

# TELUS Digital secures customer trust and innovation with Palo Alto Networks



## RESULTS AI-powered solutions drive greater efficiency and protection.

65%

Faster time to respond to security incidents.

>38M

Threats blocked in just 30 days.

35%

Reduction in endpoint security false positives.

TELUS Digital, a division of Canadian telecom giant TELUS, plays a critical role in delivering transformative business process outsourcing (BPO) solutions across customer experience, AI services, content moderation and digital consulting. With over 78,000 employees in 31 countries, the company's mission is to empower the human experience through secure, innovative digital enablement.

TELUS Digital's customers trust the company with their digital interactions containing sensitive data, including financial records and proprietary business information. Leadership saw an opportunity to modernize their security strategy away from multiple vendors and toward platformization, reducing complexity while bringing integrated visibility and control over their landscape.

### CHALLENGE

#### On a mission to build and maintain trust.

Given its immense responsibility to secure every digital interaction, TELUS Digital needed to take proactive measures to protect its data, systems and customers. Steve Jablonski, CISO of TELUS Digital, shares, "We came to the conclusion that given our size and spend, going with a platform approach would help us achieve what we wanted very quickly."

The team wanted to:

- Reduce vendor sprawl and security tool complexity.
- Increase visibility and granularity of security controls.
- Provide consistent secure access and policies across global environments.
- Free security staff from excessive manual tasks.
- Secure rapid digital innovation.

### SOLUTION

#### Establishing an application-aware security foundation

TELUS Digital began its transformation by replacing its legacy firewalls with high-availability pairs of Palo Alto Networks Next-Generation Hardware Firewalls across global office locations. This upgrade enabled deep traffic inspection, SSL decryption and application-aware controls that empowered TELUS Digital to enforce policy at a granular level.

The company also deployed similar robust protections for its Google Cloud environment with Next-Generation Software Firewalls. For advanced protection of its network traffic, TELUS Digital added Cloud-Delivered Security Services, including Advanced WildFire, Advanced URL Filtering, Advanced Threat Prevention and Advanced DNS Security.

#### Empowering secure access and user experience everywhere

To better support its globally distributed workforce, TELUS Digital deployed Prisma Access to remote workers worldwide. Security Architect Matt Sarich notes, "With Prisma Access, we can add an entire region with a few clicks and have the same security policies as our firewalls configured, rapidly delivering secure access to our users."

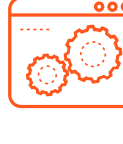
The company also chose Autonomous Digital Experience Management (ADEM) to proactively improve employee experience with applications and Strata Cloud Manager for centralized visibility across its entire network. This comprehensive view showed that the combination of Prisma Access and Next-Generation Firewalls blocked over **38 million threats in just 30 days**.

#### Protecting customer data in the cloud

As TELUS Digital expanded its cloud footprint, it wanted more robust security for its cloud infrastructure and applications. Prisma Cloud allows the company to monitor and secure its clouds, providing comprehensive visibility into cloud assets, vulnerabilities and compliance with security policies. Cortex Xpanse provides an additional layer of security with continuous monitoring of the digital attack surface.

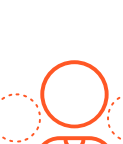
Julio Vivas, Director of Cybersecurity, notes, "Prisma Cloud and Cortex Xpanse are instrumental in helping us secure our infrastructure by providing a holistic view of our cloud environment, enabling us to protect against cyberthreats efficiently."

#### CUSTOMER



TELUS Digital

#### INDUSTRY



High Tech

#### EMPLOYEES



78,000

#### COUNTRY



Global



#### PRODUCTS & SERVICES

Next-Generation Firewalls

- Hardware Firewalls
- Software Firewalls

Cloud-Delivered Security Services

- Advanced WildFire®
- Advanced URL Filtering
- Advanced Threat Prevention
- Advanced DNS Security

Prisma® SASE

- Prisma® Access
- Prisma® Access Browser
- Autonomous Digital Experience Management

Strata™ Cloud Manager

Prisma® Cloud

Cortex Xpanse®

Cortex XDR®

Cortex XSOAR®

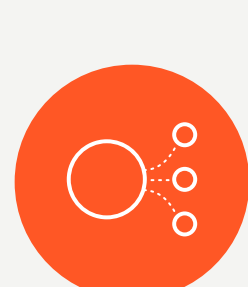
Unit 42® Managed Detection & Response

Unit 42® Retainer

Unit 42® Proactive Services

38M+ threats blocked in 30 days with NGFWs + Prisma Access.

### Path to platformization



**Network segmentation and advanced security treatment**

Next-Generation Hardware and Software Firewalls  
Cloud-Delivered Security Services



**Secure remote access and user experience**

Prisma Access  
ADEM  
Strata Cloud Manager



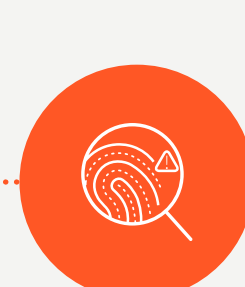
**Cloud-native application protection**

Prisma Cloud



**SOC modernization**

Cortex XDR  
Cortex XSOAR  
Cortex Xpanse



**Cybersecurity expertise and managed services**

Unit 42 MDR  
Unit 42 Retainer  
Unit 42 Proactive Services

### Streamlining investigations for value-add work

Another important area of focus for TELUS Digital was modernizing its security operations. The company replaced legacy endpoint security and incident response automation solutions with Cortex XDR and Cortex XSOAR. The built-in analytics of **Cortex XDR reduced false positives by 35%**, enabling security analysts to focus on the issues that matter most. Automated playbooks from Cortex XSOAR can respond to most threats without the need for human intervention. The combination of automations, analytics and comprehensive visibility has streamlined investigative processes, **reducing mean time to respond (MTTR) by 65%**.

### Scaling a lean team with managed services

To manage the global scale of the organization, TELUS Digital added Managed Detection and Response (MDR) from Unit 42 to improve its cyber defenses with 24/7 monitoring, expertise, proactive threat hunting and remediation. Vivas notes, "Our security posture is strengthened with Unit 42 MDR and its ability to correlate events across our comprehensive suite of Palo Alto Networks products, from firewalls to endpoints and cloud environments, enabling faster and more accurate response to threats." Unit 42 MDR helps TELUS Digital protect 20% more endpoints with no increase in staff.

The company also added a Unit 42 Retainer to not only have incident response experts on call for deeper investigation of any suspicious activity, but also to enhance preparedness through proactive services like tabletop exercises.

35% reduction

in false positives with Cortex XDR.

65% faster time

to remediate security incidents with Cortex XDR + XSOAR.

What we're excited about with Prisma AIRS is the ability to see how API calls are being made. We can look at malicious detections that are being performed by AI tools across the board."

Steve Jablonski, CISO, TELUS Digital

### Making plans for tomorrow's security challenges

As teams within TELUS Digital rely more on AI tools, namely **Fuel iX™**, the company has begun evaluating Prisma AIRS to provide comprehensive runtime protection against new AI-related risks. "What we're excited about with Prisma AIRS is the ability to see how API calls are being made. We can look at malicious detections that are being performed by AI tools across the board," says Jablonski.

Recognizing how the increasing use of SaaS has made the browser the primary location for work, the company is also piloting Prisma Access Browser. Sarich shares, "Prisma Access Browser will give us granular control into the browser-based applications that our employees use and the actions they can perform within them."

The solution allows organizations to onboard and offboard employees in minutes. Its Chromium-based design delivers a familiar browsing experience for users that requires zero learning curve, securing the workspace on any device with no disruption.

### Holistic visibility and control brings peace of mind.

By platformizing with Palo Alto Networks, TELUS Digital has gained peace of mind over the security posture of its infrastructure, apps, data, users and devices. Jablonski confirms, "This approach has enabled us to accelerate the overall deployment of security to the organization, giving us significantly more visibility and control across a global landscape." The security team can now drive the business forward with proper oversight, enabling the company to lead the digital solutions industry in secure innovation.

Find out more about how Palo Alto Networks **AI-driven network security platform** and **AI-driven security operations platform** can transform your organization.

Working with Palo Alto Networks, we've been able to simplify our overall security footprint and deliver tremendous value, not only to our organization, but to our customers as well."

Steve Jablonski  
Chief Information Security Officer  
TELUS Digital

Get started with platformization to simplify your security approach.

CONTACT US