CLAROTY

E-BOOK

The Claroty Platform: Enhancing Federal Efficiency Through Robust OT Security

Table of Contents

I. Executive Summary

Federal agencies are under increasing pressure to enhance operational technology (OT) security while simultaneously adhering to strict fiscal and efficiency mandates. The core challenge lies in safeguarding legacy OT infrastructure and a rapidly expanding array of cyber-physical assets, all while driving down operational costs. This complex landscape necessitates a strategic shift in federal OT cybersecurity, moving from a compliance-centric approach to one that prioritizes measurable outcomes.

Claroty, a recognized leader in cyber-physical systems (CPS) protection encompassing OT, IoT, IoMT, and Facilities Related Control Systems/ Building Management Systems (FRCS/BMS), offers a powerful platform uniquely positioned to help federal agencies achieve these critical efficiency initiatives. By providing a unified, comprehensive view of all connected cyber-physical assets and their vulnerabilities—along with impact-centric remediation and threat mitigation—the Claroty Platform directly addresses inefficiencies from fragmented technology and labor-intensive processes, while delivering a clear path to **quantifiable cost savings** and **enhanced operational resilience.**

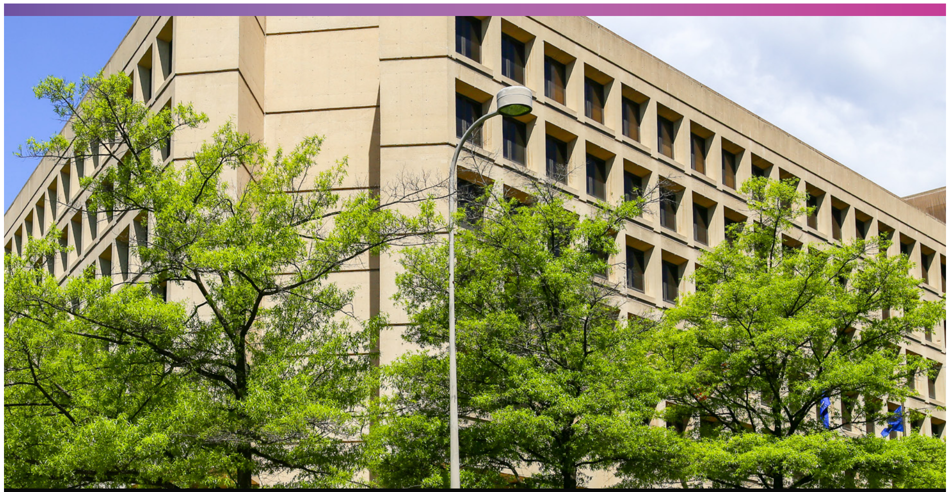
II. Achieving Cost Efficiencies While Improving OT Security

As federal agencies modernize their infrastructure, they are poised for positive transformation in OT and cyber-physical security. A growing focus on achieving measurable cost efficiencies, alongside a shift from compliance-based metrics to outcome-based performance metrics that evaluate cybersecurity resilience, signals a broader commitment to both improving security and maximizing the return on cybersecurity investments.

Selecting the right OT security vendor can accelerate this shift in several key areas:

- Rapid, ongoing asset discovery and impact-centric exposure remediation for most critical exposures
- Automation of manual tasks and inter-tool optimization
- Agility that supports scarce OT expertise, where and when needed
- Consolidation and elimination of redundant tools

The Claroty Platform delivers a clear path to quantifiable cost savings and enhanced operational resilience in these four key areas. Automating asset discovery, vulnerability management, and threat detection across diverse OT and CPS environments, it significantly reduces the manual effort and specialized expertise traditionally required. This not only streamlines operations but also proactively mitigates the escalating threat landscape, preventing costly disruptions and ensuring the continuity of essential government services.

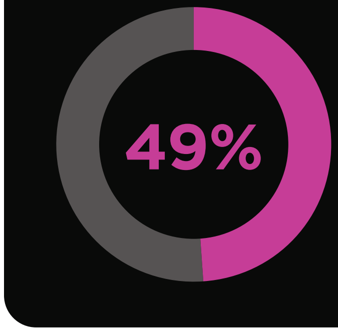


Selecting the right OT security vendor can accelerate this shift in several key areas:

- Rapid, ongoing asset discovery and impact-centric exposure remediation for most critical exposures
- Automation of manual tasks and inter-tool optimization
- Agility that supports scarce OT expertise, where and when needed
- Consolidation and elimination of redundant tools

A. Rapid and ongoing asset discovery and impact-centric exposure remediation

In the private sector, CPS breaches can carry staggering financial consequences, with 49% of attacked organizations experiencing 12+ hours of downtime per CPS breach, and industrial manufacturers facing an estimated $50 billion in annual downtime costs[1]. For the federal government, the impact and cost of disruptions to missions and operations, such as those involving navigation, fueling, and even weapons, can be difficult to quantify but can be devastating.



49% of attacked organizations experienced 12+ hours of downtime per CPS breach

This urgency is further underscored by the escalating cyber threat posed by nation-states such as China, Russia, and Iran. The U.S. Department of Homeland Security has deemed these adversaries the "most pressing" threat and warned of their explicit intent to carry out disruptive and destructive cyber-physical attacks.[2] In this context, proactively identifying and securing exposed OT assets across all critical functions is not just prudent—it's essential to national resilience.

Claroty: delivers swift asset discovery and impact-centric exposure management through several key capabilities designed to meet federal agency needs:

- Enhance visibility for faster identification and remediation of gaps and exposures.
- Increase automation to improve the speed of achieving security outcomes.

One of Claroty's flexible asset discovery methods, Claroty Edge, is a lightweight executable that enables rapid asset identification in minutes without requiring switch upgrades or new infrastructure. Leveraging insights from Edge, the platform applies an impact-centric approach to risk reduction, allowing agencies to prioritize remediation based on contextual risk. This approach considers the unique risk and potential impact of a compromised asset within the specific OT environment and calculates the most likely attack scenarios.

Passive Monitorning

Continuous Monitoring of network traffic to identify asset profiles

Safe Queries

Targeted discovery of assets in their native protocol

Claroty Edge

Speedy, host-based asset profiling through localized queries

Project File Analysis

Regular ingestion of offline configuration files for asset enrichment

Integrations

Enriching visibility without hardware or configuration changes

[1] Claroty, "The Global State of CPS Security 2024: Business Impact of Disruptions"

[2] Homeland Threat Assessment 2025, https://www.dhs.gov/sites/default/files/2024-10/24_0930_ia_24-320-ia-publication-2025-hta-final-30sep24-508.pdf

The platform continuously compares each discovered asset against insecure protocols, configurations, substandard security practices, and the latest CVE data and automates vulnerability “priority group assignments” to escalate the most critical assets with the most critical vulnerabilities for prioritized remediation. This allows a view of how the overall risk of an environment is affected by the processes involved in a device’s use—such as production lines, building floors, and hospital wings—and prioritizes risk reduction efforts based on potential impact to government outcomes. This also bridges the gap between OT security and other CPS personnel and functional teams.

Results: Claroty’s discovery capabilities and impact-centric approach to exposure management deliver:

- **Reduced MTTR:** Real-time asset visibility—including location, status, utilization, and network communication—enables faster failure detection, minimizes downtime, and improves repair planning and resource allocation.
- **Optimized labor and travel costs:** Automated asset discovery eliminates the need for in-person, onsite inspections, accelerating exposure assessment and remediation while increasing operational agility.
- **Smarter resource allocation:** Context-aware exposure prioritization ensures cybersecurity efforts focus on the assets with the greatest potential operational impact.
- **Cost Avoidance:** By preventing major disruptions and avoiding unnecessary remediation of low-risk assets, agencies reduce both direct costs and operational inefficiencies.
- **Increased ROI on Security Investments:** Streamlined, targeted security operations translate into higher value from existing tools and teams.
- **Accelerated Exposure Assessment and Remediation:** Automated identification and prioritization of vulnerabilities allows agencies to rapidly evaluate and mitigate risks, minimizing the attack surface and reducing remediation timelines.
- **Greater Agency Agility:** Support for portable and lightweight deployment options such as flyaway kits enables rapid, on-demand asset discovery and risk assessment in disconnected or remote mission environments.
- **Improved Employee Safety:** Personnel can manage assets and risks remotely, avoiding the need to manually canvass potentially hazardous or restricted environments.

B. Automation of manual tasks and inter-tool optimization

The disproportionate allocation of federal cybersecurity budgets to labor presents a significant area for efficiency improvement. Automation of manual tasks, particularly leveraging labor that is better spent on more strategic objectives or time-sensitive tasks, can help improve efficiency, improve the speed and accuracy of threat detection and response, and provide continuous, in-depth visibility into complex CPS environments.

Claroty: The Claroty Platform automates both routine and complex security tasks to drive efficiency across organizations. Key benefits include:

- **Long-term operational cost reduction:** Automation minimizes manual effort and reduces the need for large Security Operations Centers (SOC) teams.
- **Resource optimization:** Frees up skilled personnel to focus on higher-value, strategic initiatives.
- **Productivity maximization:** Streamlines workflows across tools and teams to accelerate security operations and response times.

The platform automates tasks across four primary areas:

- Automated asset discovery
- Automated generation of network security policies
- Artificial Intelligence (AI)-based solutions in threat detection
- Automated remediation and risk-based response mechanisms

Automated asset discovery and inventory: The platform eliminates manual inventorying and streamlines asset discovery through multiple automated discovery methods. Passive monitoring continuously analyzes network traffic to automate the discovery and profiling of cyber-physical assets, while also powering real-time threat detection and other key CPS security capabilities.

For environments where passive methods aren't feasible, Claroty Edge offers a non-passive alternative, safely discovering assets via localized queries—no hardware deployment or traffic learning cycles required. This reduces operational friction, accelerates deployment, and lowers costs for OT teams.

Finally, the platform integrates seamlessly with existing IT systems—including CMDBs, EDR platforms, and other security tools—to automatically ingest and correlate additional asset data. This enriches the asset inventory with deeper context and creates a centralized, accurate view of both IT and OT environments. By leveraging automation end-to-end, the platform reduces reliance on manual data collection and ensures up-to-date asset visibility at scale.

Automated vulnerability and exposure management and prioritization: The platform continuously analyzes discovered assets for insecure protocols, misconfigurations, substandard security practices, and known vulnerabilities using the latest CVE data. It then automates the prioritization of remediation efforts based on the unique risk each issue poses to the specific OT environment. In addition to identifying and prioritizing vulnerabilities, the platform assesses potential attack paths and calculates the most likely scenarios, delivering actionable mitigation recommendations. Integrations with third-party tools like ServiceNow further streamline vulnerability management by automating data exchange and enabling a unified view of IT and OT risks.

Automated network protection and segmentation: The Claroty Platform automatically maps cyber-physical system (CPS) networks and groups assets into logical "virtual zones" based on normal communication patterns, establishing a behavioral baseline. Using this baseline, it automatically generates granular segmentation policy recommendations to minimize lateral movement and contain threats. Through integrations with next-generation firewalls, these policies can be automatically enforced, limiting or blocking communication between zones or specific assets when anomalous activity is detected. This automation reduces reliance on manual network monitoring and enables proactive, scalable network protection.

Automated threat detection and alerting: Building on its behavioral baselining and anomaly detection, the Claroty Platform automatically identifies deviations from normal operations, triggering real-time alerts for potential unknown threats, including zero-day attacks. For known threats, it uses Indicators of Compromise (IoCs), signatures, and proprietary intelligence from Claroty's Team82 research team. The platform also monitors operational behavior down to the code level, detecting subtle changes in asset configurations or activity that could indicate an attack or operational issue.

To reduce alert fatigue and accelerate response, the platform automatically assigns risk scores based on contextual factors and correlates related events into a single, prioritized alert, enabling automated root-cause analysis. Integrations with SIEM and SOAR tools ensure seamless delivery of threat data to existing SOC workflows, supporting automated response actions. By continuously monitoring the OT environment for early signs of ransomware, equipment failure, insider threats, or misconfigurations, the Claroty Platform helps minimize downtime and ensure operational continuity.

Results: Claroty's automation and integration capabilities reduce alert fatigue and accelerate prioritization, leading to measurable improvements across key security and operational metrics:

- **Reduced MTTR:** Granular network segmentation limits lateral movement and isolates issues, simplifying detection, monitoring, and repair for faster resolution.
- **Faster MTTD:** Automated workflows and cross-functional integrations enable quicker visibility and response, accelerating MTTD.
- **Resource optimization:** By reducing reliance on manual analysis, the platform frees up security personnel to focus on higher-value tasks.
- **Reduced attack surface:** Continuous monitoring, automated policy enforcement, and proactive risk mitigation collectively reduce the overall threat landscape and attack surface.

C. Agility that supports scarce OT expertise

OT or CPS security solutions that provide agility—with flexibility in deployment options—can provide faster time to value, swifter deployment, rapid adaptation to changing needs in the field, optimized resourcing, and data-driven scaling with a validate-then-accelerate approach to investment. In essence, agility in CPS security solutions moves the government away from rigid, long-term planning and towards a more responsive, adaptable, and value-driven approach. This directly contributes to cost efficiency by reducing waste, accelerating the realization of benefits, optimizing resource use, and effectively managing risks inherent in complex government initiatives.

Claroty: The Claroty Platform's deployment models include on-premise, portable, and SaaS-powered solutions without compromising on platform value. An on-premises solution provides an option for air-gapped, restricted or specialized scenarios, while portable deployment provides swift, on-the-fly deployments for assessments, attack investigations, and threat hunting that can be used through a choice of TSA-approved hardware from Claroty partners. SaaS-powered solutions provide a greater level of flexibility where the network environment has stable, secure internet connectivity and reasonable bandwidth.

Results: Claroty's flexible deployment model helps agencies overcome OT talent shortages and adapt quickly to evolving conditions by enabling:

- **Faster time to value:** Rapid deployment empowers agencies to deploy OT security expertise on demand for a breadth of use cases. From regular assessments to threat hunting to attack investigations, OT security expertise can be flown on-site when needed, while still providing critical insights and remediation.
- **Rapid adaptation to changing needs:** As security needs and priorities shift rapidly due to policy changes, emergencies, or evolving realities, agencies can quickly pivot and adjust their investments while adapting to change, rather than being locked into outdated plans.
- **Improved resource allocation:** By deploying OT expertise only when and where it's needed, agencies maximize impact and adapt to changing security realities and workloads while minimizing overhead—supporting tasks like asset discovery, vulnerability assessments, and impact-driven remediation more cost-effectively.
- **De-risked investment decisions:** By focusing on small, incremental deployments where feasible, particularly in rapidly changing conditions, agencies can gauge viability, identify potential risks and technical challenges, all while making longer-term investment decisions, such as gradual modernization, and minimizing delays in time-to-value or even the chance of project failure.

D. Consolidation and elimination of redundant tools

The proliferation of disparate security tools, known as "tool sprawl," has inflated costs, and created operational inefficiencies, leading to Security Operations Center personnel burden and reduced visibility. Related to tool sprawl, compliance-focused efforts have sometimes unintentionally led to compliance-focused purchases. Federal agencies have historically spent approximately 80% of their security budgets on labor and support, double that of the private sector[3]. Only about 20% has been invested in technology, meaning $1 on technology for every $4 on labor[4]. This imbalance highlights an opportunity for technology to streamline and improve security, including that of OT.

The federal government's move towards integrated, platform-based solutions over siloed products will lead to greater cost efficiency, improved resource utilization, and enhanced security in the OT domain. The Department of Defense's (DoD) emphasis on software modernization and autonomous systems will further improve agility and enable rapid deployment of advanced capabilities.

Claroty: The Claroty Platform drives cost efficiency by replacing multiple point solutions with a single, integrated platform. It secures a broad range of legacy OT and other CPS assets—including FRCS/BMS, modern IoT, IoMT, and IoLT systems—and also provides a purpose-built remote access solution designed specifically for CPS environments. By eliminating redundant tools, optimizing communication between functions, and simplifying the security stack, agencies can reduce licensing fees, maintenance costs, and overhead associated with managing disparate systems while improving efficiency and overall security.

The Claroty Platform also enables compliance across various federal mandates and guidelines, providing a comprehensive solution that covers the broadest set of mandates in one, from Binding Operational Directives (BODs) to executive orders and frameworks. This inherent optimization reduces tool sprawl caused by compliance, while streamlining the satisfaction of compliance objectives.

Additionally, Claroty's Technology Alliances Program (CTAP) enhances interoperability by integrating seamlessly with a wide range of security and workflow tools. This optimized coordination across IT and OT systems enables agencies to streamline operations, improve end-to-end orchestration, and maximize the value of their cybersecurity investments for stronger, more efficient and effective protection.

Results:

- **Significant cost savings:** With reduced licensing fees, maintenance costs, SOC labor burden and overhead, a unified platform approach yields considerably reduced costs and improved TCO.
- **Reduced Mean Time to Detect (MTTD) and Mean Time to Respond (MTTR):** The seamless integration with existing IT security operations and existing agency tools directly helps agencies achieve desired outcome-based metrics.
- **Streamlined operational efficiency:** The unified platform's workflow automation supports greater efficiency, increased productivity, improved visibility, and therefore greater security efficacy with compliance satisfaction.

[3] Federal IT modernization needs strategy and more money, Information Technology and Innovation Foundation (ITIF), https://itif.org/publications/2022/05/31/federal-it-modernization-needs-strategy-and-more-money/

[4] Driving efficiency while improving federal agencies' cybersecurity postures - Nextgov/FCW, accessed June 9, 2025, https://www.nextgov.com/ideas/2025/04/driving-efficiency-while-improving-federal-agencies-cybersecurity-postures/404760/

III. Closing: Maximizing Mission Impact Through Quantifiable Cost Savings and Efficiency Gains in Federal CPS/OT Environments

The Claroty Platform addresses the unique and complex challenges in federal OT and broader CPS environments, translating directly into tangible efficiency gains and significant cost savings. The platform's ability to deliver quantifiable cost savings through Total Cost of Ownership (TCO) optimization, mitigation of financial impacts from cyber incidents, and efficiency gains through automation makes it not just a cybersecurity tool, but a critical enabler of operational efficiency and financial prudence, demonstrating how advanced technology can directly contribute to fiscal responsibility.

By implementing The Claroty Platform, federal agencies can move beyond basic compliance, achieving a higher level of security maturity that directly translates into operational optimization and fiscal responsibility. The platform's ability to deliver measurable outcomes in asset visibility, attack surface reduction, threat detection, and operational uptime provides a clear path to quantifiable cost savings and enhanced operational resilience. With quantifiable Return on Investment (ROI), platform consolidation capabilities, and direct contribution to outcome-based security, Claroty can empower the US federal government to not only meet its cost savings objectives but also to build a more secure, efficient, and resilient mission-critical infrastructure for the future.

The Claroty Platform drives tangible efficiency gains and significant cost savings that directly translates into operational optimization and fiscal responsibility with:

- Improved MTTD
- Improved MTTR
- Increased security operational efficiency
- Maximized return on security investments
- Significant cost savings
- Improved resource allocation
- Faster time-to-value
- Reduced threats and overall attack surface

CLAROTY

About Claroty

Claroty empowers organizations to secure automation, control, and other cyber-physical systems across industrial, healthcare, commercial, and public sector environments: i.e. the Extended Internet of Things (XIoT). The company's unified platform integrates with customers' existing infrastructure to provide comprehensive controls for visibility, risk and vulnerability management, threat detection, and secure remote access. Backed by the leading investment firms and industrial automation vendors, Claroty is deployed at thousands of sites globally. The company is headquartered in New York City with U.S. federal headquarters in Leesburg, VA. To learn more, visit clarotygov.us.