FORRESTER®

# Palo Alto Networks CDSS Enterprise IoT Security Helps Organizations Gain Visibility Into IoT Devices And Streamlines Management To Reduce Risk And Improve Operational Efficiency

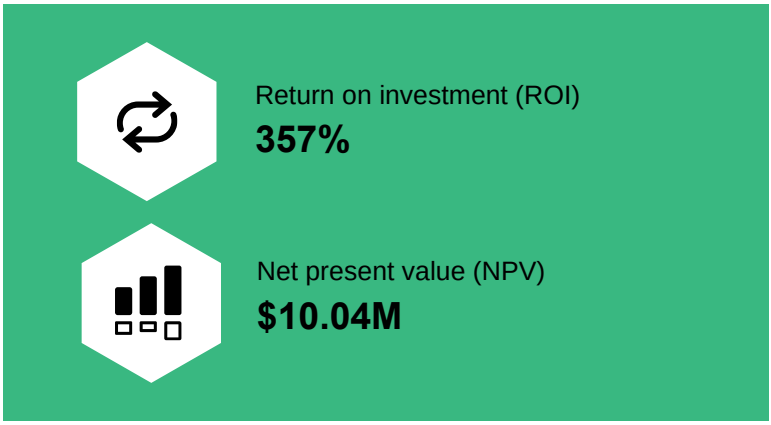
Internet-of-things (IoT) cybersecurity attacks have evolved significantly in recent years, necessitating the adoption of robust IoT security solutions. With the proliferation of interconnected devices, the attack surface has expanded exponentially, making IoT networks prime targets for adversaries. Forrester research shows that IoT devices are the most commonly reported target of external attacks, above employee- or corporate-owned mobile devices or computers.[1]

The same report includes examples of numerous recent IoT-related attacks such as ongoing attacks from Mirai malware variants like Meris, enemy bots, and Fodcha. These attacks target vulnerabilities in particular devices, and they even use IoT devices to break into networks.

Incidents like these expose the vulnerabilities inherent to unsecured IoT devices and help attackers break into networks. IoT devices are being targeted or used to launch broader attacks because: IoT devices generally lack built-in endpoint security, reuse of known credentials is common, business operations still need legacy devices, and outbound connections to the internet make IoT devices a conduit for command-and-control attacks.

With the increasing complexity and sophistication of attacks targeting IoT devices, investing in a solution like Palo Alto Networks Enterprise IoT Security can be essential to safeguarding sensitive information, preserving business continuity, and maintaining the trust of customers and partners.

Palo Alto Networks commissioned Forrester Consulting to conduct a Total Economic Impact™ (TEI) study and examine the potential return on investment (ROI) enterprises may realize by deploying Palo Alto Networks Cloud Delivered Security Services (CDSS).[2] This abstract will focus on Palo Alto Networks Enterprise IoT Security and its value to their organizations.




Forrester spoke with the following representatives of organizations using Enterprise IoT Security:

- An information security architect and CISO at a healthcare organization with $2.2 billion in annual revenue, and 11,000 employees. The firm uses IoT devices such as medical devices.
- An enterprise network architect at a government organization with $16 billion in annual revenue and 400,000 employees. The firm uses IoT devices such as cameras and consumer home devices.

Enterprise IoT Security uses a three-tier machine learning (ML) model, Palo Alto Networks App-ID technology, and crowdsourced telemetry to help with

**READ THE FULL STUDY**

speed, accuracy, and scalability in device profiling. It helps users understand attack surface and compliance gaps, and it gives real-time risk assessment on threats, exploits, risk, and device context.

The interviewees said that prior to deploying Palo Alto Networks for network security needs, their organizations leveraged various point solutions to secure their environments, but they lacked modern security technology because their security and IT teams struggled to keep up with evolving business needs. Digital transformation initiatives pushed more data, applications, and processes to the cloud and edge, while other core business functions remained on-premises.

After the investment in Enterprise IoT Security, the interviewees' organizations were able to realize various operational efficiencies across different activities, which significantly reduced investigational effort and freed up valuable resources to focus on enhancements and securing more of the network.

Key results from the investment include efficiency gains for IT, security, and networks operations teams, business end users, and in-store workers. Furthermore, interviewees' organizations benefited from a reduced likelihood of experiencing a data breach as well as reduced costs associated with licensing and managing legacy point-solution infrastructures.

## KEY CHALLENGES

The interviewees' organizations adopted Enterprise IoT Security to increase visibility into devices and usage statistics and to consolidate and integrate their IoT security with other Palo Alto Network tools to ease management. These organizations struggled with several challenges in their legacy environments, including:

- **Legacy disparate solutions led to gaps in IoT visibility and security operational toil.** Interviewees noted that using disparate solutions in their organizations' prior environments led to a lack of visibility into their IoT environments and gaps in their security. They said that either the legacy solutions were not comprehensive enough to provide full coverage against ever-evolving cybersecurity threats or that the different point solutions neither integrated together nor worked well with one another.

  The enterprise network architect at a government organization said: "Before [using Enterprise IoT Security], our security team was working blind. They couldn't do an effective job of protecting things that they didn't know were there. We're heavily leveraging IoT to see into customer networks to see what we need to protect. For example, how many cameras, storage networks, and home consumer-grade devices do we need to protect? We need to know what's there so we can protect our customers from being compromised. That's where [Enterprise IoT Security] has been invaluable."

- **Legacy solutions led to additional security operational toil.** Interviewees said their organizations either did not have a comprehensive view into their IoT devices or they undertook manual efforts to bring that visibility together through information from multiple solutions. The information security architect and CISO at a healthcare organization said: "Prior to using [Enterprise IoT Security], our inventory was dependent on devices identified by [our legacy solutions]. We would then have to manually convert that information to and from different platforms and correlate that information together. It wasn't an easy process. [Enterprise IoT Security] helped us obtain that visibility in a central repository."

## INVESTMENT DRIVERS

The interviewees' organizations chose to invest in Palo Alto Networks Enterprise IoT Security to:

- **Gain visibility into existing devices and usage statistics to reduce the risk from known and unknown threats.** Enterprise IoT Security expands visibility to all devices for IT and security teams, and it provides 24/7 real-time risk assessment of threats, exploits, risk, and device context. Enterprise IoT Security also protects against known exploits, web threats, command-and-control (C2) attacks, and malware, which reduces the risk of threats.

  The information security architect and CISO at a healthcare organization told Forrester: "For IoT, our clinical engineering side maintains the medical devices within our ecosystem, and the audit finding there was that they did not have a good inventory of the medical devices in our operations. An IoT solution helps facilitate the identification of those devices."

- **Improve availability and reduce downtime.** Interviewees' organizations sought a solution to minimize device downtime and business disruptions. Enterprise IoT Security employs Zero Trust frameworks to segment IoT devices from the rest of the network by creating granular segmentation policies to prevent the lateral movement of threats.

  The information security architect and CISO at a healthcare organization said: "The aggressiveness of the scanning that's done by [our legacy solution] can sometimes trigger a negative consequence like having to take a device down. [With Enterprise IoT Security,] there's a lot less risk that detecting a vulnerability will result in a disruption in service or cause the device to be taken out of service."

- **Integrate with other Palo Alto Networks solutions to drive ease of management and use.** The integration of Enterprise IoT Security with other Palo Alto Networks solutions allows IT and security teams to access insights in a single console, which minimizes the "swivel chair" effect and reduces the time to manage different platforms.

  The information security architect and CISO said: "[Enterprise] IoT Security also had a nice integration with other Palo Alto Networks solutions as well as a good interface compared to other vendors. [Enterprise IoT Security] had a real clean interface [and it was] very intuitive as far as the user functionality of it [with] the features and functions."

  The enterprise network architect in government said: "With Palo Alto [Networks], we've ended up deploying a lot more of the Palo Alto suite. I definitely see a lot of benefit from looking at a suite of products that play together. Everything is integrated. It's allowed us to optimize and make our security better, faster, and cheaper."

## KEY RESULTS

Forrester combined the results from the interviews into a three-year financial analysis for a composite organization. Risk-adjusted present (PV) quantified benefits for the composite organization include:

**Reduced number of security incidents requiring manual investigation by 25% to 60%, decreased mean time to resolution (MTTR) by 20%, and reduced number of endpoint devices requiring reimaging, all resulting in $1.1 million saved over three years.** By using Palo Alto Networks CDSS in combination with the other solutions implemented in its security environment, the composite organization reduces the number of security incidents that require manual investigation, the time to respond and resolve incidents, and the number of endpoint devices that require reimaging. This is a result of the organization being able to track the performance and usage of the

different implemented solutions in one place, which gives the SecOps and IT ops teams the ability to quickly identify and respond to potential threats.

The information security architect and CISO at a healthcare organization said: "[Enterprise IoT Security] my information security team to go to our platform teams with identified vulnerabilities rated at a given severity risk we have, and it helps prioritize what remediations we should focus on given the variety of network-connected devices that are out there."

**Improved end-user productivity with better system availability and less intrusion to the network, totaling $5.2 million in business value over three years.** The composite organization realizes end-user productivity gains by minimizing disruption caused by its security investigations and from better overall system availability of the environment. This is a product of the better integration and compatibility of the different Palo Alto Networks solutions as well as improved overall performance.

**Decreased likelihood of a data breach by 50% after three years, worth close to $2.8 million.** The different tools that fall under Palo Alto Networks CDSS provide the composite organization with a more secure environment for various activities and use cases. As a result, it decreases the likelihood of a significant data breach.

The information security architect and CISO in healthcare shared: "Our IoT helps us get visibility on our medical device inventory. Where do they reside? How often are they used? Are there any FDA recalls? That helps us reduce risk related to our devices."

**Avoided and rationalized security infrastructure, saving $3.4 million over three years.** Using Enterprise IoT Security allows the composite organization to consolidate its spending on security tech stack vendors.

**Reallocated roughly 50% of full-time security professionals to higher-value initiatives due to management efficiencies from a common platform, saving $378,000 over three years.** Related to the vendor consolidation benefit, the composite organization also realizes efficiencies for its employees who manage the different tools. By having a common platform to manage all Palo Alto Networks solutions, the composite organization can repurpose certain employee time or even entire team members to other prioritized or higher-value work.

> **"The main value of CDSS is having a better understanding of our assets in the potential deficiencies those assets may have from a security perspective [and] the vulnerabilities and exposure that we could have from the biases that govern the network access into the organization."**
>
> *Information security architect and CISO, healthcare*

**TOTAL ECONOMIC IMPACT ANALYSIS**

For more information, download the full study: "The Total Economic Impact™ Of Palo Alto Networks CDSS," a commissioned study conducted by Forrester Consulting on behalf of Palo Alto Networks, November 2023.

**STUDY FINDINGS**

While the value story above is based on four interviews, Forrester interviewed four total representatives at organizations with experience using Enterprise IoT Security and combined the results into a three-year financial analysis for a composite organization. Risk-adjusted present value (PV) quantified benefits for this composite organization include:

**Return on investment (ROI)**

**357%**

**Net present value (NPV)**

**$10.04M**

## Appendix A: Endnotes

[1] Source: "The State Of IoT Security, 2023," Forrester Research, Inc., May 18, 2023.

[2] Total Economic Impact is a methodology developed by Forrester Research that enhances a company's technology decision-making processes and assists vendors in communicating the value proposition of their products and services to clients. The TEI methodology helps companies demonstrate, justify, and realize the tangible value of IT initiatives to both senior management and other key business stakeholders.


FORRESTER®