EBOOK

Accelerating Zero Trust Capabilities

Saviynt & DoD: Minimizing embedded trust to empower a more secure mission.

Saviynt

Table of contents

Saviynt

We recently explored the Department of Defense's new Zero Trust strategy, including digging into its ambitious architecture goals

Behind this cyber defense effort is a clear vision: *an Information Enterprise secured by a fully implemented, Department-wide Zero Trust cybersecurity framework.*

To achieve this, US cyber officials propose seven "trust pillars." Together, these form the basis for the national capabilities roadmap, execution plan, and reference architectures.

In order to ensure standardization and execution of the strategy, Department of Defense (DoD) officials emphasize that Zero Trust capabilities must be built, deployed, and operated within these pillars.

DoD Zero Trust Pillars

- **User**: Authenticate, access, and monitor user activity patterns to govern users' access and privileges while securing all interactions.
- **Devices**: Understanding the health and status of devices informs risk decisions. Real-time inspection, assessment, and patching levels dictate every access request.
- **Applications & Workloads**: Secure everything from applications to hypervisors, including protecting containers and virtual machines.
- **Data**: Ensure data transparency and visibility enabled and secured by enterprise infrastructure, applications, standards, robust end-to-end encryption, and data tagging.
- **Network & Environment**: Segment, isolate, and control (physically and logically) the network environment with granular policy and access controls.
- **Automation & Orchestration**: Automate security responses based on defined processes and security policies enabled by AI (e.g., blocking actions or forcing remediation based on intelligent decisions).
- **Visibility & Analytics**: Analyze events, activities, and behaviors to derive context and apply AI/ML to achieve a highlighted personalized model that improves detection and reaction time in making real-time access decisions.

For each of these pillars, DoD requires agencies to leverage both cyber principles and enterprise solutions to address specific Zero Trust (ZT) capabilities.

As visualized below, the DoD offers roadmaps by breaking down the ZT reference architecture into 45 specific capabilities. Each of these aligns with one of the seven DoD Zero Trust Pillars, depicted horizontally.

Working together to accelerate initiatives requires agencies to execute toward alignment with the required maturity model by 2027.

Saviynt & DoD: Realizing a Zero Trust Identity Vision

Saviynt is an identity security company that helps governments and commercial organizations modernize identity programs and build Zero Trust foundations.

In this guide, we hone in on the three specific pillars that require agencies to protect users, systems, and data at the identity layer.

The following discussion is broken down into three parts.

1. First, we map DoD Zero Trust pillar capabilities to Saviynt identity solutions.
2. Next, we break down the *User, Applications and Workloads, and Visibility and Analytics* pillars. For each, we identify what Zero Trust outcomes will look like.
3. Then, we highlight what security tools DoD agencies can leverage to meet Zero Trust requirements.

1 Solution Mapping: ZT Pillars & Capabilities

Four major tenets influence the DoD Zero Trust Architecture (ZTA):

- *Assume a hostile environment*
- *Presume breach*
- *Never trust, always verify*
- *Scrutinize explicitly and apply unified analytics*

As agencies roadmap ways to fulfill required capabilities, they must first assess whether solution vendors also architect their own platforms with the same assumptions. Some, like Saviynt, do.

Saviynt Enterprise Identity Cloud (EIC) is a fully converged identity platform that unites core identity governance and security capabilities to protect people, data, and infrastructure.

EIC engages AI/ML to contextualize and reduce risk, automate identity lifecycles, and provide smart recommendations to increase security effectiveness.

Four modular identity security capabilities converge to form the single-platform EIC:

- Identity Governance and Administration (IGA)
- Cloud Privileged Access Management (PAM)
- External Identity & Risk Management
- Application Access Governance (AAG)

EIC integrates and shares contextual risk intelligence with other identity and cybersecurity tools, including SIEM, XDR, and SASE, to enhance threat detection and incident response.

Below, we describe the primary ways Saviynt supports key DoD's Zero Trust pillar activities, including a cross-pillar, security transformation effort that enhances mission readiness.

DoD ZT Pillar	Saviynt Capability Alignment	Saviynt Services
User	• 1.1 User Inventory • 1.4 Privileged Access Management • 1.7 Least Privilege • 1.9 Integrated ICAM Platform	• IGA • Cloud PAM • External
Applications & Workloads	• 3.3 Software Risk Management • 3.5 Continuous Monitoring & Ongoing Authorization	• IGA • AAG
Visibility & Analytics	• 7.3 Common Security & Risk Analytics • 7.4 User & Entity Behavior Analytics • 7.6 Automated Dynamic Policies	• IGA • AAG

** Importantly, Saviynt also delivers solutions across a joint-partner ecosystem to address dozens of other capabilities across DoD ZT pillars.*

2 ZT Pillar Breakdowns

[based on DoD Zero Trust Capability Execution Roadmap]

Pillar 1 - User

Cybersecurity incidents resulting from immature capabilities in identity, credential, and access management (ICAM) are on the rise. Often, government agencies are in the crosshairs. According to BlackBerry Cybersecurity's second *Quarterly Threat Intelligence Report,* attacks against government agencies and public sector services rose 40% in the second quarter of 2023 compared to the first.

Adopting an identity-centric security architecture will help DoD organizations minimize the risks of a data breach by reducing instances of unauthorized access and theft.

The "user" pillar focuses on managing user access in a dynamic risk environment. To prove maturity, agencies need capabilities across identity management, credential management, access management, federation, and governance.

- **1.1 User Inventory:** Agencies must ensure that regular and privileged users are identified and integrated into an inventory supporting regular modifications. This includes ensuring that applications, software, and services that have local users are also inventoried.

  Outcomes and Impact to Zero Trust
  System owners will have control, (including visibility and administrative rights), of any authorized and authenticated network user. By policy, access is denied for any unauthorized users.

- **1.1 User Inventory:** Agencies must ensure that regular and privileged users are identified and integrated into an inventory supporting regular modifications. This includes ensuring that applications, software, and services that have local users are also inventoried.

  Outcomes and Impact to Zero Trust
  System owners will have control, (including visibility and administrative rights), of any authorized and authenticated network user. By policy, access is denied for any unauthorized users.

- **1.4 Privileged Access Management:** Agencies must establish an ability to remove permanent, elevated privileges. This will include introducing a PAM solution and migrating users to it. This capability should progressively mature with functionality including approvals automation and analytics-driven anomaly detection.

  Outcomes and Impact to Zero Trust
  Organizations must control, monitor, secure, and audit privileged identities (e.g., through JIT provisioning, and password vaulting) across their IT environments. Through this, critical assets and applications are secured, controlled, monitored, and managed through admin access limits.

- ***1.7 Least Privilege Access:*** DoD organizations need to govern access to data/access/applications/services (DAAS) using the absolute minimum access required to perform routine tasks or activities. This first requires application owners to identify the necessary roles and attributes for standard and privileged user access.

  Outcomes and Impact to Zero Trust
  In terms of outcomes and impact to Zero Trust, once elevated privileges are audited and removed, network users will only have access to the DAAS for which they are authorized and authenticated over a specific time frame.

- ***1.9 Integrated ICAM Platform:*** DoD organizations employ enterprise-level identity management systems to track user and non-person entities (NPE) identities across the network and ensure access is limited to only those who have a need and the right to know. Organizations will establish this through a credential management system, an identity governance and administration tool, and an access management tool.

  Outcomes and Impact to Zero Trust
  The identities of users and NPE are centrally managed to ensure authorized and authenticated access to DAAS resources regardless of location.

Pillar 3 - Applications & Workloads

IT environments today blend on-prem, private, and managed and public cloud applications and infrastructure elements. From a governance, risk, and management perspective, agencies need to better control access to and within varied applications and workloads, including as-a-service applications and infrastructure assets.

Every application has its own security model to protect privileged and sensitive data and that's the challenge. Without consolidated visibility across all applications, cross-application control violations, and other access risks, remediation becomes a highly manual, error-prone process, which may not completely resolve the issues. Left unchecked, this can put critical information at risk.

The "applications and workloads" pillar represents security capabilities across systems, programs, and services within on-premises and cloud environments. In true zero trust contexts, users strongly authenticate into applications, not into the underlying networks.

- ***3.3 Software Risk Management:*** Agencies establish a software/application risk management program supported by controls including Bill of Materials risk management, Supplier Risk Management, approved repositories and update channels, and vulnerability management program. In addition, DoD organizations will adopt Continual validation within the CI/CD pipelines. These form the cornerstone of a broader effort to add supply chain cybersecurity and strengthen DevSecOps.

  Outcomes and Impact to Zero Trust
  Code used in DAAS and other supply chain components is secure, vulnerabilities are reduced, and security leaders are aware of risks as they arise.

- ***3.5 Continuous Risk Monitoring:*** Organizations will employ automated tools and processes to continuously monitor applications and assess their authorization to operate.

  Outcomes and Impact to Zero Trust
  Agencies will achieve near real-time visibility into the effectiveness of the security controls they deploy.

Pillar 7 - Visibility & Analytics

Using advanced analytics to improve identity security is critical to outpace cybersecurity threats. More in-depth use of analytics technologies grows risk awareness and decision-making for identity-related business processes.

Visibility and analytics go hand-in-hand. With actionable analytics, enterprises can visualize data and risks, and promptly respond. Examples of this may include real-time insights into user risk changes due to excessive access or the presence of activities outside a role/user's typical behavior. Better insight leads to smarter controls, too, including creating and managing access policies and roles.

The "visibility and analytics" pillar emphasizes cyber-related data analysis and improved visibility across key systems. Through this, DoD organizations can make better policy decisions, plan responses, and build out risk profiles in order to develop proactive security measures before a cyber incident occurs.

- ***7.3 Common Security & Risk Analytics:*** Any Computer Network Defense Service Provider (CNDSP) or security operations center (SOC) will employ necessary, big data tools throughout their enterprises (that support multiple data types) to unify data collection and examine events, activities, and behaviors.

  Outcomes and Impact to Zero Trust
  CNDSPs/SOCs will support more integrated analysis efforts, while prioritizing efforts based on risk, complexity, and better reporting.

- ***User & Entity Behavior Analytics:*** Agencies begin by employing analytics to profile and create an activity baseline for users and NPEs. In addition, analytics will help correlate user activities, behaviors, and detect anomalies. CNDSPs/SOCs will mature this capability through the use of increasingly advanced analytics.

  Outcomes and Impact to Zero Trust
  Analytics capabilities will become a key part of the effort to detect anomalous users, devices, and NPE actions and advanced threats.

- ***7.6 Automated Dynamic Policies:*** DoD organizations will deploy ML & AI solutions to dynamically update security profiles and device configuration through continuous security posture monitoring, risk and confidence scoring, and automated patch management.

  Outcomes and Impact to Zero Trust
  Users and NPEs will be denied access based on automated, real-time security profiles. These profiles will be established based both on external conditions, as well as evolving risk and confidence scores.

3 Fit-for-purpose tools to meet ZT goals

Saviynt Enterprise Identity Cloud enables organizations to close identity security gaps, standardize and streamline identity lifecycle management, and mature their identity and access operations:

- Inventory and categorize all of their digital identities – both standard and privileged – on one converged platform
- Get 360-degree visibility across identities and access
- Leverage built-in analytics and policy engines to make risk-aware access decisions throughout the identity lifecycle
- Remove the need to have always-on, excessively privileged accounts and instead, attach time-bound, task-specific privileges as defined by organization policy, then monitor which assets were accessed and what actions were taken

Saviynt solution: Identity Governance and Administration (IGA)
Capabilities enabled: *1.1 User Inventory, 1.9 Integrated ICAM platform, 7.4 User & Entity Behavior Analytics, 7.6 Automated Dynamic Policies*

Saviynt Identity Governance and Administration (IGA) ensures your users have seamless access to necessary resources on-premises, in the cloud, or in hybrid environments.

As agencies demand more efficiency and agility, IGA adds automation and intuitive identity workflows. Our IGA solution is powered by a comprehensive identity warehouse and features an extensive controls library for risk-based, continuous compliance and security.

Due to our direct integration approach, we can predictably show results in the Microsoft ecosystems. We utilize a direct connection to source information and don't allow for unknown time delays in the Joiner, Mover, and Leaver activities. For example, with Saviynt's Microsoft Azure Active Directory (AD) connector you can make a connection to an application in less than 10 minutes, and start implementing dynamic policies, and begin performing behavior analytics.

To help agencies advance across the ZT maturity spectrum, Saviynt IGA is 'intelligent at its core', which means faster access decision-making with AI/ML-driven recommendations, remediation, and auto-provisioning capabilities. Security teams can easily ingest any identity, analyze complex access and usage data, and make risk-aware access decisions throughout the identity lifecycle.

Saviynt solution: Cloud Privileged Access Management (PAM)
Capabilities enabled: *1.4 Privileged Access Management, 1.7 Least Privilege Access, 3.5 Continuous Risk Monitoring*

One goal underpins Saviynt's risk-based approach to Privileged Access Management (PAM): Eliminate persistent accounts and standing privilege with built-in identity governance.

Saviynt's converged identity governance and just-in-time privilege approach enables you to go from managing privilege to eradicating privilege to get as close as possible to the nirvana zero standing privilege (ZSP) state. Saviynt Enterprise Identity Cloud offers security leaders the capability to configure, approve, and monitor time-bound, role-based privileged sessions. This includes enabling just-in-time elevated access to resources, and monitoring privileged activity while it occurs. You get a clear picture of what a person does with their access and the risk associated with the totality of a user's access across the organization.

In order to mature Zero Trust environments, DoD organizations must deploy PAM solutions that support more ephemeral cloud resources. Today, fixed interval environment scans no longer work. Today's complex hybrid environments require a PAM solution that continuously discovers cloud risks. Saviynt Cloud PAM scans for changes within elastic workloads, new privileged accounts, and access – all in real-time. Misconfigured objects are easily flagged, and remediation steps (including session termination or access removal) trigger automatically.

The power of Saviynt's converged identity platform also enables you to reduce the complexity around ZSP for external personnel as well as non-human identities like IoT and edge platforms, and field-deployed equipment with remote just-in-time access provisioning.

Saviynt solution: External Identity & Risk Management
Capabilities enabled: *1.1 User Inventory, 1.7 Least Privilege, 1.9 Integrated ICAM Platform, 7.4 User & Entity Behavior Analytics*

Saviynt's External Identity & Risk Management solution helps DoD organizations provision and manage federated access across all environments with confidence, and solve third-party risks at the identity layer.

Legacy identity governance tools were not designed for non-employee identity governance, and many organizations end up using non-purpose built tools and cumbersome policies, which can sacrifice mission speed. With our FedRAMP authorized converged identity cloud, organizations no longer have to sacrifice speed for security.

Saviynt External Identity & Risk Management enables organizations to inventory third-party users within one converged identity platform to create more trusted, strategic relationships. Organizations can make significant improvements to their security posture while reducing the complexity and manual effort required to manage external access through non-purpose built tools. Consider these examples:

1) **Government to government users.** For example, let's suppose a financial application owned by one agency that needs to share access to members of another agency. The originating agency owns the risk but they don't have control of the users. They can leverage Saviynt EIC to provision access as an external identity and monitor the application itself for access risk.

2) **Logistics and combat support entities.** Each branch deals with outside support agencies, such the Defense Logistics Agency (DLA), the US Military's end-to-end global combat logistics supply chain, and the Defense Information Systems Agency (DISA). With Saviynt EIC, agencies can develop risk-based access policies, enabling support teams to get the right access at the right time.

3) **Shared Maintenance and Repair Operations (MRO).** These facilities provide logistics support to multiple branches. For example, an Air Force facility may also share services with mission partners, including the US Navy. Saviynt EIC allows you to set risk-based entity and identity access policies to ensure that all of your partners, contractors, maintenance workers, and suppliers can get the right access at the right time to perform their mission.

4) **US Government to other allied mission partners and governments.** There may be a need to bring applications into theater for a joint exercise and in order to meet the mission, access will need to be provisioned to these alliance partners.

Security leaders can manage the identity program with pre-built templates, robust control libraries, and an intuitive wizard to reduce application onboarding effort. Saviynt also supports automated access provisioning, requests, and approval — along with essential Joiner, Mover, and Leaver processes. When combined with Cloud PAM, security leaders can add just-in-time privileges and session monitoring capabilities to detect misuse.

In order to enforce compliance controls and create readily accessible audit documentation, Saviynt helps map compliance controls to user type and offers auto-remediation policies to remediate non-compliant identities.

Saviynt solution: Application Access Governance (AAG)
Capabilities enabled: *3.3 Software Risk Management, 3.5 Continuous Monitoring & Ongoing Authorization*

Saviynt's Application Access Governance (AAG) solution helps agencies bring identity management and application GRC under one roof to align security policies across all apps, devices, and operating platforms. Whereas Saviynt IGA ensures holistic control over user identities, roles, and access. Saviynt AAG controls at the application level to address risks unique to each application and across complex global software deployments.

Organizations can stop access risks in their tracks with centralized, fine-grained entitlement management, real-time intelligence, and automated remediation to secure applications, users, and data.

Our AAG capability
We also provide integration with mission-critical enterprise tools to improve visibility into access permissions and user activities. Our AAG solution also features preventive and detective Separation of Duties (SoD) analysis capabilities, as well as out-of-the-box rulesets for a granular view of application risk.

These capabilities support ongoing audit readiness with continuous compliance across popular cloud applications and on-premise applications. For many enterprise applications, Saviynt has rulesets with preset definitions for risky combinations of fine-grained entitlements and maintains continuous compliance with Sarbanes-Oxley, HIPAA, FISCAM, CMMC, and hundreds of other government regulations and standards.

Conclusion

For Department of Defense agencies aiming to fortify their Zero Trust capabilities, integrating robust identity security measures is not a strategic choice, but a mission necessity.

By embracing a comprehensive identity security framework and incorporating cloud-built identity solutions, agencies can both resist evolving cyber threats and make progress toward fiscal year 2027 implementation demands.

With Saviynt, organizations can ensure that every access request is stringently verified, every identity is continuously authenticated, and access privileges are controlled and monitored in a centralized way. Embracing this shift in identity security is not merely an upgrade; it's a critical step in securing national interests in the digital age.

To learn more about how Saviynt FedRAMP authorized **Enterprise Identity Cloud** accelerates the pathway toward Zero Trust, **talk to our team.**

Saviynt

Headquarters, 1301 E
El Segundo Bl, Suite D, El Segundo, CA
90245, United States

310. 641. 1664 | info@saviynt.com
www.saviynt.com