Trellix

SOLUTION BRIEF

Unified Protection: Trellix XDR Supports Federal Civilian Zero Trust Efforts

Highlights

- **Native and Open XDR 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.
- **Meet 100% of DoD "target" requirements**
  Through integrations and partnerships within the Trellix XDR ecosystem, our solutions reach all ZT requirements.

Trellix XDR 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 civilian federal 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 Zero Trust 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, poly-cloud environment.

Trellix empowers Federal Civilian ZT initiatives through a holistic, integrated security ecosystem approach.

Extended Detection and Response (XDR) is the technology to facilitate this vision. The Trellix XDR Platform delivers security incident detection and automated response capabilities for security infrastructure. Furthermore, XDR integrates threat intelligence and telemetry data from multiple sources with security analytics to contextualize and correlate security alerts. Trellix believes XDR should be **native** and **open**, allowing 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.

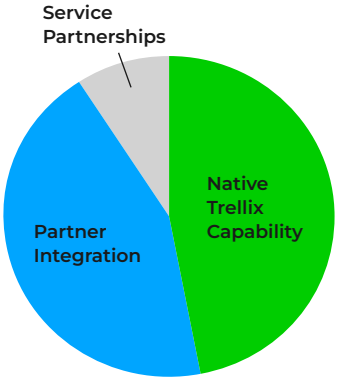
Our approach is straightforward:

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

XDR Integrations

User	Device	Application and Workload	Data	Network and Enviornment	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)



100% Coverage DoD Zero Trust Activities

Trellix speeds up the implementation of Zero Trust initiatives using our integrated, AI-powered XDR platform that collects insights from over 1,000 data sources. 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 Zero Trust implementation.

The AI-powered Trellix XDR Platform accelerates detection, response, and investigation times. Here's how:

- Multi-vector, multi-vendor detections to prevent breaches and automated analysis reduce 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)

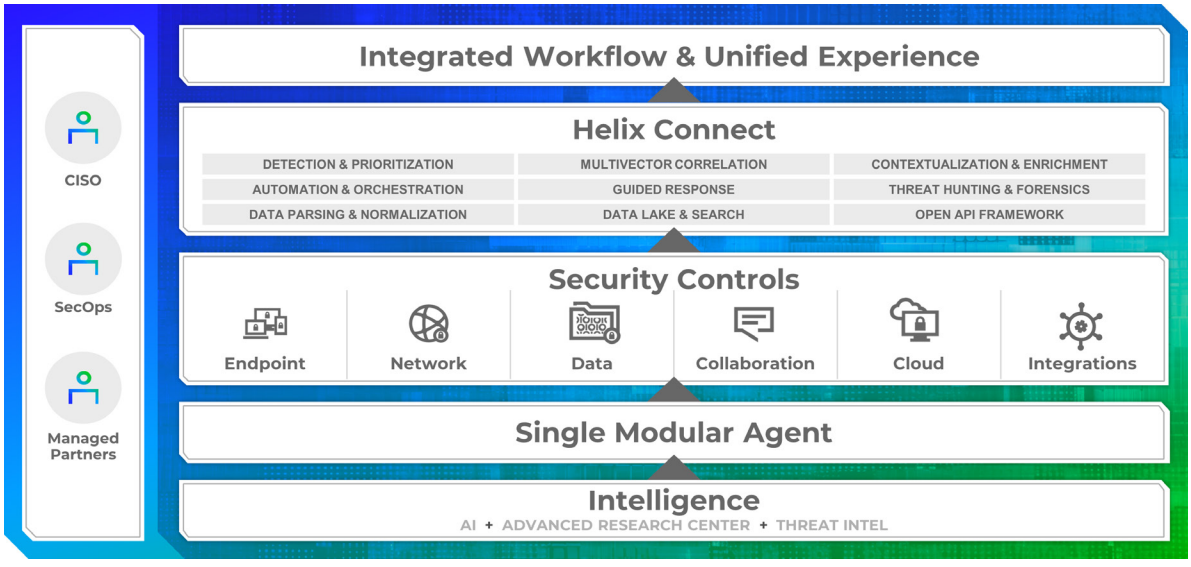
References

- CISA Zero Trust Maturity Model
- DoD Reference Architecture

No single vendor possesses all of the tools, skills, or capabilities for complete Zero Trust 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 replacing your current investments.

While CISA is intentionally non-prescriptive, the Department of Defense (DoD) has taken a more prescriptive approach to guide DoD components to Zero Trust 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 our XDR ecosystem. Our integrated (people and processes) partnerships help organizations reach 100% of the DoD-defined "target" ZT requirements. This same work can be translated to other Zero Trust frameworks being used within Federal Civilian Agencies.

XDR incorporates Network Detection and Response (NDR) capabilities to monitor network traffic and detect anomalous activities, including lateral movement and network-based threats, facilitating quick incident response and ensuring network-based access controls adhere to Zero Trust principles. By incorporating the Trellix XDR platform into your Zero Trust 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.



Having a Zero Trust Strategy is a must for robust security hygiene. Implementing a Zero Trust Strategy requires visibility into endpoint activity, email messages, network traffic, cloud security posture, data security, and many other sources. Only Trellix offers an AI-powered XDR platform with unparalleled visibility across native security controls and third-party integrations.