CASE STUDY

Global retailer cuts insurance premiums by 30% with Palo Alto Networks' security overhaul

When a cyber insurance security assessment flagged several significant issues in a global retailer's environment—and planned to tack on a rate increase—the retailer faced a wake-up call. The company sought out Palo Alto Networks to help it implement a transformational shift to gain greater visibility and better threat intelligence across its distributed environment.

paloalto NETWORKS

IN BRIEF

Industry

Retail

Country

United States

Challenge

A global retailer's cyber insurance premiums were about to increase due to security gaps.

Its legacy antivirus solution was no longer adequate and required time-consuming manual effort.

Its security team lacked visibility across its 700+ locations and could not respond fast enough to threats.

Solution

The retailer required a modern security solution it could deploy as quickly as possible. It found the solution by using Palo Alto Networks platforms and services, including:

+ Cortex XDR®
+ Cortex XSOAR®
+ Cortex Xpanse®
+ Unit 42® Managed Threat Hunting (MTH)

Results

Leveraging the integrated capabilities of Palo Alto Networks Cortex and Unit 42, the retailer was able to:

+ Improve alert quality and reduce false positives.
+ Streamline its security operations.
+ Speed up investigation and response times.
+ Augment the team's capabilities by leveraging external partnerships and validation.
+ Instead of increased cybersecurity insurance premiums, the cost decreased by 30%.

CHALLENGE

A lack of visibility comes at a premium

A global retailer using a legacy antivirus solution was left with numerous blindspots in its security environment that could become vulnerabilities and threats if not properly managed. Its security team was receiving many false positive alerts and had a long mean time to detect and respond.

"We had so many questions," recalls the company's security and compliance program manager. "What's going on in our environment? What can we see better? How can we take more timely action?"

When its cyber insurer conducted an annual security assessment and notified the company of an upcoming premium increase, the company knew it had to make improvements.

The three-person security team was responsible for over 700 locations across 13 countries and over 10,000 employees, and it understood its limitations.

The company needed a modern approach that leveraged:

- Automation to reduce manual effort
- An extended detection and response (XDR) solution that could be deployed quickly and evolve over time
- Visibility into vulnerabilities across its assets
- Managed threat hunting to gain visibility into sophisticated threats

The security and compliance program manager made speed a priority: "I wanted to have a solution running across thousands of endpoints as fast as I possibly could."

REQUIREMENTS

A small security team needed a robust, easy-to-use solution—right away

The company sought a security partner with a comprehensive suite of products and services that would integrate well together and enhance the efforts of its small team. Whatever solution it chose needed to deliver extensive coverage and exceptional levels of service—while being easy to implement and operate.

With teams of threat actors working around the clock to target global retailers, the company required in-depth, real-time insight into network traffic, user behaviors, system configurations, and application activity. It needed the ability to investigate, identify, and contain potential threats within minutes—not months, weeks, or even days.

To mitigate risks and exposures, the company required:

- Threat intelligence enrichment that automatically detects potential malicious domains that warrant further investigation
- Full visibility into all resources across its environments, both active and inactive, to identify potential vulnerabilities
- Mapping of external threats to incidents impacting its network
- Proactive threat hunting to seek out advanced threats
- A faster, more efficient way to investigate and respond to incidents

Bottom line? The retailer required a modern security solution it could deploy on thousands of endpoints, as quickly as possible.

SOLUTION

Greater visibility empowers teams and enables faster threat response

After evaluating several different security vendors, the company chose Palo Alto Networks with its integrated Cortex portfolio, including Cortex XDR, Cortex XSOAR, Cortex Xpanse, and Unit 42 Managed Threat Hunting (MTH). Together, these solutions form a robust foundation for security intelligence and preparedness.

True to its goal, the team was able to deploy Cortex XDR on several thousand endpoints within the first week. To say that it provided a different experience from the company's former environment is an understatement.

The security and compliance program manager recalls: "It was like turning on the firehose and going: 'Wow, there's all this stuff we didn't know.' It was very notable. Once [Cortex XDR] makes connections and learns what matters and what doesn't, you get a lot better results."

In the past, it could take the team up to a month to get to the root of the problem. With Cortex XDR, the company is immediately notified of any potential security issues, allowing them to respond faster.

To avoid being overwhelmed, they quickly set up automated daily threat reports, alert management, and endpoint detection. The team is now able to focus on what really matters, and has gained new levels of control and visibility.

> We deployed XDR very quickly, it was a breeze. We did it in just one day."
>
> **— Security & Compliance Program Manager**

Smart automation makes a small team more powerful

With a security team of only three people, task automation was a must. That's where Cortex XSOAR came in. Previously, email impersonation alerts consumed a great deal of the company's time. Team members had to manually make lists of potential malicious IP addresses and URLs, create tickets, and send details to the firewall admin. With XSOAR, they can handle the entire workstream in a single click.

"It's now automated, which is awesome. We've got that playbook running really well," says the company's data analyst. With XSOAR enriching threat intelligence indicators, they can automatically identify potential malicious domains and update the firewall to keep them out.

Next up on their automation roadmap? The team plans to automate employee onboarding and offboarding. "Our provisioning process to date has been completely manual," says the security and compliance program manager. "There are certain things that XSOAR has the ability to automate much more richly, simply because of where it sits in the stack."

Cortex XSOAR makes it very easy for the company to customize and unify its intelligence. With a vast ecosystem of over 1,000 security tools (and growing), possibilities for integrations are endless.

> One of the things I really like about XSOAR is ... for a product that is put out by a major player in the security space, it plays really nicely with others."
>
> **— Security & Compliance Program Manager**

New capabilities uncover assets past their prime

After multiple acquisitions, the company's IT environment had expanded—but its visibility had not. Cortex Xpanse enabled the team to identify potential risks and discover legacy assets and services it was previously unaware of and no longer needed. As a result, it was able to decommission outdated solutions and realize significant cost savings.

Going forward, the company will continue to use this active discovery feature to identify, prioritize, and remediate risks from unknown or unmanaged assets. "Xpanse will become a lot more useful because it can give us a lot more targeted, accurate information about things we're going to keep around and spend time on," says the security and compliance program manager.

With Cortex Xpanse Active Response, the company will not only be able to identify unknown risks but proactively fix them using automation.

Proactive threat hunting creates a stronger security posture

With threats and threat actors evolving at a rapid pace, the team not only needed to know what to look for but required a substantial amount of time and resources to proactively track them down. Recognizing its limited capacity, the team engaged Palo Alto Networks Unit 42 Managed Threat Hunting (MTH) service.

> I really appreciate the proactiveness of the service. When you hear a lot of noise about a new vulnerability, Unit 42 lets you know whether you're impacted or not—just having that reassurance is really valuable."
>
> **— Security & Compliance Program Manager**

The team also uses Unit 42 MTH as a second set of eyes when it's nearly certain—but not quite—about a particular threat. Having external validation gives the team the confidence needed to take the next step.

Team members look forward to the weekly threat report from Unit 42, which they combine with Cortex XDR data and roll up to leadership, giving the board reassurance that they've got things handled.

RESULTS

A transformational solution delivers peace of mind

With solutions from Palo Alto Networks, the retailer has made significant leaps in its security management and operations, accomplishing far more without expanding its security team.

Not only did its false positives drop while mean time to respond (MTTR) shortened, but it now has fewer disparate tools to manage. The company has simplified its security stack while reducing complexity and eliminating time-consuming manual tasks—improving the day-to-day workflows for everyone on the small team.

> Palo Alto has probably been the best vendor I have ever worked with. I don't give that praise lightly. Whenever and whatever I needed support for, they've been there. And it's been very proactive. When there are obstacles, they get knocked out of the way really quickly."
>
> **— Security & Compliance Program Manager**

The team can now identify verified threats faster, across locations and environments. Thanks to expanded visibility and insights from Unit 42 MTH, team members can report back to business leaders and board members with confidence.

What about the cybersecurity insurance findings that launched the company on this journey? After deploying the robust suite of solutions from Palo Alto Networks, the company was able to provide completely different answers in its yearly review cycle than it had before. As a result, instead of increasing the company's insurance premiums, the insurer reduced premiums by 30%.

Today, with a solid security foundation in place and a trusted partnership with Unit 42, the company has the peace of mind and confidence it needs to continue growing the business.

> This process has been transformational for us. It's like going from wandering around the desert to walking into the city and having Times Square in front of you."
>
> **— Security & Compliance Program Manager**

Learn more about Cortex XDR, Cortex XSOAR, Cortex Xpanse, and Unit 42 Managed Threat Hunting on our website.

paloalto NETWORKS

3000 Tannery Way
Santa Clara, CA 95054

Main: +1.408.753.4000
Sales: +1.866.320.4788
Support: +1.866.898.9087

www.paloaltonetworks.com