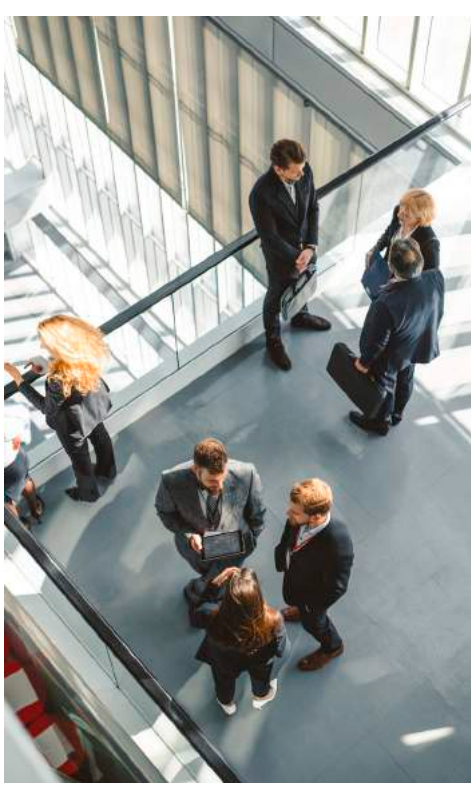
Making Zero Trust Work For You

Zero Trust is a security framework that operates on the tenant that no actor, system, network, or service operating outside or within the security perimeter is trusted. Anything and everything attempting to establish access must be verified. This is different from how we have previously secured our infrastructure, networks, and data which was to verify once at the perimeter. Zero Trust requires continual verification of each user, device, application, and transaction.

A transition to a Zero Trust Architecture (ZTA) is mandated by Executive Order 14028, improving the Nation's Cybersecurity. The steps to get to Zero Trust are detailed in OMB memos and department cyber guidance. But more than meeting a mandate, the transition to Zero Trust makes sense as a way to maintain a strong, secure cyber infrastructure while enabling digital modernization – both critical for the success of our nation.

Zero Trust is a maturity journey that is not achieved with one single technology. Rather, it is dependent on multiple, complex technologies working together to provide the validation of trust in a way that is seamless to end users. ServiceNow is positioned to play a role in several key areas that will help agencies comply with mandates and (more importantly) become more secure and efficient in their mission operations. A critical step is understanding all IT assets and being able to manage them.



Enabling the Zero Trust Journey with Discovery

Agencies must effectively catalog their digital assets and intellectual property in terms of potential risk and implement procedures to identify, manage, and monitor the users, devices, and applications accessing this data.

ServiceNow Discovery discovers your entire IT infrastructure, creating an accurate and up-to-date record in your ServiceNow CMDB. This provides a view of all IT infrastructure and services, spanning both multi-cloud and on-premises environments.

The Now Platform allows agencies to carry out critical inventory, certificate management, and audit tasks in an automated fashion to improve security posture and response in line with Zero Trust goals. This includes:

- **Discovery**—discovers physical and logical configuration items (CIs), such as servers, switches, routers, virtual machines, storage elements, databases, and applications as well as the relationships between these CIs.
- **Service Mapping**—builds on this discovered infrastructure data, creating end-to-end maps of organization's services. It identifies all of the CIs that support each service, along with their service-specific relationships.
- **Vulnerability Response**—comprehensive view of all vulnerabilities affecting a given asset or service as well as the current state of all vulnerabilities affecting the organization. Ensure focus on the most critical risks to respond faster and more efficiently across security and IT teams.

Modern Visibility and Coordination

To manage a Zero Trust Architecture, organizations need tools that enable visibility, application of analytics, as well as automation and orchestration. ServiceNow helps meet these needs in a variety of ways.

When connected to the Now Platform, security solutions and monitoring tools can be coordinated to work simultaneously to respond to events. They can activate automated cross-functional workflows to notify security officers, quarantine suspect systems, update vulnerable assets, and lock suspicious accounts, reducing business risk. The ServiceNow platform can also correlate threat intelligence feeds from multiple security tools. This connection allows for the mapping of threats, security incidents, and vulnerabilities for prioritization and risk scoring based on business impact.

- **Hardware Asset Management**—automate the lifecycle of tracking and managing hardware inventory details. Prescriptive workflows based on industry practices eliminate manual processes. Workflow asset lifecycle and business processes help create greater efficiency and better employee and customer experiences without relying on a host of point tools. Get a big picture view and prove where assets are in each lifecycle stage. Know when it's time to retire, return, or recycle assets and certify that they were wiped and disposed of properly.
- **Software Asset Management**—transform from reactive software asset management practices to a proactive culture of always being audit ready. Users can receive alerts for potential issues before they occur. IT can remediate non-compliance by streamlining software purchasing and revocation and take control of software spend and compliance at the source by leveraging the Service Catalog to automate the request and allocation processes. Finally, software asset managers can reclaim unused software and ensure it is uninstalled from an end user's device.
- **Remediation and Patch Management**—with discovery and software asset management being coordinated via ServiceNow, the automation of patch and remediation of vulnerabilities can be more automated and proactive.
- **IT Service Management (ITSM)**—consolidate tools, transform the way you deliver services, and improve customer experience. Automate workflows, gain real-time visibility, and improve IT productivity.

Portals built with ServiceNow provide administrators with a single pane of glass to manage the solutions and the data they provide. With this centralization, organizations can better track requests to identify patterns and also audit users to ensure policy compliance.

Supporting ICAM solutions

OMB guidance directs agencies to ensure that "Federal staff have enterprise-managed accounts, allowing them to access everything they need to do their job while remaining reliably protected." Identity, credential, and access management (ICAM) is designed to create a secure and trusted environment in which users can access authorized resources. ICAM also allows the agency to see who is on the network at any given time.

The ServiceNow platform provides a single architecture and data model with extensive third-party integration capabilities that can help organizations bridge organizational gaps, technology gaps, and processes. It can help administrators support their ICAM security solutions by providing a self-service portal with predefined "access request" workflows and approval capabilities that document each request. This creates an audit trail with detailed information about the request, such as why an employee needs to access a resource and how long access is required. ServiceNow brings together legacy and modern technologies to coordinate security efforts, verify user access, and mitigate vulnerabilities.

Getting to Zero Trust is a process that requires commitment and the right partners to bring all of the tools and processes together. To learn more about how ServiceNow supports your Zero Trust contact us at **federalmarketing@servicenow.com**