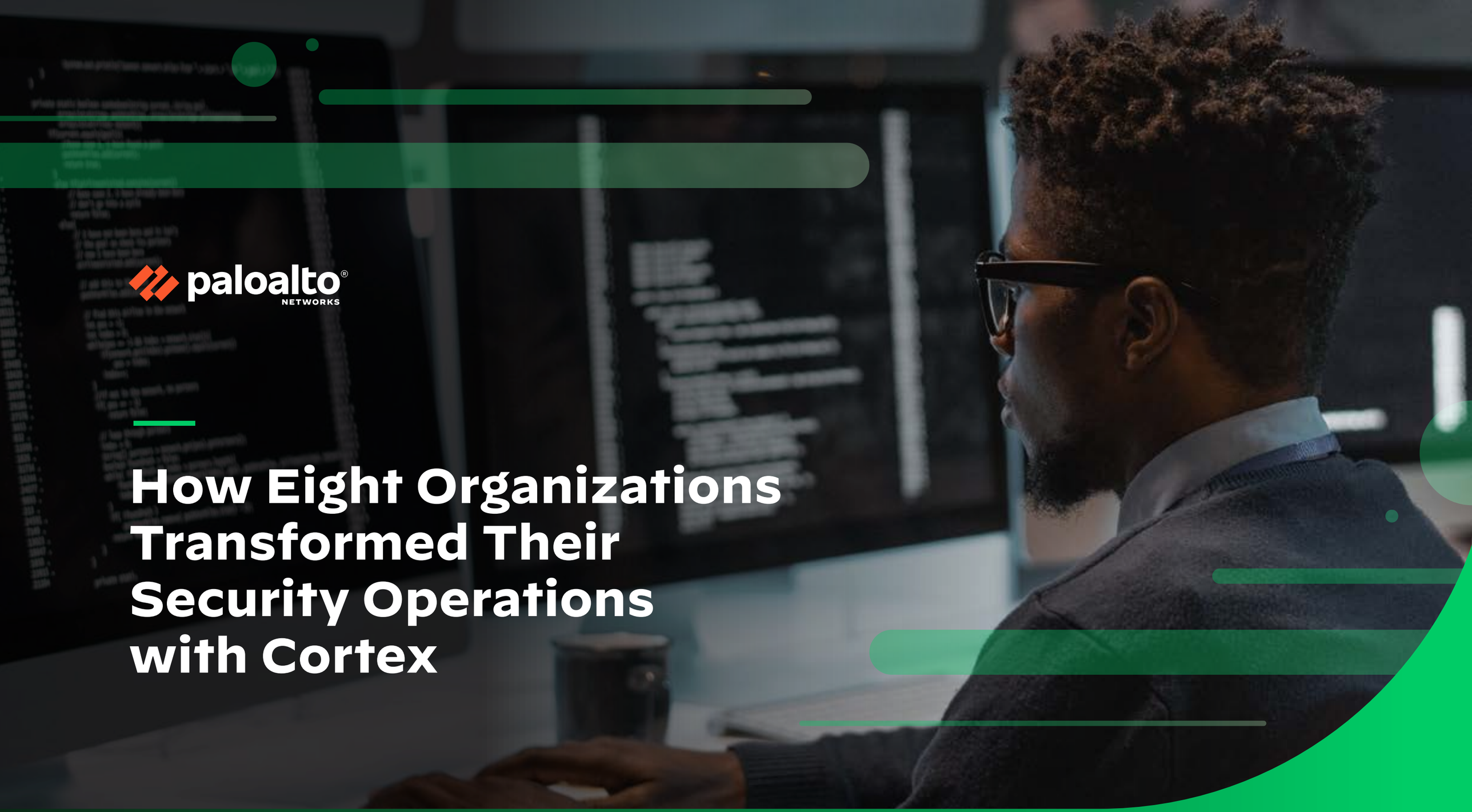


How Eight Organizations Transformed Their Security Operations with Cortex

PREFACE

Tomorrow's SOC today

We've entered into a time in which people can't keep up with cybersecurity.

It doesn't matter how big the SOC team is, or how brilliant its members are. There's no way for people to respond fast enough to stop an attack in progress.

We need AI—the right models, the right resources, and the right data—to automate cybersecurity so we can handle the volume and sophistication of the threats seen on our networks today.

That's why we built Cortex—a new vision for cybersecurity designed to shorten the time it takes to detect and respond to security threats from days to seconds.

As you'll see in this e-book, customers who use Cortex elevate their SOC teams and improve their results, all while making security more visible, comprehensive, and future-ready.

We're pleased to partner with these organizations as their security provider, and we're grateful to them for the opportunity to tell their stories here.

paloalto NETWORKS

SNAPSHOT ONE: STATE OF NORTH DAKOTA

A future-proof SOC for the public sector

The State of North Dakota is committed to providing its citizens with access to technology. To support this mission, North Dakota Information Technology (NDIT) provides security to every government entity, from urban centers to rural regions. The scale and complexity of this network rivals that of a Fortune 30 company, making security as much of a challenge as it is a priority.

Industry
Public sector

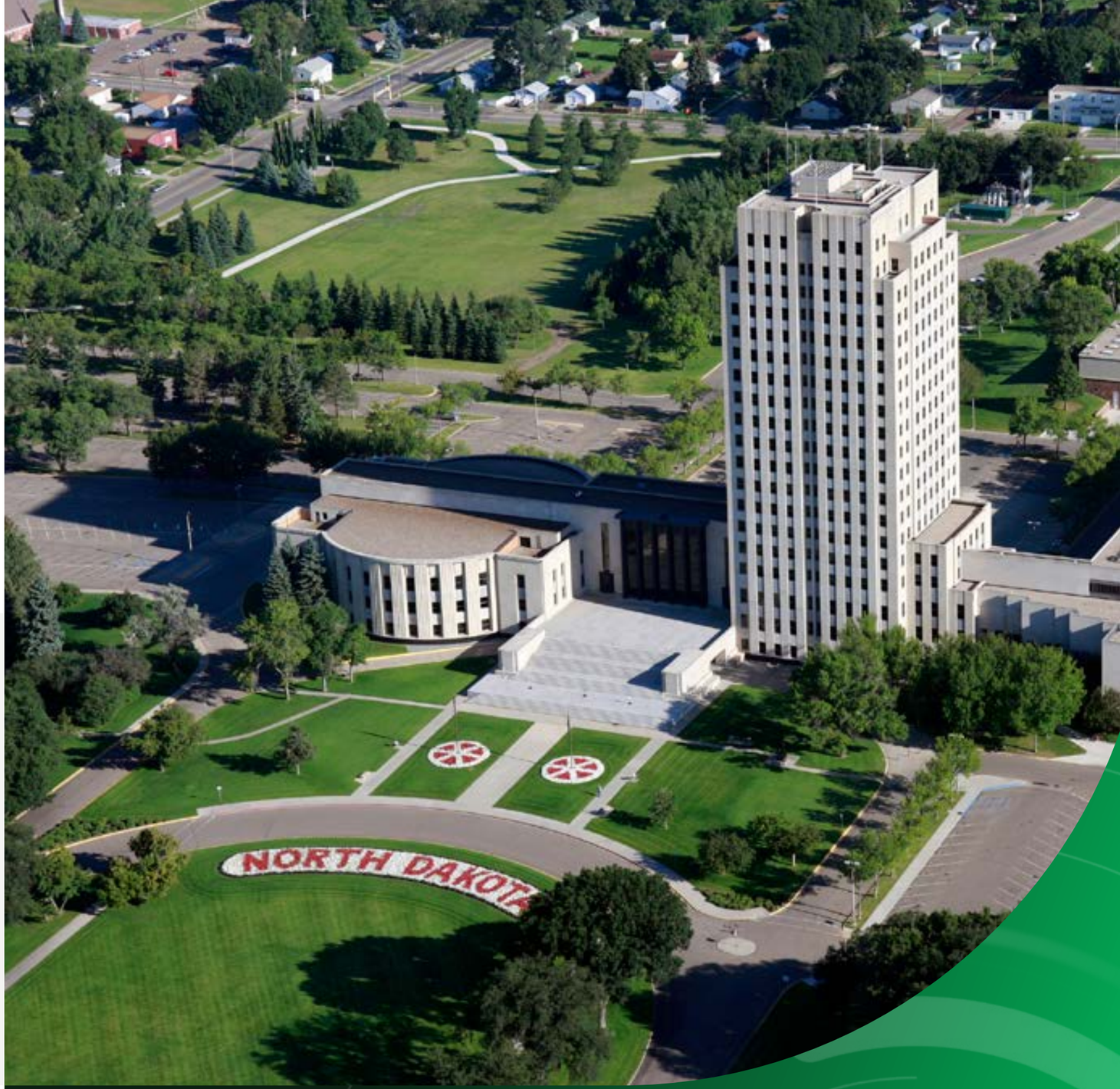
Country
United States of America

Website
www.ndit.nd.gov

800K+
CITIZENS

1,600+
CITIES AND TOWNSHIPS

183
INDEPENDENT SCHOOL DISTRICTS



NDIT has become a model for successful security operations in the public sector, delivering automated, proactive protection to the state's citizens and agencies with no major incidents.

> We now operate with about half the resources as a similarly sized Fortune 30 company. That's come about through automation and revising playbooks to use machine learning. This allows the SOC team to focus on high-priority tasks that add value to the business."

— Michael Gregg, Chief Information Security Officer, North Dakota Information Technology

The Challenges

With hundreds of thousands of users, thousands of integrations and applications, and innumerable endpoints, NDIT needed to plan, design, and build its own SOC that could work across systems with unparalleled efficiency.

+ Increasingly sophisticated cyberattacks threatened both citizen data and agency operations.
+ Needed an integrated solution to manage threat detections that doubled to 4.5 billion in 2021.
+ The solution needed to be scalable, comprehensive, and future-ready.

The Solution

NDIT partnered with Palo Alto Networks to build its SOC over a three-year period. Incorporating the complete Cortex product portfolio, including Cortex XDR, XSOAR, and Xpanse, provided a comprehensive foundation for endpoint security, task asset discovery, and workflow automation.

+ A unified framework improves first call resolution and reduces mean time to respond (MTTR).
+ Shift of 2.17 FTE's work to systems in the background, freeing team members to focus on high-priority analysis and threat remediation.
+ A more transparent organizational structure, mapped to National Institute of Standards and Technology frameworks.

SNAPSHOT TWO: HEALTHPARTNERS

Reinventing security at a healthcare leader

HealthPartners, based in Bloomington, Minnesota, is an award-winning integrated healthcare system providing both clinical services and a health plan. Its mission is to improve the health and well-being of members, patients, and the community. The largest consumer-governed nonprofit in the U.S., with 25,000 employees, HealthPartners serves 1.8 million medical and dental members. Its clinical services include a multispecialty group practice of approximately 1,800 physicians who care for more than 1.2 million patients.

HealthPartners

Industry
Healthcare

Country
United States of America

Website
www.healthpartners.com

25K	1.8M	1,800
EMPLOYEES	MEMBERS	PHYSICIANS

paloalto NETWORKS

Cortex accelerates HealthPartners' digital initiatives by empowering the SOC to eliminate vulnerabilities proactively, automate detection and investigation, and focus staff time on the small fraction of threats that require manual intervention.

> Because of the consistency and high percentage of true positives we get from the Palo Alto Networks platform, we have the confidence now to automate threat mitigation. That's something we've never had the opportunity to do until now."
>
> **— Joel Pfeifer, Principal Security Analyst, HealthPartners**

The Challenges

With cyberattacks constantly threatening private patient data from both clinical services and the health plan, HealthPartners needed to improve its overall security solution—without investing significantly in new hardware.

+ Legacy firewalls no longer delivered the security HealthPartners needed.
+ Inadequate endpoint protection created vulnerabilities across the organization's devices.
+ Unfiltered alerts lacked granularity, requiring manual analysis in the SOC.

The Solution

HealthPartners implemented the Palo Alto Networks Cortex portfolio, including Cortex XDR, XSOAR, and Xpanse.

+ Cortex consolidates multiple systems into one platform at half the cost of competitors.
+ Integrated threat intelligence blocked dozens of cyberattacks in the first year.
+ End-to-end visibility and deep insight into cyberthreat activity and point of origin elevates the SOC.

SNAPSHOT THREE: BETTER.COM

Streamlined security for a finance innovator

As one of the fastest-growing digital homeownership platforms in the U.S., Better.com is simplifying how customers secure mortgages and insurance by using technology to make the processes faster, more transparent, and more accessible. With over $95 billion in home loans funded, protecting its customers' data and the technology that drives its business is of the utmost concern.

Better

Industry
Finance

Country
United States of America

Website
www.better.com

5K+
EMPLOYEES

10K+
ENDPOINTS

$95B
IN LOANS

paloalto NETWORKS

Cortex made Better.com's security faster and more efficient, enabling the SOC team to become proactive instead of reactive—and freeing the company to focus on initiatives that simplify homeownership for its clients.

> The XSOAR investigations and automations we can do in conjunction with XDR have made it incredibly seamless to run commands within a workflow, build out a full kill chain event, and remediate very, very quickly."
>
> **— Jeff White, Director of Security, Better.com**

The Challenges

Better.com needed to empower the SOC to move faster to assess vulnerabilities and remediate threats across a large and rapidly growing network.

+ The existing EDR solution produced unreliable alerts with insufficient granularity.
+ The SOC was overwhelmed with manual workflows and remediation steps.
+ The company needed end-to-end visibility across all data.

The Solution

Better.com adopted a comprehensive set of security solutions and managed services from Palo Alto Networks, including Cortex XDR, XSOAR, Unit 42 MDR, NGFWs, Panorama, and Prisma Access to make security simpler and more proactive.

+ A single pane of glass provides visibility across data, users, applications, infrastructure, and endpoints.
+ Automating EDR and orchestrating the response improves workflows and broadens coverage.
+ The solution thwarts all attacks and provides full visibility into attempts, across the network and in penetration testing.

SNAPSHOT FOUR: KHIPU NETWORKS

Creating peace of mind for security clients

An award-winning international cybersecurity company, KHIPU Networks delivers world-class secure networks across global markets for customers across multiple sectors. With customers concerned that a cyberattack could damage their data, disrupt their digital strategies, or harm their reputations, KHIPU Networks launched the UK's first eXtended Managed Detection and Response (XMDR) service in 2019.

By Appointment to
Her Majesty the Queen
Network Security Provider
KHIPU Networks Limited
Hampshire

KHIPU CYBER SECURITY

Industry
Cybersecurity

Country
United Kingdom

Website
www.khipu-networks.com

1ST
XMDR VENDOR IN THE UK

19+
YEARS IN CYBERSECURITY

500+
CUSTOMERS

paloalto NETWORKS

Powered by Cortex, KHIPU Networks can confidently aggregate security insights from its diverse, worldwide customer base, improving detection and response, and building ongoing threat intelligence.

> The Palo Alto Networks portfolio stands out from other security operations solutions by nature of its simplicity, automation, and accuracy. We can offer customers complete visibility from a single data source and the ability to respond as a managed service across the whole environment."
>
> **— Guy Jermany, Chief Information Officer, KHIPU Networks**

The Challenges

To succeed, KHIPU Networks needed to deliver the benefits of an in-house SOC as a managed service to clients in diverse industries with differing and complex needs.

+ Clients struggled with security through growing IT complexity, post-pandemic remote working, hybrid on-premises and cloud infrastructure, and other challenges.
+ The solution needed to be flexible to meet each client's requirements, environment, priorities, and budgets.
+ Clients had difficulty recruiting and retaining effective cybersecurity expertise, especially when 24/7 availability was crucial for response and investigation.
+ KHIPU Networks needed to respond to and contain ransomware in an environment of escalating cyberattacks.

The Solution

KHIPU Networks built its XMDR service around Palo Alto Networks Cortex XDR and XSOAR, ensuring proactive detection and response along with the analysis, workflows, and task management needed to support the SOC.

+ Enhanced integration with multiple point products enables KHIPU Networks to provide immediate response, containment, and investigation of threats.
+ Automated AI and ML processes prevent, detect, and eliminate threats, allowing KHIPU Networks to act as the SOC for numerous organizations.
+ Surfacing every step of an attack reduces investigation time, maximizing the value of KHIPU Networks' analysts.
+ Affordable, flexible, and scalable cybersecurity services allow organizations of any size in any vertical market to invest confidently in KHIPU Networks' XMDR service.

SNAPSHOT FIVE: ASCEND MONEY

Automating the SOC at a fintech unicorn

Ascend Money was founded in 2013 to bring cutting-edge financial technology to the underbanked throughout Southeast Asia and is currently Thailand's fastest-growing startup. Today, TrueMoney Wallet, the company's digital e-wallet, is used by more than 50 million people in Thailand, Indonesia, Vietnam, Myanmar, Cambodia, and the Philippines.

Industry
Finance

Country
Thailand

Website
www.ascendmoneygroup.com

2K	50M	6
EMPLOYEES	CUSTOMERS	COUNTRIES

As threats skyrocketed during recent international crises, Cortex XDR and XSOAR kept Ascend Money protected, giving the company confidence that the data of its partners and customers remained secure.

> Cortex XDR from Palo Alto Networks offered us simplified integration and security automation, thereby reducing operation time significantly."
>
> **— Kanokwan Aimsumang, Head of IT Security and Governance, Ascend Money**

The Challenges

With fintech companies constantly under attack, Ascend Money needed a solution that would protect its assets—and the financial information of its rapidly expanding customer base.

- A growing network created concerns about potential gaps in endpoint security.
- The SOC was struggling with a high volume of unfiltered alerts.
- Ensure no disruption to the business in the event of a cyberattack.
- Help to upgrade technology to use AI and ML.

The Solution

Ascend Money leveraged Cortex XDR to automate endpoint detection and response in conjunction with Cortex XSOAR provided through a security partner, True Digital Cyber Security.

- XDR's extended endpoint protection broadens coverage to close potential gaps.
- AI- and ML-driven security automation focuses the SOC on high-value tasks.
- The scalability of XDR and XSOAR allows security to keep pace with continued growth.
- Simplified integration and security automation significantly reduced operation time.

SNAPSHOT SIX: FORVIA FAURECIA

Security to match manufacturer's digital transformation

Forvia Faurecia, one of the world's foremost automotive component manufacturers, is rapidly deploying next-generation technologies to keep pace with the industry's shift toward autonomous driving, electrification, connectivity, and other trends. With operations spanning the globe, this requires a modern, resilient cybersecurity strategy to steer digital transformation, ensure uptime, and reduce risk.

Industry
Manufacturing

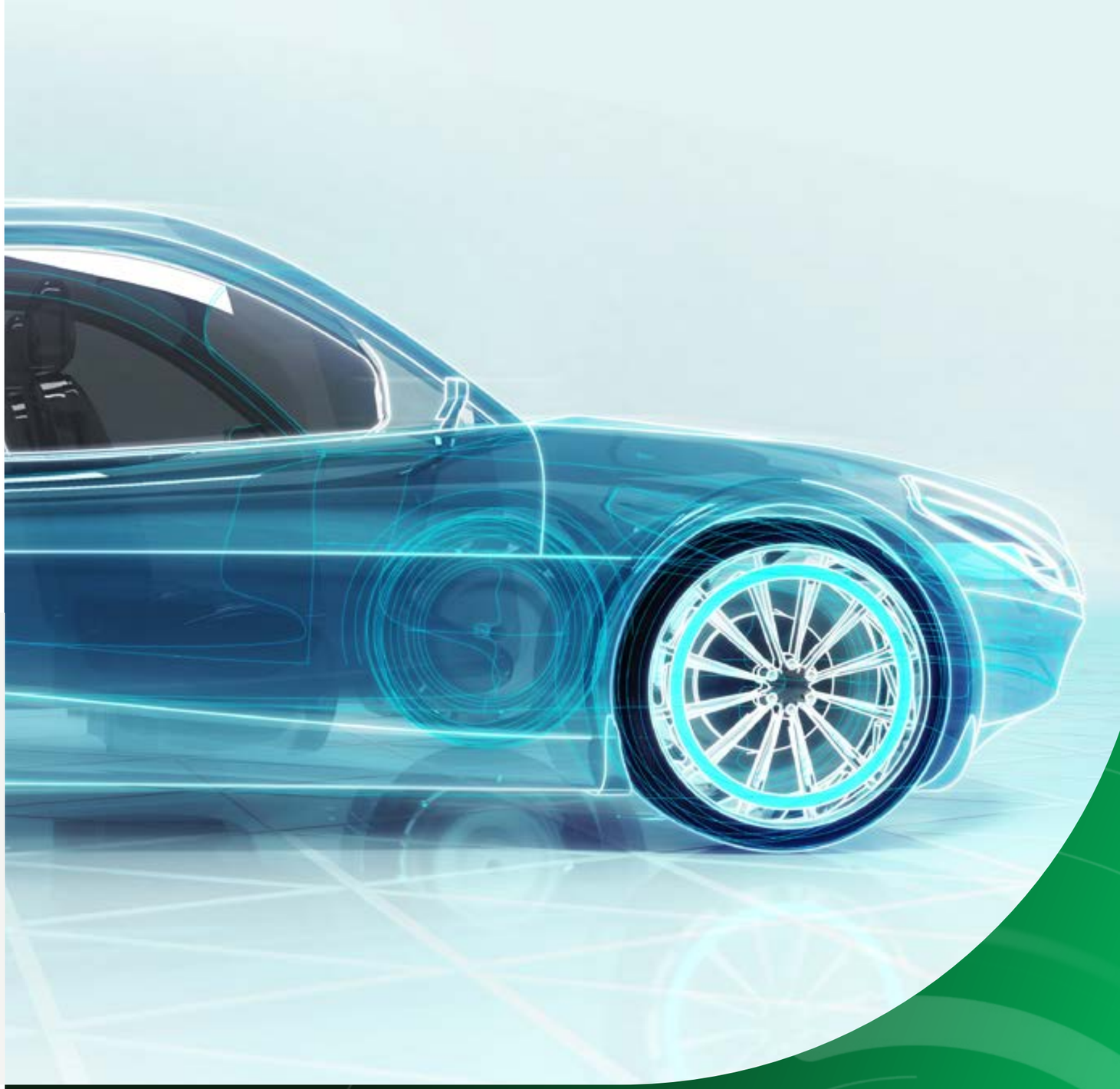
Country
France

Website
www.faurecia.com

100K+
EMPLOYEES

30+
COUNTRIES

250+
INDUSTRIAL SITES



Cortex XSOAR has made the SOC team's response more intelligent, efficient, and unified—driving a 70 percent increase in productivity.

> The recent release of a new internal solution generated nearly 20,000 alerts, but fewer than 200 alerts were handled manually. Everything else was done automatically. This represents a 99% reduction in manual workload and achieved an immediate return on our XSOAR investment."
>
> **— Matthieu Favris, Incident Response Manager, Forvia Faurecia**

The Challenges

With unfiltered alerts coming from EDR and SIEM systems, multicloud environments, and end users, the SOC team was crumbling under the workload.

+ The SOC team could not distinguish between low-priority alerts and real emergencies.
+ It lacked a single platform to intake and process alerts.
+ Failure to respond to all alerts put the business at risk.

The Solution

Forvia Faurecia implemented Cortex XSOAR to integrate alerts and support task management for its SOC.

+ XSOAR fully integrates alerts collected from the SIEM, EDR, and other sources.
+ Defining incident analysis and response procedures using digital workflows focuses the SOC on strategically valuable tasks.
+ Threat intelligence and automation significantly reduce the SOC workload.

SNAPSHOT SEVEN: BANCO DE GALICIA Y BUENOS AIRES

Elevating the SOC at a banking leader

With over 350 offices providing comprehensive banking services to businesses and individuals throughout Argentina, Banco de Galicia y Buenos Aires is one of the largest private banks in its country. Over three million customers trust it to manage their financial interests and to provide the flexibility and digital connections modern customers expect. Through digitization, it's working to bring banking services to its customers where they are—in branches, online, and through its Galicia app.

Industry
Finance

Country
Argentina

Website
www.bancogalicia.com

350	5K+	3M
OFFICES	EMPLOYEES	CUSTOMERS

Adopting XSOAR saves time in the SOC, allowing the team to focus on serious threats and remediate them quickly. That means less disruption to bank employees and greater productivity across the organization.

> With the implementation of Cortex XSOAR, we are able to manage [common alerts] almost fully automatically. What took us several minutes before is now managed in seconds."
>
> **— Ezequiel Invernon, SOC & IR Manager, Banco de Galicia y Buenos Aires**

The Challenges

The constant threat of phishing, data exfiltration, ransomware, and other attacks complicated the bank's efforts to pursue digitization and automation across the organization.

+ Alerts from numerous, siloed security products made it impossible to identify the most serious threats.
+ Manual remediation of low-level alerts exhausted the SOC team's resources.
+ The team ran the risk of missing serious threats, compromising the bank's security.

The Solution

Banco de Galicia y Buenos Aires adopted Cortex XSOAR to consolidate alert management across its security solutions and content services.

+ XSOAR seamlessly integrates alerts across security products and the bank's technologies, providing a single, consolidated view.
+ Playbooks for IoCs, phishing incidents, DLP, and privilege escalation automate and orchestrate SOC workflows.
+ Automated incident response focuses the team's resources on high-priority alerts.

SNAPSHOT EIGHT: AVRASYA TÜNELI

Automated security for an intercontinental crossing

Running beneath the Bosphorus Strait between Istanbul and Göztepe in Turkey, Avrasya Tüneli (the Eurasia Tunnel) connects the continents of Europe and Asia. A sophisticated technology infrastructure manages tolls, cameras, ventilation, incident response, and a host of other functions to keep the route safe for more than 65,000 travelers a day. The infrastructure needs to be protected from cyberthreats, and Murat Çalışırişçi, Director of Information Technology, required a security solution as state-of-the-art as the tunnel itself.

Industry
Transportation

Country
Turkey

Website
www.avrasyatuneli.com

150
EMPLOYEES

200+
ENDPOINTS

2K+
IoT DEVICES

For Avrasya Tüneli, any security incident could impact the safety of 65,000+ drivers daily. With Cortex XDR, the tunnel maintains a confident security posture without the need to hire additional staff.

> It's integrated, automated, and simple. [Palo Alto Networks] integrated platform offers holistic protection, connecting all key security data through a single pane of glass. Every component of the platform is best in class, and their future product map demonstrated them to be a visionary partner."
>
> **— Emrah Dündar, Senior Manager, Information Technologies, Avrasya Tüneli**

The Challenges

Avrasya Tüneli needed to protect the technology infrastructure that supports the tunnel without increasing demand on a staff of only three security professionals.

+ The security team needed end-to-end visibility through a single interface.
+ More than 200 endpoints and over 2,000 IoT devices required 24/7/365 monitoring.
+ Response times were critical to ensure tunnel safety.

The Solution

Avrasya Tüneli implemented Cortex XDR for extended detection and response, in combination with an integrated suite of Palo Alto Networks security products and managed services (MDR) from Unit 42.

+ XDR blocked every threat during solutions tests in a custom lab environment.
+ Automation reduces manual workloads, maximizing employee productivity.
+ Integrated ML-based network traffic analysis, detection from endpoints, and user behavior analytics simplify monitoring, including IoT devices.

Take the next step

Cortex brings together best-in-class threat detection, prevention, attack surface management, and security automation capabilities into one integrated platform. This lets you build an efficient, adaptable, and responsive security operations center that's designed for a constantly evolving threat environment.

As these customers' experiences show, Cortex partners with enterprises of all sizes to simplify, automate, and accelerate security operations and incident response.

Learn more about how Cortex can elevate your SOC.

Click here →

The Cortex portfolio is transforming the security landscape—freeing organizations to pursue their digitization strategies while providing peace of mind to the SOC teams that keep them safe.

- **Cortex XDR®** is the industry's first XDR solution that natively integrates endpoint, network, cloud, and third-party data to stop sophisticated attacks.
- **Cortex® XSOAR™**, the industry's most comprehensive security orchestration platform, elevates security operations with automated workflows for any security use case.
- **Cortex® Xpanse™** maps the unknown across the evolving internet attack surface to make the invisible visible, improving ROI on all security investments.
- **Cortex® XSIAM™** is an autonomous SOC platform harnessing the power of AI-driven automation to radically improve security outcomes and transform security operations.
- **Unit 42® MDR** applies our years of experience to monitor your environment and look for anything suspicious. Our analysts work 24/7, sorting through Cortex XDR data to bring the full picture together.