Trellix

DATA SHEET

Trellix® GovCloud for Continuous Diagnostic and Mitigation (CDM)

Benefits

- **Reclaim Budget: Typically 50% Savings**
  Trellix CDM delivers superior value at ~50% lower cost than competitors, freeing up funds for new initiatives.
- **Automated Triage, Reduce MTTR**
  Automatically triage, scope, and prioritize alerts with remediation guidance to reduce mean time to respond (MTTR).
- **End Silos Across Teams & Tech**
  Trellix Helix Connect integrates data and correlates threat events, giving teams the complete story of an attack so they can collaborate on remediation.
- **Drive ROI & Operational Efficiency**
  Save 8+ hours of analyst work per 100 alerts using Trellix Wise to help maximize your current security investments..

Spend less, secure more, and move faster

Federal agencies struggle to maintain a strong cybersecurity posture as evolving threats, workforce shortages, and budget constraints outpace the capabilities of today's CDM tools.

Trellix GovCloud for CDM offers a comprehensive, AI-driven alternative designed to alleviate these pressures. By integrating critical security functions, Trellix enables agencies to reduce costs, proactively detect and prevent advanced threats, improve visibility, and streamline compliance within a FedRAMP-certified framework.

Trellix Cuts Costs for Civilian Agencies

50%
Cost Savings

70%
Reduction in False Positives

5x
SOC Productivity Gain

Trellix Solutions for CDM

Trellix Endpoint Security

Trellix Endpoint Security delivers comprehensive and unified protection for hybrid networks, meeting critical CDM requirements. Trellix Endpoint Detection and Response (EDR) enhances threat detection by leveraging AI and behavioral mapping aligned to the MITRE ATT&CK® framework, enabling automated alert prioritization and simplified investigations. It uses rapid one-click response capabilities to address threats quickly.

Benefits (cont.)

- **Accelerate Zero Trust Initiatives**
  Trellix is FedRAMP High certified, supporting Zero Trust with unified data visibility and analytics per EO 14028.
- **Protect Complex Environments**
  Deploy and manage across on-prem, cloud, hybrid, and air-gapped environments.
- **Reduce Noise, Accelerate Investigations**
  Cut false positives by 50% to 70% and accelerate investigations with AI-guided workflows.

Complementing this, Trellix Endpoint Forensics (HX) offers a modular approach to threat protection, detection, investigation, and response. HX employs multiple engines, including machine learning and behavioral analysis, alongside real-time IoC-based EDR and rapid forensic data collection across thousands of endpoints.

With a proven track record of safeguarding over 3 million federal endpoints across various agencies, including its integral role in protecting 600,000 Civilian Federal Endpoints and serving as a key component for DoD Cyber Protection Teams, Trellix demonstrates its capability to meet the stringent security demands of the U.S. government.

Trellix Helix Connect

Trellix Helix Connect offers a unified view of threats by correlating data across tools. Rather than pivoting across multiple consoles to see the complete story of a threat, security teams can see a timeline of activity, create cases, assign actions, and collaborate across teams.

Introducing Trellix Wise™ + Helix Connect*

Helix Connect uses Trellix Wise, Trellix's AI capability built on over a decade of AI modeling and 25 years in threat intelligence, analytics, and machine learning. Trellix Wise's capabilities relieve alert fatigue and surface stealthy threats. It leverages GenAI-powered investigations to increase efficacy and coverage while lowering the cost and skill set required to stop these attacks. By making decisions that analysts would make while scaling capability far beyond what analysts alone can achieve, Trellix Wise provides a trustworthy path to automation.

With Trellix Wise, Helix Connect automatically investigates, triages, and prioritizes alerts with GenAI-enriched context that assists in addressing talent gaps. Its built-in automation and analytics correlate data for proactive threat detection and response, significantly improving MTTD/MTTR. Helix Connect provides a consolidated threat and risk reporting interface, utilizing a complete view of the story through integration and correlation. Trellix supports a shared services model that eliminates silos, enhances visibility, and improves collaboration across different entities.

*Please note that some features of Trellix Wise are not available in all locales or regions. Please validate with your Trellix account team if there are any restrictions based on your specific region and use case.

Trellix Thrive Elite for Public Sector

Delivering advanced services and expert support, Trellix Thrive Elite for Public Sector helps federal agencies strengthen cybersecurity resilience, meet compliance mandates, and respond rapidly to mission-critical threats. Designed specifically for U.S. government environments, it

includes elevated support service level objectives (SLOs), priority routing for Severity 1 cases, and exclusive access to U.S. citizen-based support teams.

Key Capabilities

Threat protection, detection, and response

Empower SOCs to connect the dots and achieve unparalleled threat investigation and response using AI-driven correlation powered by rich endpoint data from Trellix EDR and Endpoint Forensics.

Single hybrid solution: on-prem, air-gapped, and cloud

As a centralized security management platform, Trellix GovCloud for CDM empowers you to orchestrate and manage all of your endpoints for comprehensive protection across your on-prem and cloud resources.

AI to up-skill teams, improve threat prevention

Trellix Wise investigates 100% of alerts, automating triage and remediation. Its built-in decision-making, guidance, and conversational AI facilitate learning and on-the-job threat hunting for analysts at every experience level.

Dedicated on-site engineer

Access Trellix experts to optimize the deployment, configuration, and operation of Trellix solutions, ensuring maximum ROI and alignment with best practices.

The Trellix CDM solution offers public sector and government agencies a robust and integrated platform to effectively manage cybersecurity risks, reduce operational costs, and improve overall security posture. Trellix enables agencies to confidently navigate the evolving threat landscape and fulfill their critical missions by combining advanced threat protection, AI-driven automation, and expert services.

For more information, visit trellix.com.