services, or altering system integrity. The timeframe for this phase varies widely. ***Exfiltration of sensitive data, for instance, can be accomplished within hours or even minutes, depending on the attacker's access and the volume of data targeted.*** Conversely, operations aimed at system disruption or manipulation may take days or weeks to execute fully.

Florida's digital security teams can anticipate adversarial actions and implement strategies to disrupt attacks at every stage by analyzing the cyber-attack process. Understanding the stages, and timeframes in which they unfold, underscores the importance of a proactive and structured approach to digital security. ZTA effectively mitigates threats across the cyber-attack process and supports a robust defense of state systems and services.

What Is Zero Trust

Zero Trust challenges the conventional perimeter-based security model, which assumes that everything inside the network is inherently trustworthy once initial barriers are breached. This outdated assumption creates significant vulnerabilities, as evidenced by numerous high-profile data breaches that exploited internal weaknesses[3]. Zero Trust mandates that users, devices, and applications be verified each time they attempt to access resources, rather than relying on a single point of entry to secure and entire system. ZTA requires a continuous cycle of authentication, authorization, and validation, ensuring that the security posture of users and devices is maintained in real time. The objective is to minimize the attack surface, reduce the impact of security breaches, and provide granular control over access.

[3] 110 of the Latest Data Breach Statistics. https://secureframe.com/blog/data-breach-statistics

Key Principles of Zero Trust

- **User Verification:** Ensuring secure access begins with verifying each user, device, and both system and data resources before granting permissions. Access at every level, whether to systems, applications, or data, is granted explicitly and continuously verified. This ensures that permissions are narrowly scoped, actively monitored, and adjusted based on real-time risk. Zero Trust employs MFA and IAM solutions, which dynamically adapt based on contextual information such as user behavior, location, and device health. This adaptive approach to verification reduces the risks of unauthorized access and insider threats by continuously assessing and responding to potential vulnerabilities.

- **Restricted Access:** Access is restricted to resources and data categories necessary for a user or device to perform its designated function. By enforcing this principle of least privilege access, organizations minimize unauthorized access and limit the possibility of lateral movement within the network by enforcing the principle of least privilege access. Least privilege access is a cornerstone of Zero Trust, as it helps to contain potential breaches and prevent attackers from moving freely within the environment. By continuously evaluating user roles and permissions, organizations can ensure that privileges are dynamically adjusted in response to changing needs and evolving threats.

- **Micro-segmentation:** Zero Trust divides the network into isolated segments, often referred to as microsegments, to contain the impact of a breach. If one segment is compromised, the attacker is prevented from easily accessing other parts of the network. Micro-segmentation allows for precise control over traffic between different segments, ensuring that security policies are applied consistently across the network. By implementing micro-segmentation, organizations can enforce more precise security controls, reducing the risk of a breach escalating into a full-scale attack. This approach enables more effective monitoring and threat detection by enhancing visibility into network traffic.

- **Monitoring and Tracking:** Ongoing monitoring and logging of all activities within the network are crucial for identifying anomalous behaviors and responding promptly to potential threats. Continuous monitoring provides real-time visibility into user and device activity, allowing security teams to detect suspicious behavior before it escalates into a major incident. Organizations can identify patterns that reveal malicious activity by utilizing advanced analytics and machine learning that enables proactive threat hunting and rapid response. Continuous monitoring, which includes network traffic, user actions, system changes, and application behaviors, provides a holistic view of the organization's security posture.

- **Establishment and Enforcement of Policies:** Policies are enforced based on real-time assessments of identity, device posture, and contextual factors to determine the appropriate level of access for each request. Adaptive policies are central to the Zero Trust framework because they allow organizations to dynamically adjust security controls in response to evolving risks. For example, access requests from an unfamiliar location or device may trigger additional verification steps, while requests from trusted environments may be granted more easily. This adaptive approach ensures

that security measures are proportional to the level of risk, minimizing friction for legitimate users while maintaining robust protection against potential threats.

Zero Trust is a comprehensive approach involving the integration of various security solutions, technologies, and processes to create a unified defense system. Moving away from implicit trust and towards a model of continuous and pervasive verification requires a cultural shift within agencies and the enterprise. Organizations can build a resilient security posture that is better equipped to handle the complexities of modern cyber threats by adopting ZTA.

Addressing the Cyber Attack Process with Zero Trust

Zero Trust principles offer a comprehensive framework to effectively mitigate and disrupt adversarial activity at every phase of the cyber-attack process. Zero Trust creates multiple layers of defense that adapt to the evolving digital threats by embedding dynamic security controls and proactive measures. The visualization below is an illustration of a typical multi-staged attack to breach organizational data. A Zero Trust based defense approach provides protection to potentially block this attack at every stage[4].

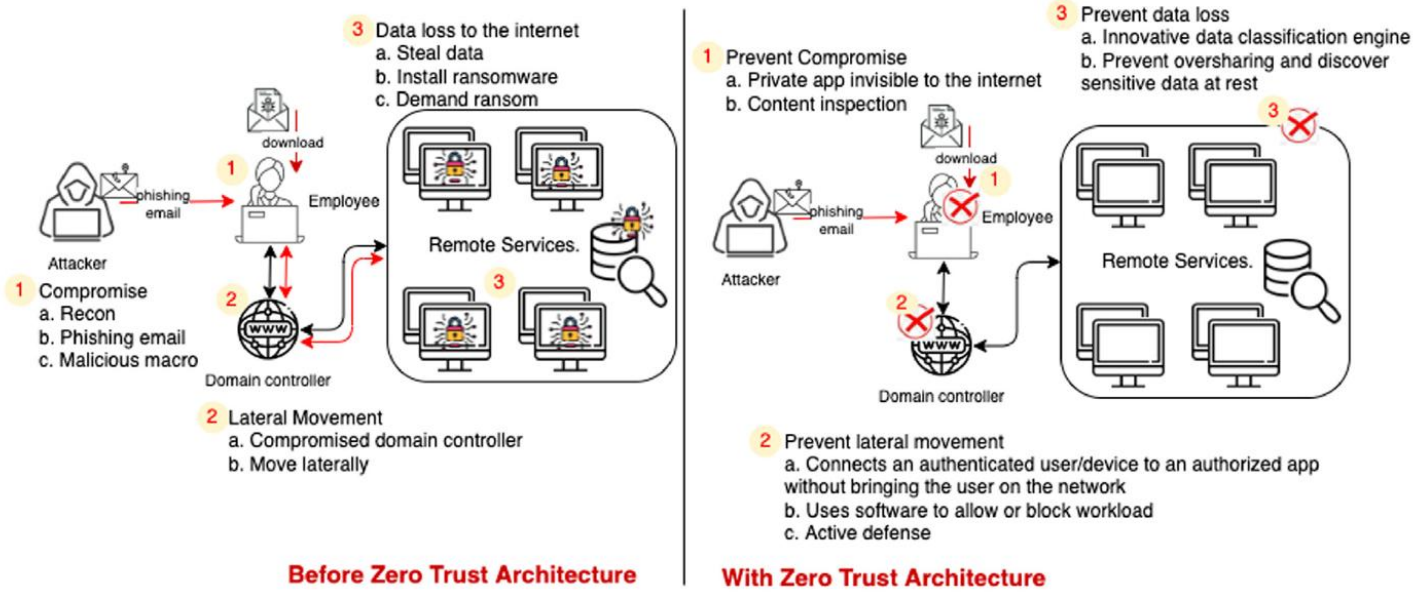


Figure: Impact of Zero Trust Architecture on Cyber Threats

[4] Adahman, Z., Malik, A. W., & Anwar, Z. (2022). An analysis of zero-trust architecture and its cost-effectiveness for organizational security. *Computers & Security, 122*, 102911.

- **Reconnaissance:** Zero Trust begins with continuous monitoring and granular visibility across systems and networks. This visibility is achieved through the integration of advanced tools such as network traffic analyzers, endpoint detection systems, and security information and event management (SIEM) platforms. These technologies, some of which are currently deployed within agencies and are being expanded at the enterprise level by FLDS, enable the real-time collection and correlation of data from diverse sources, offering a comprehensive view of system activities and supporting informed, timely decision-making. Proactive measures like micro-segmentation, combined with behavioral analytics and anomaly detection algorithms, further enhance the ability to identify and address potential threats during the reconnaissance phase. Advanced micro-segmentation restricts access to sensitive assets, rendering them invisible to external adversaries conducting reconnaissance. Rapid identification of suspicious activities is facilitated by real-time anomaly detection, behavioral analytics, and integration of threat intelligence feeds. This approach deters attackers from mapping networks or exploiting vulnerabilities, forcing them to expend resources without gaining actionable intelligence.

- **Delivery:** The Zero Trust framework employs MFA and IAM protocols to validate every access attempt. Adaptive email filtering, advanced threat protection tools, and AI-driven security measures neutralize common payload delivery methods, such as phishing emails and malicious attachments. ZTA minimizes the risk of successful delivery by dynamically adjusting access parameters based on contextual factors, including location, device health, and user behavior. These measures, which include email, web-based downloads, and file-sharing, create a cohesive defense against payload delivery.

- **Exploitation:** Enforcing the principle of least privilege access ensures that an attacker's ability to exploit system vulnerabilities is constrained even if the initial barriers are breached. IAM systems continuously evaluate user roles and permissions to prevent exploitation. Context-aware policies, such as conditional access and time-bound privileges, adapt to changes in user behavior, device posture, and access patterns, ensuring permissions remain tightly controlled. However, implementing least privilege access poses challenges, including the complexity of defining granular access levels across diverse systems and the potential for operational disruptions if permissions are overly restrictive. Addressing these challenges requires a careful balance of automation and manual oversight, supported by monitoring and analytics tools. Zero Trust utilizes endpoint detection, response (EDR) technologies, and continuous device posture monitoring to identify and isolate compromised endpoints. Adaptive security controls, including conditional access policies and just-in-time (JIT) privileges, respond dynamically to potential exploits. This reduces the likelihood of exploitation by automatically restricting access to critical digital assets based on risk factors.

- **Installation:** Zero Trust's continuous authentication framework, coupled with automated threat detection systems, mitigates the installation of malicious software. Endpoint security solutions rapidly identify unauthorized installations, while automated response mechanisms quarantine infected systems to prevent persistence. Micro-segmentation ensures that installed malware remains confined to a specific segment of the network. Regular integrity checks and application whitelisting further enhance the ability to detect and block malicious installations before they can propagate.

- **Command and Control (C2):** Adversaries rely on establishing communication channels to maintain control over compromised systems. A common C2 tactic uses encrypted communications through legitimate services, like cloud-based platforms, or leveraging DNS tunneling to mask malicious activity. Zero Trust limits attacker's ability to communicate with compromised systems through strict network segmentation, outbound traffic monitoring, and DNS filtering. Behavioral monitoring tools further enhance defenses by detecting irregular patterns, such as unexpected data flows or connections to unauthorized external servers, and identifying anomalous patterns in communication, such as attempts to connect with known malicious servers or irregular data flows. Security Orchestration, Automation, and Response (SOAR) platforms enable security teams to sever these connections in real time, effectively cutting adversaries off from their assets. These capabilities, combined with (SOAR) platforms, allow security teams to identify and sever C2 channels in real time, effectively neutralizing the adversary's ability to maintain control.

- **Impact:** Zero Trust minimizes the impact of adversarial objectives by restricting their ability to exfiltrate data or disrupt operations. Continuous monitoring, robust encryption protocols, and adaptive access policies ensure that sensitive data remains protected, even in the event of a breach. Organizations can preemptively block exfiltration attempts by employing DLP tools and zero-day exploit detection. Furthermore, rapid recovery and containment is enabled by incident response plans powered by real-time analytics and predictive insights that reduce downtime and mitigating damage.

Organizations can build a layered defense strategy that anticipates and neutralizes adversarial activities by applying ZTA principles to each phase of cyber-attack process. Zero Trust provides continuous verification, adaptive access controls, and dynamic monitoring, unlike traditional perimeter-based security models. These features ensure a strong defense against both external and internal threats by minimizing lateral movement, restricting access to critical assets, and identifying threats in real-time. Understanding these stages underscores the necessity of a structured, adaptive cybersecurity approach. Florida's adoption of Zero Trust provides a robust defense framework, equipping the state with the capabilities needed to address the complexities of modern cyber threats, while ensuring the continuity of critical operations.

Identity: The Central Foundational Pillar of Zero Trust

Identity management provides the essential foundation upon which all other security measures are built. Florida's implementation of Zero Trust must prioritize a comprehensive and integrated approach to identity management[5] to ensure protection against unauthorized access. This approach extends to other areas of cybersecurity, forming a seamless connection between foundational principles and advanced operational practices. As cyber threats grow in sophistication, Florida's implementation of Zero Trust must prioritize a comprehensive and integrated approach to identity management. This foundational strategy will ensure protection against unauthorized access, minimize security gaps, and enhance overall operational efficiency.

Implementing a Federated Identity Framework (FIM) alongside agency-specific identity management systems is critical for seamless and secure access. This enables employees and contractors to access multiple agency systems using a single set of credentials, which streamlines workflows and reduces security vulnerabilities. FIM services enable employees and contractors to access multiple agency systems using a single set of credentials. This approach reduces the need for multiple logins, enhances user experience, and strengthens security, by minimizing password-related vulnerabilities. Additionally, FIM fosters cross-agency collaboration by enabling seamless and secure data sharing, while maintaining compliance with strict access control policies. This simplifies access administration and significantly reduces the attack surface for malicious actors. Agencies can enforce consistent security policies while improving the user experience by centralizing governance and standards for identity management, while allowing technical implementation to remain federated.

Moreover, FIM facilitates secure collaboration between different agencies and external partners. Florida can enhance inter-agency cooperation, while maintaining stringent security protocols, by providing a federated authentication process. This capability is particularly valuable in emergency scenarios requiring rapid and coordinated responses.

[5] Federal Identity, Credential, and Access Management (FICAM). (n.d.). Zero Trust.

Automating the provisioning and de-provisioning of identities further enhances security by minimizing the risk of orphaned accounts and unauthorized access. This critical process ensures access permissions are promptly updated or revoked by automated systems, as personnel roles evolve, or employees exit the organization. This reduces administrative overhead and strengthens security by eliminating outdated access privileges that could be exploited.

Furthermore, automated identity lifecycle management enhances scalability, allowing Florida to efficiently manage identities across a growing workforce. Scalability ensures that as the state's workforce expands or agency needs evolve, the identity management system can adapt without compromising performance or security. This approach supports seamless integration of new technologies and workforce structures, aligning with long-term sustainability goals and ensuring Florida remains agile in addressing future demands. By integrating Florida's human resources system, such as PeopleFirst and agency-specific platforms, identity lifecycle automation ensures seamless onboarding and offboarding processes, reducing delays and human errors that could compromise security.

An essential component of this strategy is the implementation of Privileged Access Management (PAM)[6]. Privileged accounts, such as administrative or database management accounts, are frequent targets for cyber-attacks due to their elevated access levels, making controls for these accounts indispensable. Implementing PAM tools is essential to protect these accounts from misuse or compromise. PAM solutions enforce strict controls over privileged account usage, including session monitoring, just-in-time access provisioning, and MFA. Additionally, PAM provides detailed audit trails for privileged activities, enabling agencies to monitor and investigate potential security incidents. Florida can mitigate the risks associated with privilege abuse and ensure compliance with regulatory requirements by securing privileged accounts.

[6] Fusion Cyber. (n.d.). *Zero trust strategy: The importance of identity.*

Comprehensive logging and auditing play a vital role in supporting the broader objectives of Zero Trust[7]. Logs that capture details such as login attempts, access modifications, file transfers, and system changes are particularly valuable for compliance and forensic investigations. These detailed records allow security teams to trace the origins of suspicious activity, identify potential insider threats, and ensure adherence to regulatory requirements. Detailed logs provide enhanced visibility into user actions, supporting auditing, compliance, and forensic investigations. Agencies can detect anomalous behavior in real time and respond swiftly to potential threats by capturing granular data on access requests, system changes, and user interactions.

Logging and auditing also play a vital role in demonstrating compliance with cybersecurity standards and regulations. Florida can ensure accountability and transparency across its enterprise operations by maintaining a robust logging infrastructure.

With identity management providing a secure foundation, DSPM becomes critical by linking data security directly to IAM systems. This integration operationalizes Zero Trust principles, ensuring seamless coordination between identity verification and data protection. DSPM operationalizes Zero Trust Architecture by providing continuous monitoring and safeguarding digital assets, which ensures that identity verification and data protection are seamlessly integrated.

To operationalize DSPM effectively, several core functionalities are integral to its implementation:

- **IAM Integration:** DSPM integrates seamlessly with IAM platforms to enforce robust authentication and authorization protocols. This ensures that only verified entities can access sensitive datasets, aligning with Zero Trust principles and significantly enhancing data security. DSPM reduces administrative complexities and improves overall security posture by unifying identity and data security.

[7] Microsoft. (n.d.). *Identity and access management development best practices for Zero Trust.*

- **Data Classification and Protection:** DSPM provides advanced data classification capabilities, enabling agencies to prioritize security resources based on the sensitivity and criticality of data assets. This strategic allocation optimizes risk mitigation and ensures that critical digital assets receive the highest level of protection. DSPM's classification tools support compliance with data protection regulations by enabling accurate reporting and documentation. The synergies between DSPM and identity management further underscore its strategic importance within a Zero Trust framework.

- **Continuous Verification:** DSPM perpetually monitors user identities, device statuses, and application interactions to enforce real-time verification. This dynamic adaptability helps to maintain an active defense posture by addressing evolving threats and maintaining an active defense posture. Continuous verification ensures that access permissions remain appropriate, even as user behaviors or device conditions change.

- **Least Privilege Access:** By systematically identifying and eliminating unnecessary access rights, DSPM upholds the principle of least privilege. This approach minimizes potential attack vectors and prevents unauthorized lateral movement within the network. Least privilege enforcement is particularly effective in mitigating insider threats and reducing the scope of damage from compromised accounts.

- **Micro-Segmentation:** DSPM facilitates granular access control by segmenting network assets based on their classification and sensitivity. Asset classification is determined through a combination of automated tools and established governance policies, which assess factors such as data type, criticality, and regulatory requirements. DSPM ensures consistency and accountability in protecting sensitive assets by aligning the process with existing data governance policies. Micro-segmentation confines potential breaches to isolated segments, reducing the operational impact of security incidents. This layered approach enhances resilience against advanced persistent threats (APTs) and other sophisticated attacks.

- **Threat Detection and Response:** Equipped with advanced analytics and machine learning algorithms, DSPM identifies anomalies and potential threats with precision. DSPM capabilities enable timely intervention, safeguarding operational continuity, and mitigating risks to data integrity. DSPM enhances its ability to detect emerging threats and adapt defenses accordingly by integrating threat intelligence feeds.

Enhancing collaboration and integration between systems and agencies strengthens Florida's cybersecurity posture. The integration of DSPM functionalities within an IAM ecosystem enables Florida to establish a dynamic and resilient security framework. This approach ensures seamless coordination between identity and data security, enhancing the state's ability to respond to cyber threats. Florida can achieve a unified defense posture by fostering collaboration among different agencies and aligning security strategies.

Moreover, DSPM's role in facilitating secure data sharing and collaboration across agencies addresses current limitations in data-sharing security, thereby supporting mission-critical operations while reducing risks of unauthorized access. This is particularly valuable in sectors such as healthcare, public safety, and transportation, where timely access to accurate data is essential.

Florida can build a security framework that addresses both current and future challenges by adopting a holistic approach to Zero Trust. Current challenges include mitigating risks associated with insider threats, managing the complexities of securing hybrid cloud environments, and ensuring compliance with evolving cybersecurity regulations. Future challenges may involve integrating advanced technologies such as artificial intelligence and machine learning, addressing the security implications of expanding remote workforces, and safeguarding against increasingly sophisticated cyberattacks. The synergy between identity management and DSPM enhances the state's ability to protect sensitive assets while maintaining operational efficiency. This integration aligns with Zero Trust principles and ensures comprehensive protection for the state's identity and data assets across enterprise operations.

Florida: Current State and Challenges for Identity and Access Management

State agencies and contractors use IAM to secure access to digital resources by creating and managing user identities. Agency personnel often require access to systems or applications belonging to other agencies, necessitating the creation of new accounts. This proliferation of credentials complicates identity management, particularly when employees change roles or leave the organization. Such complexity heightens the risk of unauthorized access, as it becomes challenging to ensure the timely de-provisioning of all accounts and credentials.

A privilege escalation attack allows an attacker to gain deeper access to networks and sensitive data. To address these process inconsistencies, FLDS is exploring enterprise-level integration with the People First human resources system to enable automated, standardized identity lifecycle management across agencies.

Overview of the Federal Zero Trust Mandate

The current federal mandate for Zero Trust began from a combination of executive direction and official guidance documents aimed at modernizing and strengthening the digital security posture of U.S. government systems. Executive Order (EO) 14028, "Improving the Nation's Digital security," issued on May 12, 2021[8], directed federal agencies to move toward ZTAs. Following this EO, the Office of Management and Budget (OMB) released Memorandum M-22-09 ("Moving the U.S. Government Toward Zero Trust Cybersecurity Principles") on January 26, 2022[9]. This memo sets forth a comprehensive strategy and deadlines for federal agencies to achieve specific Zero Trust goals by the end of Fiscal Year 2024.

Federal agencies, following EO 14028 and OMB M-22-09, have faced challenges including integrating legacy systems, ensuring consistent MFA deployment, and user resistance to new verification workflows. Lessons learned emphasize the importance of phased rollouts, early stakeholder engagement, and investment in user training to ease transitions. Florida can leverage these insights to anticipate hurdles and adopt proven mitigation strategies.

[8]Executive Order on Improving the Nation's Digital security. https://www.whitehouse.gov/briefing-room/presidential-actions/2021/05/12/executive-order-on-improving-the-nations-digital security/
[9] Moving the U.S. Government Toward Zero Trust Cybersecurity Principles. https://www.whitehouse.gov/wp-content/uploads/2022/01/M-22-09.pdf

Core Components of the Federal Zero Trust Strategy

Central Framework and Decentralized Approach:

The federal Zero Trust strategy establishes a central governance framework that outlines key principles and guidelines for federated implementation by individual agencies. The technical deployment of Zero Trust is decentralized, allowing each agency the flexibility to integrate Zero Trust capabilities within their existing IT environments. This approach ensures consistency in core security objectives, such as identity verification and access control, while respecting the unique operational needs of each agency. A decentralized model helps achieve compliance with overarching policies and enhances the adaptability of individual agencies, enabling them to effectively respond to specific threats and operational challenges.

The federal Zero Trust strategy calls for shifting from a perimeter-based security model to one that assumes no implicit trust for any user, device, or network. Key tenets include:

- **Continuous Verification:** Agencies must continually authenticate and authorize requests, employing strong identity management and MFA.
- **Least Privilege Access:** Users and systems only receive the minimum level of access needed to perform their tasks.
- **Micro-Segmentation:** Systems and data are segmented into smaller zones to control lateral movement within the environment.
- **Visibility and Analytics:** Deep telemetry, logging, and analytics are used to detect anomalies and respond to threats swiftly.
- **Automated Security Enforcement:** Security policies are applied dynamically and automatically based on real-time data.

The CISA Zero Trust Model

The Cybersecurity and Infrastructure Security Agency (CISA) developed a model for implementing Zero Trust, which focuses on five key pillars that serve as the foundation of a mature ZTA. CISA's model emphasizes a holistic approach to digital security, integrating identity, device, networks, applications and workloads, and data protection to create a comprehensive security framework[10].

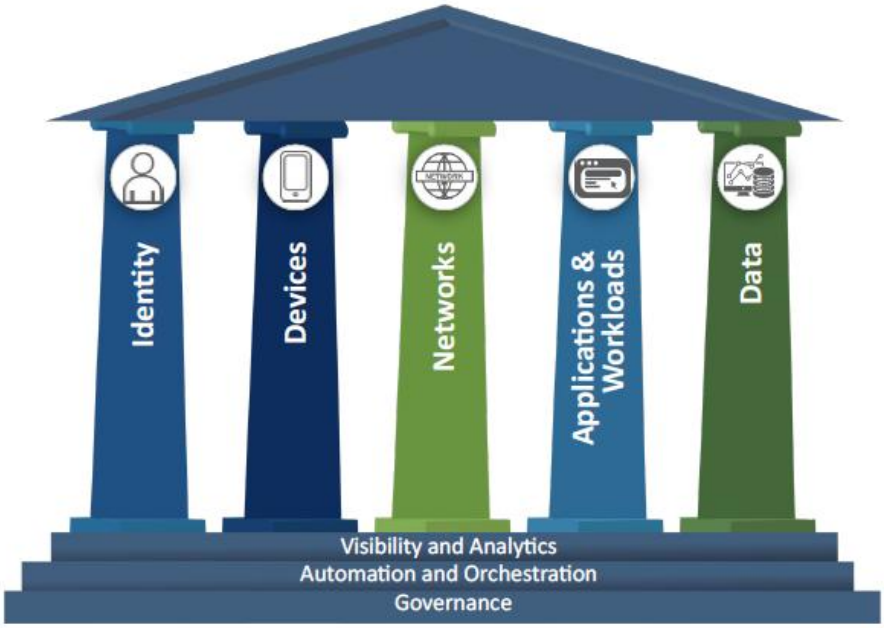


Figure: CISA Zero Trust Pillars

[10] Digital security and Infrastructure Security Agency. (n.d.). Zero Trust maturity model. U.S. Department of Homeland Security. https://www.cisa.gov

Identity is the basis of the Zero Trust model. CISA emphasizes that all access decisions must be grounded in a rigorous verification of every entity attempting to engage with system resources. This requires deploying identity verification mechanisms, including MFA, identity governance, and advanced identity analytics. These mechanisms collectively ensure continuous validation of user credentials, behavioral patterns, and device health, thereby minimizing the risk of identity compromise at any stage. Adaptive risk assessment must be incorporated into identity verification to trigger additional authentication steps when anomalies, such as access attempts from unfamiliar locations or devices, are detected. Organizations can protect against credential-based attacks, unauthorized access, and insider threats by utilizing identity as the foundational pillar of Zero Trust. Moreover, integrating identity management with endpoint security and network segmentation facilitates a holistic approach, restricting access to verified and trusted entities. Effective identity verification involves the use of identity federation, enabling seamless and secure access across diverse systems and domains, ultimately enhancing security and optimizing user experience.

The devices pillar ensures that all devices connected to the network are secure, compliant, and trustworthy. Continuous monitoring of device health, along with rigorous assessment of their compliance with security policies, such as patch management and system integrity checks, is essential before access is granted. This is achieved through the deployment of EDR systems, device health assessments, and adherence to security protocols. Effective device management is critical to mitigating risks posed by compromised endpoints, which could otherwise provide attackers with unauthorized access to sensitive data. Beyond endpoint protection, it is also imperative to secure mobile devices, Internet of Things (IoT) devices, and other non-traditional endpoints that may introduce distinct security challenges. By maintaining a comprehensive inventory of all connected devices and continuously assessing their security posture, organizations can ensure that only trusted devices gain access to critical assets.

Traditional network architectures relied on perimeter defenses to protect IT infrastructure. In contrast, the CISA Zero Trust model emphasizes a transformative approach, employing micro-segmentation and network traffic encryption to secure each layer of the network. In this model, even internal network communications are treated with skepticism, requiring continuous verification. Technologies such as virtual private networks (VPNs), software-defined networking (SDN), and micro-segmentation play key roles in preventing unauthorized users from navigating within the network. Zero Trust network security mandates the use of technologies that segment and encrypt network traffic, ensuring that data remains protected irrespective of its location. By utilizing SDPs, organizations can establish adaptive, context-aware boundaries that dynamically respond to changing network conditions. This approach not only enhances security but also improves the agility and efficiency of network resource management, resulting in more effective security operations.

In the Zero Trust paradigm, securing application workloads extends beyond user authentication to encompass continuous verification and monitoring to ensure that workloads remain secure and behave as expected. CISA advocates for the implementation of secure coding practices, containerization, and runtime application self-protection (RASP) to protect workloads from potential threats. Furthermore, application workloads must adhere to the principle of least privilege, where applications are granted only the permissions necessary for their specific functions. Organizations can ensure that applications are designed, developed, and deployed with security as a foundational element by embedding security practices within the development lifecycle (DevSecOps). Continuous monitoring of workloads facilitates the early detection of vulnerabilities and anomalous behaviors, allowing for timely responses to emerging threats. By applying stringent security controls to application workloads, organizations can minimize the risk of compromise and maintain the integrity of critical business operations.

Data security is at the core of the Zero Trust model, playing a pivotal role in safeguarding sensitive and classified information. CISA emphasizes the importance of encryption, DLP measures, and real-time monitoring to protect data throughout its lifecycle. Data must be encrypted, both at rest and in transit, to protect it from unauthorized access. Furthermore, data classification must be performed to enforce granular access controls, ensuring that sensitive information is protected against unauthorized disclosure, alteration, or destruction. Within a Zero Trust framework, data protection involves comprehensive tagging and classification to align security measures with the sensitivity of each data type. Data-centric security policies should be enforced to ensure that access controls are contextually appropriate, providing tailored protection to different types of data. Real-time monitoring of data access and usage patterns further strengthens security by enabling the detection of potential exfiltration attempts and preventing data breaches before they occur. This multifaceted approach ensures that data remains resilient to both internal and external threats, aligning with the Zero Trust principles of continuous verification and minimal trust.

The Department of Defense (DoD) Zero Trust Model

The DoD Zero Trust Model emphasizes a multi-layered approach to security, involving multiple defense mechanisms such as network segmentation, identity verification, continuous monitoring, and endpoint security to ensure comprehensive protection. It highlights the importance of stringent access controls in high-stakes environments where national security is at risk. The model addresses the complexities of defense environments, which often involve diverse systems, classified data, and the need for collaboration across various branches and partners. Below, we explore the key components of the DoD's Zero Trust model[11].

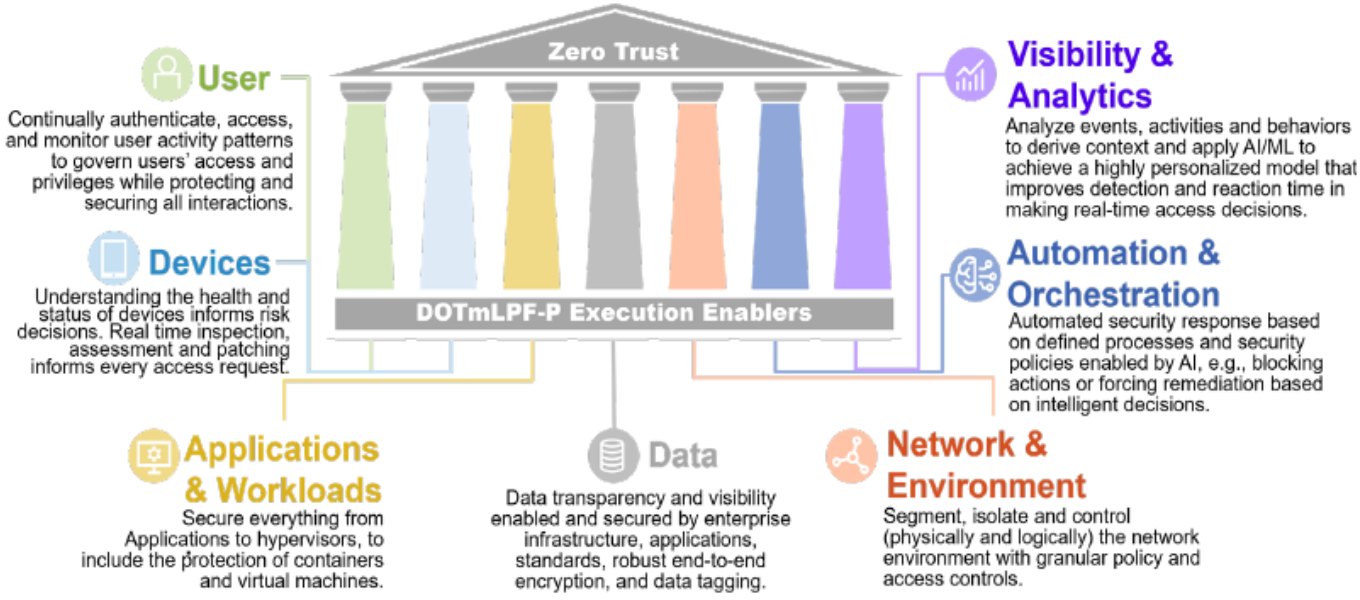


Figure: DoD Zero Trust Model[12]

[11]Department of Defense Zero Trust Reference Architecture. https://dodcio.defense.gov/Portals/0/Documents/Library/(U)ZT_RA_v2.0(U)_Sep22.pdf

[12] DoD Zero Trust Strategy. https://dodcio.defense.gov/Portals/0/Documents/Library/DoD-ZTStrategy.pdf

The DoD ZTA places significant emphasis on governance and visibility. Governance involves establishing a robust policy framework that dictates how Zero Trust principles are implemented across all systems and networks. Effective governance ensures that security policies are consistently enforced and that all stakeholders understand their roles and responsibilities in maintaining security. Visibility is equally critical, as it provides the situational awareness needed to detect anomalies, potential threats, and signs of compromise. Achieving visibility requires comprehensive monitoring of network activities, user behaviors, and system interactions. By maintaining high visibility, the DoD can detect and respond to threats more effectively, reducing the risk of successful attacks. The DoD model incorporates advanced analytics, such as User and Entity Behavior Analytics (UEBA), to monitor user behaviors and detect abnormal activity patterns. UEBA utilizes machine learning and statistical analysis to establish baselines of normal behavior and identify deviations that may indicate insider threats, compromised accounts, or attempts to misuse credentials. For example, UEBA can detect a situation where a user who typically accesses systems during regular business hours suddenly attempts to access sensitive data late at night from an unfamiliar location, prompting further investigation[13]. This proactive approach is particularly critical in defense environments, where the consequences of a security breach can be severe. By detecting anomalous behavior early, UEBA helps the DoD to prevent malicious actions before they escalate into significant security incidents.

A key feature of the DoD Zero Trust model is the use of automation to enforce security policies consistently across the enterprise. Automated policy enforcement minimizes the potential for human error, which can often be a significant vulnerability in complex security environments. Automation ensures that security controls are applied uniformly and in real time, improving efficiency and reducing the likelihood of misconfigurations or gaps in security coverage. This is especially important in defense settings, where the speed and accuracy of policy enforcement can be the difference between thwarting an attack and suffering a breach. By leveraging automation, the DoD can maintain a robust security posture without overburdening personnel with manual tasks.

[13] Johnson, M., & Smith, L. (2020). Advanced user and entity behavior analytics. Cyber Defense Review.

In addition to initial identity verification, the DoD Zero Trust model emphasizes continuous authentication and authorization. This means that once a user or device is granted access, they are continually re-verified to ensure they still meet the necessary security criteria. Continuous authentication uses contextual factors, such as changes in user behavior, device health, and network activity, to dynamically assess whether access should be maintained. This approach is particularly important in environments where access to classified information must be tightly controlled. The DoD can ensure that users and devices maintain compliance with security policies throughout their session, thereby reducing the risk of unauthorized access by implementing continuous authentication,

Given the scale and scope of DoD operations, Zero Trust principles must be implemented in a way that can scale across different branches, regions, and partners. The DoD model emphasizes scalability by incorporating SDPs and software-defined networking (SDN) solutions, which allow for dynamic and adaptive security policies that can be tailored to different operational requirements. Scalability is crucial in defense settings, where the number of users, devices, and data flows can vary significantly depending on the mission. By using SDPs and SDN, the DoD can create flexible security architectures that adapt to the needs of different environments, ensuring consistent protection regardless of scale or complexity.

Like the CISA model, the DoD Zero Trust framework places a strong emphasis on data protection. Data-centric security involves classifying data based on its sensitivity and applying appropriate access controls, encryption, and monitoring to prevent unauthorized access or breaches. The DoD recognizes that data is one of its most valuable assets, and protecting it is paramount to maintaining national security. By adopting a data-centric approach, the DoD ensures that sensitive information is secured at every stage of its lifecycle. This includes creation, where data is classified and tagged; storage, where encryption and access controls are applied; transmission, where secure channels are used to prevent interception; and destruction, where data is thoroughly wiped or physically destroyed to prevent recovery. This includes the use of advanced encryption methods, DLP tools, and continuous monitoring of data access patterns to detect and respond to potential threats.

Implementation Roadmap for Zero Trust in Florida

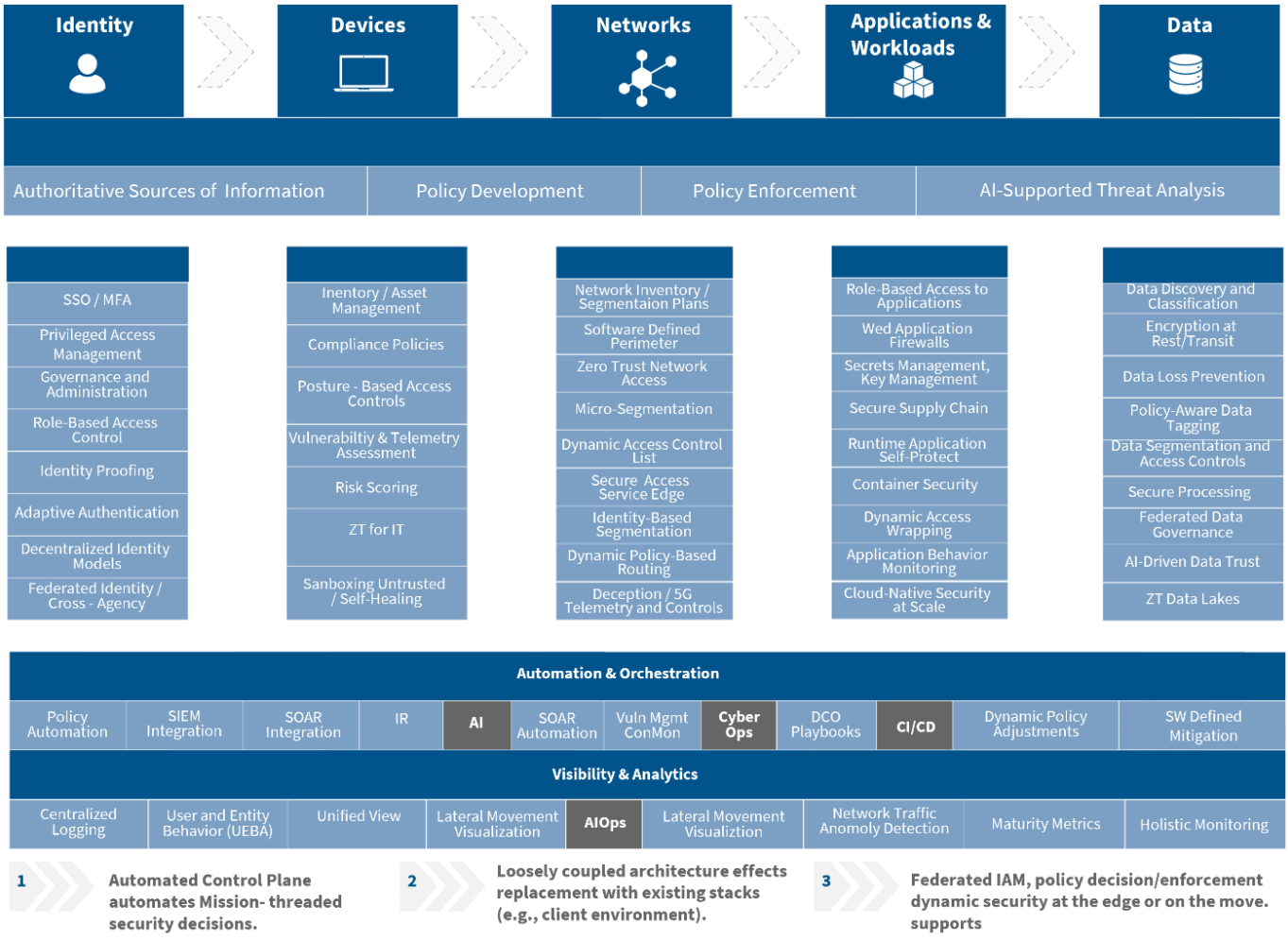


Figure: FLDS Draft Zero Trust Reference Architecture

Zero Trust is a continuous journey requiring adaptation to an ever-changing threat landscape. For the State of Florida, implementing Zero Trust involves embedding its principles across five foundational domains: identity, applications/workloads, devices, networks, and data. This approach requires a methodical, phased adoption that aligns with organizational objectives, minimizes disruptions, and bridges the gap between current practices and the aspirational state of a fully realized Zero Trust framework. Zero Trust demands a cultural shift, encompassing governance, policies, and processes to reorient digital security strategies. Zero Trust mandates continuous validation of every access request, internal or external, treating all as untrusted until verified. This iterative process preserves security posture amid evolving threats and operating conditions.

Achieving Zero Trust in Florida will require the adoption of core practices, emphasizing business-driven transformation over purely technological endeavors, standardization of identity management services, and a commitment to minimizing operational disruptions during the transition. Success depends on stakeholder engagement, comprehensive inventory assessments, and integration capabilities that enable a seamless implementation. A culture of continuous improvement is also vital. Iterative feedback loops and lessons learned from each implementation phase must be leveraged to refine subsequent efforts. Ultimately, integrating security practices seamlessly into daily operations positions digital security as a facilitator rather than an impediment to achieving strategic business goals.

FLDS Zero Trust Reference Architecture Overview

The draft FLDS Zero Trust Reference Architecture establishes a rigorous and adaptable framework to modernize and secure the State of Florida's enterprise technology landscape. It addresses the complexities of a federated enterprise by balancing centralized governance with the operational independence required by state agencies.

Grounded in Zero Trust principles this architecture requires continuous verification and enforcement of access privileges across all system layers. ZTA mitigates evolving cyber threats, strengthens technological resilience, and ensures the uninterrupted delivery of critical services.

At its core, the architecture is structured around five foundational domains: *Identity*, *Devices*, *Networks*, *Applications & Workloads*, and *Data*. Each domain provides discrete yet interdependent capabilities that collectively enable a Zero Trust environment, serving as building blocks for a comprehensive security strategy. These domains ensure a holistic approach to security, governance, and operational efficiency by addressing specific aspects of identity, devices, networks, applications, and data. Together, these domains form the foundation for mitigating risks, enforcing policy, and enabling secure and scalable technology operations across the enterprise.

- **Identity Domain:** Serves as the cornerstone of the architecture and is dedicated to securing the foundational relationships between users and systems. Identity Domain implements access controls through mechanisms such as Single Sign-On (SSO), MFA, and role-based access control (RBAC). FIM frameworks and decentralized identity models further enable cross-agency interoperability while maintaining stringent security standards. The inclusion of adaptive authentication and identity proofing mechanisms adds layers of verification, addressing contextual risks and mitigating the potential for compromised credentials.
- **Devices Domain:** Focuses on ensuring the integrity, security, and compliance posture of all endpoints—whether state-owned, third-party, or unmanaged. By implementing continuous posture-based assessments, asset inventory management, and advanced telemetry analysis, the architecture systematically reduces endpoint vulnerabilities. Risk scoring and self-healing automate proactive threat mitigation, while sandboxing untrusted devices that contain anomalous behaviors. This streamlined approach reduces the endpoint risk surface and reinforces the Zero Trust principle of least privilege access.

- **Networks Domain:** Introduces a comprehensive suite of capabilities designed to achieve secure, granular segmentation of communication pathways. Network inventory and segmentation plans, coupled with dynamic access control lists, support continuous enforcement of policy-based connectivity. Mechanisms such as Zero Trust Network Access (ZTNA), micro-segmentation, and software-defined perimeters ensure that access to resources is tightly governed by identity and contextual criteria. SASE models further enhance policy enforcement across hybrid and cloud infrastructures, where traditional perimeter-based approaches are rendered obsolete. These measures collectively constrain lateral movement and limit adversarial access within the network.

- **Applications & Workloads Domain:** The architecture ensures resilience and integrity across diverse operational environments, including on-premises, cloud-native, and hybrid deployments. Capabilities such as container security, runtime application self-protection, and dynamic access wrapping safeguard applications against evolving threats. Secrets management, key lifecycle governance, and secure supply chain practices fortify data confidentiality and operational continuity. Agencies can proactively address vulnerabilities, ensuring that workloads remain secure while enabling scalable service delivery by integrating behavioral analytics and automated anomaly detection.

- **Data Domain:** Serves as the nexus of the architecture, highlighting the state's commitment to protecting its most critical asset—data. Core capabilities, including data discovery, classification, and encryption, secure sensitive data throughout its lifecycle. Policy-aware tagging dynamically enforces access controls, while Zero Trust Data Lakes enable secure storage, analysis, and governance across federated systems. AI-driven trust models enhance governance, by ensuring compliance with state and enterprise standards and facilitating real-time, data-driven decision-making.

Automation & Orchestration and Visibility & Analytics facilitate the Zero Trust framework, underpinning and enhancing the effectiveness of the five foundational domains. Automation delivers streamlined policy enforcement, incident response, and operational workflows, integrating tools like SIEM, SOAR, and AI-driven processes. Automation optimizes resource allocation and accelerates responses to emergent threats, strengthening the security posture by reducing human intervention.

Visibility & Analytics provide a unified operational perspective essential for proactive risk management and informed decision-making. Capabilities such as centralized logging, UEBA, lateral movement visualization, and AI Operations (AIOps) offer comprehensive insights into enterprise activity. These tools

empower state leadership and IT practitioners to identify trends, anticipate risks, and drive data-informed security and performance enhancements.

The draft Reference Architecture represents a pivotal evolution in Florida's enterprise strategy, addressing the confluence of security imperatives, technological modernization, and operational agility. By aligning technology investments with the state's strategic objectives—enhancing digital security posture, improving inter-agency efficiency, and fostering innovation—the architecture establishes a scalable, secure foundation capable of addressing both present and emergent challenges. This framework will adapt to the dynamic needs of state agencies, while ensuring adherence to overarching governance principles, through an iterative process of collaboration, refinement, and feedback. Ultimately, this architecture embodies the State of Florida's commitment to safeguarding digital assets, protects citizen data, and enables the delivery of secure, modernized services to constituents statewide.

Phased Implementation Approach

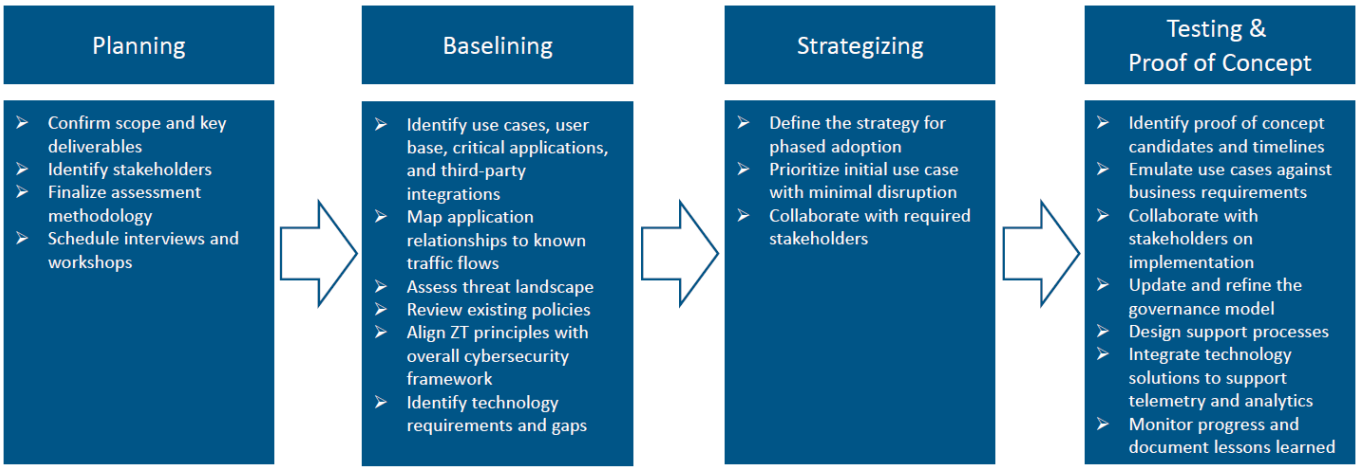


Figure: Phased Implementation Approach

Phase 1: Planning

The initiation of Florida's Zero Trust journey necessitates an intricate and deliberate planning process to define the program's scope and establish the foundational structure for implementation. This phase is critical for aligning diverse stakeholder perspectives and ensuring that the overarching objectives are articulated with precision. It is during this stage that strategic vision and operational alignment converge, setting the trajectory for success. Key activities include:

1. **Confirming Scope and Key Deliverables:** Clearly delineate strategic objectives, measurable outcomes, and comprehensive performance metrics that will gauge the effectiveness of Zero Trust adoption and establish definitive roles and responsibilities to mitigate future ambiguities. In this process, it is crucial to define the interplay between organizational objectives and digital security mandates to create a unified framework.

2. **Identifying Stakeholders:** Assembling a coalition of stakeholders encompassing IT specialists, security professionals, policy advisors, and executive leaders from all pertinent agencies will ensure alignment with enterprise-wide priorities and operational mandates. Consideration should also be given to external advisors or federal partners who can provide additional expertise and context.

3. **Finalizing Assessment Methodology:** Formulate a systematic and rigorous framework for assessing the current environment. This should include a thorough examination of technological readiness, policy deficiencies, and workforce competencies, using standardized instruments such as scoring matrices or diagnostic tools. This methodology must also include contingency plans for addressing unforeseen challenges during implementation.

4. **Scheduling Interviews and Workshops:** Facilitate collaborative sessions with stakeholders to solicit diverse perspectives, foster alignment, and build consensus around the Zero Trust vision. Workshops should also serve as platforms for disseminating foundational Zero Trust concepts and addressing stakeholder concerns. Additionally, these sessions should highlight interdependencies between agencies and the collective benefits of Zero Trust adoption.

Phase 2: Baselining

A comprehensive baselining phase provides an understanding of the current technological and organizational landscape, forming the empirical foundation for targeted interventions. This phase ensures a data-driven pathway to Zero Trust implementation, aligning the initiative with measurable indicators of progress and areas requiring immediate attention. Key components include:

1. **Use Case Identification:** Develop a granular inventory encompassing user demographics, critical applications, data interactions, and third-party integrations. These elements should be prioritized based on operational significance and inherent risk profiles. Each use case should be mapped against organizational objectives and compliance requirements to ensure alignment.

2. **Traffic Flow Mapping:** Conduct an exhaustive analysis of inter-application communications, data flows, and connectivity pathways. This enables the identification of systemic vulnerabilities and informs the design of precise micro-segmentation strategies. An extended focus should also be placed on emerging technologies and how their integration impacts traffic flows.

3. **Threat Assessment:** Undertake a threat landscape analysis, encompassing emergent risks such as advanced persistent threats, ransomware, and insider threats. This assessment should directly inform the architecture of resilient Zero Trust policies. Additional emphasis should be placed on understanding threat vectors unique to Florida's public sector and its diverse agency landscape.

4. **Policy Review and Revision:** Reevaluate the enterprise's existing digital security policies to ensure alignment with Zero Trust principles, such as enforcing least privilege and continuous authentication. Policies should be revised or augmented to eliminate inconsistencies and bridge security gaps. This review must also account for future policy adaptability to evolving regulatory standards.

5. **Gap Analysis:** Identify deficiencies across technological, procedural, and human dimensions. Emphasis should be placed on addressing the challenges posed by legacy systems, fragmented identity infrastructures, and insufficient automation capabilities. Documenting these gaps in a structured format provides a roadmap for addressing them in subsequent phases.

Phase 3: Strategizing

Strategizing involves the synthesis of insights from previous phases into a coherent and actionable roadmap for phased Zero Trust adoption. This phase demands a balance between ambition and pragmatism to guarantee implementation success, ensuring that both high-level objectives and operational details are addressed. Key strategic elements include:

1. **Defining the Strategy for Phased Adoption:** Develop a comprehensive roadmap, delineating milestones, timeframes, and resource allocations. The roadmap should articulate a clear progression from foundational use cases to enterprise-wide adoption, including contingency measures and performance metrics for tracking progress.

2. **Prioritizing Initial Use Cases:** Identify use cases with manageable complexity for early implementation, thereby demonstrating quick wins and cultivating stakeholder confidence. This prioritization should also highlight the scalability of each use case to ensure long-term applicability.

3. **Collaborating with Stakeholders:** Foster sustained collaboration across agencies, leveraging platforms for continuous dialogue to refine policies and processes in real-time. Collaboration and engagement with stakeholders can address interdependencies and regulatory realignment, including iterative feedback loops to continuously refine strategies.

Phase 4: Testing and Proof of Concept

Testing and validation are indispensable for ensuring the feasibility and efficacy of Zero Trust implementations before full-scale rollout. Proof of Concept (PoC) initiatives serve as a controlled environment for iterative refinement, enabling the identification of potential challenges and their mitigation strategies. Key steps include:

1. **Identifying PoC Candidates and Timelines:** Select critical yet achievable use cases for initial testing. It is key to clearly define the objectives, establish realistic evaluation timelines to ensure manageable scope, and incorporate diverse scenarios to test the resilience and flexibility of proposed solutions.

2. **Emulating Use Cases Against Business Requirements:** Construct rigorous test environments that mirror operational conditions to validate the functionality and integration of Zero Trust policies. This emulation should include stress testing to evaluate system performance under adverse conditions.

3. **Collaborating with Stakeholders on Implementation:** Engage stakeholders during PoC to incorporate their insights into iterative policy adjustments and technology configurations. Highlighting the benefits of stakeholder involvement is critical for broader acceptance and smoother scaling.

4. **Updating and Refining the Governance Model:** Adapt governance frameworks to reflect the operational demands of Zero Trust, ensuring clarity in accountability structures and escalation protocols, including provisions for monitoring and compliance.

5. **Designing Support Processes:** Establish robust support mechanisms, including incident response procedures, escalation pathways, and comprehensive training modules to enhance system resilience. Expand these processes to include post-implementation review mechanisms.

6. **Integrating Technology Solutions:** Embed advanced solutions for telemetry, analytics, and automation to ensure real-time enforcement and monitoring of Zero Trust principles. Priority should be given to modular solutions to allow for future scalability and upgrades.

7. **Monitoring Progress and Documenting Lessons Learned:** Employ data-driven metrics to evaluate PoC outcomes, capturing actionable insights to inform subsequent phases. Creating a repository for lessons learned can guide future initiatives.

Phase 5: Scaling and Optimization

Scaling and optimization represent the culmination of the Zero Trust implementation, transitioning from isolated pilots to comprehensive, enterprise-wide adoption. This phase emphasizes continuous improvement, adaptability, and long-term sustainability. Key activities include:

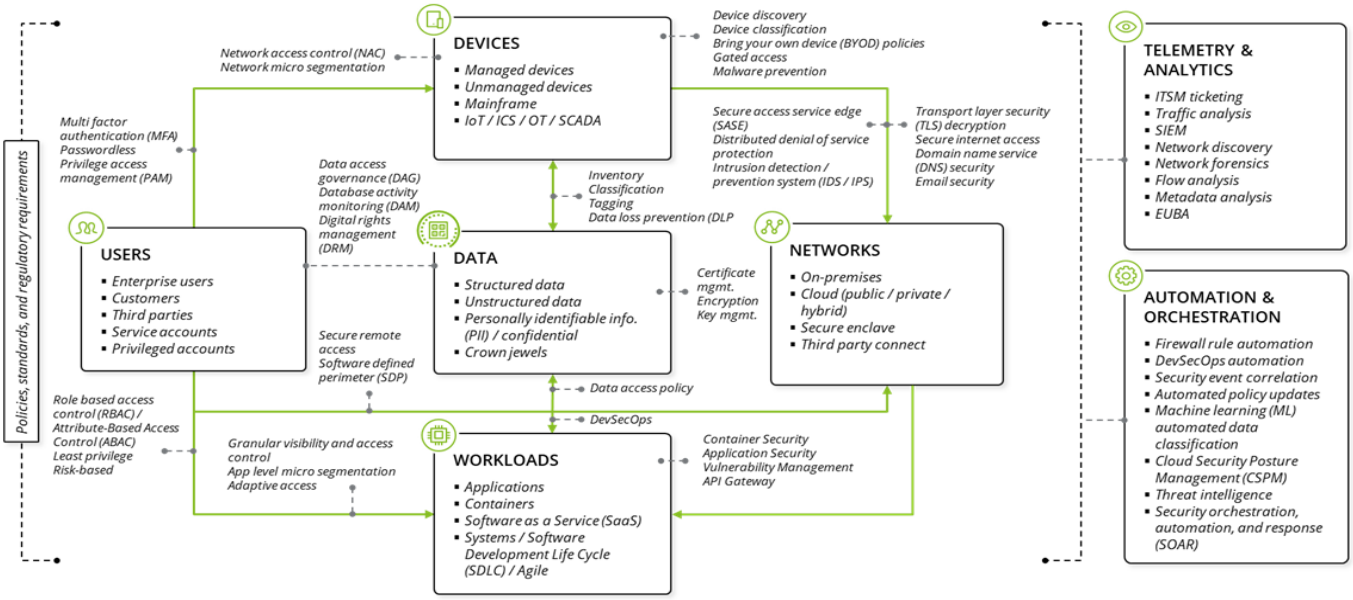
1. **Incremental Expansion:** Gradually extend Zero Trust coverage to high-complexity environments, including inter-agency platforms and high-privilege administrative systems. Addressing cross-agency interdependencies can streamline processes.
2. **Advanced Analytics Deployment:** Leverage sophisticated tools, such as UEBA, to enhance threat detection and enable proactive mitigation measures. Integrating these tools with incident response protocols for end-to-end threat management is critical.
3. **Policy Refinement Through Telemetry:** Utilize real-time telemetry to dynamically adjust access policies, ensuring resilience against evolving threat landscapes and incorporate predictive analytics to preempt emerging risks.
4. **Full Automation for Repetitive Tasks:** Streamline processes, such as access provisioning and compliance reporting, through end-to-end automation to enhance efficiency and reliability. Automation can be expanded to include anomaly detection and response workflows.
5. **Ongoing Training and Awareness Campaigns:** Foster a culture of vigilance and adaptability by institutionalizing continuous education programs on Zero Trust principles and digital security best practices. Gamification and advanced learning tools can enhance engagement.

This phased, methodical approach ensures that Florida's Zero Trust initiative achieves its immediate security objectives and establishes a robust framework for long-term resilience and adaptability. The integration of advanced analytics, collaborative governance, and iterative improvement facilitates a highly effective and sustainable enterprise framework.

Illustrative Zero Trust Reference Architecture

The visualization below illustrates Zero Trust's end-to-end approach to network/data security that encompasses the five Zero Trust domains and the interconnecting infrastructure between them.

Figure: FLDS Draft Zero Trust End-to-End Reference Architecture



The Zero Trust implementation plan provides a structured approach to modernizing Florida's digital security framework. Florida can create a resilient, scalable, and secure digital environment that protects its assets and serves its citizens effectively by focusing on foundational principles, phased adoption, and continuous optimization.

Strategic Objectives to Achieve Zero Trust

Identity

Identity management prioritizes verifying and validating every user, device, and application seeking access to state resources. Establishing a standardized, federated IAM framework ensures a consistent approach to user identity verification across all agencies, reducing silos and enhancing collaboration. This approach strengthens the security posture and aligns identity processes with real-time risk analytics, enabling adaptive responses to threats and ensuring that trust is never implicit but continuously verified. In doing so, the state ensures that its systems remain resilient against both internal and external threats, while providing seamless and secure access to authorized users.

Objective #1: Establish a Federated Identity and Access Management Framework

A federated IAM framework is crucial for achieving a ZTA. While establishing a central framework (governance), the technical implementation should adopt a decentralized or federated approach, allowing each agency to maintain autonomy over their systems while ensuring a consistent identity verification mechanism across the state. The State of Florida can streamline identity verification across all agencies and ensure a consistent approach to managing user access by establishing a centrally governed IAM framework for policies and standards, while allowing agencies to implement solutions within this framework. This addresses the fragmentation of identity solutions and creates a cohesive environment where user authentication, authorization, and monitoring are uniformly enforced while allowing agencies the flexibility they need for local implementations. The state can effectively minimize unauthorized access risks and provide seamless and secure services by implementing MFA, RBAC, and attribute-based access control (ABAC). Additionally, an IAM framework supports better visibility and control over user activities, reducing the attack surface, and enabling rapid detection and response to potential threats.

- Implement a reliable identity model to manage user authentication, authorization, and continuous monitoring. This involves integrating a diverse set of identity sources across agencies and ensuring a standardized approach to identity validation.
- Enable MFA to enhance security and user experience by implementing MFA as a mandatory feature across all access points to ensure that only authenticated users gain access to critical resources, reducing risks of compromised credentials.
- Standardize continuous authentication and authorization through dynamic access policies based on risk assessments and real-time analytics. Leveraging contextual information, such as user

location, device health, and behavior analytics, to fine-tune access decisions, will ensure they align with current risk levels.

- Develop a standardized identity governance structure to enforce compliance, RBAC, and ABAC policies effectively. This governance model should include auditing and monitoring capabilities to detect and mitigate unauthorized access attempts, while allowing agencies to implement these controls within their environments.
- Provide regular training and awareness programs for users on best practices in identity management, emphasizing the importance of secure password practices, recognizing phishing attempts, and the proper use of MFA.

Devices

Devices are a critical aspect of ZTA, because they serve as the entry points through which users access state resources. Securing endpoint devices ensures that threats are minimized before they can infiltrate the network. The State of Florida must establish comprehensive policies for endpoint security, including real-time asset discovery, compliance enforcement, and continuous monitoring. Endpoint management should encompass all types of devices, including managed, unmanaged, and Bring Your Own Device (BYOD) scenarios. This approach reduces the risks of unauthorized devices connecting to sensitive systems, enhances visibility across the device ecosystem, and ensures that all devices adhere to established security baselines. The state can effectively mitigate risks and maintain a proactive security posture that safeguards endpoints from evolving threats by focusing on continuous threat detection and leveraging AI/ML-driven solutions,

Objective #2: Secure All Endpoint Devices

Securing all endpoint devices is a fundamental aspect of ensuring the success of a ZTA. Endpoint devices are often the most vulnerable entry points into an organization's network, making them a primary target for cyber-attacks. This objective provides continuous visibility and control over all endpoint devices, whether they are managed, unmanaged, or part of a BYOD program. The State of Florida can effectively reduce risks associated with compromised devices by enforcing compliance policies through centralized endpoint management tools and implementing advanced threat detection mechanisms. Furthermore, transitioning to a domain-less environment ensures that trust is not implicitly granted based on network location, making endpoint security a critical layer of defense. Continuous monitoring, AI/ML-driven threat detection, and clear incident response playbooks are all essential components of this objective, helping to mitigate threats before they can affect critical systems and ensuring that all devices adhere to stringent security baselines.

- Conduct continuous discovery and monitoring of hardware and software assets by establishing automated mechanisms for real-time asset discovery, including inventory management systems that track the addition, removal, and movement of endpoint devices.
- Enforce endpoint compliance through centralized management and policy enforcement by deploying UEM tools to enforce security baselines for all devices, including patching, antivirus updates, and compliance checks.
- Transition to a domain-less environment, reducing inherent trust based on network location, by implementing SDP approaches, to remove implicit trust from traditional domain-based models, ensuring that all devices are verified regardless of network position.

- Implement continuous threat detection and response capabilities using AI/ML-driven tools by deploying EDR and advanced AI-based monitoring solutions to quickly detect unusual behaviors or potential threats on endpoints, ensuring rapid mitigation.
- Develop clear incident response playbooks that address endpoint-related threats, ensuring swift action in case of device compromise. These playbooks should include procedures for isolation, remediation, and recovery of affected endpoints.
- Incorporate a BYOD policy that mandates compliance checks and access restrictions to prevent untrusted devices from connecting to critical systems.

Networks

Networks are a crucial component of Zero Trust, as they serve as the conduit through which data flows and resources are accessed. The goal is to eliminate implicit trust within network boundaries and ensure that all connections are continuously authenticated, authorized, and monitored. The State of Florida must implement secure network access strategies that include robust segmentation, SDPs, and eventually a complete compliment of SASE capabilities. Critical services can be made resilient and accessible without compromising security by adopting a hybrid cloud strategy. Micro-segmentation ensures that attackers cannot move laterally within the network, effectively containing potential breaches. Additionally, continuous network discovery and behavior analytics help in detecting unauthorized access and unusual activities, ultimately reinforcing the state's security posture.

Objective #3: Enable Secure Network Access

Enabling secure network access is critical to the success of the Zero Trust by ensuring that only verified users, devices, and applications can communicate across the network. This objective aims to mature the state's approach to network discovery, monitoring, and segmentation to effectively manage the transport paths and access points within the state's infrastructure. Florida can create highly secure network environments where access is granted on a need-to-know basis by deploying SDPs and implementing micro-segmentation practices, thereby reducing the potential attack surface. Furthermore, migrating enterprise services to a hybrid cloud environment enhances the resilience of state services, ensuring availability even during disruptions. Continuous network behavior monitoring and advanced analytics help in identifying anomalies and responding proactively, making the network more adaptive and secure. Ultimately, these initiatives support the Zero Trust principle of eliminating implicit trust, maintaining strong controls over all network interactions, and aligning network policies with the dynamic security environment.

- Mature network discovery and monitoring to manage transport paths and access points. Utilizing advanced network monitoring tools can provide continuous insights into network activity, including unauthorized connections and network misconfigurations.
- Deploy SDPs close to protected resources to minimize the attack surface. Creating logical perimeters that provide fine-grained access controls around sensitive resources can effectively reduce exposure.
- Migrate enterprise services to a hybrid cloud environment to provide resilient, secure access. Implementing a hybrid cloud strategy that combines on-premises and cloud services provides failover capabilities and maintaining business continuity.

- Mature segmentation practices to the lowest level to enhance visibility and control. Applying micro-segmentation within data centers and across networks to prevent lateral movement will ensure that attackers are unable to exploit vulnerabilities across different segments.
- Develop redundancy and failover systems for critical network components to ensure resilience against Distributed Denial-Of-Service attacks and network failures.
- Implement network behavior analytics to detect anomalous activities, using machine learning models to establish normal network behavior and trigger alerts for deviations.

Applications

Applications are a key focus of Zero Trust, as they represent critical resources that must be protected from unauthorized access and potential threats. The State of Florida can ensure that applications are not only securely accessed but also continuously monitored for potential vulnerabilities by achieving comprehensive application-level visibility and control. Integrating applications into the Zero Trust framework means onboarding mission owners and clearly defining access policies and roles, which strengthens accountability and transparency. Modernizing legacy applications and adopting secure software development practices are essential to reducing vulnerabilities and improving the overall security of the application landscape. The state can build a resilient application environment that aligns with Zero Trust principles with centralized permissions, access control, and ongoing vulnerability management, ultimately minimizing the risk of breaches and ensuring that applications remain secure throughout their lifecycle.

Objective #4: Achieve Application-Level Visibility and Management

Achieving application-level visibility and control is essential to safeguarding the State of Florida's digital assets and ensuring that applications are resilient against evolving threats. This objective focuses on continuously monitoring all applications, from legacy systems to modern cloud-native ones, to detect potential vulnerabilities and proactively address them. By onboarding applications, including modern and, where feasible, legacy systems, into the Zero Trust framework and defining clear policies for each, Florida can enforce least privilege access, thereby minimizing unauthorized exposure and reducing risk. Centralized permissions and access control mechanisms are critical to maintaining strict oversight over application interactions, ensuring that sensitive information remains secure. Adopting secure software development practices and continuously scanning for vulnerabilities ensures that applications are built and maintained with security as a top priority, thus strengthening the state's overall digital security posture.

- Continuously discover and monitor all application activities to identify and prioritize legacy modernization. Application performance monitoring (APM) tools can be used to gain insights into app usage, performance bottlenecks, and vulnerabilities that require modernization.
- Onboard applications and mission owners into the Zero Trust framework with clear policies and roles. Developing an onboarding checklist that ensures every application has a defined owner, security policies, and is evaluated for risks prior to integration into the Zero Trust framework is critical.

- Implement centralized permissions and access controls to ensure secure, least privilege access by integrating PAM solutions that centralize access requests, limit privileged user sessions, and provide session auditing.
- Establish Secure Software Development Lifecycle (SSDLC) practices for all applications to ensure they adhere to security best practices, including secure coding standards, automated testing for vulnerabilities, and continuous integration/continuous deployment (CI/CD) pipelines with embedded security checks.
- Develop a vulnerability management program that regularly scans applications for known vulnerabilities and rapidly remediates any detected weaknesses.
- Legacy applications that cannot fully conform will be assessed for risk and guided through mitigation or modernization strategies.

Data

Data is at the core of Zero Trust, serving as the new perimeter that needs stringent protection and continuous monitoring. In the context of Zero Trust, protecting data means implementing a comprehensive strategy that ensures visibility, control, and security throughout the data lifecycle, from creation and storage to usage and destruction. The State of Florida must prioritize data discovery, tagging, and classification to understand the location and sensitivity of all data assets. By doing so, the state can apply appropriate security controls and ensure that data is only accessed by authorized users under the principle of least privilege. Additionally, utilizing robust encryption methods for data at rest and in transit, along with DLP tools, ensures that sensitive information remains secure from unauthorized access and accidental exposure. Ultimately, treating data as the new perimeter means building a culture of data security that permeates every level of the organization, supporting compliance, resilience, and the overall goal of a secure digital environment.

Objective #5: Treat Data as the New Perimeter

Treating data as the new perimeter is a core principle of Zero Trust, emphasizing the need to secure data itself rather than relying solely on network boundaries. This objective focuses on ensuring continuous data visibility, control, and protection throughout its entire lifecycle. By implementing comprehensive data discovery processes, the State of Florida can identify and classify sensitive information, applying appropriate security measures such as encryption and DLP. ABACs ensure that data access is tightly regulated based on multiple contextual factors, providing granular control over who can view or modify information. Furthermore, establishing strong data governance through tagging, labeling, and retention policies helps the state manage data effectively and meet regulatory requirements. By treating data as the perimeter, Florida can significantly reduce the risk of data breaches, ensuring that critical information remains secure regardless of where it resides or how it is accessed.

- Establish continuous data discovery to ensure visibility and control over all data assets. Use data discovery and classification tools to continuously locate sensitive data, both in structured and unstructured forms, and apply appropriate security controls.
- Implement and govern continuous data tagging and labeling for effective data management. Ensure that data tagging processes are automated to label data according to its sensitivity level, facilitating proper handling, encryption, and access control measures.
- Tightly control data visibility and access using robust ABACs. before allowing access to critical data, deploy ABAC mechanisms that consider multiple attributes, such as user identity, role, data sensitivity, and environment

- Deploy DLP analytics to protect data throughout its lifecycle. Integrate DLP solutions that monitor data flows, characterize data, identify potential leaks, and enforce preventive measures such as encryption or blocking unauthorized transfers.
- Ensure that encryption is applied to sensitive data both at rest and in transit, using advanced encryption standards (AES) and ensuring key management best practices.
- Establish data retention policies and ensure compliance with legal and regulatory requirements, specifying how long different types of data are kept and when they should be safely deleted.
- The implementation of Zero Trust data protections, including tagging and classification, is dependent on the progress of the statewide data catalog initiative. Data cataloging maturity may impact the speed at which granular access controls and DSPM capabilities are fully deployed

Visibility and Analytics

Visibility and analytics are crucial components of Zero Trust, as they provide the insights needed to make informed security decisions and respond to threats in real-time. To effectively secure the state's digital assets, Florida must develop comprehensive capabilities to collect, analyze, and act on security data across endpoints, networks, and applications. Establishing centralized log collection and deploying SIEM tools across agencies will enable the state to detect anomalies and potential threats early in the attack lifecycle. Implementing advanced analytics, such as UEBA, helps establish baselines of normal activity and quickly identifies deviations, ensuring a proactive approach to security. Enhanced visibility into security metrics through dashboards also supports informed decision-making, while integrated Security Operations Centers (SOCs), including agency-specific SOCs and coordinated support from the State Cybersecurity Operations Center (CSOC), provide the means to swiftly respond to emerging threats. By building robust visibility and analytics capabilities, the state can achieve continuous situational awareness, enabling dynamic adjustments to security policies and minimizing the risk of undetected threats.

Objective #6: Enhance Visibility and Analytics

Enhancing visibility and analytics is essential for maintaining a proactive and adaptive security posture in a Zero Trust environment. This objective focuses on providing comprehensive situational awareness by collecting, analyzing, and acting upon data from all components of the IT ecosystem. By centralizing log collection, using advanced analytics, and integrating these capabilities with Security Operations Centers (SOCs), the State of Florida can gain real-time insights into potential threats and detect anomalies early. Leveraging UEBA tools helps establish behavior baselines, enabling quick identification of deviations and potential security incidents. Additionally, advanced threat alerting mechanisms and intuitive security dashboards empower decision-makers with actionable insights, allowing them to make informed decisions rapidly. Ultimately, a robust visibility and analytics framework ensures continuous monitoring, rapid threat response, and adaptive security measures that evolve alongside emerging risks and threats.

- Develop comprehensive log collection and analysis capabilities to monitor, detect, and respond to threats. For real-time threat analysis, centralize log collection using Big Data Platform, which provides enhanced scalability, advanced analytics, and cross-agency data correlation capabilities not currently available through existing CSOC tools. Employ SIEM or other analytics tools to gather data from endpoints, networks, and applications.

- Implement advanced threat alerting mechanisms integrated with Security Operations Centers (SOCs). Correlation rules, behavior-based detection, and automated alert triaging streamline the detection process and ensure SOC teams focus on the highest priority threats.

- Establish identity and entity behavior baselines to detect anomalies and dynamically adjust security policies. UEBA tool use can create baselines of normal behavior for users, devices, and applications, and trigger alerts when deviations occur.
- Develop dashboards that provide visibility into key security metrics, ensuring decision-makers have clear, actionable insights into the organization's security posture.
- Conduct regular reviews of analytics and alerting rules to improve precision and minimize false positives, ensuring SOC teams remain effective and efficient.

Automation and Orchestration

Automation and orchestration are vital components of Zero Trust, as they help streamline security processes and ensure rapid responses to threats. By leveraging automation, the State of Florida can reduce manual intervention in security operations, thereby minimizing human error and increasing efficiency. Automation tools, such as SOAR platforms, play a crucial role in automating repetitive security tasks, such as incident triage and response, freeing up security teams to focus on strategic decision-making. Additionally, orchestration allows different security technologies to work in concert, enhancing overall effectiveness by connecting disparate systems and automating workflows. Integrating AI/ML technologies further enhances the state's ability to detect and respond to threats, as these technologies provide the capability to analyze large data sets, identify anomalies, and predict potential incidents. By embracing automation and orchestration, the state can achieve a resilient, adaptive security posture that responds dynamically to emerging threats while improving operational efficiency.

Objective #7: Automate Security Operations and Responses

Automating security operations and responses is a critical objective in the Zero Trust journey, as it aims to enhance the efficiency and effectiveness of digital security measures while minimizing the risk of human error. By implementing automation, the State of Florida can streamline security processes, enabling quicker and more consistent responses to emerging threats such as AI-based attacks and nation-state actors. SOAR platforms play a key role in this effort by automating routine tasks, such as threat detection, incident triage, and remediation, which allows security personnel to focus on more complex challenges that require human expertise. Integrating AI and machine learning further empowers automated systems to learn from historical incidents, predict potential risks, and adapt responses dynamically, ensuring an evolving and resilient security posture. Automation also facilitates seamless collaboration across various security tools and platforms, enabling a coordinated response to incidents and reducing response times. Ultimately, by automating security operations, Florida can achieve greater agility, reduce operational costs, and maintain robust defenses against an increasingly sophisticated threat landscape.

- Develop and inventory policies for automating security tasks and responses. Identifying common, repetitive security tasks that can be automated and define clear policies will ensure consistency and compliance.
- Enrich workflows by automating repetitive and predictable security functions. SOAR platforms automate workflows such as alert triage, incident investigation, and response.

- Deploy automated defensive cyber maneuvers using integrated SOAR and SIEM solutions. Automated playbooks detect and respond to threats, such as isolating compromised endpoints or blocking malicious IP addresses, reducing response time.
- Utilize AI/ML technologies to support security operations, enhance incident response, and optimize threat detection. Machine learning model implementation improves threat detection accuracy, identify patterns that humans may miss, and enhance the efficiency of incident response processes.
- Develop a framework for continuous evaluation and optimization of automated processes, ensuring that they remain effective and aligned with evolving threats.
- Integrate security automation with IT service management (ITSM) systems to create tickets, assign tasks, and maintain a clear record of incident management activities.

Conclusion

Florida's adoption of a Zero Trust represents a pivotal step toward the modernization of its digital security framework, ensuring robust protection for sensitive systems and data. By systematically addressing vulnerabilities within identity management, network segmentation, and data security, the state aims to establish a resilient and scalable IT environment. Centralized procurement, adherence to open standards, and a phased implementation approach will position Florida to better safeguard its digital assets.

This strategic endeavor aligns with statutory requirements while concurrently ensuring that Florida's digital infrastructure is well-defended against evolving cyber threats. Through a commitment to innovation, inter-agency collaboration, and continuous enhancement, Florida aspires to set a benchmark for digital security excellence within the public sector. The journey towards Zero Trust will require sustained commitment and support at all levels; however, with a structured approach, stakeholder engagement, and a strong emphasis on foundational digital security principles, Florida can achieve a secure, resilient, and forward-thinking digital environment.

Florida's focus on foundational practices, phased implementation, and continuous optimization will serve as a model for other states seeking to bolster their digital security defenses. By taking a business-driven approach to transformation and prioritizing operational continuity, Florida will demonstrate how government entities can successfully implement and sustain Zero Trust. Although the journey towards Zero Trust is inherently complex, embracing collaboration, effectively leveraging technology, and fostering a culture of security will position Florida to protect its citizens and digital assets against an increasingly sophisticated threat landscape.

Glossary of Terms, Concepts, and Organizations

Terms or Concepts

Adaptive Authentication: A dynamic security process that adjusts the authentication method based on contextual risk factors, such as the user's location, device, and behavior patterns. For example, accessing from an unknown device may require additional verification steps.

Automation and Orchestration: Automation refers to the use of technologies to perform routine security tasks, such as incident detection or response, without human intervention. Orchestration integrates multiple automated tools and workflows to ensure cohesive and efficient security operations across different systems.

Attribute-Based Access Control (ABAC): A security approach that grants access based on multiple attributes, such as user role, location, time, and device type, rather than static roles. This ensures more granular and context-aware access management.

Bring Your Own Device (BYOD): A policy allowing employees to use personal devices (e.g., smartphones, laptops) to access organizational systems, requiring security measures to ensure compliance and prevent unauthorized access.

Cyber Kill Chain: A structured framework outlining the stages of a cyberattack, including reconnaissance, weaponization, delivery, exploitation, installation, command and control (C2), and actions on objectives (e.g., data theft). It helps in analyzing and disrupting attacks.

Continuous Authentication: A security practice involving ongoing verification of a user's identity during their session to detect and respond to any unusual or unauthorized activity.

Data Classification: The process of organizing data based on its sensitivity and value (e.g., public, confidential, sensitive) to apply appropriate security controls.

Data Loss Prevention (DLP): Tools and processes designed to prevent unauthorized access, sharing, or leakage of sensitive data, such as encrypting data in transit and flagging suspicious transfer attempts.

Data Security Posture Management (DSPM): A set of tools and processes used to monitor, classify, and secure data throughout its lifecycle, ensuring compliance and minimizing risks of data breaches.

Domain-less Environment: A security architecture paradigm that eliminates reliance on traditional domain-based trust models, where access is granted based on network location or membership within a defined perimeter (e.g., corporate Active Directory domains). Instead, it enforces a "never trust, always verify" approach, ensuring that all users, devices, and applications are authenticated, authorized, and continuously monitored regardless of their network position. This paradigm enables dynamic, identity-centric security, supports modern hybrid and multi-cloud environments, and minimizes implicit trust to reduce the attack surface.

Endpoint Detection and Response (EDR): A security solution providing visibility, threat detection, and incident response capabilities for endpoint devices like laptops and servers. It monitors behaviors and detects anomalies in real time.

Federated Identity Management (FIM): A system allowing users to access multiple systems or organizations using a single set of credentials, improving usability, and security through centralized authentication.

Identity and Access Management (IAM): A framework ensuring that the right individuals and devices access the right resources at the right time. It typically involves features like user authentication, access control, and identity lifecycle management.

Least Privilege Access: A principle that grants users or devices only the access necessary for their specific tasks, minimizing potential damage from breaches or misuse.

Micro-segmentation: The practice of dividing networks into isolated segments to restrict access and limit the spread of threats within a network. Each segment enforces its own security policies.

Multi-Factor Authentication (MFA): A security protocol requiring users to provide two or more verification factors, such as a password, a security token, or biometric data, before accessing a system.

Network Segmentation: The practice of dividing a network into multiple zones to isolate sensitive resources and control access. This minimizes the risk of unauthorized lateral movement within the network.

Privileged Access Management (PAM): Tools and processes to secure and monitor privileged accounts with elevated permissions. PAM includes features like credential vaulting, session monitoring, and just-in-time access.

Role-Based Access Control (RBAC): A static access control model that assigns permissions based on predefined roles within an organization, such as "admin" or "user."

Security Information and Event Management (SIEM): A system that aggregates logs and security data from across an organization to detect and analyze threats in real time. It provides a centralized platform for threat management.

Software Defined Perimeter (SDP): A digital security model that dynamically creates secure, virtual perimeters around resources, requiring authentication before granting access. It is an alternative to traditional perimeter-based models.

Secure Software Development Lifecycle (SDLC): The process of integrating security practices into each phase of the software development lifecycle to prevent vulnerabilities and ensure robust application security.

Threat Intelligence: Data and insights about potential and actual threats to an organization, used to predict, prevent, and respond to cyberattacks effectively.

User and Entity Behavior Analytics (UEBA): Advanced tools that use machine learning to establish baselines of normal behavior for users and entities, detecting anomalies that may indicate threats like insider attacks or compromised credentials.

Visibility and Analytics: The processes and tools that provide insights into security-related data, enabling real-time monitoring, detection, and response to threats across systems, networks, and applications.

Zero Trust Architecture (ZTA): A security model based on the principle of "never trust, always verify." It assumes no user or device is trustworthy by default and enforces strict identity verification, least privilege access, and continuous monitoring.

Organizations

CISA (Cybersecurity and Infrastructure Security Agency): A U.S. federal agency responsible for protecting the nation's critical infrastructure from cyber and physical threats. CISA provides resources, guidance, and models like the Zero Trust Maturity Model to assist public and private sectors in enhancing digital security.

CJIS (Criminal Justice Information Services): A division of the FBI that governs the security policies for handling Criminal Justice Information (CJI). CJIS provides standards for state and local law enforcement agencies to securely access and manage federal criminal data.

DoD (Department of Defense): The U.S. federal department responsible for national security and military operations. The DoD has developed its own Zero Trust model emphasizing strict access controls, continuous monitoring, and scalability to protect classified and mission-critical systems.

FBI (Federal Bureau of Investigation): The primary U.S. federal law enforcement agency, responsible for investigating and enforcing laws related to national security, including cybercrime. The FBI oversees the CJIS Security Policy for protecting criminal justice data.

FLDS (Florida Digital Service): The state agency leading digital transformation and digital security efforts for Florida. FLDS is tasked with implementing frameworks like ZTA to protect state resources and citizen data.

MS-ISAC (Multi-State Information Sharing and Analysis Center): A resource for state, local, tribal, and territorial (SLTT) governments, providing threat intelligence, best practices, and digital security services. MS-ISAC facilitates collaboration among SLTT entities to bolster their defenses.

OMB (Office of Management and Budget): A federal office that provides guidance on government policies, including digital security. OMB released Memorandum M-22-09, which directs federal agencies toward adopting Zero Trust principles.

SLCGP (State and Local Cybersecurity Grant Program): A federal funding program that provides resources to state and local governments for enhancing their digital security capabilities, including Zero Trust implementations.

DoJ (Department of Justice): The U.S. federal agency responsible for enforcing laws, protecting citizens, and ensuring public safety. Through entities like CJIS, the DoJ plays a role in setting digital security standards for law enforcement agencies.

Appendix A: Market Analysis: Zero Trust

This market analysis of Zero Trust, a digital security framework that assumes no implicit trust and requires continuous verification of all users and devices, captures the ongoing shift in digital security strategies across industries. Zero Trust's rise is primarily driven by the escalating sophisticated cyber threats, such as ransomware attacks, AI-fueled-threats, and supply chain breaches like the SolarWinds incident, the growing adoption of cloud-first environments, and the urgent need for remote work security. As traditional perimeter-based defenses become increasingly inadequate, Zero Trust provides a modern approach that aligns with the dynamic and distributed nature of today's digital ecosystems. With its principle of "never trust, always verify," Zero Trust ensures secure access through continuous monitoring, stringent identity verification, and adaptive access controls. With an anticipated compound annual growth rate (CAGR) of approximately 17.3%[14], the Zero Trust market is projected to grow from $30 billion in 2023 to $95 billion by 2030[15], reflecting the significant investments being made in security transformations worldwide. These growth projections underscore the increasing importance of Zero Trust as organizations seek to mitigate the risks associated with evolving cyber threats, address regulatory requirements, and adapt to the complexities of cloud-first and remote work environments.

[14] The Rise of Zero Trust Architecture Market: A $38.5 billion Industry Dominated by Tech Giants - VMware (US), Zscaler (US), Akamai (US) | MarketsandMarketshttps://www.globenewswire.com/

[15] Zero Trust Security Market Size, Share & COVID-19 Impact Analysis, By Application (Network Security, Data Security, Cloud Security, Endpoint Security, and Others), By Authentication Type (Single-factor Authentication and Multi-factor Authentication), By Industry (BFSI, Retail, IT & Telecom, Government, Healthcare, and Others), and Regional Forecast, 2023-2030 https://www.fortunebusinessinsights.com/zero-trust-security-market-108832

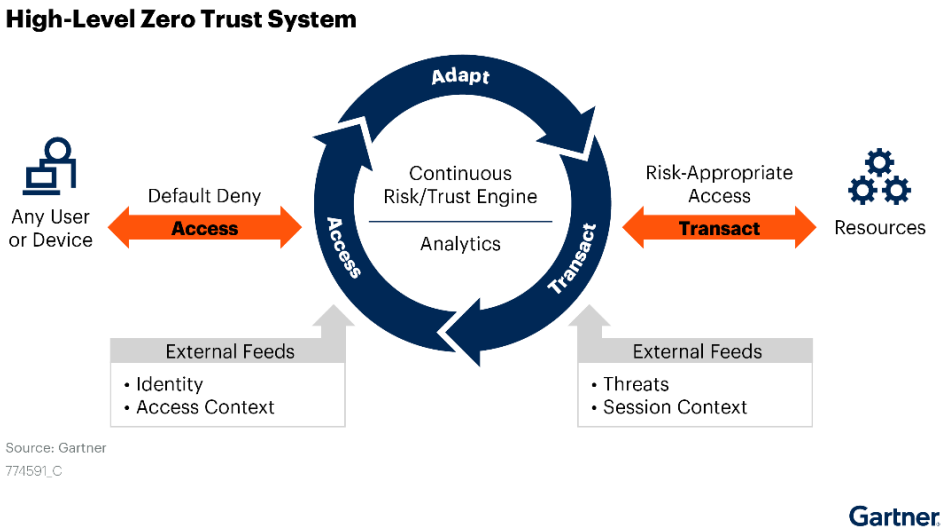


Figure: Strategic Roadmap for Zero Trust Security Program Implementation[16]

The growth in this sector is fueled by several key factors, including the escalation of cyber threats, rapid digital transformation initiatives, and the need to adhere to stringent regulatory requirements such as CJIS, HIPAA, and other industry standards. Organizations across the globe are increasingly recognizing the importance of moving away from perimeter-based security models and adopting a Zero Trust approach that provides comprehensive visibility and control. Unlike perimeter-based models that rely on a trusted internal network, Zero Trust continuously verifies all users and devices, minimizing the risk of insider threats and lateral movement by attackers. It also offers enhanced protection for cloud and remote environments, making it more effective in the modern, distributed IT domain. Key drivers include the ongoing cloud migration, the expansion of remote work environments, government mandates promoting stronger digital security measures, and a heightened need for regulatory compliance across sectors like healthcare, government, financial services, and critical infrastructure. North America currently leads the adoption of Zero Trust[17], driven by advanced IT infrastructures, regulatory pressures, and significant government investments. Europe follows closely behind, with robust data protection regulations contributing to widespread adoption[18]. Meanwhile, the Asia-Pacific region is rapidly emerging as a key growth area, propelled by large-scale digital transformation, growing digital security awareness, and proactive government initiatives aimed at securing digital ecosystems.

[16] Watts, J., MacDonald, N., & Lintemuth, T. (2024, November 21). *Strategic roadmap for Zero Trust security program implementation* (ID G00774591). Gartner.
[17] Fortune Business Insights. (2022). Zero trust security market size, share, and COVID-19 impact analysis, by authentication type (single-factor authentication, multi-factor authentication), by deployment (on-premises, cloud), by enterprise size (large enterprises, small and medium enterprises), by end-user (BFSI, IT and telecom, government and defense, healthcare, retail, and e-commerce, others), and regional forecast, 2023–2030
[18] Markets and Markets. (n.d.). *Zero trust security market by solution (data security, endpoint security, network security, API security), authentication type, deployment mode (cloud and on-premises), organization size (large and SMEs), vertical and region - global forecast to 2027*

Zero Trust Financial Implications

Zero Trust employs a multi-layered, highly integrated defense strategy, significantly mitigating both the frequency and impact of data breaches. Central to its framework are identity-centric technologies such as MFA and FIM, which bolster access controls. Complementary mechanisms, such as micro-segmentation, isolate network segments to prevent lateral movement by malicious actors, while behavioral analytics continuously monitor user activity to detect anomalies in real time. Together, these features form a cohesive security architecture capable of addressing sophisticated and persistent threats.

Empirical analyses demonstrate that organizations implementing ZTA experience, on average, a 42.3% reduction in data breach costs compared to those relying on traditional perimeter-based models[19]. These financial benefits underscore ZTA's pivotal role in enterprise risk management. For example, the Ponemon Institute's 2023 report[20] highlights Zero Trust's ability to reduce the global average cost of breaches, which rose to $4.24 million in 2021, the highest recorded to date.

Beyond direct financial savings, Zero Trust significantly reduces reputational harm and stakeholder distrust often associated with data breaches. Its strict adherence to the principle of least privilege ensures that even if an attacker gains entry, their movements within the system are restricted. This proactive approach preserves both operational integrity and public confidence in the organization. For example, Target Corporation's 2013 data breach incurred $292 million in recovery, compliance costs, settlements, and fines. Implementing Zero Trust tools such as IAM and Endpoint Protection would have reduced this cost to approximately $43.06 million, reducing the impact by up to 85.25%[21] by limiting lateral movement and accelerating breach detection. Similarly, Uber's 2016 breach, which resulted in $158.75 million in fines and settlements, could have been mitigated by Zero Trust measures costing just $3.19 million, representing a mere 2.01% of the breach cost[22].

[19] Adahman, Z., Malik, A. W., & Anwar, Z. (2022). An analysis of zero-trust architecture and its cost-effectiveness for organizational security. *Computers & Security, 122*, 102911.
[20] Adahman et al., "An Analysis of Zero-Trust Architecture," 2022
[21] Adahman et al., "An Analysis of Zero-Trust Architecture," 2022
[22] Adahman et al., "An Analysis of Zero-Trust Architecture," 2022.

The financial benefits of Zero Trust extend beyond individual organizations. Globally, data breaches have reached an average cost of $4.24 million[23], driven by remote work and cloud vulnerabilities. Organizations adopting full-stack Zero Trust solutions report reduced breach costs and faster containment times. For instance, breaches detected and mitigated using Zero Trust are resolved 27% faster, translating into significant operational and financial savings. Additionally, reduced recovery times contribute to improved resource allocation and decreased long-term risk exposure.

Zero Trust's adaptability is evident in its application across various industries and organizational scales. A multinational financial services firm successfully leveraged Zero Trust to secure its hybrid cloud environment, achieving a 30% reduction in unauthorized access attempts. Similarly, a government agency deploying Zero Trust principles to secure remote access for its workforce saw a 20% improvement in system uptime and a measurable decrease in endpoint vulnerabilities.

[23] Adahman et al., "An Analysis of Zero-Trust Architecture," 2022.

Zero Trust: U.S. Market Analysis; Focus on Federal and State Governments

The U.S. Zero Trust market is at the forefront of global adoption, driven by robust digital security initiatives, regulatory mandates, and increasing sophistication of cyber threats targeting critical infrastructure and government systems. With escalating risks such as ransomware attacks on state-level systems, election interference, and vulnerabilities in supply chains, ZTA has emerged as a vital digital security strategy. The U.S. market is projected to grow at a CAGR of 19.1%, outpacing global averages due to accelerated federal and state adoption[24,25]. High-profile incidents, such as the SolarWinds breach and Colonial Pipeline ransomware attack, have catalyzed government investments in Zero Trust.

The federal government has been a leader in Zero Trust adoption, spearheaded by executive orders and regulatory frameworks aimed at modernizing digital security defenses. EO 14028 (May 2021) mandates federal agencies to adopt ZTA principles, emphasizing MFA, EDR, and encryption[26]. Agencies are required to align with the Cybersecurity and Infrastructure Security Agency (CISA)'s Zero Trust Maturity Model[27]. The DoD and the Department of Homeland Security (DHS) have implemented ZTA frameworks to secure military systems and critical infrastructure, with initiatives like the Continuous Diagnostics and Mitigation (CDM) Program[28] emphasizing real-time threat detection and compliance monitoring.

Federal funding underscores the prioritization of digital security, with the FY2024 budget allocating over $11 billion for federal civilian agency digital security initiatives. Of this, approximately 30% is earmarked specifically for Zero Trust efforts[29] This percentage aligns with industry trends where organizations typically allocate 20–30% of their cybersecurity budgets to Zero Trust initiatives, highlighting its critical role in modernizing digital security strategies. A significant portion of this funding is dedicated to Zero Trust efforts, including the modernization of legacy systems, micro-segmentation, and the integration of AI-driven threat detection technologies[30].

[24] Grand View Research. (2021, October 20). *Cloud computing market size worth $1,251.09 billion by 2028 | CAGR: 19.1%: Grand View Research, Inc.* PR Newswire.
[25] Grand View Research. (2022). *Contactless payments market size, share, and trends analysis report by device (smartphones, wearables), by component (hardware, software, services), by application, by region, and segment forecasts, 2022 - 2030.*
[26] Executive Office of the President. (2021). Executive Order 14028: Improving the Nation's Digital security.
[27] Digital security and Infrastructure Security Agency (CISA). (n.d.). *Zero trust maturity model.*
[28] Department of Homeland Security (DHS). (n.d.). *Continuous diagnostics and mitigation (CDM) program.*
[29] The CyberWire. (2023). *Digital security in the U.S. president's budget for fiscal year 2024*
[30] Federal News Network. (2023, September). *Maximizing the proposed FY24 budget starts with zero trust.*

State Government Adoption State and local governments face unique challenges, including budget constraints, fragmented IT systems, and an increasing frequency of ransomware attacks targeting education, healthcare, and public services. Federal grants, such as those under the State and Local Cybersecurity Grant Program (SLCGP)[31], provide funding for states to implement Zero Trust strategies. States like New York, California, and Texas lead adoption due to larger budgets and more mature IT infrastructures[32]. With heightened concerns about election security, states are deploying Zero Trust to secure voter databases and prevent interference, integrating identity verification, and behavioral analytics to ensure only authorized access to sensitive election systems. States are increasingly collaborating with CISA to align digital security initiatives with federal Zero Trust guidelines, with regional consortia, such as the Multi-State Information Sharing and Analysis Center (MS-ISAC), supporting resource-sharing for Zero Trust implementation.

Since the issuance of EO 14028 in 2021 and OMB Memorandum M-22-09, federal agencies have made notable progress in Zero Trust adoption. Key achievements include widespread implementation of multi-factor authentication (MFA) and the establishment of Zero Trust Architecture (ZTA) roadmaps across departments. However, challenges persist, particularly in integrating legacy systems, ensuring consistent enforcement of policies, and managing cross-agency interoperability.

Agencies that adopted phased implementation strategies and prioritized workforce training achieved smoother transitions. Lessons learned emphasize the need for early stakeholder engagement, scalable infrastructure investment, and strong executive support. Florida can leverage these insights by establishing clear compliance milestones, investing in workforce readiness, and aligning legacy modernization efforts with Zero Trust adoption goals.

[31] Federal Emergency Management Agency (FEMA). (n.d.). *State and local cybersecurity grant program (SLCGP)*
[32] Government Technology. (n.d.). *In 2024, SLED IT spending takes a whole-of-state focus.*

The Zero Trust Market

The Zero Trust market is marked by intense competition among established digital security providers and emerging innovators. Industry leaders such as Palo Alto Networks, Zscaler, Microsoft, and Cisco dominate the space with comprehensive product portfolios that cover multiple aspects of Zero Trust, ranging from identity management to endpoint protection and network security. These players leverage their extensive research and development capabilities, as well as strategic partnerships, to provide integrated solutions that meet the evolving needs of enterprises. In addition to these major players, specialized vendors like Okta, which focuses on identity security, and Illumio, which emphasizes micro-segmentation to contain breaches, are carving out significant niches within the market. Key trends shaping the competitive market include the integration of AI and ML with Zero Trust frameworks to enhance threat detection and response capabilities. Additionally, the convergence of Zero Trust and SASE is gaining momentum, enabling organizations to adopt comprehensive, scalable security solutions tailored to distributed workforces[33].

[33] Gartner Research. (2024). Differentiation strategies in the digital security market.

Market Analysis Aligned to Zero Trust Pillars

Identity and Access Management

IAM serves as the backbone of Zero Trust frameworks, ensuring robust identity verification and access control. By integrating real-time risk assessments and adaptive authentication, IAM enforces secure and verified access policies. Key technologies include MFA, privileged access management (PAM), and single sign-on (SSO), which collectively enhance user authentication, streamline access, and reduce vulnerabilities[34,35,36,37,38,39,40].

- **Market Overview:** IAM is a cornerstone of Zero Trust, projected to grow at a CAGR of 14.2% to reach $25.6 billion by 2030.
- **Key Drivers:** Regulatory pressures, remote work adoption, and cloud-based systems drive demand.
- **Key Players:** Okta, Microsoft Entra, Ping Identity, CyberArk, ForgeRock, IBM Security, and vendors offering robust CIAM solutions such as Auth0 and SecureAuth.
- **Opportunities:** Growth in customer identity and access management (CIAM) and federated identity solutions, with a focus on CIAM innovation as highlighted by Gartner's Magic Quadrant analysis.
- **Cost-Effectiveness:** IAM reduces breach recovery costs by up to 50%, with emerging technologies such as FIDO2 passkeys reducing reliance on passwords and enhancing authentication resilience.

[34] Gartner. (2024). *Magic Quadrant for Access Management*. Retrieved December 23, 2024
[35] The Rise of Zero Trust Architecture Market: A $38.5 billion Industry Dominated by Tech Giants - VMware (US), Zscaler (US), Akamai (US) | MarketsandMarkets.
[36] Gartner. (2024b). *Key drivers and market overview for identity and access management (IAM)*. Gartner, Inc. Retrieved from Gartner database.
[37] Allied Market Research. (2023). *Identity and access management market to reach $25.6 billion by 2030*. Retrieved from Allied Market Research database.
[38] Gartner. (2024a). *Magic Quadrant analysis on customer identity and access management (CIAM)*. Gartner, Inc. Retrieved from Gartner database.
[39] IBM. (2023). *IAM reduces breach recovery costs and enhances authentication resilience*. Retrieved from IBM database.
[40] Gartner. (2024c). *The role of FIDO2 and emerging technologies in IAM cost-effectiveness*. Gartner, Inc. Retrieved from Gartner database.

Device Security

Device security ensures that all endpoints, including IoT devices, are secured and compliant within the Zero Trust framework. EDR and UEM technologies are critical for real-time monitoring, threat detection, and automated incident response[41,42,43].

- **Market Overview:** Endpoint security is projected to reach $20 billion by 2030.
- **Key Drivers:** The rise of BYOD policies and IoT proliferation. Additionally, increased focus on hybrid workspaces and the integration of endpoint tools into broader workspace security strategies further accelerate growth.
- **Key Players:** CrowdStrike, Palo Alto Networks, SentinelOne, Sophos, Trend Micro, and ESET. Vendors like Microsoft and VMware are also leveraging their ecosystems to enhance endpoint security offerings.
- **Opportunities:** Enhancing endpoint integration with Zero Trust frameworks and leveraging GenAI capabilities for improved incident explainability, threat hunting, and compliance monitoring.
- **Cost-Effectiveness:** Advanced EDR reduces detection and response times by 40%, with bundled workspace security solutions offering cost savings for small and midsize organizations.

[41] Gartner. (2024). *Magic Quadrant for Endpoint Protection Platforms*. Retrieved December 23, 2024
[42] Statista. (2023b). *Endpoint security market projected to reach $20 billion by 2030*. Retrieved from Statista database.
[43] Forrester. (2023). *The impact of BYOD policies and IoT proliferation on endpoint security*. Forrester Research. Retrieved from Forrester database.

Network Security

Network security integrates Zero Trust principles through technologies like SASE, ZTNA, and Software-Defined Wide Area Networks (SD-WAN). A complete SASE solution combines SD-WAN for optimized connectivity, Cloud Access Security Broker (CASB) for cloud application security, Secure Web Gateway (SWG) for web content filtering, and ZTNA for access control, all orchestrated to deliver secure, scalable, and adaptive network environments. These components work together to minimize vulnerabilities in multi-cloud and hybrid setups while enhancing connectivity and performance for distributed workforces.

- **Market Overview:** Growing at a CAGR of 16%, driven by SD-WAN and SASE innovations. SD-WAN penetration reached approximately 65% in 2024, and its market continues to expand due to demand for integrated networking and security solutions.
- **Key Drivers:** The refresh of branch-office router equipment, MPLS replacements, and application rollouts that leverage cloud and multicloud resources. The need for scalability, agility, and automation to support digital transformation further accelerates adoption. Gartner highlights the shift toward SD-WAN/SSE combinations for deep integration in dual-vendor SASE architectures.
- **Key Players:** Zscaler, Cisco, Fortinet, and Netskope. Vendors like Broadcom (post-VMware acquisition) and HPE (post-Juniper acquisition) are reshaping the competitive landscape by integrating advanced SD-WAN functionalities into broader SASE portfolios.
- **Opportunities:** Lightweight SD-WAN solutions are ideal for hybrid work environments, while SD-branch solutions simplify the integration of SD-WAN, LAN, WLAN, and security for smaller branches. Enhanced AI networking capabilities for automation and policy optimization present additional growth areas.
- **Cost-Effectiveness:** Transitioning from MPLS to SD-WAN with integrated security reduces operational expenses. Opex-friendly subscription models for SD-WAN deployments offer scalable cost management, with evaluations factoring hardware, software, and maintenance costs over three years.

Application Security

Application security safeguards the integrity of software and APIs within Zero Trust frameworks. Technologies like Runtime Application Self-Protection (RASP) and API security tools enhance real-time protection, ensuring secure interactions and mitigating risks. Additionally, Cloud-Native Application Protection Platforms (CNAPPs) provide a unified and integrated approach to securing cloud-native infrastructure and applications. These platforms incorporate artifact scanning, security guardrails, configuration management, risk detection, and behavioral analytics, offering visibility, governance, and control from code creation to production runtime[44,45].

- **Market Overview:** Worldwide end-user spending on application security tools reached $3.4 billion in 2022, a 27% increase from 2021. The market is expected to grow at a CAGR of 18%. Spending trends show North America dominating at 68%, followed by the EU and U.K. at 17%, and the Asia-Pacific region at 12%, with other regions emerging.

- **Key Drivers:** Adoption of microservices, containerized architectures, and API-driven solutions. Regulatory mandates, high-profile incidents related to insecure code, and the shift towards securing cloud-native applications and the software supply chain are key contributors. Organizations are retooling their existing tools to address these evolving challenges.

- **Key Players:** Imperva, Checkmarx, Contrast Security, Synopsys, Veracode, and Snyk. Significant market activity includes acquisitions like Synopsys acquiring WhiteHat Security for dynamic scanning, Snyk's purchase of Fugue to bolster cloud-native capabilities, and Veracode integrating ML-powered auto remediation technology through its Jaroona acquisition.

- **Opportunities:** Increasing focus on application security posture management and cloud-native application security presents significant growth potential. Advanced DevSecOps integration and AI-powered vulnerability management are emerging as key differentiators.

- **Cost-Effectiveness:** Effective application security strategies reduce operational recovery costs by 30%. However, buyers should prepare for potentially higher pricing due to strong demand, leveraging negotiation strategies to optimize investments.

[44] Gartner. (2024). *Magic Quadrant for Application Security Testing*. Retrieved December 23, 2024

[45] Koeppen, D., Winckless, C., MacDonald, N., & ElTahawy, E. (2024, July 22). *Market guide for cloud-native application protection platforms* (ID G00790337).

Data Security

Data security prioritizes the protection and governance of sensitive information. Modern solutions, such as Data Security Platforms (DSPs), provide a unified approach to data protection by combining data discovery, policy enforcement, and governance capabilities. DSPs streamline data access controls and improve compliance by integrating encryption, tokenization, and dynamic data masking into a centralized platform. Additionally, DLP solutions have evolved to incorporate adaptive risk-based techniques, insider risk management (IRM), and behavioral analytics, enhancing their effectiveness against data exfiltration and insider threats[46,47].

- **Market Overview:** Projected to reach $11 billion by 2028. Increasing adoption of DSPs and advanced DLP solutions has been driven by their ability to secure large-scale cloud-based data lakes and support AI/ML use cases.
- **Key Drivers:** Growing ransomware threats, regulatory compliance requirements, and the need for enhanced data governance for cloud-native environments. The convergence of DLP with IRM and the shift to adaptive, risk-based approaches provide more comprehensive protection. Behavioral analytics and anomaly detection enable proactive identification of threats.
- **Key Players:** Symantec, Proofpoint, Netskope, IBM Security Guardium, Protegrity, and Thales CipherTrust Data Security Platform. Additionally, key DLP vendors like Microsoft Purview Adaptive Protection, Palo Alto Networks Enterprise DLP, and Zscaler Cloud DLP are addressing emerging challenges.
- **Opportunities:** Integration with data catalogs, AI-driven policy management, and edge/cloud security enhancements. Privacy-enhancing computation (PEC) technologies such as differential privacy and synthetic data generation also provide a competitive edge. Organizations adopting cloud-native DLP tools gain better visibility and control over public cloud environments.
- **Cost-Effectiveness:** Consolidating data security controls into DSPs and leveraging adaptive DLP solutions reduces administrative overhead and compliance-related fines by up to 70%. Organizations report significant savings in managing complex data environments and improved threat response efficiency.

[46] Chugh, R., & Bales, A. (2023, September 4). *Market guide for data loss prevention* (ID G00776480). Gartner, Inc. Retrieved from Gartner database.
[47] Fritsch, J., Lowans, B., & Bales, A. (2024, January 5). *Market guide for data security platforms* (ID G00787800). Gartner, Inc. Retrieved from Gartner database.

Visibility and Analytics

Visibility and analytics provide real-time insights into security events, enabling proactive detection and mitigation of threats. SIEM, Extended Detection and Response (XDR), and UEBA solutions are essential for centralized monitoring and advanced analytics, with UEBA adding the ability to detect anomalous behaviors across users and entities to preemptively address potential threats[48,49].

- **Market Overview:** The SIEM market grew from $5.03 billion in 2022 to $5.7 billion in 2023, reflecting a 13% annual growth rate. XDR, with a market size between $3.0 billion and $3.5 billion in 2024, is rapidly emerging as a complementary technology. These tools are influenced by trends like cloud adoption, cost management, and a demand for simpler detection stacks. Vendors are increasingly integrating telemetry, enhancing analytics capabilities, and reducing operational complexity.
- **Key Drivers:** Buyers prioritize capabilities such as real-time analytics, batch analytics, and user- and entity-based analytics for detecting advanced threats. XDR extends these functionalities by integrating across diverse environments, improving alert fidelity, and enabling proactive response.
- **Key Players:** SIEM leaders include Splunk, IBM Security QRadar, and Microsoft Sentinel. Prominent XDR vendors such as Palo Alto Networks Cortex XDR, CrowdStrike Falcon Insight, and Trend Micro Vision One are advancing cross-platform capabilities to meet evolving needs.
- **Opportunities:** AI-driven analytics and unified dashboards enable predictive modeling and operational efficiency. Integrated solutions with ITSM tools and automation further enhance incident response while catering to diverse organizational sizes.
- **Cost-Effectiveness:** SIEM and XDR reduce data ingestion costs and consolidate detection tools, streamlining operations, and improving efficiency. These solutions also support exposure management, risk profiling, and compliance tracking, demonstrating measurable ROI.

[48] Gartner. (2024). *Magic Quadrant for Security Information and Event Management*. Retrieved December 23, 2024
[49] Gartner. (n.d.). *Market Guide for Extended Detection and Response*. Retrieved December 23, 2024

Automation and Orchestration

Automation and Orchestration refer to the use of technologies and workflows to streamline and enhance security operations by automating repetitive tasks, integrating various security tools, and orchestrating incident responses. These solutions, such as SOAR, are critical for modern organizations to handle increasing security threats efficiently while aligning with Zero Trust principles. By automating processes, security teams can focus on higher-value tasks, improve response times, and ensure consistent policy enforcement across diverse IT environments[50,51].

- **Market Overview:** Security automation and orchestration tools are growing at a CAGR of 16.4%, with strong adoption of SOAR technologies. This growth is fueled by organizations recognizing the need for scalable, efficient solutions to address increasingly complex security challenges and heightened regulatory pressures, positioning SOAR as a vital component of modern cybersecurity strategies.

- **Key Drivers:** The exponential growth in security alerts and the imperative to reduce response times drive automation adoption. Furthermore, the need to integrate disparate security tools and create seamless workflows adds to the urgency, especially as security operations centers (SOCs) face resource constraints and demand for operational scalability grows.

- **Key Players:** Industry leaders like Palo Alto Networks, Splunk Phantom, and Siemplify offer robust SOAR platforms tailored for Zero Trust environments. Additionally, IBM QRadar, SOAR, and Swimlane have emerged as strong competitors, providing versatile, low-code platforms that cater to diverse operational needs.

- **Opportunities:** Automating Zero Trust policy enforcement and integrating with agile DevSecOps workflows can streamline operations. The expansion of use cases into cloud security posture management and proactive threat hunting further broadens the potential applications for these technologies.

[50] Lawson, C., & Shoard, P. (2023, June 23). *Market Guide for Security Orchestration, Automation and Response Solutions* (ID G00774602). Gartner, Inc. Retrieved from Gartner database.
[51] Gartner. (2023, December 13). *Voice of the Customer for Security Orchestration, Automation and Response Solutions* (ID G00805446). Gartner, Inc. Retrieved from Gartner database.

- **Cost-Effectiveness:** Automation reduces costs related to manual investigations by up to 30%, making it a strategic investment for enterprises. Beyond cost savings, automation enhances incident response capabilities, reduces dwell times, and enables organizations to scale operations without proportionally increasing headcount, thus achieving greater efficiency.

SWOT Analysis: Zero Trust for the State of Florida

Strengths

- **Enhanced Security:** Zero Trust provides a comprehensive security model that significantly reduces attack surfaces and prevents lateral movement within state networks. By enforcing strict verification of all access requests, Florida can ensure that only authenticated users and devices gain access, effectively mitigating potential security breaches. This results in a more resilient infrastructure that is well-protected against both internal and external threats.

- **Regulatory Compliance:** Zero Trust supports adherence to rigorous digital security standards and regulations, helping Florida meet NIST, federal, and state-level compliance requirements. By aligning with national standards and implementing security best practices, Florida can reduce compliance-related risks and ensure the continued security of sensitive government data.

- **Granular Access Control:** Zero Trust enforces least privilege access and continuous verification, ensuring that only authorized users can access critical resources. Granular access control helps prevent unauthorized access and minimizes the risks posed by compromised accounts or devices, enhancing overall security. This also contributes to a more effective incident response by isolating incidents to specific user or device contexts.

- **Scalable Implementation:** Zero Trust principles can be incrementally rolled out, allowing Florida state agencies to implement changes in phases. This phased approach minimizes disruption, makes it easier to manage resources, and allows agencies to prioritize critical systems and high-risk users. It also facilitates continuous improvement as agencies learn from each phase and adjust implementation strategies accordingly.

Weaknesses

- **Complex Implementation:** The complexity of deploying Zero Trust across legacy and diverse IT systems is a significant challenge, particularly within state agencies reliant on older infrastructure. Integrating Zero Trust with these systems requires extensive planning, modifications, and possible system upgrades, all of which add to the implementation timeline and cost. Overcoming this complexity requires a dedicated focus on technical planning and stakeholder collaboration.

- **High Initial Costs:** The significant initial investment required for technology upgrades, workforce training, and system integration poses challenges for budget-constrained agencies. Costs include acquiring new tools, upgrading infrastructure, hiring skilled professionals, and implementing new processes, which can be prohibitive for smaller agencies. To alleviate this burden, Florida may need to explore federal grants or public-private partnerships to support Zero Trust initiatives.

- **Vendor Lock-In:** Proprietary solutions may lead to vendor lock-in, complicating future upgrades or transitions to other solutions. Once an agency commits to a particular vendor's ZTA, switching to a different provider can be challenging and costly due to proprietary technologies, incompatibility issues, and the need for additional training. Agencies must carefully evaluate vendor offerings and prioritize solutions that support interoperability and open standards.

- **Skill Gaps:** Implementing Zero Trust effectively requires specialized skills and expertise, necessitating additional training or hiring. Many state agencies may lack staff with the knowledge needed to configure and manage Zero Trust components, such as micro-segmentation, IAM, and endpoint security. Addressing this skill gap requires investment in workforce development, targeted training programs, and partnerships with digital security training providers.

Opportunities

- **Digital Transformation:** Zero Trust aligns well with Florida's digital transformation initiatives, providing a strong foundation for secure remote access to resources and cloud adoption. As agencies adopt more cloud-based services and support remote sites across the state, Zero Trust can ensure that all access points are secured, regardless of user location or device type. This strengthens Florida's ability to provide robust security for a modern, agile government workforce.

- **Federal Funding:** Growing federal emphasis on digital security could result in funding opportunities for implementing Zero Trust. Federal grants and funding initiatives aimed at improving state and local government digital security can help Florida accelerate the adoption of Zero Trust, alleviate budget constraints, and enable agencies to acquire necessary technologies. Collaboration with federal agencies will also ensure compliance with national digital security standards.

- **Public Trust:** Demonstrating robust digital security practices can enhance public trust. By implementing Zero Trust, Florida can showcase its commitment to protecting citizen data and ensuring the integrity of public services. Enhanced public trust can lead to increased citizen engagement with digital services, ultimately improving the efficiency and effectiveness of government operations.

- **Technology Integration:** Integration with emerging technologies such as AI, SASE, and cloud-native platforms can lead to more automated and comprehensive security solutions. AI can assist in continuous threat analysis and adaptive policy enforcement, while SASE offers a unified approach to secure remote access. By leveraging these technologies, Florida can develop a sophisticated security ecosystem that is both efficient and effective in mitigating risks.

- **Leveraging Predictive Technologies:** The growing role of predictive technologies, such as AI for automated threat detection and adaptive policy generation, presents an opportunity for Florida to proactively mitigate threats. AI-driven solutions can enhance the state's ability to counteract sophisticated attacks, including ransomware and AI-based phishing attempts, by providing real-time analysis and automated response mechanisms.

- **Mitigating Non-Human Identity Abuse:** The rise of non-human identity-based attacks, as highlighted in recent digital security predictions, presents both a challenge and an opportunity. By focusing on comprehensive identity management systems, Florida can mitigate the risk of abuse by automated accounts and non-human identities, ensuring that access is tightly controlled and monitored.

Threats

- **Evolving Threat Landscape**: Cyber threats continue to evolve, increasing the need for Florida to continually update its ZTA. Attackers are employing more sophisticated tactics, including supply chain attacks, advanced persistent threats (APTs), and targeted ransomware campaigns, all of which demand constant vigilance and adaptation. Industry predictions for 2025 suggest an increase in ransomware attacks, as well as the exploitation of AI and automated accounts, underscoring the necessity for continuous monitoring and proactive security measures[52].

- **Budget Constraints:** Financial limitations could hinder the comprehensive implementation of Zero Trust. Competing budget priorities may limit the availability of funds needed to invest in new technologies, upgrades, and training programs. Budget constraints may lead to fragmented implementations or a lack of coverage for lower-priority systems, ultimately leaving vulnerabilities that could be exploited by attackers.

- **Integration Challenges:** Integrating new Zero Trust solutions with existing legacy systems can be difficult and slow the implementation process. Many legacy systems lack the compatibility required to seamlessly integrate with modern Zero Trust technologies. Addressing these challenges requires careful planning, phased integration, and potentially significant upgrades to ensure that all systems are covered by Zero Trust protections without disrupting essential services.

- **Resistance to Change:** Organizational resistance and cultural inertia within agencies may hinder the successful adoption of Zero Trust principles. Employees accustomed to traditional network models may be resistant to new protocols that require more frequent verification, additional training, or changes to daily workflows. Overcoming resistance requires strong leadership, effective communication, and a focus on the long-term benefits of enhanced security and risk reduction.

- **Increased AI Exploitation:** The potential for increased exploitation of AI systems and large language models by adversaries poses a significant threat. As predictive capabilities and AI-driven automation become more prevalent, attackers may use these technologies for sophisticated social engineering, impersonation, and other malicious activities. Florida must adopt advanced AI security measures to mitigate these emerging threats effectively.

[52] RQ. (2025). 2025 Digital security Predictions: Navigating the Future of Cyber Threats. RQ Corporation.

Nevertheless, the outlook for Zero Trust remains highly promising as a central strategy for enhancing security and compliance in the face of evolving cyber threats. Advancements in AI, edge computing, and IoT security will further expand the applicability of Zero Trust principles, enabling more granular and dynamic security controls. Adoption of Zero Trust could provide organizations with a decisive advantage, not only in safeguarding their digital assets but also in maintaining regulatory compliance and building resilience against future threats. Adopting Zero Trust could position Florida to effectively navigate the increasingly complex digital security environment, ensuring that they are prepared to meet the challenges of tomorrow.