paloalto NETWORKS | PRISMA CLOUD BY PALO ALTO NETWORKS

Cloud Security Spotlight – Seamless Security from Code to Cloud™ and Beyond

INTRODUCTION

How Leading Organizations Secure Their Cloud Environments

To remain competitive in the market and respond to ever-changing business dynamics, organizations are increasingly migrating to the cloud. Yet attacks in the cloud are becoming more sophisticated. Many companies are unprepared to defend against modern-day threats, hampered by understaffed security teams, operational inefficiencies, and siloed tools and point solutions.

The complexity of multicloud and hybrid cloud environments and different types of workloads calls for securing modern applications wherever they run.

In this e-book, we'll explore how Palo Alto Networks Prisma Cloud and software firewalls, like VM-Series virtual firewalls, help leading organizations protect applications and workloads from zero-day threats, easing operational burden, reducing risk, and preventing breaches with agile, best-in-class security for all clouds and everything that networks with them.

Palo Alto Networks helps leading organizations predict and prevent risk in near real-time across their clouds and everything that connects with them, achieving better security outcomes and decreasing operational costs.

Software firewalls deliver*:

163%
ROI over three years with immediate payback

67%
Reduction in end-user downtime

50%
Reduction in time required to attain security posture

Firewall platform options include:	Virtual Firewalls	Container Firewalls	Managed Cloud Firewalls Services
	VM-Series	**CN-Series**	**Cloud NGFW for AWS** **Cloud NGFW for Azure**

Prisma Cloud delivers*:

276%
ROI

60%
Reduction in DevOps effort to fix vulnerabilities

64%
Reduction in total audit time

*Source: The Total Economic Impact™ of Palo Alto Networks Software Firewalls, Forrester Consulting, October 2023

paloalto NETWORKS | PRISMA CLOUD BY PALO ALTO NETWORKS

REDUCE RISK

SNAPSHOT TWO: TEADS

Faster innovation and better security with a cloud-native application protection platform

Teads is a global advertising technology organization, providing publishers and advertisers with a modern, digital marketing communications platform. Teads' platform is used by leading holding companies and many of the world's most sophisticated advertisers and publishers.

Teads

Industry
Advertising Technology and Services

Country
HQ in New York with 41 offices in 32 countries

Website
www.teads.com

€613M	1,000	1.9B
REVENUE	EMPLOYEES	MONTHLY USERS

paloalto NETWORKS | PRISMA CLOUD BY PALO ALTO NETWORKS

SNAPSHOT TWO: TEADS

It takes half the time to manage cloud security with Prisma Cloud as it would to use multiple cloud-native tools on separate platforms

> “Everything is so easy with Palo Alto Networks. The native integration is seamless, the visibility is complete, and the automation takes care of the vast majority of monitoring. There’s no impact on our resources either.”
>
> **– Oussama Benzaouia, CISO**
> **Teads**

The Challenges

Teads collects data from nearly two billion people every month. The company already had strong security processes in place to protect that data, but business growth and governance requirements demanded a new strategic security program that would cover the entire application development lifecycle:

Consistent, comprehensive visibility into data stored in cloud platforms

Managing the end-to-end, container-based development cycle

Remediating vulnerabilities at an early stage

The Solution

Teads implemented Prisma Cloud to support their entire cloud infrastructure, relying on the CNAPP to eliminate cloud blind spots, achieve compliance, and proactively address risks.

Unified cloud security posture management (CSPM) provides complete visibility and control over all cloud environments from a single console.

Cloud infrastructure entitlement management (CIEM) capabilities identify baseline behavior and where users connect from.

Infrastructure-as-Code (IaC) scanning and code fixes are embedded directly into developer tools so cloud risks are addressed earlier in the development process.

Read the full case study

PREVENT BREACHES

SNAPSHOT THREE: REGISTERS OF SCOTLAND

Achieving digital ambitions with unified, automated protection against cyberattacks

Registers of Scotland are responsible for managing public registers of Scottish land and property. The organization holds more than 21 public registers containing nationally critical information that dates back 400 years, and was on a mission to digitize its paper-based services to improve operational efficiency.

Registers of Scotland

Industry
Public Sector

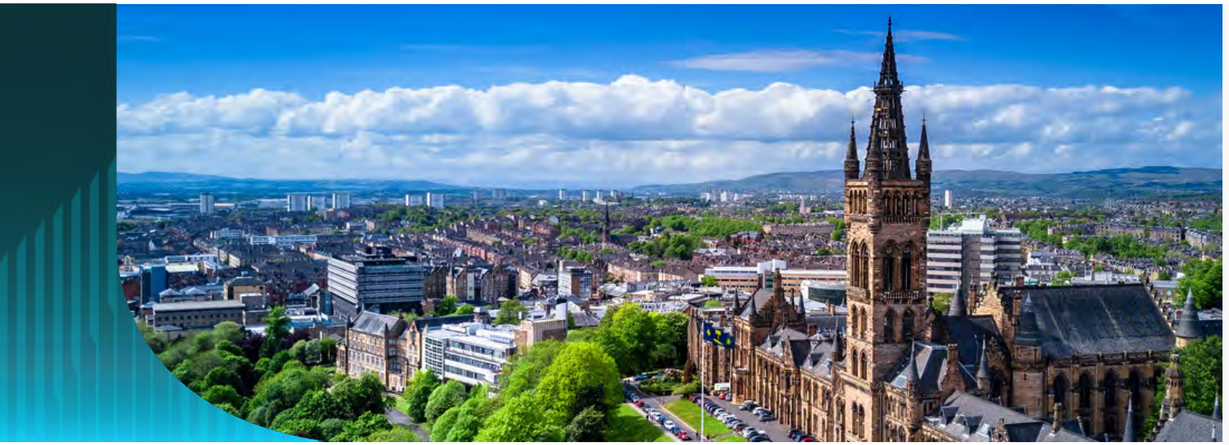
Country
Scotland

Website
www.ros.gov.uk

677K	1,000	1.9B
ANNUAL REGISTRATION APPLICATIONS	EMPLOYEES	MONTHLY USERS

paloalto NETWORKS | PRISMA CLOUD BY PALO ALTO NETWORKS

SNAPSHOT THREE: REGISTERS OF SCOTLAND



One partner, with one best-in-class security portfolio.

> “The Palo Alto Networks portfolio makes sense on every level. Instead of relying on point security solutions, we have a suite of best-practice, interconnected security technologies that are proven to deliver. Our team can focus on value-add tasks, confident that critical security processes are running in the background, protecting our new digital infrastructure.”
>
> **– Bob Bowden, Security Architect**
> **Registers of Scotland**

The Challenges

Driven by the pandemic, Registers of Scotland scrambled to digitize their paper processes, an effort hampered by a legacy, siloed security infrastructure.

Manual vulnerability scanning efforts were time-intensive to process.

Lack of security resources made it impossible to manage multiple endpoint solutions.

A Security Lifecycle Review highlighted high-risk applications and vulnerabilities that required a uniform cybersecurity platform to address.

The Solution

Registers of Scotland implemented virtually the entire Palo Alto Networks portfolio. The unified portfolio provides the organization with the transparent visibility, trusted intelligence, and flexibility it needs to effectively secure its entire digital environment.

ML-Powered Next-Generation Firewalls secure the network, continuously learning to detect threats.

The Prisma Cloud CNAPP eliminates blind spots and detects threats, providing complete visibility, continuous threat detection, and automated response.

The unified security portfolio simplifies the customer application journey, enabling faster application processing and improved visibility of registrations.

Read the full case study

paloalto NETWORKS | PRISMA CLOUD BY PALO ALTO NETWORKS

REDUCE RISK

REDUCE OPERATIONAL BURDEN

SNAPSHOT FOUR: GLOBE TELECOM

Long-term partnership ensures effortless cutting-edge security from code to cloud

Globe Telecom, the largest mobile operator in the Philippines, considers customer data protection paramount. The company wanted to fortify its cybersecurity efforts so it invested heavily in establishing an end-to-end cybersecurity team that could scale according to the needs of the company.

Globe

Industry
Telecommunications/Financial Services

Country
Philippines

Website
www.globe.com.ph

₱151.5B	8,000+	54M+
REVENUE	EMPLOYEES	SUBSCRIBERS

paloalto NETWORKS | PRISMA CLOUD BY PALO ALTO NETWORKS

REDUCE RISK

REDUCE OPERATIONAL BURDEN

SNAPSHOT FOUR: GLOBE TELECOM

Palo Alto Networks has 1,000 accounts on Prisma Cloud across approximately 18 physical sites and 1,000 accounts on AWS public cloud.

> "With their Layer 7 firewalls and filtering, Palo Alto Networks was at the forefront in terms of capabilities, but it was their completeness of vision with regard to our technology requirements that won us over. They offered us world-class, advanced technology solutions, with a keen finger on the pulse for what lay ahead, thereby ensuring they stayed ahead of the curve."
>
> **– Anton Bonifacio, Chief Information Security Officer, Globe Telecom**

The Challenges

Driven to provide comprehensive, best-in-class security for their digital transformation initiatives, Globe Telecom was on the hunt for a trusted, proven cybersecurity partner that could alleviate key challenges:

Securing an expanding infrastructure with siloed legacy solutions

Managing multiple security vendors

Ensuring private and public cloud security through significant acceleration in cloud adoption

The Solution

Palo Alto Networks secured Globe Telecom's digital transformation initiatives and addressed the complexity of both infrastructure and operations.

Standardized security through an end-to-end security solution provider enabled consolidation and simplification.

Automatable, scalable, and easy-to-deploy virtual firewalls boosted cloud security by safeguarding critical systems.

CSPM and Cloud Workload Protection modules made it easy to implement and manage cloud security across the entire application lifecycle.

Read the full case study

paloalto NETWORKS | PRISMA CLOUD BY PALO ALTO NETWORKS

REDUCE RISK

REDUCE OPERATIONAL BURDEN

SNAPSHOT FIVE: US SIGNAL

US Signal, primed to scale, protects sensitive information

US Signal is a leading provider of data center and cloud services, delivering best-of-breed security services powered by its own secure, robust fiber network. The company was looking to expand its cloud footprint and data protection capabilities to meet increasing demand for its services during the pandemic.

Industry
Telecommunications and Technology

Country
United States of America

Website
www.ussignal.com

$41M	200	225
REVENUE	EMPLOYEES	DATA CENTERS & POPS

REDUCE RISK REDUCE OPERATIONAL BURDEN

SNAPSHOT FIVE: US SIGNAL

US Signal engineers were comfortable using the platform within a week and became experts within six months.

> “Palo Alto Networks platform stepped up to the challenge; it had already instantly blocked the SolarWinds issue. There was nothing to worry about. The firewalls were automatically set up to receive up-to-the-minute updates. We put the Palo Alto platform, with all security subscriptions turned up, through numerous tests and we have yet to find a scenario where the firewall was lacking. The firewall performance speaks for itself and has proven why it is an industry leader.”
>
> **– Brandon Prim, Cloud Security Engineer**
> **US Signal**

The Challenges

As a leading provider of data center and cloud services, security was always top of mind for US Signal. But increasing demand for their services drove a critical need for a more streamlined approach to security that would reduce risk while increasing productivity through automation.

Rapid expansion of services drove the need for scalability.

Provisioning firewalls was cumbersome and time-consuming.

Multiple firewall platforms for disparate vendors reduced visibility and increased risk.

The Solution

US Signal chose Palo Alto Networks industry-leading, Virtual Next-Generation Firewalls to provide complete Zero Trust security for both its internal IT infrastructure and as product offerings that US Signal deploys to customers. By taking advantage of Palo Alto Networks automated provisioning and integration, US Signal deployed every virtual firewall with a full suite of cloud-delivered security services.

Scalable platform designed to protect critical data, workloads, and applications helped customers mitigate risk and achieve compliance.

Automation reduced the likelihood of human error, drove down costs, and expedited deployments.

Consolidated platform approach improved security posture and streamlined the customer experience.

Read the full case study

REDUCE RISK

PREVENT BREACHES

SNAPSHOT SIX: TIDLOR

TIDLOR augments visibility and protection for customer data and applications across public cloud IaaS

As a leading Thai microfinance company guided by a vision to empower people and enrich lives, TIDLOR takes the security of customer data seriously. When on-premises infrastructure was nearing its end-of-life, they took the opportunity to increase protections on their public cloud infrastructure as a service (IaaS).

Industry
Financial Services

Country
Thailand

Website
www.tidlor.com

฿15,274M	1,600	1M+
REVENUE	BRANCHES	FUNDING RECIPIENTS

paloalto NETWORKS | PRISMA CLOUD BY PALO ALTO NETWORKS

REDUCE RISK PREVENT BREACHES

SNAPSHOT SIX: TIDLOR

Centrally managed policies across physical and virtual firewalls, along with streamlined workflow automation, reduced staff time spent on monitoring and remediation from days to minutes.

"After installing the new solution, TIDLOR has benefited from increased application-level visibility, precise control, security optimization, prevention of security breaches, automation of endpoint security and increased productivity."

– Pakamon Tulyapizitchai, SVP, Head of Digital Transformation TIDLOR

The Challenges

TIDLOR had never suffered a breach, but they weren't taking any chances. They updated existing security systems with a solution that could advance their security initiatives and eliminate ongoing challenges.

Lack of application-level visibility across public cloud IaaS

Cumbersome, siloed security practices that made it difficult to monitor data across the organization

Inability to segment mission-critical applications and data compromised security posture

The Solution

TIDLOR selected Palo Alto Networks, deploying the VM-Series Virtual Next-Generation Firewall on AWS cloud and integrating it with AWS's Gateway Load Balancer. The new solution has improved TIDLOR's ability to prevent cyberthreats and breaches.

Improved security for virtualized applications, data, and workloads prevented data loss that would lead to business disruption.

Implementing user-based controls to grant access to applications eliminated known and unknown threats.

VM-Series firewall supported increased application-level visibility and enabled precise control by providing visibility across all ports.

Read the full case study

paloalto NETWORKS | PRISMA CLOUD BY PALO ALTO NETWORKS

paloalto NETWORKS | PRISMA CLOUD BY PALO ALTO NETWORKS

Protect Your Applications with Proven, Best-of-Breed Security

Securing applications in the cloud is a challenge—one that can't be solved with disparate tools and solutions.

To defend against modern threats, you need a comprehensive Code to Cloud security solution that can prevent breaches and reduce risks in near-real time across your clouds and everything that connects with them.

You need Palo Alto Networks.

A respected industry leader, regularly featured in various Gartner Magic Quadrants and recognized in marquee reports, such as the Forrester Wave and the GigaOm Radar, Palo Alto Networks offers best-in-class security to protect applications from code to cloud. For customers, that means unparalleled risk prevention, extensive visibility and control, and superior runtime protection.

Learn more about why Palo Alto Networks is the proven cybersecurity partner of choice, helping organizations predict and prevent risk by delivering unified cloud security with the industry's most proven platforms, people, and precise data.

Palo Alto Networks delivers comprehensive cloud security platforms that protect applications across public, private, and hybrid clouds. Near real-time breach prevention and risk reduction capabilities ensure the security of cloud data and applications—even against zero-day threats. Comprehensive Code to Cloud™ solutions also foster seamless collaboration between security and development teams, accelerating the creation of secure cloud applications throughout your digital transformation journey.

Palo Alto Networks
Enabling innovation at speed and scale

8x Faster incident investigations

44% Lower cost

95% Reduction in alerts