



SOLUTION BRIEF

Unified Protection: Zero Trust for Civilian Agencies

How the Trellix® Security Platform supports federal civilian Zero Trust efforts

Highlights

Native and Open Platform

Leverage current investments and provide increased value from their security architecture.

Continuous Monitoring

Trellix integrates with identity and access management (IAM) systems to verify behavior and authentication activities in real time.

Accelerated Implementation

Trellix combines insights from over 1,000 data sources into a unified console, eliminating blind spots for robust ZT implementation.

Capability to Meet DOD “Target” Requirements

Through integrations and partnerships within the Trellix Security Platform ecosystem, Trellix solutions satisfy ZT requirements.

Trellix Security Platform helps bring ZT to federal civilian agencies

Zero Trust (ZT) is a cybersecurity model based on the core principle of “Never trust, always verify.” It assumes that users and devices inside and outside an organization’s network have been breached and cannot be trusted. It means no user or device is trusted by default, even inside the organization’s network. Instead, all access to applications and data is granted on a least-privileged basis. Before being permitted to connect, continuously assess, authenticate, and authorize users and devices.

The Cybersecurity and Infrastructure Security Agency (CISA) produced a maturity model defining a path for federal civilian agencies to achieve successful Zero Trust outcomes. While not prescriptive, the maturity model provides guidance for federal civilian agencies to advance ZT maturity across each of the pillars by emphasizing automated analysis and action to track ZT progress.

One thing is clear: vendor partnerships and tight integrations are crucial to meet ZT’s intent. Organizations need a strategy that eliminates isolated systems to unify the ZT pillars. The same approach must enable automation, visibility, and intelligence sharing across all integrated capabilities in a hybrid, multicloud environment.

Trellix empowers federal civilian ZT initiatives through a holistic, integrated security ecosystem approach

The [Trellix Security Platform](#) delivers security incident detection and automated response capabilities for security infrastructure. Furthermore, the platform integrates threat intelligence and telemetry data from multiple sources with security analytics to contextualize and correlate security alerts.

The open Trellix Security Platform allows organizations to leverage current investments and provide increased value from their security architecture. Operationalization is key; Trellix has a long history of global deployment and performance at scale across many federal civilian environments and a proven record of success.

Our approach is straightforward:

1. Protect your most important asset—data. Mission resiliency is critical.
2. Embrace a multivendor approach through an open platform.
3. Prioritize and automate security operations workflows across all controls.
4. Stay at the forefront of ZT requirements through cutting-edge developments and partnerships.

Trellix Security Platform Integrations

User	Device	Application and Workload	Data	Network and Environment	Automation and Orchestration	Visibility and Analytics
1.1 User Inventory	2.1 Device Inventory	3.1 Application Inventory	4.1 Data Catalog Risk Mgmt.	5.1 Data Flow Mapping	6.1 Policy Decision Point (PDP) & Policy Orchestration	7.1 Log All Traffic (Network, Data, Apps, Users)
1.2 Conditional User Access	2.2 Device Detection & Compliance	3.2 Secure Software Development	4.2 DoD Enterprise Data Governance	5.2 Software Defined Network (SDN)	6.2 Critical Process Automation	7.2 Security Information & Event Management (SIEM)
1.3 Multi-Factor Authentication	2.3 Device Authentication with Real-Time Inspection	3.3 Software Risk Mgmt.	4.3 Data Labeling & Tagging	5.3 Macro Segmentation	6.3 Machine Learning	7.3 Common Security & Risk Analytics
1.4 Privileged Access Management	2.4 Remote Access	3.4 Resource Authorization & Integration	4.4 Data Monitoring & Sensing	5.4 Micro Segmentation	6.4 Artificial Intelligence	7.4 User & Entity Behavior Analytics
1.5 Identity Federation & User Credentialing	2.5 Partially & Fully Automated Asset, Vuln & Patch Mgmt.	3.5 Continuous Monitoring	4.5 Data Encryption & Rights Mgmt.		6.5 Security Orchestration, Automation & Response (SOAR)	7.5 Threat Intelligence Integration
1.6 Behavioral, Contextual, ID, and Biometrics	2.6 Unified Endpoint Mgmt. & Mobile Device Mgmt.		4.6 Data Loss Prevention (DLP)		6.6 API Standardization	7.6 Automated Dynamic Policies
1.7 Least Privileged Access	2.7 Endpoint & Extended Detection & Response (EDR/XDR)		4.7 Data Access Control		6.7 Security Operations Center (SOC) & Incident Response (IR)	
1.8 Continuous Authentication						
1.9 Integrated ICAM Platform						

Native Trellix Capability
Partner Integration
Service Partnerships (People & Processes)

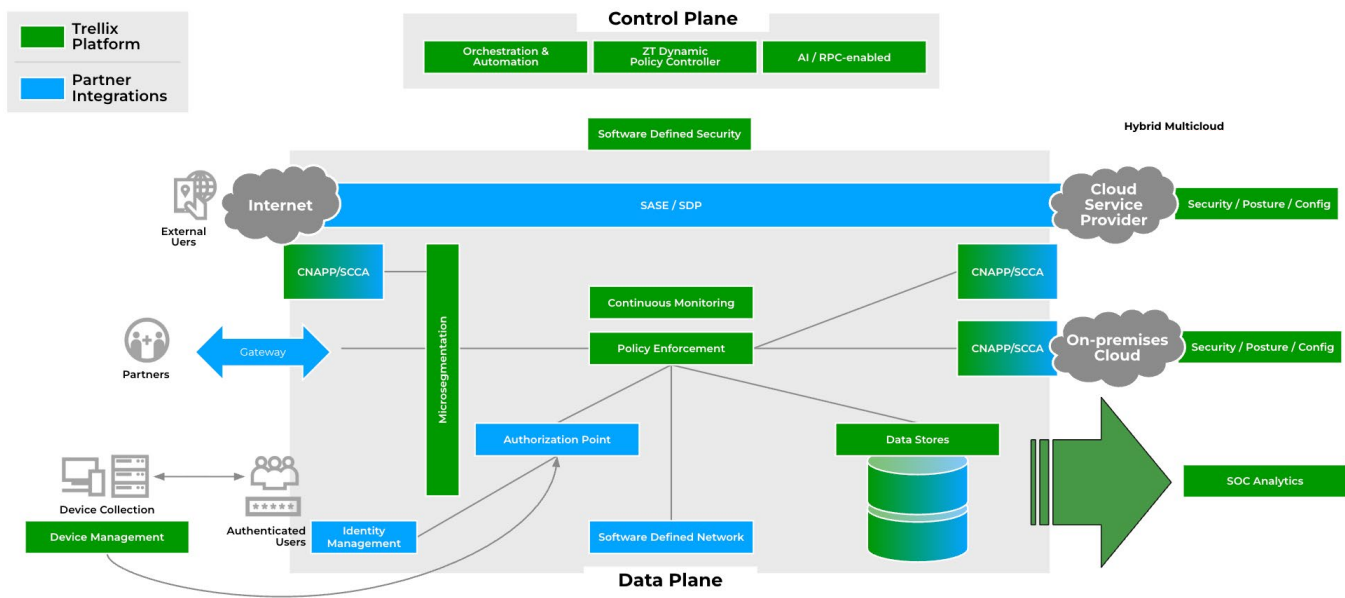
Accelerate detection, response, and investigation with the Trellix Security Platform

The integrated, AI-powered Trellix Security Platform with [Trellix Wise™](#) collects insights from over 1,000 data sources, speeding up the implementation of ZT initiatives. The platform simplifies the security environment through consolidated native controls, integrated identity and access management (IAM) providers, and a unified console that uncovers and eliminates blind spots, ensuring robust ZT implementation.

- Multivector, multivendor detections help prevent breaches and automate analysis, reducing mean time to detect (MTTD)
- Guided responses empower SOC teams for faster mean time to response (MTTR)
- Security operations playbooks improve mean time to investigate (MTTI)

No single vendor possesses all of the tools, skills, or capabilities for complete ZT implementation. Choosing the right partners and leveraging an ecosystem is vital. Trellix offers unmatched integrations across a broad partner ecosystem that work within your existing architecture to speed up time to value without requiring you to replace your current investments.

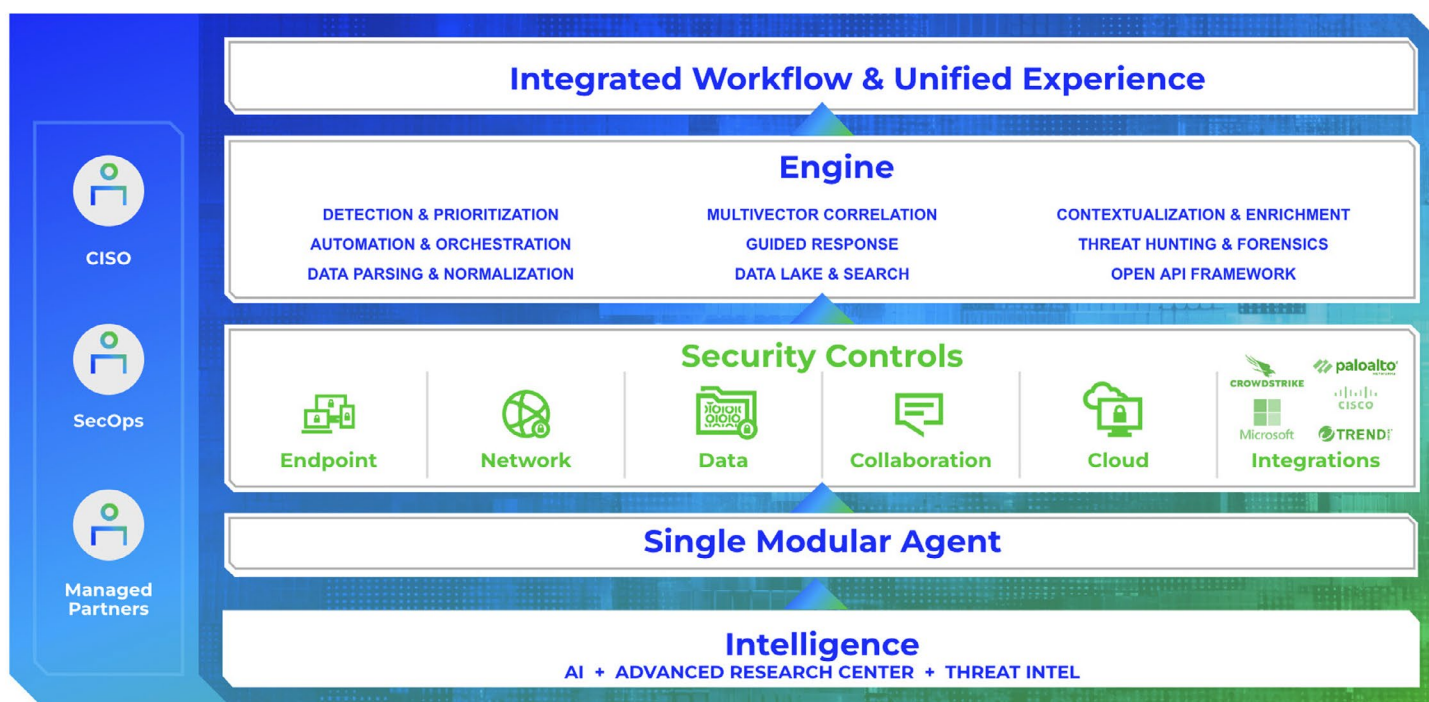
Trellix Zero Trust Architecture



While CISA is intentionally nonprescriptive, the Department of Defense (DOD) has taken a more prescriptive approach to guide DOD components to ZT outcomes. We've analyzed each DOD ZT activity requirement and pinpointed specific areas where we fulfill the criterion through our broad portfolio of solutions. For requirements that are better suited for other tools, Trellix integrates with vendors to deliver on those requirements as part of the Trellix Security Platform ecosystem. Our integrated (people and processes) partnerships help organizations reach DOD-defined "target" ZT requirements. This same work can be translated to other ZT frameworks being used within federal civilian agencies.

The Trellix Security Platform incorporates network detection and response (NDR) capabilities to monitor network traffic and detect anomalous activities, including lateral movement and network-based threats. This facilitates quick incident response and ensures network-based access controls adhere to ZT principles.

By incorporating the Trellix Security Platform into their ZT strategy, federal civilian organizations can establish a more robust and adaptive security posture that continuously verifies trust and mitigates threats across these critical areas of their digital environment.



References

[CISA Zero Trust Maturity Model](#)

[DOD Reference Architecture](#)

A ZT strategy is a must for robust security hygiene. Implementing a ZT strategy requires visibility into endpoint activity, email messages, network traffic, cloud security posture, data security, and many other sources. Only the AI-powered Trellix Security Platform offers unparalleled visibility across native security controls and third-party integrations.

To learn more about Trellix's approach to Zero Trust, visit trellix.com.