How Eight Organizations Implemented Zero Trust to Secure Their Modern Networks

PREFACE

Strategic Security Strengthens Digital Transformation

Pairing Modern Networks with Zero Trust

The acceleration of digital transformation makes the network more important than ever. The network is the lifeline of global organizations—from connected enterprises to the Internet of Things to the critical infrastructures supporting the world.

Every new connection must be protected from sophisticated cyber threats. However, this is an increasingly difficult task, as more than 96% of organizations reported attacks in 2021. Unfortunately, many of these organizations suffered multiple successful breaches[1]

Enterprises are looking to Zero Trust architecture as a way forward, but the path to a Zero Trust security posture is not well understood. 98% of CxOs surveyed by Palo Alto Networks say that it is challenging to implement Zero Trust[1]
Zero Trust can be successfully implemented by following a step-by-step roadmap complemented by best practices and leading-edge technology. Palo Alto Networks has helped many organizations achieve complete Zero Trust and secure their critical digital assets from the most evasive zero-day threats.

Following are the stories of eight organizations that have benefited from Palo Alto Networks' robust solutions that bring a Zero Trust approach to modern networks.

[1] Source: Palo Alto Networks What's Next in Cyber survey
https://start.paloaltonetworks.com/whats-next-in-cyber-report

SNAPSHOT ONE: VILLAGE ROADSHOW

Modernize aging network and enhance security infrastructure

Village Roadshow began operating in 1954 and is now a leading entertainment company. Based in Melbourne, Australia, Village Roadshow has well-recognized retail brands, including Warner Bros. Movie World, Sea World, Wet'n'Wild, Paradise Country, and Australian Outback Spectacular—with 150 rides, slides, and attractions as well as over 400 hotel rooms. Village Roadshow welcomes between 20–30 million guests annually, either in their cinema sites or across their theme parks.

VILLAGE ROADSHOW PICTURES

Industry
Media & Entertainment

Country
Australia

Website
villageroadshow.com.au

20-30M
ANNUAL GUESTS

5000
EMPLOYEES

1954
COMMENCED OPERATIONS

paloalto NETWORKS

Village Roadshow achieved a network and security transformation along with realizing savings of thousands of hours per month by consolidating and future-proofing with a single-vendor SASE approach.

> “Palo Alto Networks with Prisma Access, Panorama, and GlobalProtect was the only solution that was able to meet all criteria. With their reputation as a market leader in cybersecurity and the most complete SASE solution in the industry, we knew we could trust Palo Alto Networks to deliver the right outcomes for our business.”
>
> **– Michael Fagan, Chief Transformation Officer**
> **Village Roadshow Limited**

The Challenges

Village Roadshow needed to move from legacy MPLS architecture to a next-gen network with cybersecurity designed and optimized for the cloud. Addressable challenges included:

- Aging infrastructure of systems from multiple vendors, designed for a bygone era.
- Network lacked agility and scalability, had sub-par security, and relied on proprietary carrier systems.
- Application performance was impaired, resulting in poor user experience and lost productivity.
- Network plagued by delays due to the backhauling of all traffic from branch offices to a hub or data center required for advanced security inspection services.

The Solution

Village Roadshow partnered with Palo Alto Networks to re-architect and re-design their network and broadened their scope from SD-WAN to a complete SASE architecture. As a result, Village Roadshow:

- Achieved a stronger security posture and a seamless, consistent user experience, irrespective of the location of staff members, by adopting cloud-delivered security and networking with Palo Alto Networks Prisma SASE.
- Eliminated the headaches of dealing with unexpected outages and multiple vendors. productivity.
- Phased out two incumbent vendors by partnering with with Palo Alto Networks to consolidate to a single vendor with a complete SASE solution.
- Saves more than 5,000 man-hours every month by solving interoperability challenges.

SNAPSHOT TWO: WESTFIELD

Advance digital transformation in a rapidly changing retail environment

Westfield operates malls around the world and strives to create landmark shopping destinations with great experiences, providing a unique platform for retailers and brands to connect with consumers. Digitization and shifting consumer preferences are creating new challenges for its business model while also opening new opportunities.

Westfield

Industry
Retail

Country
United States

Website
www.westfield.com

900M	78	12
ANNUAL GUESTS	SHOPPING CENTERS	COUNTRIES

Westfield significantly reduced costs and is able to respond quickly to a changing market by enhancing connectivity and security based on a Zero Trust approach and seamlessly integrating its technology and business operations.

> “Prisma SASE with Zero Trust gave us the ability to secure our users regardless of their status, what device they’re using, or where they’re working from.”
>
> **– Ken Ogami, Senior Vice President & CIO U.S.
> Westfield North America**

The Challenges

Westfield’s ability to rapidly adapt and expand was limited by its legacy systems with a monolithic approach to applications and infrastructure. This created multiple challenges.

- Legacy networking meant limited bandwidth, which made it difficult to execute high-bandwidth operations like streaming live performances from its venues.
- Developing custom applications for the legacy environment took a long time.
- Systems were not optimized for the sudden shift to remote work.
- Westfield could not provide an enhanced digital experience at its existing brick-and-mortar locations and build web-based and mobile apps.
- Digital tools needed by customers and retail partners were lacking.

The Solution

Westfield seamlessly integrated its technology and business operations by deploying Prisma SASE. Among the many results achieved with this solution were:

- Improved employee productivity, increased customer engagement, and provided its retail partners with a better business environment by updating connectivity to support high-bandwidth traffic seamlessly.
- Significantly enhanced security by adopting a cloud-based Zero Trust solution for networks and apps.
- Reduced the overall network operating costs by 60 percent while significantly improving performance by consolidating security and SD-WAN were consolidated.

Enhanced cybersecurity and risk management to support future learning opportunities

Rangsit University (RSU), a leading private university in Thailand, is fully accredited by the Thai Government's Commission on Higher Education, Ministry of Education. RSU is synonymous with academic excellence and looks to provide accessible, personalized, quality education opportunities for both local and international students. RSU is committed to providing highly planned and skillfully created academic programs that reflect the best in academic tradition and are constantly evolving to keep pace with technological advances, educational methods, and technology.

RSU
Rangsit University
International College

Industry
Education

Country
Thailand

Website
www.rsuip.org

30K
STUDENTS

2,000
INSTRUCTORS/ STAFF MEMBERS

1986
ESTABLISHED

RSU enabled the security team to easily implement consolidated policy creation and centralized management features, securing users, applications, and data, no matter where they reside by deploying network security management.

> “Overall, Palo Alto Networks was leaps and bounds ahead of the other vendors but scored particularly high when it came to innovation. Looking at the pace of potential threats in the future, we opted for a partner that was crucial to help us stay ahead of the attack curve.”
>
> **– Dr. Chetneti Srisa-an, Vice President, Technology**
> **Rangsit University**

The Challenges

With ever-increasing cybersecurity incidents, RSU needed smarter threat detection, prevention, and response tools to stay ahead of threats. To address the security challenges that it faced, RSU needed to:

- Enhance active protection against malware threats.
- Overcome visibility limitations and performance deficiencies.
- Extend detection and response capabilities and enable retrospective analysis.
- Implement a system that provides a single platform and easy integration with current infrastructure and existing security tools.

The Solution

Palo Alto Networks Panorama network security management and Palo Alto Networks NGFW were selected to secure the firewall and enable RSU to move from legacy security tools to prevention-based architecture. This has allowed RSU to:

- Actively protect against malware and sophisticated threats by collecting data automatically and correlating it across multiple security layers, including endpoint, email, server, cloud workload, and network.
- Stops attack before they escalate by conducting a retrospective analysis of potential attacks.
- Streamline operations and reduce costs by moving to a single, unified platform that integrates Palo Alto Networks solutions with current infrastructure and existing security tools.

SNAPSHOT FOUR: NOVAGROUP

Lead the way for digital transformation with cloud security and Zero Trust

NovaGroup is a multi-industry conglomerate consisting of three key member companies—Novaland Group, Nova Service Group, and Nova Consumer Group. These groups operate in the fields of property, trading and service, and agriculture-consumer goods. In 2021, NovaGroup continued to complete its ecosystem, operating mainly in service, technology, and industry. To support this, it established five more corporations—Nova Tech, Nova Capital Partners, Nova Logistics, Nova Industry, and Nova Finance, bringing the total to eight member companies.

NOVA GROUP
CHO CUỘC SỐNG BỪNG SÁNG

Industry
Multi-industry Conglomerate

Country
Vietnam

Website
www.novaland.com.vn

5,000+
EMPLOYEES

10,600
HECTARES OF LAND BANK

30
YEARS OF OPERATION

NovaGroup realized 50% savings with seamless work-from-home (WFH) capabilities made possible using Palo Alto Networks Zero Trust architecture, Next-Generation Firewall (NGFW), Threat Prevention, GlobalProtect, Advanced URL Filtering, and WildFire.

> “Within a mere week or two, we had switched from in-office mode to work from home for hundreds of companies belonging to the NovaGroup ecosystem. This was exceptionally timed by the team from Palo Alto Networks, bearing in mind the urgency of the requirement.”
>
> **– Mr. Trần Phú Nghĩa, Cyber Security Director**
> **NovaGroup - Cyber Security Committee (CSC)**

The Challenges

The cybersecurity team needed to find a solution that could enable a Zero Trust architecture to make the company cyber resilient in the face of increasing threats. The goal was to overcome challenges including:

- The sudden shift to work from home (WFH) highlighted security gaps for users connecting from remote locations.
- A rise in advanced threats was not sufficiently addressed with existing security systems.
- Complex, legacy firewalls made it difficult to detect fast-moving threats within the network.
- New systems needed to provide multi-vendor compatibility to ease integration with the existing cyber ecosystem within the NovaGroup parent company and subsidiaries.

The Solution

NovaGroup accelerated the deployment of Palo Alto Networks security solutions to its newly established security operations center (SOC). Among the results achieved are:

- Minimized risk by proactively detecting cyberattacks.
- Realized more than 50% cost savings by consolidating hardware and software licenses.
- Leverage existing investments by easily integrating Palo Alto Networks solutions into existing systems.
- Significantly enhanced security by implementing Palo Alto Networks Zero Trust architecture.
- Seamless shifted thousands of employees to work from home with the new solutions.

SNAPSHOT FIVE: STATE OF NORTH DAKOTA

Increase protection with a Zero Trust Approach and IoT Security

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, which makes security as much of a challenge as it is a priority.

NORTH Dakota
Be Legendary.™

Industry
Government

Country
United States

Website
www.nd.gov

800K
CITIZENS PROVIDED TECHNOLOGY AND SERVICES

250-400K
DEVICES CONNECTED

10k+
IOT DEVICES IN ONE K-12 SCHOOL

paloalto® NETWORKS

The State of North Dakota extended its cybersecurity leadership with Palo Alto Networks IoT Security for advanced protection bolstered with a Zero Trust architecture.

> "I still remember when we deployed our first Palo Alto Networks firewall. Finally, we could actually see what was going on natively in the firewall. That was a huge moment for us. If you don't know what's on your network, you really can't control anything."
>
> **– Ryan Kramer, Enterprise Infrastructure Architect**
> **North Dakota Information Technology**

The Challenges

As the North Dakota Information Technology (NDIT) team matured and expanded its approach to security, it identified challenges that put systems and users at risk, including:

- The tools the team was using to scan its network for threats were not providing an accurate picture.
- The NDIT team lacked complete visibility into what was connecting to the network.
- IoT introduced additional visibility issues, risks, and protection gaps.

The Solution

NDIT selected Palo Alto Networks IoT Security solution and adopted its Zero Trust architecture. This helped NDIT security across the network with a scalable solution that allowed them to:

- Gain ML-powered visibility of the IoT landscape across all state institutions.
- Improve threat prevention.
- Enhance enforcement of security policies that include IoT devices.
- Surface unmanaged device data across the network.
- Access device risk analysis.
- Facilitate the enforcement of recommended device risk-based policies to minimize risk.

SNAPSHOT SIX: EURASIA TUNNEL

Eliminate vulnerabilities without an increase in headcount

The Eurasia Tunnel is a road tunnel in Istanbul, Turkey that crosses underneath the Bosphorus Strait to link Europe with Asia. This 5.4km tunnel helps reduce travel time and alleviates Istanbul's traffic problems. It has also led to the improvement and widening of the roads leading to the tunnel. Around 50,000 vehicles pass through this tunnel daily. The team implemented a forward-thinking, efficient IT security strategy to protect end-to-end IT infrastructure and ensure a fast, uninterrupted journey for drivers every day.

AVRASYA TÜNELİ

Industry
Transportation

Country
Turkey

Website
www.avrasyatuneli.com

50K+
DAILY DRIVERS

2,000+
IOT DEVICES

2,000+
SCADA OT DEVICES

The Eurasia Tunnel team enhanced and optimized its security strategy to protect end-to-end IT infrastructure and connected devices by implementing Palo Alto Networks' all-in-one automated solution.

> "Their 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 roadmap demonstrated them to be a visionary partner."
>
> – Emrah Dündar, IT and Security Manager
> Avrasya Tüneli

The Challenges

The team needed a modern, adaptive security solution to support safe, continuous tunnel traffic. Several challenges would need to be addressed, including finding a solution for the new operation that could:

- Effectively protect the network, endpoints, and more than 2,000 Internet of Things (IoT) devices.
- Provide automation so the small team would not be overwhelmed with manual tasks and managing disparate systems.
- Eliminate visibility gaps from IoT devices.
- Scale to meet increased demand.
- Proactively eliminate vulnerabilities without demanding an increase in headcount.

The Solution

Following a rigorous evaluation of vendors, the Eurasia Tunnel team chose the Palo Alto Networks portfolio of solutions, because it:

- Protects every aspect of the driver's journey and the tunnel's infrastructure with a modern, end-to-end security platform.
- Delivers complete protection and policy enforcement for every IoT device by providing integrated IoT security.
- Simplifies day-to-day security tasks with automation that leverages ML and AI.
- Ensures consistent security and closes gaps in network visibility by integrating seamlessly with other parts of the IT.
- Provides 24/7 threat visibility across all systems by giving the team a unified view of all security operations.

Create a modern, agile property register based on a cloud-first strategy

Registers of Scotland is a non-ministerial office of the Scottish administration responsible for keeping public registers of land, property, and other legal documents in Scotland. A land register is a publicly accessible register of property rights. Most, like ours, are underpinned by state guarantees. Land registration offers the certainty of title to property owners, potential purchasers, and lenders to prove ownership of what is being sold or borrowed against. The Keeper of the Registers of Scotland is directly accountable to the Scottish Parliament.

Registers of Scotland

Industry
Public Sector

Country
Scotland

Website
www.ros.gov.uk

60%
APPLICATIONS DESPATCHED WITHIN 35 DAYS

1,200
EMPLOYEES

20
PUBLIC REGISTERS MAINTAINED

Registers of Scotland accelerates digital transformation with Palo Alto Networks' security portfolio, supporting the secure processing of thousands of digital property registration documents through these new systems every day.

> "The security visibility and focus on prevention are enabling Registers of Scotland to achieve the cloud migration at great speed without unquantified risk."
>
> – Bob Bowden, Security Architect
> Registers of Scotland

The Challenges

During the pandemic, Registers of Scotland had to shift from paper-based systems to digital systems quickly. An entirely new secure digital process was needed to scan incoming digital documents to eliminate malware risk. Registers of Scotland was challenged to find a system that could:

- Automatically scan incoming digital documents for malware without compromising customer experience.
- Automatically share intelligence to provide in-depth defense.
- Manage security services from a single, intuitive pane of glass.

The Solution

Integration with Palo Alto Networks WildFire via the API underpins the fast, seamless submission of digital registry submissions. The innovative application of this CDSS prevents unknown threats, automates protection, and allows Registers of Scotland to focus its valuable resources elsewhere. Created in less than three weeks, this solution:

- Improves customer experience by simplifying the application journey.
- Expedites the processing of applications.
- Increases agility and scalability.
- Provides greater visibility into the registration process.
- Eliminates the need for physical documents.
- Ensures compliance with statutory and regulatory obligations.

SNAPSHOT EIGHT: US SIGNAL

Increase services for customers and strengthen security posture

US Signal is a leading provider of data center and cloud services. With eight data centers in the Midwest, the company hosts cloud solutions, provides colocation space, and delivers best-of-breed security services powered by its secure, robust fiber network. Customers in health care, banking, and other industries rely on US Signal's HIPAA- and PCI-compliant infrastructure to keep information safe. They consider US Signal an extension of their IT security teams and trust the company to protect their businesses from cyber threats, ransomware, and online attacks.

US SIGNAL®

Industry
Telecommunications and Technology

Country
United States

Website
www.ussignal.com

225
DATA CENTERS AND POPS

9,500
MILE NETWORK OF LIT FIBER

<30
SECONDS TO REACH SUPPORT BY PHONE

US Signal created a centralized system for providing a secure infrastructure internally and for customers by consolidating firewall platforms with Palo Alto Networks.

> “We put all the vendor solutions through the test for everything we do and pitted them against each other. Palo Alto Networks brought the best solution holistically for us.”
>
> **– Brandon Prim, Cloud Security Engineer**
> **US Signal**

The Challenges

US Signal was operating multiple firewall platforms from several vendors. To streamline its expansion, US Signal wanted to consolidate platforms and work with a single vendor. Doing so would mean its engineers would not need to learn the ins and outs of multiple systems and would gain a centralized perspective of the company’s security infrastructure. US Signal was struggling with several challenges.

- It was operating multiple platforms from different vendors, which increased the likelihood of human error, exposing them to data breaches.
- Provisioning firewalls for customers was a cumbersome, time-consuming process.
- Customers were confused by having too many product choices.

The Solution

US Signal partnered with Palo Alto Networks, and together they developed a package of products and services that allowed US Signal to scale and roll out security enhancements to customers quickly. With the solutions provided by Palo Alto Networks US Signal:

- Benefits from best-in-class security that protects their infrastructure and customers.
- Can seamlessly scale to keep up with the company’s appetite for expansion.
- Has the ability to automate the deployment of virtual firewalls to hundreds of customers.

Take the next step

See for yourself how Palo Alto Networks can help you drive your best security posture and optimal firewall health. Take a Virtual Ultimate Test Drive. More than just a demo, this virtual workshop is customized to enhance your understanding with a hands-on experience designed for every experience level.

LEARN MORE →