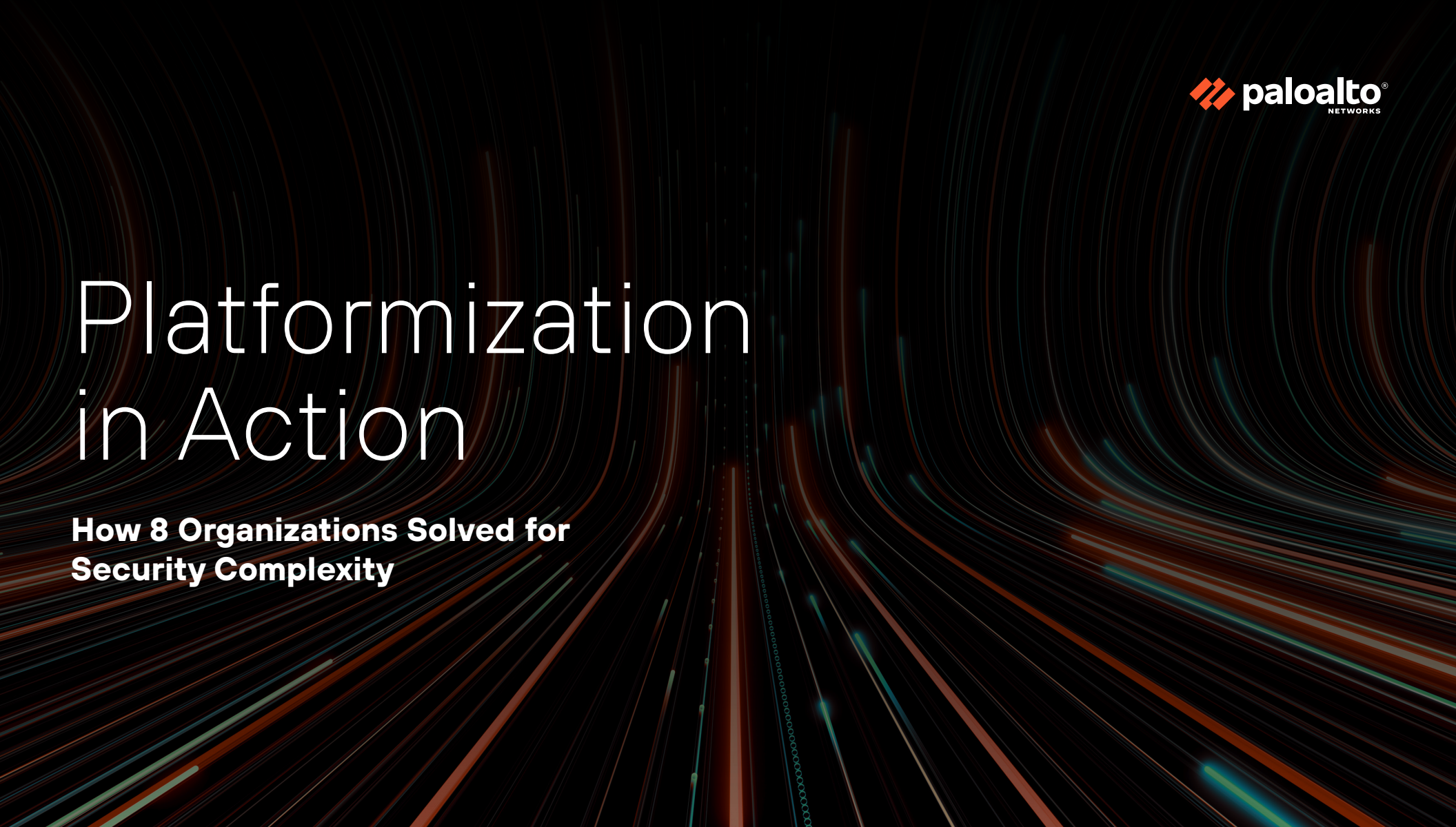

paloalto
NETWORKS
Platformization
in Action
How 8 Organizations Solved for
Security Complexity

From chaos to control

Imagine a large construction project with multiple contractors—each skilled but with its own tools, materials, and blueprints. Coordinating efforts would be formidable, delays inevitable, and safety compromised.

That's what cybersecurity is like today. Recent research from the IBM Institute for Business Value and Palo Alto Networks® shows that enterprises are juggling an average of 83 security solutions from 29 different vendors, resulting in a tangled, expensive mess that frustrates teams and compromises security.

It's time for a better approach: security platformization.
Much like unifying construction under a single general contractor with standard equipment and procedures, platformization simplifies operations, eliminates redundancies, and reduces risk.

ORGANIZATIONS WITH DISPARATE TOOLS

52%

of executives cite complexity as the #1 obstacle to effective cybersecurity

ORGANIZATIONS WITH A PLATFORM APPROACH

96%

of security executives in platformized organizations see security as a source of value, compared to only 8% in nonplatformized organizations

All material on this page is sourced from *Capturing the cybersecurity dividend: How security platforms generate business value*, IBM Institute for Business Value and Palo Alto Networks, 2025.

What's the path to platformization?

The drive for platformization is unique for every organization, though it often includes a need to rein in complexity, reduce backlogs and burden, scale security to new areas, and/or strengthen defenses. Whatever the incentive, platformization tends to happen in one of three ways: step-by-step over time, building from scratch, or going deep in one area.

In the following pages, you'll find the stories of eight customers who have platformized with Palo Alto Networks.

Step-by-Step Platformization

Adding Capabilities as Needs Evolve and Time Allows

Platformization as One Initiative

Adopting Multiple Solutions at the Same Time

Focused Platformization

Establishing a Platform in One Realm of Protection

COLGATE-PALMOLIVE

Colgate-Palmolive raises the standard for secure manufacturing

Industry
Consumer packaged goods

Location
Multinational

Size
34,000 employees

The CISO sets out to simultaneously improve the company's posture and make security an enabler of the business.

THE RESULTS

6
tools consolidated in a single console for incident investigation

900
applications enhanced with better performance

200K+
threats blocked per month on average

"I sleep better at night knowing that Palo Alto Networks is there to support our organization. Whether it's our Security Operations Center, our network, or our connections to the internet, we know Palo Alto Networks solutions are there to protect us."

– Alexander Schuchman, CISO, Colgate-Palmolive

THE CHALLENGE

Establish consistent security and connectivity everywhere.

- Secure operational technologies at manufacturing sites to the same standard as IT within offices
- Enhance performance for critical applications across manufacturing and business sites
- Provide visibility and consistent security to support employees working from anywhere
- Improve the efficiency and efficacy of the security operations center (SOC)
- Drive greater collaboration between teams and eliminate redundant solutions

THE SOLUTION

Bring tools, teams, and processes together with platformization.

The organization platformized with Palo Alto Networks across network security, remote access, and security operations to reduce complexity, ensure consistent protection, and enable line-of-business employees to be as collaborative and productive as possible from wherever they work. The approach increased collaboration between security and networking teams to ensure critical manufacturing sites remained operational and hardened against cyberthreats.

STEP-BY-STEP PLATFORMIZATION

IT and OT network segmentation

PA-Series Firewalls

Deployed at factories, corporate offices and data center

Advanced security treatment

Cloud-Delivered Security Services

Advanced Threat Prevention, Advanced URL Filtering, WildFire®

Branch transformation

Prisma® SD-WAN

Application uptime, resiliency and troubleshooting

Secure remote access

Prisma® Access

Secure connectivity for remote locations and users

SOC automation

Cortex XSOAR®

Playbooks for automated incident response

READ THE FULL STORY

Schnucks

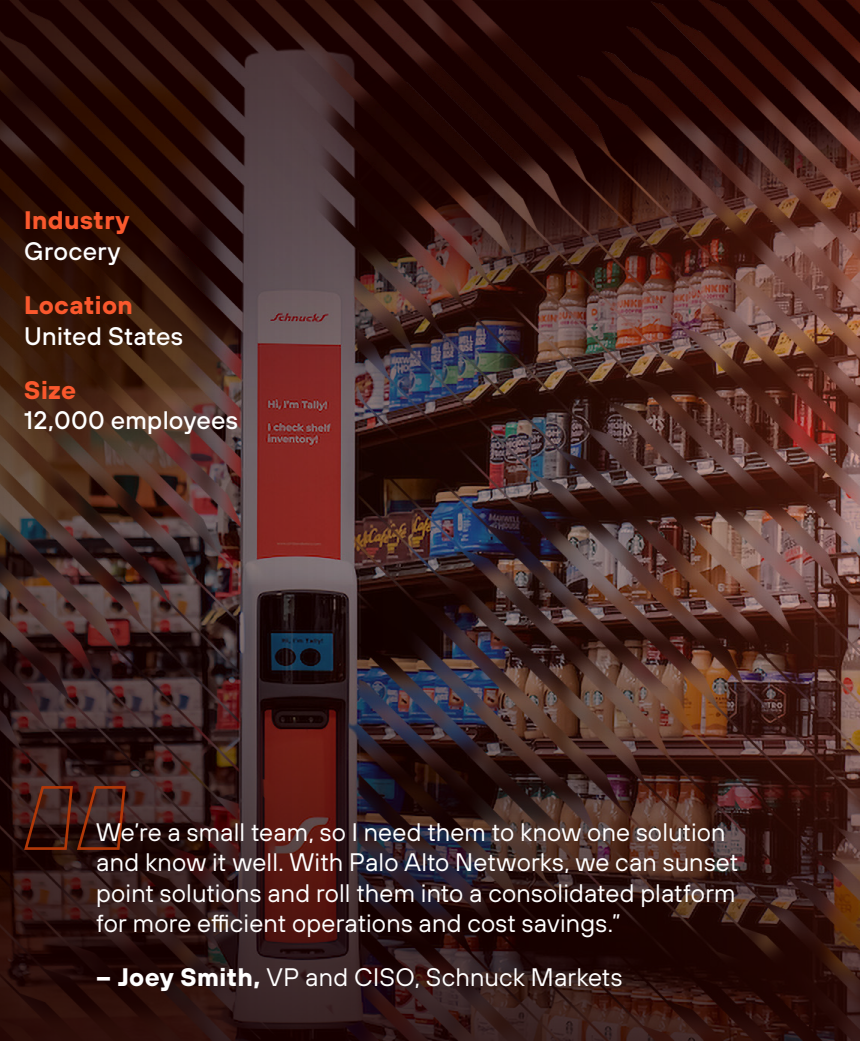
Schnuck Markets secures an innovative advantage

Forbes' "Most Innovative Grocer in America" builds a foundation to enable cybersecurity transformation.

Industry
Grocery

Location
United States

Size
12,000 employees



THE RESULTS

>1M
threats blocked in 30 days

>300
malware attacks prevented in a year

Significant savings
realized with a platform approach

> We're a small team, so I need them to know one solution and know it well. With Palo Alto Networks, we can sunset point solutions and roll them into a consolidated platform for more efficient operations and cost savings."
>
> **– Joey Smith,** VP and CISO, Schnuck Markets

THE CHALLENGE

Tool up to meet the modern security challenge.

- Optimize and streamline the security stack
- Increase visibility into the company's endpoints, network, and IoT devices
- Improve detection and protection against unknown threats
- Eliminate disruptive, expensive security incidents that diminished trust

THE SOLUTION

Scale security and streamline costs through platformization.

Platformizing with Palo Alto Networks, Schnucks not only strengthened IT security and optimized operations but also built a foundation that enabled this transformation. Taking a unified platform approach has been essential to keeping the business running as budgets tighten across the retail grocery industry.

STEP-BY-STEP PLATFORMIZATION

Securing offices, storefronts, and warehouses

PA-Series Firewalls with Cloud-Delivered Security Services

IoT visibility and control

IoT Security

Devices such as shelf-scanning robots and electronic shelf labels (ESLs)

Extended detection and response

Cortex XDR®

Replacing legacy AV software and preventing business disruptions

Incident response and cyber risk expertise

Unit 42® Retainer

Experts on call to handle any cybersecurity event

Cloud-native application protection platform

Prisma® Cloud

Holistic visibility into cloud security posture with data security at every layer

READ THE FULL STORY

Informatica

Informatica builds a secure cloud and AI foundation

Through continued growth, the company safeguards customer data, operates resiliently, and earns trust.

Industry
High technology

Location
Multinational

Size
5,000 employees

THE RESULTS

85%
reduction in security alerts

96%
reduction in cloud security point products

Speed to market
through FedRAMP-certified products

"As a SaaS company, the security of our cloud infrastructure is paramount. Palo Alto Networks showed us that we could trust them to secure multiple areas of our business."

– Jatinder Singh, Head of Product Security, Informatica

THE CHALLENGE

Consolidate security to reduce complexity and risk.

- Ensure security of cloud workloads, cloud-native app development, and app hosting
- Meet FedRAMP compliance requirements to attract new federal customers
- Simplify management and free security teams from repetitive manual tasks
- Provide a framework for secure AI app development

THE SOLUTION

Improve security solutions to support new cloud investments.

By taking a unified platform approach across network, cloud, and endpoint security, Informatica achieved greater automation and speed to market. FedRAMP-certified solutions massively accelerated Informatica's journey to serve federal customers, which it intends to build on with more advanced security controls in the future.

STEP-BY-STEP PLATFORMIZATION

Securing corporate offices

PA-Series Firewalls

Network security for 34 sites and a data center

Endpoint security

Cortex XDR

Customer-facing and corporate environments

Cloud-native application protection

Prisma Cloud

Across AWS, GCP, Azure, and Oracle workloads

Advanced security treatment

Cloud-Delivered Security Services

- Threat Prevention
- WildFire
- URL Filtering

Branch connectivity

Prisma SD-WAN

Application reliability and performance

READ THE FULL STORY

Grupo Bimbo protects its global supply chain

The $20B company safeguards food production worldwide with simple, connected Palo Alto Networks platforms.

Industry
Food manufacturing

Location
Mexico

Size
139,000 employees

THE RESULTS

2x
the insurance coverage with no increase in premium

1 hr
mean time to resolution reduced from days

$100K
in monthly connectivity cost savings in one country alone

"Our focus is on bread, not security. Palo Alto Networks helps preserve Grupo Bimbo's financial advantage by making the business more agile, flexible, and reliable. Protecting the global infrastructure with one common, simple platform means we can focus more resources on our sales, customers, and growth."

– Erwin Campos, CISO, Grupo Bimbo

THE CHALLENGE

De-silo platforms to securely serve millions daily.

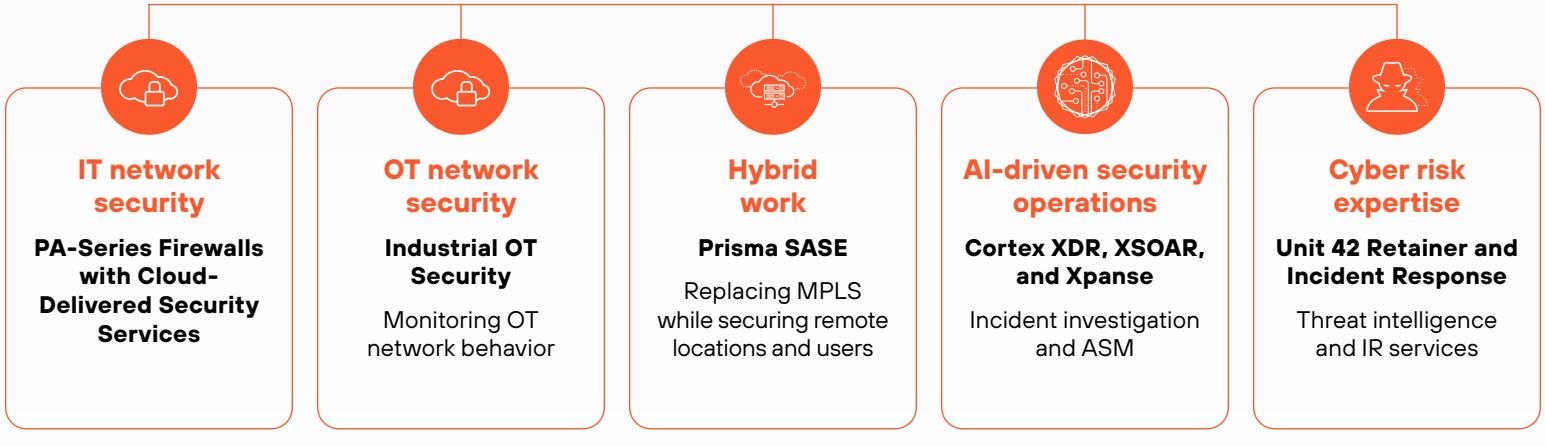
- Siloed platforms were increasing risk, reducing productivity, and raising operational costs
- The attack surface needed reduction without impacting performance or hybrid-user experience
- To minimize production downtime, IoT networks had to be protected from cyberthreats

THE SOLUTION

Unite the company's cloud-centric future on standard, scalable platforms.

Grupo Bimbo standardized on simple, comprehensive Palo Alto Networks platforms—a strategy so resilient that the company's insurers doubled coverage without raising the premium. As a result, the organization is driving down risk, reducing complexity, and automating multiple security processes. This platformization strategy leverages breakthroughs in artificial intelligence, analytics, automation, and orchestration to protect the organization worldwide across multiple clouds, networks, and mobile devices.

PLATFORMIZATION AS ONE INITIATIVE



READ THE FULL STORY

Cordis

Cordis rebuilds cybersecurity to protect patient data and block emerging threats

After a split from its parent company, the medical device pioneer engineers its security framework from the ground up.

Industry
Medical device manufacturing

Location
Global

Size
3,500 employees

THE RESULTS

40%
savings across its full security stack over 3 years

<24 hrs
to investigate and identify a potential vulnerability

500K
threats blocked in 30 days

"Palo Alto Networks is the only solution that gives you a comprehensive security platform with a unified approach, and also gives you benefits down the road."

– Robert Wines, CISO, Cordis

THE CHALLENGE

Strengthen compliance and resilience to threats.

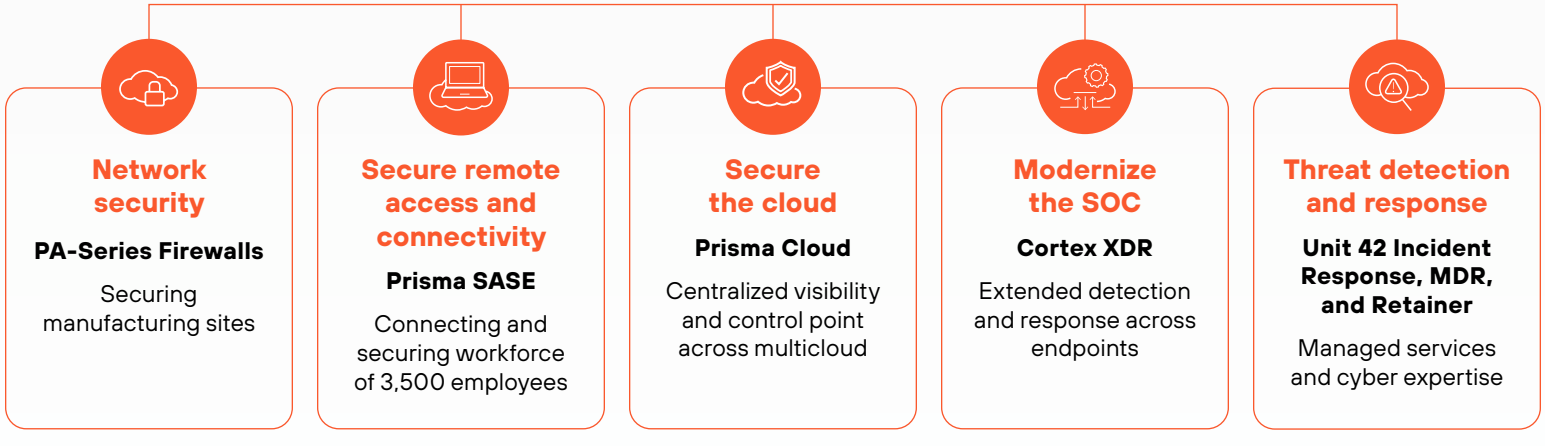
- Network security infrastructure and solutions needed to be fully functional within six months
- New solutions had to comply with healthcare security standards, including those set by the FDA and NIST
- The solution needed to scale across a diverse on-prem and multicloud environment and a dispersed hybrid workforce
- Security operations had to be modernized and scalable, making it easier for a small IT team to keep up and respond to threats in a timely manner

THE SOLUTION

Unify on platforms backed by strong partnership.

By selecting the Palo Alto Networks unified security platforms, Cordis IT and security teams gained comprehensive visibility and the ability to more consistently enforce security across the entire organization. The integrated value of the platform approach is also paying dividends: Cordis will see savings of more than 40% over three years across its security stack.

PLATFORMIZATION AS ONE INITIATIVE



READ THE FULL STORY

cbts

CBTS delivers IT transformation, internally and for its clients

Leadership sets out to strengthen security, reduce complexity, and embrace automation and AI with a single security partner.

Industry
IT services

Location
United States

Size
2,400+ employees

THE RESULTS

13 seconds
median time to resolution, reduced from days

100%
incident close-out rate

20
SOC tools consolidated to 1

80%
increase in visibility into network traffic

"The platform approach—having all the data in a single place with all those integrations, plus the AI capabilities—has been a game-changer. It's enabled me to keep my headcount flat and to have our team focus on the more high-value strategic pieces of keeping our business safe."

– Chris DeBrunner, VP of Security Operations, CBTS

THE CHALLENGE

Facing high stakes, burdened by legacy.

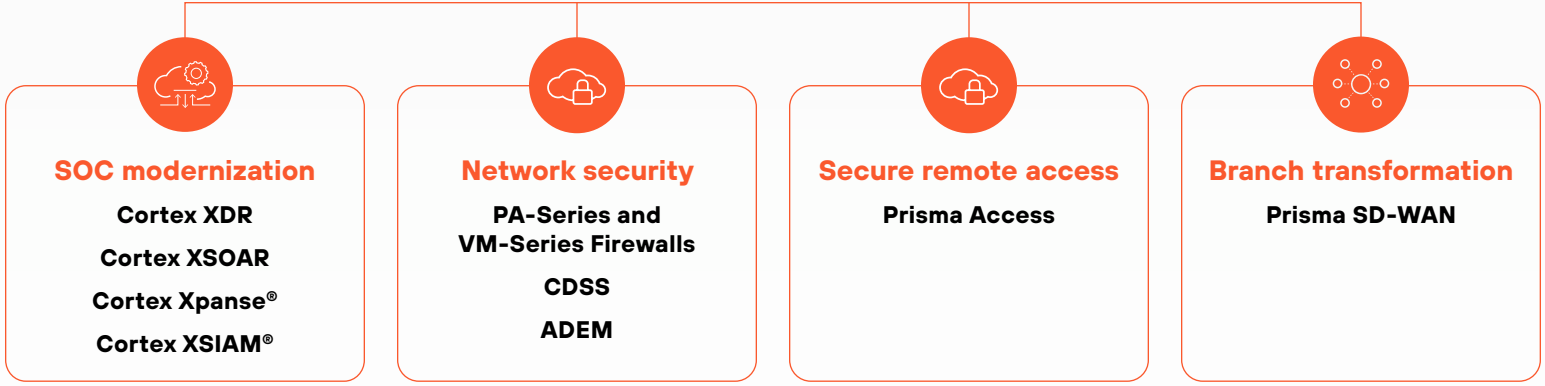
- The risk of exposing customer data was extremely high, given the organization's role as a managed security service provider (MSSP)
- A lack of automation and visibility from a complex mix of security products was reducing speed and effectiveness in detection and response
- A Zero Trust infrastructure was impossible to build with existing point security tools and would have required unattainable resources to become viable

THE SOLUTION

A complete transformation of enterprise security.

From network security to data protection, endpoint security, vulnerability management, identity management, and a SIEM, CBTS adopted a platformization strategy from Palo Alto Networks. This strategy allowed CBTS to strengthen security and visibility while reducing complexity and inefficiency.

PLATFORMIZATION AS ONE INITIATIVE



READ THE FULL STORY

AUTODESK

Autodesk modernizes network and security architecture with SASE

With a boost from automation, the software leader achieves secure, high-performing connectivity for its anywhere workforce.

Industry
Design software

Location
United States

Size
14,100+ employees

THE RESULTS

60+
global offices migrated to Prisma Access

3x
network transfer speed improvement

85%
increase in remote network availability

"This implementation underscores Autodesk's commitment to leveraging technology to enhance operational efficiency and scale as we grow."

– **Prakash Kota,** SVP and CIO, Autodesk

THE CHALLENGE

Improve app performance and user experiences.

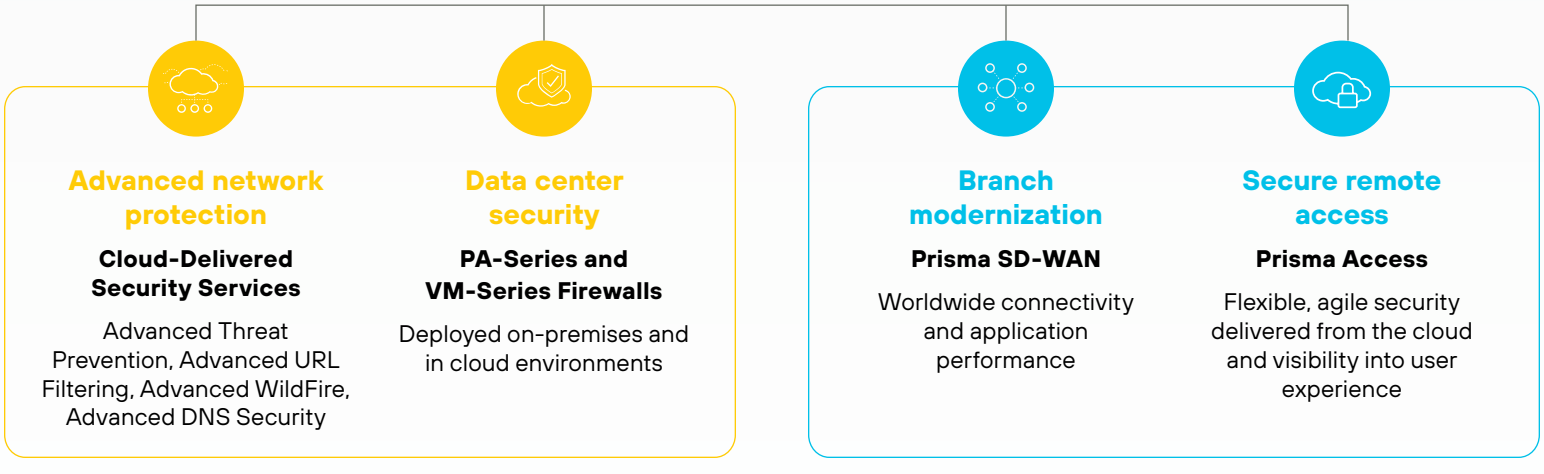
- 80% of the applications employees accessed over the network were SaaS-based, requiring consistent policies and flexibility.
- Traditional VPN solutions were difficult to scale and didn't allow for quick access to data centers and cloud workloads
- Managing multiple on-premises VPN solutions was challenging for IT and complex for users
- Routing SaaS traffic back to the data center slowed app performance

THE SOLUTION

Leverage AI-powered SASE to boost network performance.

Autodesk's IT team saw an opportunity to modernize network and security architecture by migrating to a SASE solution, consolidating networking and security in a single platform. As a Prisma SD-WAN customer, the company realized it could easily adopt Prisma Access to unify security services across all firewall form factors. After piloting the solution, Autodesk rolled out Prisma Access company-wide—to 60+ campus offices in under seven months—and retired its on-premises VPN solutions.

PLATFORMIZATION ACROSS NETWORK SECURITY



READ THE FULL STORY

NORTH Dakota | Information Technology
Be Legendary.

North Dakota IT safeguards citizens with integrated, AI-driven security operations

Industry
Government

Location
United States

Size
15,000 employees/
800,000 citizens

Leadership unifies IT services across the state and builds a modern SOC on a Palo Alto Networks platform.

THE RESULTS

99.6%
decrease in open alerts, from 16,000 to ~50

60%
of total incidents are resolved automatically

Minutes
to find a true positive, down from weeks

> The Cortex portfolio has really helped our SOC mature. With so many threats coming in, having that toolset has really been a big benefit for us."
>
> **– Michael Gregg,** CISO, North Dakota IT

THE CHALLENGE

Rein in costs while fighting sprawl.

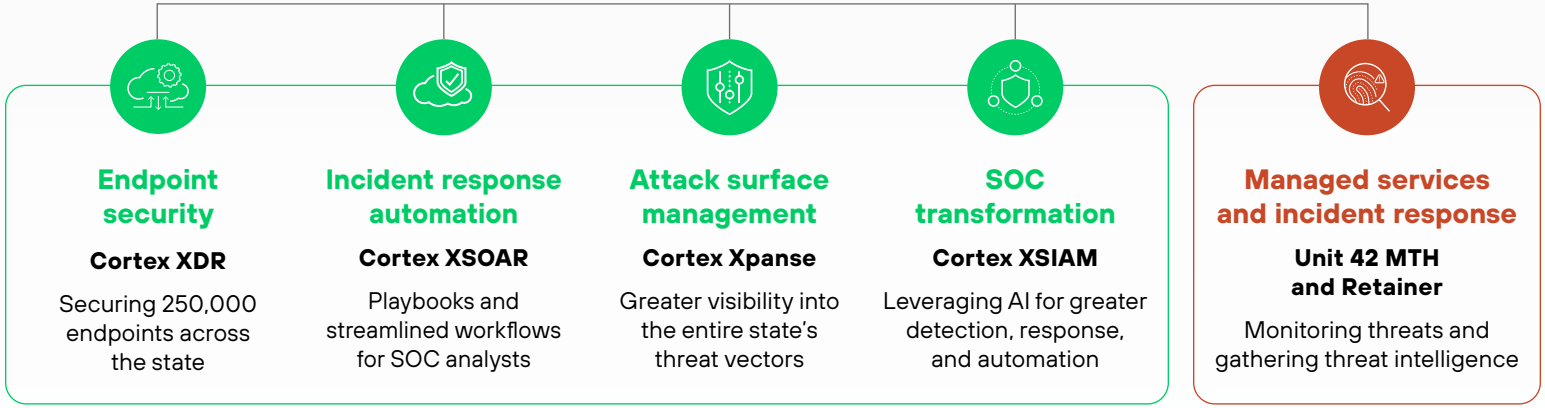
- Scale security from 20,000 endpoints to 250,000 without increasing security staff
- Unify over 600 state entities, overcoming siloed security tooling and unique processes
- Enable broad and granular visibility of the threat landscape, statewide or at a single entity
- Reduce the burden of handling tens of thousands of daily incidents for security operations staff
- Strengthen and accelerate detection and response to cyberthreats

THE SOLUTION

Accelerate security response and optimize IT spend with a platform approach.

NDIT platformized with Palo Alto Networks to provide the foundation for its next-generation SOC. After nearly 15 years as a Next-Generation Firewalls customer, NDIT moved to Cortex®, enhancing detection and response, reducing manual tasks through automation, and increasing employee retention. Prisma Cloud delivers a centralized view of the state's cloud assets, enabling better management of security posture across various cloud services.

PLATFORMIZATION ACROSS SECURITY OPERATIONS



READ THE FULL STORY

Experience the benefits of platformization at your own organization

Like the organizations featured above, you can transform unwieldy cybersecurity sprawl into streamlined control. An integrated platform approach from Palo Alto Networks enables you to gain strength, clarity, responsiveness, and efficiency.

Simplify your tools: Condense and unify solutions. Bring data together for centralized visibility. Scale cyber infrastructure without adding resources.

Slash your risk levels: Proactively monitor, analyze, and prevent sophisticated threats in real time to enable secure growth and innovation.

Unburden your team: Enable better, faster security—and reduced manual labor—with an integrated suite of battle-tested, AI-driven products.

It begins with a conversation.

START HERE

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