

Enable a Zero Trust Architecture with ServiceNow

Thank you for your interest in exploring this content.

Carahsoft is the **Trusted Government IT Solutions Provider**® supporting a broad portfolio of industry-leading technologies through GSA, NASA SEWP, ITES-SW2 and a wide range of other contract vehicles.

As the **Master Government Aggregator**®, Carahsoft connects government agencies, industry partners, and technology providers to deliver innovative, mission-focused solutions.

In partnership with ServiceNow, we provide technology solutions that drive modernization, strengthen operations, and ensure compliance with evolving government standards.



To learn more about how Carahsoft can support your technology needs, please visit carahsoft.com



Explore More Resources:
carah.io/SNresources



Join Events & Webinars:
carah.io/SNevents



Discover Technology Solutions:
carah.io/servicenow



Learn About Procurement:
carah.io/SNcontracts



Connect With Our Team:
ServiceNowteam@carahsoft.com
(855) ITSM-NOW

Enable a Zero Trust Architecture with ServiceNow

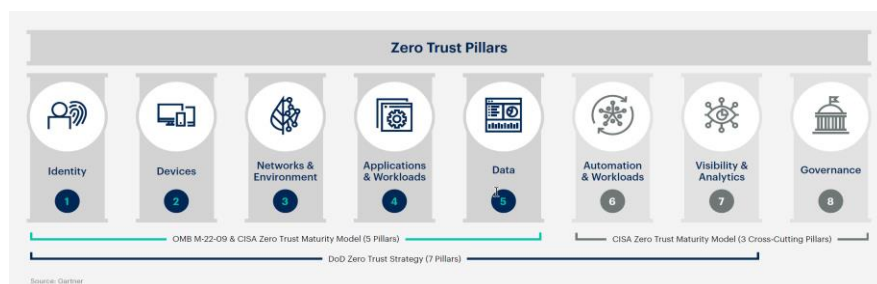
Unprecedented cybersecurity risks for government agencies

Federal agencies are grappling with increasingly complex cybersecurity challenges as adversaries exploit weaknesses in traditional perimeter-based defenses. At the same time the cybersecurity landscape, organizational infrastructure, and operations have evolved. On top of that, ransomware has proliferated, core commodity services have transitioned to "as a service" cloud offerings, and both users and customers have higher expectations for performance and resilience. A of these factors require a paradigm shift in to how we think about security.

The Zero Trust mandate for strengthening cybersecurity

The U.S. Federal Government has responded by adopting the Zero Trust Architecture (ZTA), a transformative framework based on the principle of "never trust, always verify" to protect data, systems, and users against modern threats. To provide guidance, Memorandum 22-09 (M-22-09) was drafted, requiring agencies to implement Zero Trust Cybersecurity Principles and achieve specific security goals by the end of Fiscal Year (FY) 2024, following the Zero Trust Maturity Model developed by CISA. Building on M-22-09, the Department of Defense (DoD) has expanded its Zero Trust Strategy to include two additional pillars, mandating that "all components achieve the intended Target level outcomes of each DoD Zero Trust Capability and execution enabler no later than the end of FY2027".

This solution brief provides guidance to enable a Zero Trust Architecture, helping to ensure operational resilience, compliance, and mission success.



Source: Gartner: Execute on Zero Trust Principles to Improve Your Security and Risk Posture

Outdated, disconnected technology is counter productive to Zero Trust

Zero Trust is both a security and operational necessity for addressing the evolving threat landscape. At its core, Zero Trust, is intended to build operational resilience, ensuring agencies are prepared to respond and quickly recover from attacks.

Technology is the enabler to improve your Zero Trust posture. However, for many agencies, the current programs and products at your disposal can be outdated or insufficient. When used to meet the needs of Zero Trust, they instead open the door to new risks, allow vulnerabilities to slip through the cracks, and hamper digital transformation efforts.

The most common challenge is silos of data and tools that make it impossible to get an integrated view of your security or risk posture, automate processes, or collaborate easily across functional groups.

ServiceNow advantage

Improved security posture –

Reduce the attack surface through continuous verification and proactive threat detection.

Accelerated threat response –

Automated workflows and orchestration both on-premises and in the cloud across Zero Trust pillars shortens time to remediate.

Operational resilience –

Minimize downtime and risk from cyber incidents with preparation and planning.

Mission assurance –

Improved security of tactical and strategic systems critical to national defense.

Ongoing compliance –

Alignment with DoD Zero Trust Strategy, NIST SP 800-207, and Executive Order 14028.

Scalability –

A Zero Trust Architecture that is adaptable to enterprise, cloud, and tactical edge environments.

Better decision making –

Data sharing and integration between products, including those from third parties, provide more accurate, real-time data.

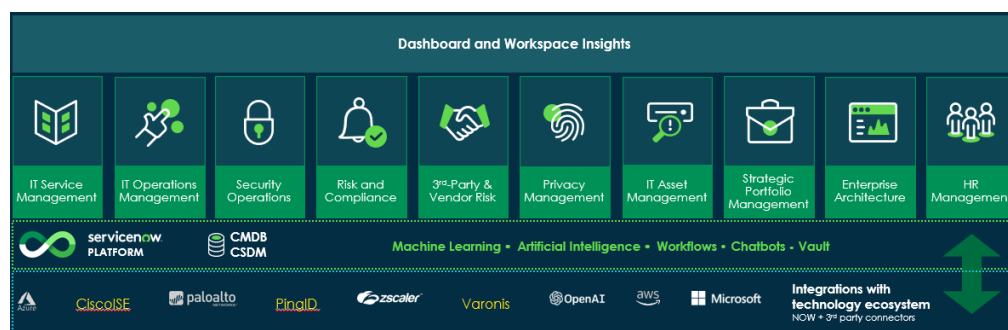
Enhanced user experience –

Easier access to information, AI/ML, and automation reduce employee burdens and increase customer satisfaction.

ServiceNow connects your people, processes, and technology

Successfully enabling Zero Trust to building resilience against evolving threats, requires an integrated program across your people, processes, and technology ecosystem that addresses all aspects of the Zero Trust Architecture.

There is no one product that can be used to enable a comprehensive Zero Trust program. It's a journey that requires a unified solution built on a single platform.



Create a unified program for Zero Trust across the pillars

Let's explore how ServiceNow enables Zero Trust for each of the five "pillars" that align with both the OMB and the DoD, in addition to the DoD's two additional pillars.

Identity

Complete and current knowledge of your mobile workforce is crucial as Zero Trust access depends on strict identity authentication and authorization based on location, device, identity, and role. Use the unified Now Platform with the ServiceNow IT Service Management, HR, and IT Operations Management to maintain accurate user data including compliance and training records that can be dynamically accessed to enable identity proofing. Through automation and Integration with credentialing systems you can adjust or revoke access in real-time, while proper governance provides the confidence that system access is compliant with identity policies.

Devices

The ability to track assets and asset health is imperative to maintain a strong security posture and protect sensitive data. Use ServiceNow IT Operations Management and IT Asset Management to discovery and classify assets (hardware, software, and cloud). Monitor deployment and asset health (location, vulnerabilities, and security tools) to identify anomalies or unmanaged assets and ensure proper security measures are put in place. Automate asset lifecycle management to maintain current records. ServiceNow Security Operations and Integrated Risk Management enable you to respond to threats and remediate issues with AI support. Use ServiceNow Third-party Risk Management to extend best practices to third-party providers, integrating risk intelligence feeds to monitor threats to the supply chain.

Network and environments

Meeting the Zero Trust network pillar requirements will necessitate some level of digital transformation across your current environment. Digital transformation efforts can dramatically improve operations, but changes can also create vulnerabilities. In your environment there are potentially hundreds of tools used to scan for vulnerabilities, manage access, identify threats, and much more. Use the Now Platform and IT Operations Management to integrate data from your technology ecosystem, including legacy systems. Dynamically manage policies, use audit functionality to drive compliance, and establish incident, problem, and change management practices to sustain a strong Zero Trust environment. ServiceNow Security Operations, Security Orchestration, Automation, and Response (SOAR) capabilities in conjunction with the MITRE ATT&CK framework reduces the opportunity for human error and streamlines incident response. Additional capabilities help maintain enterprise-compliant, secure cloud deployments to ensure compliance and proactively detect threats.

Applications and workloads

Visibility into applications and services is a requirement of Zero Trust. Use ServiceNow IT Service Management and Enterprise Architecture to ensure full visibility of applications and digital services as well as accurate inventory and vulnerability management. Manage application lifecycles, including patching schedules and compliance monitoring, to minimize risks. Use ServiceNow Integrated Risk Management and DevOps to ensure there are strict DevOps, risk, and compliance processes in place for evaluating the risk associated with new applications in pre-production, whether or not these are third-party applications or ones developed in-house. Automate risk assessments and prioritize critical applications using FIPs 199. Secure on-premises operations and cloud environments with Security Operations monitoring tools and automated workflows for cloud resource management.

Data

A primary tenet of Zero Trust is protecting sensitive data. Use the Now Platform and Vault to centralize and secure information about the location and use of sensitive data for better management and tracking. Leverage APIs and service graph connectors to integrate data across Zero Trust tools, and to accurately associate data about people, devices, and agency resources. Manage access based on data type and regulation (e.g., HIPAA, GDPR, FISMA). Implement granular access controls and use tools such as ServiceNow Data Loss Prevention (DLP) and Privacy Management to not only protect data but quickly identify data exposure risks for rapid response.

DoD specific pillars

There are two pillars specific to the DoD Zero Trust strategy. The first pillar is Automation and Orchestration, which has AI as a central theme. Use AI/ML and ServiceNow Now Assist - available with a variety of products - to accelerate your ability to respond to queries, as well as triage, consolidate, and summarize information, or to recommend remediation actions to reduce response times. ServiceNow Security Operations and Integrated Risk Management capabilities included in the second pillar (Visibility and Analytics) enable you to gain better visibility to identify vulnerabilities including misconfigurations in the cloud and ensure appropriate infrastructure provisioning.

The ServiceNow advantage

ServiceNow's integrated platform and products can help you enable Zero Trust and break down the silos. With improved visibility, increased automation, and consistent governance across all pillars of the ZTA you can build resilience against evolving threats. Rely on a unified ServiceNow Zero Trust program to help you improve your security posture and mission assurance for your systems that are critical to national defense. Gain confidence in your compliance with Zero Trust guidelines and enhance decision making with a real-time view of operations (including third parties) and AI-driven insights. It's all available on a single scalable platform to meet your digital transformation goals.

Learn more at www.servicenow.com/risk



82%

of cybersecurity professionals are actively working on implementing Zero Trust

- Zero Trust: Sentiments of Cyber Security Professionals (Beyond Identity) 2023