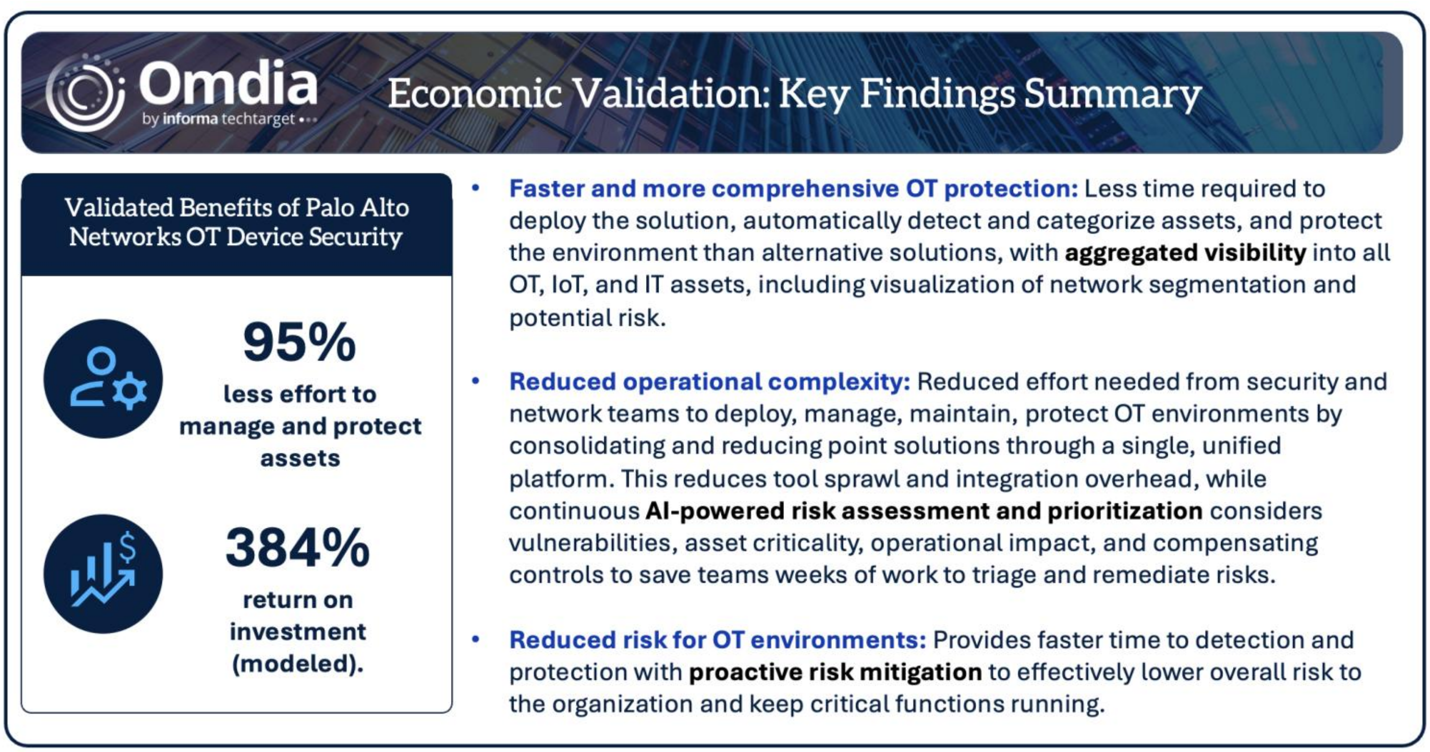
Analyzing the Economic Benefits of Palo Alto Networks OT Device Security

Lowering Risk for OT Environments and Providing a Return on Investment (ROI) of 384% With Up to 95% Lower Complexity Than Alternative OT Security Solutions

By Aviv Kaufmann, Practice Director and Principal Validation Analyst
Omdia

JANUARY 2026

Contents



Omdia
by informa techtarget
Economic Validation: Key Findings Summary
Validated Benefits of Palo Alto Networks OT Device Security
95%
less effort to manage and protect assets
384%
return on investment (modeled).
Faster and more comprehensive OT protection: Less time required to deploy the solution, automatically detect and categorize assets, and protect the environment than alternative solutions, with aggregated visibility into all OT, IoT, and IT assets, including visualization of network segmentation and potential risk.
Reduced operational complexity: Reduced effort needed from security and network teams to deploy, manage, maintain, protect OT environments by consolidating and reducing point solutions through a single, unified platform. This reduces tool sprawl and integration overhead, while continuous AI-powered risk assessment and prioritization considers vulnerabilities, asset criticality, operational impact, and compensating controls to save teams weeks of work to triage and remediate risks.
Reduced risk for OT environments: Provides faster time to detection and protection with proactive risk mitigation to effectively lower overall risk to the organization and keep critical functions running.

Introduction

This Economic Validation from Omdia focused on the benefits organizations can expect from activating the AI-powered OT Device Security SaaS subscription on their next-generation firewalls (NGFWs) from Palo Alto Networks or another vendor to better protect operational technology (OT) environments.

Challenges

Industrial environments are modernizing to better integrate their OT with their traditional informational technology (IT) networks and systems. Connecting data-driven intelligence across the business helps to optimize processes, reduce costs, and maximize operational efficiency. But legacy OT asset devices often were not designed to be converged with modern IT networks and practices. Research from Enterprise Strategy Group (now Omdia), shown in Figure 1, reveals that endpoint management and security tools routinely discover risky device vulnerabilities such as misconfigurations, a lack of patching, and open access, among others.[1]

Figure 1. Top Issues Uncovered by Endpoint Management and Security Monitoring Measures

Source: Omdia

[1] Source: Enterprise Strategy Group (now Omdia) Research Report, *The Growing Role of AI in Endpoint Management and Security Convergence*, June 2025.

OT assets are usually very susceptible to attack, as there is often no security built into the asset, poor visibility into its functioning, and unencrypted traffic. Security is paramount for the core critical infrastructure that supports manufacturing and industrial operations. Impacted operations can pose a physical threat to workers, impact revenue, cause product defects, or impact critical services to customers. Yet as they modernize, industrial and manufacturing organizations have seen significant growth in the number of OT assets that require internal and/or external connectivity to the corporate network and internet to keep critical infrastructure running, optimize efficiency, and provide insight and intelligence to the business. This brings with it several challenges:

- **Fragmented visibility into OT assets:** As the variety and quantity of OT and Industrial Internet of Things (IIoT) assets increases, pressure is placed on IT organizations and security functions to find, identify, manage, update, and secure these critical assets that, from their perspective, simply "appear and disappear" on the network whether their presence is intended or not. It is difficult to maintain a comprehensive inventory of assets and understand what a device is, what function it is serving, how it should behave, and how to best protect it. This results in an incomplete picture and blind spots across OT and IT networks.
- **Ineffective risk assessment:** Most tools used by OT organizations rely on accurate identification of devices and simple vulnerability scoring to assess and prioritize risk. But there is much more that needs to be taken into consideration such as context into the real-world function and the criticality of a device to ongoing operational processes. As such, compensating controls must be considered, as well as vendor-specific guidance and organizational priorities. Without a complete understanding of these things, risk assessments are incomplete and could result in disruption.
- **Limited options for remediation:** OT systems are difficult to patch because critical device downtime can mean lost revenue or even result in a dangerous condition, and in many cases, patches are not even available, regardless of patching complexity. Remediating issues and patching often require vendor intervention and benefit from careful planning and risk-based compensating controls that can help ensure availability and security as issues are remediated (especially for unpatchable and difficult to patch systems (as an interim solution where vendor support is lacking).
- **Inefficient processes:** On-site OT teams and corporate IT, security, and network teams are often siloed and use the tools and workflows of their choice. Many times, legacy processes have evolved that are manual and spreadsheet-driven rather than modern, unified, automated, and orchestrated. This results in poor enterprise-wide visibility and increases both time to remediate and associated risk.

Modern OT environments need a solution that provides effective visibility into OT assets. They need a solution that helps them better identify and categorize the multitude of unique assets that are on their industrial networks, quickly assess and comprehensively prioritize remediation of threats and vulnerabilities in critical environments, and create and automate comprehensive zero-trust policies to protect these assets and the network against known and unknown threats.

The Solution: Palo Alto OT Device Security

Palo Alto Networks OT Device Security is a comprehensive cybersecurity solution specifically designed to protect industrial OT environments from cyberthreats. The cloud-delivered, AI-powered platform provides complete visibility and security for manufacturing facilities, power plants, and other industrial operations by identifying and protecting all connected devices, including control systems, sensors, and machinery. The solution uses machine learning to automatically discover and profile industrial equipment, intelligently analyze and prioritize risk (including considering context and compensating controls), and create and enforce comprehensive security policies to prevent cyberattacks that could disrupt critical operations or cause costly downtime.

- **Aggregated device visibility:** Automatically creates a real-time, holistic inventory enriched with identity, posture, and behavioral attributes for every connected asset, including all IT, IoT, and OT assets and protocols in a facility. A combination of over 2,000+ attributes can be learned from network traffic and bi-directional integrations with CMDBs and other asset management tools and then defined for each asset, including vendor, model, OS, firmware, serial number, and process commands, etc. The cloud-based management platform provides deep visualizations of OT assets, risk assessments, and communication patterns in an intuitive display based on the Purdue Model Framework for Industrial Control Systems and Cybersecurity Segmentation and ISA/IEC 62443 standard zone conduit visualizations. This minimizes blind spots between OT and IT, serving as a single source of truth for risk and operations teams.
- **Risk assessment and prioritization:** Continuous AI-powered risk prioritization that leverages a multifactor scoring system that considers vulnerabilities, asset criticality, operational impact, and compensating controls rather than simply vulnerability scoring. This predictive and context-aware assessment aligns better to the processes used by experts at organizations to effectively measure and prevent OT risk today. This continuous security inspection helps to prevent or alert to, or take automated action against, zero-day threats, unknown threats, and anomalies in the ICS process to ensure integrity and safety, as well as meet internal and industry compliance requirements such as IEC-62443.
- **Proactive risk mitigation:** AI-powered risk-adaptive policies provide context-aware policy recommendations and enforcement that is based on device identity, observed and common behaviors, and criticality, all of which help to minimize the risk of operational disruptions. These policies and segmentations can then be applied and enforced on the NGFW with a single click. Palo Alto Networks' Policy Optimizer then finds cases of overlapping, conflicting, and shadow rules and recommends opportunities to consolidate and optimize policy rule sets. Proper segmentation of OT assets further protects vulnerable OT assets and connected IT systems against propagation of threats. Risk-adaptive policies can help prevent unpatched systems with a high-risk profile from connecting to the corporate network and make sure that unmanaged tablets on the floor cannot connect to critical OT applications. In addition, Guided Virtual Patching can provide compensating controls for unpatchable or sensitive systems, which helps to mitigate exposure and preserve critical device uptime.
- **Operational efficiency and integration:** OT Device Security leverages existing firewalls and workflows and deploys in minutes without the need to deploy additional sensors, modify infrastructure, or add any other additional costs. By providing unified management and consistent security policies for managed and unmanaged devices across OT, IT, and IoT, Industrial OT Device Security helps better protect OT environments from cyber events that originate mainly from IT networks. Device information can be shared natively with other tools such as network access control, security information and event management (SIEM), and IT service management platforms without intensive API integrations.

Figure 2. Palo Alto Networks OT Device Security

Source: Omdia

Omdia Economic Validation

Omdia's Economic Validation team completed a quantitative economic analysis of Palo Alto Networks OT Device Security with a focus on how organizations have been able to use the service to detect, categorize, and protect assets in their manufacturing and OT Device Security environments. Omdia's Economic Validation process is a proven method for understanding, validating, quantifying, and modeling the economic value propositions of a product or solution. The process leverages Omdia's core competencies in market and industry analysis, forward-looking research, and technical/economic validation. We conducted in-depth interviews with end users to better understand the challenges and experiences customers have had related to securing OT assets and to learn how Palo Alto Networks OT Device Security has provided savings and benefits to their organizations. The qualitative and quantitative findings were used as the basis for a conservative economic model, illustrating the savings and benefits that might be achieved by an organization.

Palo Alto Networks OT Device Security Economic Overview

Omdia's economic analysis revealed that Palo Alto Networks OT Device Security has provided its customers with significant savings and benefits in the following categories:

- **Faster and more comprehensive OT protection.** Organizations were better able to deploy the solution, detect and categorize assets, and protect the environment in less time than alternative solutions.
- **Reduced operational complexity.** Palo Alto Networks OT Device Security required less effort from security teams to deploy, manage, maintain, protect, and integrate intelligence than with other security solutions.

- **Reduced risk to the organization.** By providing faster time to protection, detection, and remediation, Palo Alto Networks OT Device Security effectively lowered overall risk to the organization.

Faster and More Comprehensive OT Protection

Palo Alto Networks OT Device Security is a service that can easily be activated on existing Palo Alto Networks NGFWs. Configuring a SPAN or mirror interface on the NGFW will provide east-west visibility and monitoring. This, combined with intelligent and automated features and an ongoing commitment to better supporting OT environments and assets means that organizations can more quickly secure their OT environments and provide more comprehensive protection from potential attacks. OT Device Security provides faster time to protection through:

- **Faster deployments and holistic visibility into connected assets.** Customers were able to minimize the time required to plan, prepare for, and install their OT security solution compared to alternative offerings that required the deployment of sensors and separate software subscriptions. The SaaS-based OT Device Security service required no additional hardware or forklift upgrade and could be implemented automatically on all currently supported PANW firewalls and PAN-OS versions in under an hour in the Panorama centralized firewall security console or Strata Cloud Managed NGFWs, or could be manually enabled on NGFWs that users already owned in less than four hours. Alternative solutions could take up to 15-20 hours to plan and prepare for, deploy sensors and software, and configure the environment. Once installed, customers reported that OT Device Security began to monitor traffic and passively detect all managed and unmanaged IT, IoT, and OT assets. AI and third-party integrations were used to identify over 2,000 device attribute combinations. This eliminated the need to reconcile data across dozens of tools and vendor websites and resulted in fewer unknown/unmanaged devices.

> **"Getting things up and running on the network required network and security exceptions. [OT Device Security] has changed that, where now they just plug it in, it gets recognized, and it's just already in whatever guardrail policy is in place. No one has to call us—there are no tickets. It just works."**

- **Faster and more intelligent creation and enforcement of policies.** Once the solution had depth and breadth of the device data, it started populating automated categories and creating intelligent policy recommendations. This took much less effort on the customers' part as opposed to alternative solutions where policy creation and ACLs must be manually created (without knowledge of insight derived from behavior baselines) for each category and profile. The customers that we spoke with had not only reduced the average time they spent on planning, creating, and tuning new policies from five hours to 15 minutes or less, but they also felt that their policies were now more comprehensive and effective – limiting the risk of potential process disruption. While initial asset profiling was fast, customers also saw continuous assessment and improvement over time; as OT Device Security was able to collect more information and monitor more traffic, learn more context, and consider user identity and device health, the precision of device profiling and policy recommendations increased. One customer stated, "OT Device Security automatically assigns newly classified profiles and recommends policies based on the data that they see on the network, so the more traffic they see, the better they can judge the asset." Policies are critical for protecting industrial environments where patching an asset to resolve vulnerability is not an option (e.g., if it requires downtime or if a patch does not exist). Guided Virtual Patching provided a good way to implement compensating controls successfully by using existing security infrastructure without disrupting device operation and mitigated the risk of vulnerabilities without patching. When new asset classifications are released (e.g., a new profile for a finer sub-segmentation of an OT asset type), OT Device Security automatically changes the associated policies without having to take the manual steps to make sure profiles and policies stay up to date and are synchronized. Policy Optimizer continuously finds cases of overlapping, conflicting, and shadow rules and then recommends opportunities to consolidate and optimize policy rule sets that otherwise would have to be manually identified and reconciled (if found at all)—reducing time, effort, and risk to the organization.

- **Faster time to identify and remediate risks with fewer blind spots.** With comprehensive visibility into assets on the network, customers reported that they were in a better position to identify and remediate potential threats to their OT assets. Customers stated that OT Device Security provided continuous AI-powered risk prioritization for their OT assets by combining static device identity attributes with live network traffic analysis, exposure data, firewall policy information, actionable risk insights based on CISA and vendor recommendations, vulnerability assessments, and security hygiene evaluations. If known exploits were detected, OT Device Security, along with Threat Prevention, was able to better protect users' environments by taking appropriate actions in the NGFW, and customers were alerted of any potential actions that should be taken. Those with subscriptions to Palo Alto Networks Threat Prevention were able to automate steps further, speeding time to remediation. PANW multi-factor prioritization framework that considers asset criticality, exploitation status, threat vector, severity, and compensating controls (as well as other information), OT Device Security has reduced the time that customers spent finding and prioritizing security risks from hours to minutes and has helped to better identify and eliminate blind spots between the OT and IT networks. One customer stated: "In the past, it has not worked too well for us to perform manual active scanning of such a large variety and quantity of assets, but OT Device Security, via passive monitoring, provides a better tool for this."

> **"As soon as we deployed OT Device Security, we started getting visibility into our assets and started getting alerts based on if patterns or behaviors changed."**

- **Faster achievement of compliance initiatives.** OT Device Security enables customers to more easily meet industrial and manufacturing compliance requirements. Enhanced visibility and segmentation help organizations align with IEC 62443, NIST, and other related frameworks. Palo Alto will continue to enable organizations to meet compliance requirements and is committed to continuing to enhance its support to ensure the future needs of customers from a compliance perspective.

Reduced Operational Complexity

Providing security for OT assets is complex and time consuming. OT Device Security provided automation and AI-assisted visibility that helped reduce manual efforts and inefficient processes to enable OT security teams to be more productive and achieve much more with the resources that they had. Teams reported far less effort required to detect, identify, and manage devices, create and enforce policies, and triage and proactively remediate risk. OT Device Security helps lower the operational complexity of providing security for OT environments through:

> **"It is hard to classify OT assets. It's more than just, 'What category of asset is this?' It is also, 'What is important?'—like a temperature sensor may not be important in one location but, in another, it could be absolutely mission critical."**

- **Automated deployment and detection.** OT Device Security has multiple deployment architectures, enabling customers to secure their OT environments regardless of their existing network architectures. OT Device Security can leverage existing NGFWs as sensors and for policy enforcement. Palo Alto Networks also has OT Device Security deployment architectures for north-south and east-west visibility and security in air-gapped environments (with their telemetry gateway solution), modern 5G-enabled environments, and secure access service edge (e.g. Prisma Access) customers. In addition, OT Device Security uses a combination of machine learning, AppID technology, and crowd-sourced telemetry data to automatically profile all assets and applications instead of having to scan and perform classification or create profile logic manually. And OT Device Security asset detection techniques have now expanded to cover virtual meta-data collector (sensor only), active discovery, device file parsing, and integrations with OT specific tools (e.g., Rockwell asset center). This manual process could take months to complete for larger environments and require a professional services engagement, and, for this reason, the work is often left incomplete and the assets are left unprotected. Additionally, environments change over time, and assets need to be continuously reclassified to better cope with changes in the environment and attack methods. This results in even more rework that OT Device Security avoids through continuous assessment and classification.
- **AI-powered visibility and management simplicity.** OT Device Security provides customers with a single pane of glass and a unified platform for protection of all assets on the network (NGFW, OT Device Security, and other security inspection services), making management and monitoring of OT assets and policies much simpler. The cloud-based SaaS platform requires no maintenance and very little training. Customers could easily see the distribution of traditional IT, network office, facility, and industrial OT assets and drill into the details of each asset to learn more about asset profiles, applications used (note application is equivalent to network protocol; e.g., HTTP, BACnet, etc.), network segmentation, and AI-powered risk prioritization to more easily manage the environment and secure assets.

"We've gotten a lot of value because Palo Alto Networks continues to add new capabilities for the systems to make things easier. If there are gaps or areas that they need to improve, they've been very good about engaging with the community and finding what those are."

- **Reduced alert fatigue and accelerated triage.** As mentioned earlier, OT Device Security's AI-powered Risk Prioritization not only accelerates triage and remediation, but multifactor risk scoring helps to decrease complexity and significantly reduce the time that must be spent by security teams to triage risks. The AI-powered risk prioritization understands asset criticality, multifactor context, and compensating controls, which help to identify and reduce the priority of otherwise noisy alerts that would take time and attention away from teams working on critical threats.
- **AI-powered intelligence and automation.** OT Device Security enabled automation and intelligence, helping to decrease the time teams normally spent on performing the manual tasks that are required on alternative offerings. Whether

"For me, the main benefit is device visibility. It's the CMDB type of aspect, where maybe we're pretty good at tracking desktops and servers, but we're not keeping track of all the cameras or printers or random other smart devices that we have on the floor. We would never be able to inventory all of that. Those are things that [OT Device Security] kind of gives us a CMDB-like experience."

reconciling information from multiple tools, creating policies, generating certificates, researching and planning, scanning for vulnerabilities, or remediating vulnerabilities, teams reported that they saved a significant amount of time due to the level of AI-intelligence and automation provided. And OT Device Security is continuously learning and adapting to new devices and threats and improving the intelligence built into Risk Prioritization. Palo Alto Networks' automated zero-trust security considers the users, assets, and context of requests against intelligent risk assessment before allowing access based on automated policies that enforce segmentation, saving up to 20x the time and effort.

- **Simplified integration with other products and services.** OT Device Security provides a unified platform that simply integrates with the firewall and contains over 40 built-in integrations to other OT, IT, and security products. Customers were able to automate workflows with playbooks and integrate OT Device Security with their existing tools and processes (such as asset discovery and management, SIEM, and work-order management) for network access control, improved visibility, threat prevention, and even remediation (if licensed for Palo Alto Networks Threat Prevention service). The automation and orchestration provided through these integrations not only save organizations valuable resources in terms of time but also maximize the value of their investments, streamline operations, and help avoid the potential for making manual mistakes.

> **"To build certificates and profiles for our 5,000 assets alone would have required a professional services engagement and months of time, and then we would have to maintain it going forward."**

Reduced Risk for OT Environments

With industrial and manufacturing operations the target of nearly a quarter of all cyberattacks and a majority of critical threats originating on the IT network and increasingly powered by AI,[2] organizations must be more diligent than ever to take action to lower risk for these environments as they come together. OT Device Security helps lower risk by eliminating unmanaged exposure through **aggregated visibility**; identifying, understanding, and responding to threats faster and more intelligently with **AI-powered prioritization;** and helping guarantee uptime and safety through **proactive mitigation** adaptive controls. OT Device Security provides:

- **Reduced risk of successful breaches and AI-powered attacks.** Customers reported that OT Device Security delivered faster and better protection for their OT assets and helped minimize the potential for successful breaches or malicious activity. Customers were able to leverage OT Device Security's AI-powered intelligence to automatically identify and protect a greater variety of OT assets and extend and enforce adaptive security policies to secure these assets against changing threat conditions. Policy enforcement and dynamic network segmentation can reduce the attack surface and limit the potential reach and impact of a successful breach by blocking access to other resources once suspicious activity is identified, potentially saving organizations millions of dollars. Customers also shared that other OT Security products they had considered were designed to alert to suspicious activity but not take any

> **"I have tested a lot of alternatives to Palo Alto Networks, but those solutions can only tell me what kind of equipment I have and which vulnerabilities may potentially exist for that class of equipment, not whether this is actually an issue for my particular device or not."**

[2] Source: "Cost of a Data Breach Report 2025" ibm.com.

immediate action to mitigate risk (such as threat prevention or enforcing network segmentation after detection like OT Device Security). In addition, Palo Alto Networks improves effectiveness by leveraging crowd-sourced threat intelligence to continuously improve knowledge of zero-day threats specific to OT assets. Without OT Device Security, many assets simply would be left undetected, unscanned, and vulnerable.

- **Greater visibility and intelligence into assets, attack surface, and risks.** OT Device Security provides an intuitive GUI with powerful visualization supporting OT-IT, Purdue Model, and IEC 62443 zone-conduit segmentation insights. Users are provided with a complete inventory of assets enriched with identity, posture, and behavioral attributes for all assets and protocols across IT, IoT, and OT. Users are able to visualize asset and network behaviors and network segmentation to ensure current implementation meets the current policies, standards, and best practices. This includes zone conduit visualizations that can help reduce the attack surface and improve incident response, security, and compliance. The OT Device Security interface delivered visibility into the network, devices, and applications; provided customers with up-to-date and ongoing risk assessments; and continuously monitored network traffic to better enable their AI/ML-assisted policy recommendations and enforcement. Customers felt that this level of visibility and intelligence provided a single source of truth for their organization and simply would not be possible using the resources that their team had on hand.

> **"Without OT Device Security, we would not know if an asset was there, if it was configured correctly, or if it was behaving in a strange way."**

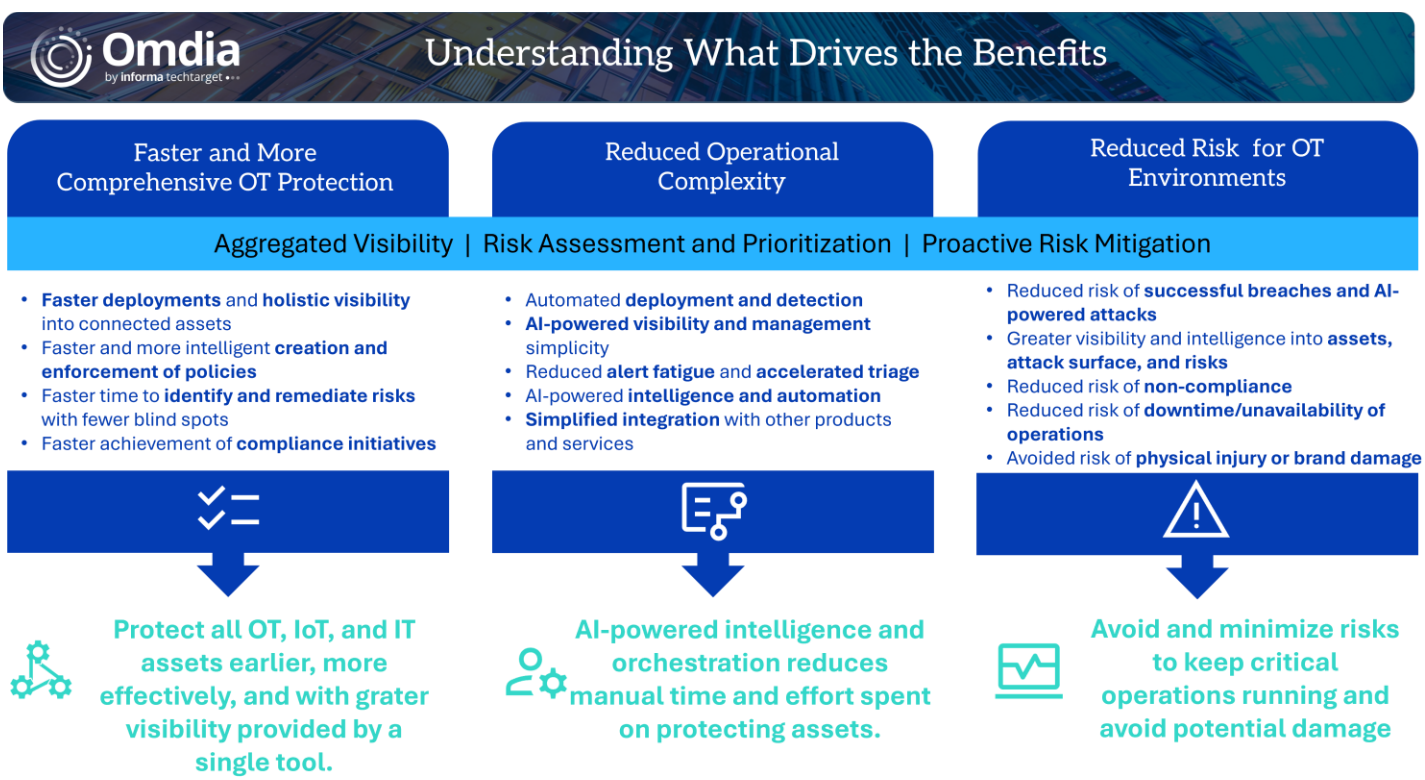
- **Reduced risk of non-compliance.** Industrial and manufacturing companies need to adhere to security guidance frameworks and enforce data residency requirements (such as IEC, ISO, NIST, and GDPR frameworks). OT Device Security can provide audit trails, policy enforcement documentation, and continuous monitoring capabilities for industry-specific security mandates. The customers that we spoke with not only felt they had greater visibility and protection, but they thought Palo Alto Networks OT Device Security was extremely useful in helping ensure global compliance across regional variability existing in OT asset manufacturers, technologies, and governance rules. OT Device Security was also extremely valuable in enforcing and protecting the integrity of existing OT processes. OT Device Security can be used to detect when critical assets go offline and identify unusual traffic patterns or out-of-range values (e.g., a high-temperature reading) on assets. Rule Engine can then be used to customize triggers, generate alerts and automate notifications, or push information to third-party integrations to take automated actions.

- **Reduced risk of downtime/unavailability of operations.** For industrial and manufacturing operations, uptime of operations is critical to generating revenue and delivering critical services. By better securing OT assets and reducing the risk of a successful attack, organizations protected by OT Device Security felt that they were in a better position to avoid any operations downtime. Palo Alto Networks OT Device Security provides continuous device health monitoring and can find and remediate risks early that otherwise might go undetected, resulting in malicious activity or ransomware that can bring operations to a halt. And because policy recommendations are based on actual, observed behaviors, the risk of Device-ID policies disrupting operational processes is reduced. With some point products that were not designed specifically for OT, active scanning of OT environments can potentially cause problems to assets and disrupt critical business processes. This could lead to unintended downtime (risk that is avoided through OT Device Security's passive log capture instead of scanning). Intelligent Risk prioritization and automated threat containment work together to permit safe and trusted functions for OT assets on the network and block everything else. Assets are able to download and safely update firmware from a trusted source or share telemetry data with approved cloud services. Keeping assets up to date and in contact with critical services places the assets in a better position to avoid security and operational issues down the road that could potentially lead to downtime.

- **Avoided risk of physical injury or brand damage.** Industrial operational networks must consider the risks they pose to health and human safety: Malicious access could cause systems or machinery to malfunction, resulting in damaged equipment, or introduce dangerous changes to the manufacturing process, causing product quality issues that could be harmful to humans. Although less likely, a lack of security can even result in a physical risk for workers (e.g., if a machine shuts down or stops during operation or if the operation of control sensors or temperature controls is compromised).

> **"Suppliers and manufacturers are not doing a great job of finding vulnerabilities. Instead, security researchers are finding them. That is not acceptable. If our manufacturing facilities went down, it would impact millions of dollars in lost production revenue, reputational harm, a potential loss of IP, as well as the cleanup efforts."**

Figure 3. Omdia Validated Benefit Summary: Palo Alto Networks OT Device Security



Source: Omdia

Omdia Analysis

Omdia leveraged the information collected through vendor-provided material, public and industry knowledge of economics and technologies, and the results of customer interviews to create a five-year TCO/ROI model. The model compared the costs and benefits of protecting OT environments with Palo Alto Networks OT Device Security instead of an alternative solution based on deploying sensors paired with an OT Device Security subscription. Omdia's interviews with customers who have recently deployed the technology, combined with experience and expertise in economic modeling and technical validation of Palo Alto Networks and alternative technologies, helped to form the basis for our modeled scenario.

Why This Matters

When considering and comparing OT security solutions, it is important to consider more than just the solution cost.

Organizations should also consider the time required to deploy and protect the environment, the operational cost savings provided through automation, and the avoided costs of risk provided through earlier and more effective protection and remediation. While these numbers around risk are difficult to predict and hard to conceptualize, a single event can make the financial pain incurred very real to an organization.

Our model assumed that a midsize manufacturing organization operated eight global manufacturing locations, each with various buildings and operational facilities. We assumed an average of five Palo Alto Networks firewalls were deployed at each distributed location, for a total of 40 NGFWs, as well as an initial average of 100 assets per firewall, for a total of 4,000 OT and IoT assets under management. We also assumed a growth rate of 5%, so by the end of the fifth year, 862 new assets were added to the networks, for a total of 4,862 assets. Finally, although the number would vary in practice, we assumed an average of 50 assets per unique profile class so that, when deployed, all assets would be classified into 80 profiles by OT Device Security. This number would grow to 97 by the end of the fifth year as new assets were deployed and profiled.

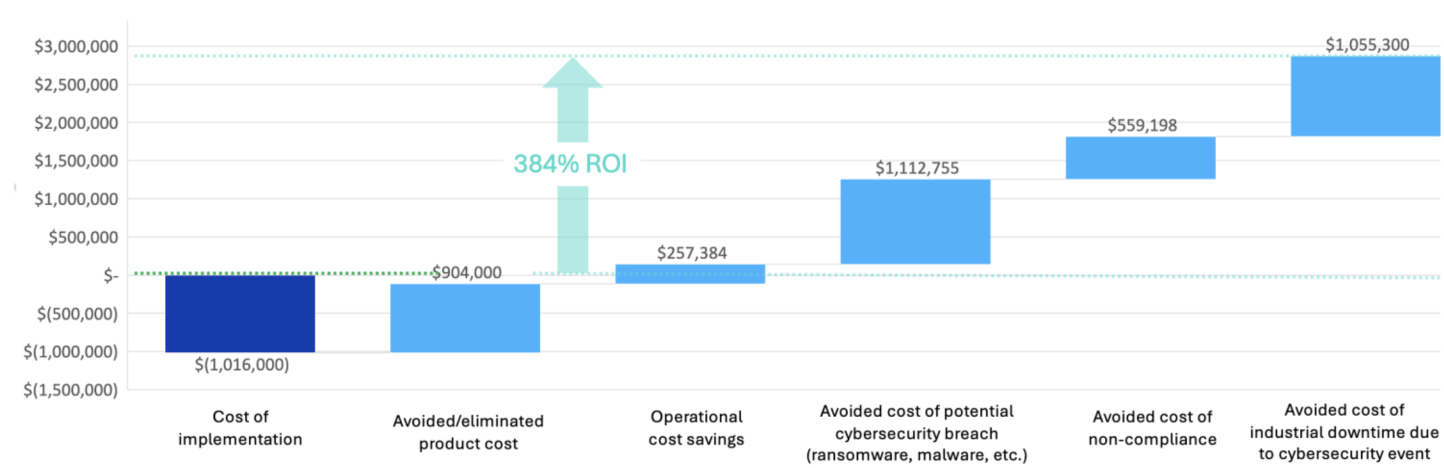
Next, we modeled the expected person-hours required to perform planning and deployment of the OT security solutions. We assumed that the OT Device Security could be enabled in about one hour and 15 mins per firewall, while the alternative sensor-based solution would take an average of 3.5 hours per sensor (assuming one sensor for each firewall). We then modeled the time for the solution to create the initial profiles using 15 minutes per profile for Palo Alto Networks and five hours of manual creation time on the alternative solution. We used similar models to show the time required to perform ongoing risk assessments (automated for Palo Alto Networks, versus manual scanning for 30 minutes per asset for the alternative), the time to assess and remediate risks (15 minutes per profile versus 10 hours per profile), and the time to identify and remediate threats (assuming 90% of threats could be avoided with Palo Alto Networks and an average time of two hours to remediate threats). The results, shown in Figure 4, predict a cost of operations that is up to 95% lower for the Palo Alto Networks OT Device Security solution, saving the modeled organization $257K in operational costs over five years.

Figure 4. Expected Cost of Person-hours to Deploy and Operate OT Security Solutions

Source: Omdia

Omdia then performed a simple cost analysis of the solutions and leveraged our proprietary models, along with conservative assumptions made in good faith, to predict the savings and benefits that could be expected from avoided cost of the solution, operational costs, and avoided risk of a potential breach, of non-compliance, and of potential downtime. Comparing the results to the investment made in Palo Alto Networks' OT Device Security subscription resulted in an expected ROI of 384% over five years. Our ROI calculation was roughly 30% higher than our report published in 2022, with benefits being increased due to continuously increased capabilities around device detection, attribution, and AI-powered risk prioritization. The results are shown in Figure 5 and described in the following section.

Figure 5. Expected Savings and Benefits Over Five Years for the Modeled Organization



Source: Omdia

What the Numbers Mean

- **Cost of implementation:** Omdia modeled the expected cost of the Palo Alto Networks (OT Device Security subscription) solution and an alternative solution (hardware sensor Capex and security solution Opex). An effort was made to ensure as "apples to apples" a comparison as possible based on the number of firewalls, maximum assets required, and similar bandwidth limits. Our cost analysis did not include the cost of NGFWs, which we assumed the customer already had and would be used in either case. It should be noted that pricing can vary dramatically based on the model of the firewall and other requirements.
- **Avoided/eliminated product cost:** For an ROI comparison, the difference in expected spending between the total five-year solution costs is shown as an avoided cost, meaning that this is the cost that has been avoided by choosing the less-expensive solution over the alternative. In a TCO comparison, this difference would simply show up as a lower cost of solution. While not included in this analysis, it should be noted that the upfront Capex spending would have to be made in year 1, tying up financial resources and providing slightly more savings based on calculating a higher net present value of making the upfront investment.
- **Operational cost savings:** This is the operational cost or expected person-hour savings required to operate the two OT security solutions described in the earlier section and depicted in Figure 4 of this report. It should be noted that both solutions are saving organizations time over manually performing the work and trying to build the solution on their own or with tools not designed for OT, which, although not the focus of this report, would represent a significantly higher level of savings.
- **Avoided cost of a potential cybersecurity breach:** Omdia's proprietary models were used to calculate the expected avoided risk and cost of a cybersecurity breach, tailored for an industrial organization. Our models considered the expected cost of a successful data breach (based on data published by IBM and the Ponemon Institute[3] for industrial organizations at roughly $5M (based on the cost to notify, respond to, detect, escalate, and impact to the business). Using Omdia's own custom assumptions for the risk of a data breach in a given year and the alternative and Palo Alto Networks reduction to this risk, we assumed that the alternative solution could lower the risk by 40% and that the Palo Alto Networks solution reduced risk by an additional 22% over the alternative solution. This assumption was based on the expected difference in time to protection. With the alternative, assets would be left exposed on the network due to manual profile creation, scanning time and effort, and longer remediation cycles. Our risk-weighted analysis showed that, over five years, the Palo Alto Networks OT Device Security solution could avoid roughly $1.12M of expected risk over the alternative solution and over $4.54M in avoided risk over not having any OT security in place.
- **Avoided cost of non-compliance:** IT teams need to be able to accurately inventory and update OT assets, ensure proper functionality, and then secure them to ensure compliance with company, industry, and even government goals and regulations. If a company is out of compliance, it risks the cost of audits, clean up, the impact on productivity, and potential fines. Using a similar proprietary model and assumptions, we assumed the risk of non-compliance is removed once all assets have been profiled and risk assessments are up to date. Using our operational calculations, we concluded a compliance risk reduction of 19% for Palo Alto Networks OT Device Security over the alternative solution, providing risk avoidance savings that added up to $559K over the five-year period.

[3] Ibid.

- **Avoided cost of industrial downtime due to cybersecurity event:** Our models, based on information provided in published reports, conservatively assumed that the typical outage for an industrial or manufacturing organization would last four hours and impact slightly over $2M in business loss, lost productivity, and risk of human injury. Accounting for the risk of an outage caused by cybercrime (27% of all outages according to the Ponemon Institute), and the 20% expected improvement of Palo Alto Networks OT Device Security over the alternative solution, our models predict a five-year savings of $1.06M due to reduced risk of potential impact to operations.

Considerations

While our models are built in good faith upon conservative, credible, and validated assumptions, no single modeled scenario will ever represent every potential environment. Palo Alto Networks OT Device Security provides significant benefits and value to organizations, especially if an organization is already an existing Palo Alto Networks customer. Omdia recommends that you perform your own analysis of available products and consult with your Palo Alto Networks representative to understand and discuss the differences between the solutions proven through your own proof-of-concept testing.

Conclusion

Industrial and manufacturing networks provide the backbone for manufacturing, production, and critical utility functions. While historically isolated from corporate networks and internet-connected assets, there is now mounting pressure to connect these critical applications, systems, and assets to corporate networks. This is to facilitate modern data collection and analysis, update and monitor critical components, and provide centralized access, among other things. But these networks are difficult to secure due to the variety of assets and technologies and the general lack of visibility. Cybercriminals have identified this challenge and, when combined with the power of AI and the potential rewards of a successful attack (revenue impact, brand damage, large-scale disruption of utilities), industrial OT is the perfect target.

Omdia validated through a series of interviews that customers have been able to use Palo Alto Networks **OT Device Security** to better manage, secure, and protect their OT assets while providing safe access to the assets and services required to modernize operations. The built-in automation, orchestration, and intelligence helped to provide faster time to value, reduced complexity of operations, and significantly helped to reduce risk to the organization. Our models predict that, by using **OT Device Security** instead of an alternative solution, organizations can realize a conservative 384% ROI while lowering the cost of managing the solution by up to 95%.

> **“To demonstrate our current lack of OT security, I walked in [to the facilities] with my laptop, connected right into a system, and within 10 minutes was able to show that anyone could control our equipment and do potential damage. This was massively educational and got everyone on board with the criticality of the situation.”**

“OT security is complex. Many companies have good strategies outlined in slides, but when you actually go to the plant to see it in practice, they are still quite far from having the technology in place.”

OT security is certainly complex, and organizations understand that there is no one turnkey solution that they can plug and play to solve all of their requirements for legacy, current, and future assets. This is especially true for extremely large and global organizations where the variety of OT assets can be quite specialized and localized. Palo Alto was one of the first vendors to really focus on OT security. It has worked with customers to understand the challenges and improve and expand the effectiveness of the product, significantly increasing the number of OT vendors, OT protocols, and OT threat signatures that they support every year. And organizations agree that **OT Device Security**, with its AI-powered asset discovery, policy creation, comprehensive visibility and risk prioritization, and proactive remediation, provides the best solution out there and trust that Palo Alto Networks is the right partner going forward.

“Palo Alto is probably the best firewall in the world. With OT Device Security, it has a vision and a target that is in line with what we need. Competitors are not thinking outside the box or using AI or even thinking globally for OT organizations.”

"Palo Alto Networks has been a very good partner with us to get this product into our environment and working well… They’re not coming back to us saying, well, this is a [customer’s company] problem. They’re partnering with us to make it work in our environment, and everyone else benefits from this too."

If your organization is looking to reduce risk for its industrial OT environment while greatly improving visibility of all OT, IoT, and IT assets; simplifying operations; and enforcing AI-powered policies, risk assessments, and remediation for assets in a modern and connected but dangerous world, Omdia suggests that you strongly consider Palo Alto Networks OT Device Security.

Get in touch: www.omdia.com askananalyst@omdia.com