NWU®

CASE STUDY

North-West University achieves an 80% increase in security efficiency with Palo Alto Networks portfolio

An intelligent, connected Palo Alto Networks portfolio provides this top-three South African university with trusted, innovative cybersecurity. Security efficiency has increased by 80%, and the university is on track to achieve a Zero Trust architecture.

paloalto® NETWORKS

IN BRIEF

Customer
North-West University

Partner
KHIPU Networks

Industry
Higher Education

Organisation Size
68,000 students and almost 7,000 staff

Location
Potchefstroom, South Africa

Challenges

See and secure a complex, large-scale environment comprising around 250 modern and legacy Windows servers. Free scarce security resources to concentrate on value-add tasks.

Requirements

+ Gain complete, automated visibility into large, complex IT infrastructure.
+ Minimize the mean time to detect and respond to vulnerabilities.
+ Move to a Zero Trust security architecture.
+ Adopt security based on behavioral analytics, not scripts.

Solution

An intelligent, connected cybersecurity portfolio comprising next-generation, integrated, network and endpoint security, using Cortex XDR, ML-Powered Next-Generational firewall, Threat Prevention, URL Filtering, WildFire, and Panorama.

CHALLENGES

One of South Africa's largest universities

North-West University (NWU) offers more than just an education: it offers people a place in the world. It is one of the largest universities in South Africa, with three integrated campuses serving more than 68,000 students and almost 7,000 administrative and academic professionals.

NWU resembles a mini-metropolis, with an extensive IT infrastructure supporting large volumes of network traffic across multiple campuses and tens of thousands of people. Previously, the university relied on legacy port-based firewalls in its three data centres. However, these firewalls lacked the security, visibility, performance, and scalability needed to control the growing volumes of data entering and leaving the network.

In response, the university standardized four Palo Alto Networks ML-Powered Next-Generation Firewalls (NGFWs) in a high-availability configuration to prevent cyberthreats and enable secure, high-performance access to private network services and the internet. The solution unites Palo Alto Networks WildFire® malware analysis and Threat Prevention—all managed via the centralized Panorama management console—to continuously and reliably secure the university's users, devices, and applications.

The change has transformed network security by:

- Reducing response time to zero-day attacks from days to seconds.
- Introducing complete, granular visibility and control over university traffic, apps, users, and content.
- Blocking known and unknown exploits, malware, and spyware regardless of evasion tactic.
- Enabling secure breakout to the internet without the need for proxies.
- Reducing the time to update firewall configurations by 75%.

REQUIREMENTS

Protection for a large-scale, complex environment

NWU is now looking to the future. With network security in safe hands, attention has turned to endpoint protection. The university was challenged to protect a complex, distributed infrastructure spanning around 250 modern and legacy Windows servers. The existing Microsoft Defender for Endpoint protection solution lacked the functionality, agility, and security insights to counter today's cybersecurity threats.

The small security team faced an array of threats, from ransomware and cyberespionage to fileless attacks and damaging data breaches. However, the biggest concern was not the endless number of risks that dominated news headlines but the frustrating, repetitive tasks they needed to perform every day as they triaged incidents and attempted to work through an endless backlog of alerts.

Martin Venter, Systems Manager at NWU, explains, "We wanted a broad XDR strategy with strong threat prevention. Microsoft Defender couldn't keep pace with the fast-moving threats. The new system needed to defend against every type of attack, provide 360-degree visibility into those attacks, and minimize the mean time to detect and respond to incidents."

The requirements included the ability to:

- Understand and track user identity information.
- Simplify and streamline security operations, automating processes where possible.
- Move NWU towards a Zero Trust security architecture.
- Safeguard large, complex legacy Windows server estate, including around 250 servers.
- Minimize the mean time to detect and respond to vulnerabilities.
- Adopt security posture based on behavioral analytics, not scripts.

Martin and his team conducted a rigorous proof of concept (PoC), analyzing five different endpoint security technologies, including Palo Alto Networks Cortex XDR in a controlled sandbox environment. Cortex XDR outperformed the other endpoint security platforms in almost every respect.

Ease of use was another determining factor in the choice. Venter continues, "Everything is managed through the intuitive Cortex XDR management console, including endpoint policy management, detection, investigation, and response. Plus, we can customize the policies to suit every type of server we use. It's more flexible than any other XDR product we looked at."

> "Cortex XDR won the PoC hands down based on performance. We benchmarked the platform against other top security providers, and Cortex XDR proved more effective than other platforms at protecting the university's endpoints from advanced threats. The visibility it provides is exceptional. The sandbox test demonstrated that the Cortex XDR behavioral analytics would dramatically reduce both alert volumes and investigation time."
>
> **– Ryno Hugo, Systems Engineer, North-West University**

SOLUTION

Next-level detection and response

NWU's Cortex® XDR™ platform blocks advanced malware, exploits, and fileless attacks using behavioural threat protection, artificial intelligence (AI), and cloud-based analysis. The team can investigate threats quickly using a complete picture of each attack, view the root cause of any alert, and swiftly stop attacks across NWU's large-scale, complex environment.

"Before Cortex XDR, we were as blind as moles," says Venter. "Now we have visibility into every transaction and every vulnerability on the servers. We can immediately identify false positives and mitigate breaches. Make no mistake; Cortex XDR has transformed our security operations."

Seamless integration with the ML-Powered NGFW has created an effective and complete cybersecurity portfolio—and moved the university forward on its journey to becoming a Zero Trust enterprise. "We want to eliminate trust from our network architecture and validate each stage of every digital interaction," says Venter. "The connected Palo Alto Networks network and endpoint security portfolio gives us an end-to-end toolkit for Zero Trust. Over time, this strategy will enable us to simplify risk management, whatever the user, user location, or access method," he adds.

This forward-thinking security strategy was spearheaded by KHIPU Networks, one of South Africa's leading cybersecurity specialists and a longstanding, trusted partner to the university.

> KHIPU is one of the most professional and forward-thinking technology partners I have ever encountered. Their professionalism, proactive approach, and expertise enabled NWU to get value from the endpoint security solution almost immediately. They are also always looking ahead, identifying innovations to help NWU stay in front of change.
>
> **– Martin Venter, Systems Manager, North-West University**

BENEFITS

The unified portfolio offers safety and security

The Palo Alto Networks portfolio is simplifying NWU's security operations with one platform for detection and response across all data.

Improved student and staff experience

People can work safely and productively, secure in the knowledge that threats are eradicated without disruption to university operations. Network and endpoint data is secure against policy violations, external threats, ransomware, fileless and memory-only attacks, and advanced zero-day malware.

Increased operational efficiency

By standardizing the portfolio, NWU has achieved an 80% increase in efficiency. This has been achieved by eliminating blind spots with complete visibility, reducing mean time to repair (MTTR), and consolidating the legacy network and endpoint security toolset.

Enhanced security, agility, and productivity

Process automation, AI-based analytics, and custom rules enable the university to react at the speed of thought to security threats. Alerts are configured specifically for the NWU environment, enabling real-time response and reduced risk. Moreover, Cortex XDR can be connected to new servers in less than one minute, compared with up to one week previously using manual processes.

Provides a simple, intuitive experience

The integrated Palo Alto Networks portfolio is easy to use, providing complete, unified visibility across the network, endpoint, and cloud data. Panorama™ network security management ensures centralized management, with powerful insights into network-wide traffic and simplifies configurations.

Looking ahead, NWU may implement KHIPU's eXtended Managed Detection and Response (XMDR) service, which itself utilizes Cortex XDR. Staffed by KHIPU's own certified and experienced cybersecurity professionals, XMDR offers everything from threat visibility, detection, and root cause analysis to behavioral analytics and threat hunting services. The XMDR service also provides a community-driven approach to security, with issues identified by other higher education providers rolled out to all university customers.

> We are benefiting from the best of both worlds. On the one hand, we trust the best-in-class Palo Alto Networks security portfolio to protect the university from sophisticated threats. On the other hand, we are partnering with KHIPU—an exceptionally talented and professional cybersecurity partner. We were like blind moles before—now we have become wise owls.

– Martin Venter, Systems Manager, North-West University

Read this case study to learn how KHIPU Networks uses Cortex XDR, Cortex XSOAR, Cortex Data Lake, and ML-Powered Next-Generation Firewalls to provide Extended Managed Detection and Response.

paloalto NETWORKS

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