ADT locks down cyberthreats with best-of-breed security

RESULTS

99.997%

reduction in data volumes

92%

of alerts resolved automatically

From days to 3 hours

faster resolution of threats

Solution

- Consolidate security platforms with a single vendor.
- Take advantage of seamless integration.
- Leverage Palo Alto Networks' outstanding customer service.

Results

- Increase in operational efficiency.
- Able to protect against growing threats without expanding security team.
- Less time required for mundane tasks and more to focus on priorities.

Introduction

ADT was founded nearly 150 years ago as American District Telegraph. It used then-state-of-the-art technology, the telegraph, to provide security systems for an initial network of 50 customers in New York City. Today, ADT is a leader in home and business security. It serves more than six million customers with 17,000 employees working from 200 U.S. locations.

Today, ADT is a leader in home and business security. It serves more than six million customers with 17,000 employees working from 200 U.S. locations.

Trust is central to the company's brand. ADT applies that core value to its own security. The company's goal is to continually improve its security posture while increasing the operational efficiency of its security team.

"Our brand is trust; we're trusted to help protect what matters most to people," says Rick DeLoach, ADT Director of IT Security. "Maintaining that trust and integrity is paramount."

CHALLENGE

Modernize security, drive greater efficiency.

ADT's success and growth in recent decades have created new security challenges and a need to improve its security team's efficiency.

Modernizing the company's security platforms has been a persistent priority. Over time, ADT acquired a number of different security point products to protect aspects of the organization. This patchwork of products created training and operational headaches and drove up costs.

ADT also faced an ever-changing threat environment. The volume of attacks is increasing and the nature of the threat is constantly evolving. "I can't control how many bad guys wake up today and decide to attack ADT," DeLoach observes. "Ransomware wasn't on top of anybody's list four or five years ago. Threats five years from now probably won't be ones we're talking about today."

This has created the need for the security team to increase operational efficiency. Given the business climate, the ADT team needed to do more with the same level of resources, simplifying workflows and enabling automation to remove the burden of repetitive and time-consuming manual processes.

The legacy security products hampered this effort; even routine tasks required team members to spend time doing duplicate data entry. "We're already giving one vendor all our information," DeLoach explains. "Then we're duplicating that information to give to a second vendor. We're not creating any value; we're paying twice the price to duplicate 95 percent of the information."

ADT had a goal to modernize its approach to managing and securing its network–to be more intentional about driving Zero Trust across the organization–and ensuring 100 percent uptime for its branch locations.

Simplifying workflows also became a goal. As ADT grew and evolved, it increasingly needed flexible solutions capable of meeting a diverse set of needs. This included working in a multicloud environment and meeting the challenges of a hybrid workforce that arose during the COVID-19 pandemic.

Solutions to work smarter and accomplish more.

In short, ADT required solutions that would allow a small team to evolve and meet new, pressing security challenges. “How do we manage productivity and efficiency to do more?” DeLoach asks. “How do I ensure that productivity gains outpace the demand for data security, knowing that I don’t control any of the levers over that demand?”

ADT’s search centered on solutions that could address five key areas:

- Threat detection and response.
- Security operations management.
- Cloud security.
- Remote access for hybrid workers.
- Branch transformation.

"XSOAR has been our platform for eight or nine years now. It continues to drive efficiency and deliver wins every year."

Rick DeLoach

Director of IT Security, ADT

SOLUTION

Integrated products to achieve key goals.

When ADT first turned to Palo Alto Networks products, it sought an alternative to its existing firewalls that could be centrally managed and automated. The security team began adopting Next-Generation Firewalls (NGFWs), and added Panorama to realize operational efficiencies through simplified management and automation.

When Palo Alto Networks began releasing Cloud-Delivered Security Services (CDSS), ADT quickly adopted them, having seen the positive value delivered by the NGFWs. The company found great utility in the new services, which included WildFire® and Threat Prevention.

As ADT used the NGFWs and CDSS, it also found that the products helped to break down the silos between the company’s networking and security teams. This enabled better collaboration and more efficient internal processes.

While these Palo Alto Networks solutions helped ADT realize significant efficiencies, the security team knew additional opportunities could be gained by consolidating and simplifying their security product estate. “It was about centralized management, administration, and

efficiency," DeLoach says. "Palo Alto Networks presented very compelling products that allow us to do remote administration and management."

To help scale and modernize a lean security operations team, ADT turned to the Palo Alto Networks Cortex suite of products. Together, these products are helping the company focus staff on the most critical threats while enabling automation to assist with threat detection and response. The solutions the company deployed include:

- Cortex XDR supports ADT's threat detection and response and helps to scale its security operations team.
- Cortex XSOAR enables the team to reduce manual tasks and speed up investigation and response through automation.
- Cortex XSIAM accelerates security operations processes through automation, intelligent data, and analytics, enabling security analysts to focus on the most critical threat data.

"XSOAR has been our platform for eight or nine years now," DeLoach says. "It continues to drive efficiency and deliver wins every year."

As ADT has grown over the years, its cloud footprint has expanded. This has created a pressing need to secure a multicloud estate more consistently. The company adopted Prisma Cloud to meet that need and secure workloads across Azure, AWS, Google, and Oracle. The switch to Prisma Cloud gave ADT greater visibility and more accurate control over its cloud domains than it had with its legacy solutions.

To ensure secure access to critical applications and data for its employees, wherever their location, ADT is also implementing Prisma Access. By replacing aging networking hardware with Prisma SD-WAN, ADT can achieve a unified SASE solution to modernize its approach to integrating security and networking.

All these capabilities are reinforced by a Palo Alto Networks Unit 42® Retainer. The Retainer places Unit 42 incident response experts—who are well-versed in ADT's environment and Palo Alto Networks solutions—on speed dial to respond quickly should an incident occur. Unit 42 Retainer credits can also be used to improve ADT's cybersecurity program with assessments and other proactive services.

RESULTS

Palo Alto Networks has become more than just a security vendor for ADT; it's now a trusted partner helping the company secure its data and that of its customers. Palo Alto Networks provides outstanding customer support and works closely with ADT whenever a problem arises.

Benefits of the unified security platforms include:

Increased efficiency

Adopting integrated Palo Alto Networks solutions has increased operational efficiencies dramatically. Redundant point solutions have been eliminated, and the mean time to resolution has significantly decreased. Previously, resolving issues took an average of several days. Now, the team can effectively address them in just 3.3 hours. “For the past four years, we’ve consistently seen significant, doubledigit efficiency gains year over year,” DeLoach says. “That’s driving efficiencies back into the business so we can do more.”

By slashing data volume by 99.997%, XSIAM unlocks unprecedented efficiency. It enables ADT to ingest a massive 9 billion events, transforming them into a manageable number of correlated incidents for further analysis.

Team members no longer have to learn to use multiple products from different vendors; this reduces onboarding time. Because the Palo Alto Networks products are integrated, the security team spends far less time on mundane data administration tasks or costly custom integrations. By automating repetitive manual tasks, the team has been freed to focus on higher-priority needs. An impressive 92% of incidents are now auto-resolved, significantly reducing alert fatigue. This enables ADT to meet expanding threats with existing resources.

“It feels really harmonized at this point,” DeLoach says.“The portfolio set feels very cohesive and anchors around holistic solutions to the security problems.”

Focus on threats

ADT has found that unified Palo Alto Networks solutions do a better job of identifying real threats. Adding Cortex XDR, in particular, has meant the “accuracy and simplicity that we came to expect in managing the NextGeneration Firewalls is there for endpoint security, too,” DeLoach notes.

The new solutions don’t require as much investigation of false positives by triggering a report criteria. “It’s really anchored to, ‘What is an alert?’” says DeLoach, and “‘How do I bubble up a contextualized, holistic timeline and artifact set?’ That’s fundamentally different from a report that means you have to run a bunch of additional queries to piece together another report.”

"For the past four years, we’ve consistently seen signif

significant, double-digit efficiency gains year over year. That’s driving efficiencies back into the business so we can do more."

Rick DeLoach

Director of IT Security, ADT

Strategic partnership advances mission of security.

By selecting Palo Alto Networks as its strategic security partner, ADT can be confident in its ability to counter growing security threats and provide high-performing connectivity. It can scale its security operations to meet the needs of the business and its customers.

The Palo Alto Networks platforms for network security, cloud security, and modern SOC management are enabling ADT to advance its mission of securing what matters most, while supporting the company's growth. "The interplay of technology and process enablement from the Palo Alto Networks suite has been what's allowed us to operate at the efficiency level we do," DeLoach says.

The combination of performance, superior product features, and unparalleled customer service has made a believer of ADT security leaders. DeLoach says he's willing to "preach from the rooftops" about the exceptional support ADT gets from Palo Alto Networks.

"If there's something wrong, Palo Alto Networks doesn't deflect; they jump in and help. I'll say that's not the norm for vendors who treat security as transactional. It's what you get in a real partnership."

Find out more about how Palo Alto Networks best-in-class solutions can improve networking and security for your organization. Additional information
info@eccoamerica.com

.