TELUS Business | paloalto NETWORKS

eBook

Integrating AI Access controls.

Secure your network in the age of Generative AI.



Table of contents

01 Introduction

02 The state of Generative AI

03 AI risks and the Canadian threat landscape

04 Defending against AI-based threats with Palo Alto Networks

05 Embedding AI guardrails with TELUS Managed Services

06 Why TELUS with Palo Alto Networks

Introduction

The reality is clear: AI has arrived, and is no longer a distant concern; it is an active operational reality.

As organizations rapidly embrace Generative AI (GenAI) to drive productivity and innovation, the traditional security perimeter has vanished. Threats now move at machine speed, requiring intelligent security that evolves just as fast.

To thrive through this shift, network security must evolve to become intelligent and adaptive. Rather than slowing progress, intelligent AI security could act as the ultimate accelerator for innovation. By embedding adaptive controls, data protection, and real-time guardrails directly into the environment, organizations can establish the trusted foundation necessary to unlock safe, high-velocity AI deployments.

Today, robust security guardrails allow organizations to confidently innovate at AI speed; and for security leaders, the mission is clear: show executive leadership that intelligent security controls don't slow down AI, they propel it forward.

By securing the environment at its core, organizations today can gain the confidence to deploy AI more broadly and faster, while still providing secure access and protecting intellectual property.



The state of Generative AI.

Today, organizations are embracing AI at an incredible pace, and this explosive growth has fundamentally altered the digital landscape. Increased adoption and usage mark a shift from GenAI as a novelty to an essential business utility.

GenAI transformation by the numbers

Stats as shown in the 2025 Palo Alto Networks publication – The State of Generative AI.

890%

GenAI traffic surged more than 890% in 2024.[1] This explosive growth may be attributable to maturing AI models, greater enterprise automation, and higher adoption due to more evident productivity gains.

2.5X

Data loss prevention (DLP) incidents for GenAI more than doubled. In 2025, the average monthly number of GenAI-related data security incidents increased 2.5X, now comprising 14% of all data security incidents.[1]

10%

Organizations saw on average 66 GenAI apps, with 10% classified as high risk.[1] The widespread use of unsanctioned GenAI tools, lack of clear AI policies, and pressure to adopt AI quickly without proper security controls can expose organizations to significant risk, especially from high risk GenAI apps.

The hidden danger of "Shadow AI."

While GenAI tools may unlock new opportunities, the widespread use of unsanctioned GenAI tools and the pressure to adopt AI quickly, often without proper security controls, could potentially expose organizations to significant risk. This introduces Shadow AI risk, which refers to the unauthorized use of AI tools by employees without the knowledge or governance of IT departments.

If employees use unapproved AI tools, they may unknowingly expose the organization to potential data leaks. Operating outside of IT oversight, Shadow AI may create blind spots where sensitive data might be leaked or even used to train third-party AI models. As unauthorized AI tools from writing assistants to coding apps become more prevalent, organizations may face escalating risk exposure.

AI risks and the Canadian threat landscape.

According to the 2025 Palo Alto Networks publication The State of Generative AI, in 2025, the average monthly number of GenAI-related data security incidents increased 2.5X, contributing to 14% of all data security incidents globally.

As Generative AI adoption accelerates across Canadian enterprises, security leaders face a dual challenge: neutralizing machine-speed cyber threats while ensuring sensitive intellectual property and customer data remain strictly governed within domestic borders.

Without proper IT security oversight, unauthorized use of GenAI apps may lead to potential risks such as:

Data exposure and exfiltration

GenAI apps require vast amounts of data to function. Sensitive data, proprietary source code, or personal information could be inadvertently leaked to third-party models if not properly controlled.

Unauthorized access

Hackers could potentially gain access to sensitive data that was inadvertently used to train third-party AI models.

Insecure AI interactions

Manipulated AI models could respond with malicious links, malware, or allow their use for unintended purposes.

AI-Generated Phishing

Bad actors may utilize adversarial AI to generate highly convincing, evasive phishing pages.

Beyond direct security risk, regulatory compliance is now a top concern for organizational leadership as well. Moving data across borders is a top risk for enterprise CISOs in Canada. Security teams must stay accountable under PIPEDA and the proposed Consumer Privacy Protection Act (CPPA), which require contractual safeguards and disclosure for data sent to third parties, while Quebec's Law 25 (where applicable), goes further and requires a formal risk assessment before data crosses provincial or national borders.

Additionally, in June 2026, the new Bill C-8 came into effect and established enforceable cybersecurity obligations and strict oversight across federally regulated sectors such as banking, telecom, energy and transportation. Under the law, organizations must systematically manage supply chain vulnerabilities and report cyber incidents to federal authorities.

Rising data risks and increasingly stringent compliance standards are putting immense pressure on today's businesses. To maintain a competitive edge, forward-thinking leaders now have the opportunity to adopt AI Access controls to help protect their organizations from AI data leaks and aim to meet strict regulatory requirements while still keeping speed to market.

Defending against AI-based threats.

Palo Alto Networks security solutions help organizations address the critical need for robust security in the face of rapid AI adoption. As a recognized global cybersecurity leader, they contribute to shaping the future with continuous innovation to seize the latest breakthroughs in artificial intelligence, analytics, and automation. To combat the specific vulnerabilities introduced by generative AI, Palo Alto Networks has pioneered tools that natively embed security into AI workflows.

AI threat defence—powered by Palo Alto Networks, Managed by TELUS Business.

Security Service Edge (SSE) with Prisma Access

Provides real-time Shadow AI discovery with an extensive, continuously updated GenAI app catalog designed to detect, profile, and track employee interactions with unapproved and unsanctioned AI platforms.

Browser Security with Prisma Browser

Embeds enterprise-grade Data Loss Prevention (DLP) and policy controls directly inside the web browser, allowing organizations to block data exfiltration. This includes pasting source code or Personal Information (PI) into unsanctioned GenAI tools by contractors and third parties operating on unmanaged personal devices.

By enforcing uniform, cloud-native platform security across every user, device, app and location, these solutions are designed to help eliminate the security gaps exploited by modern attackers. This holistic approach delivers proactive, enterprise-wide defence to neutralize advanced threat vectors and helps minimize the risk of AI-driven data breaches.



Comprehensive AI Access Security controls.

To combat technology sprawl and complexity, a modern security solution should consolidate multiple security capabilities into a single cloud-delivered platform. TELUS Managed Security Service Edge (SSE) powered by Palo Alto Networks is designed for this reality, allowing organizations to systematically implement AI guardrails and close security gaps at their own pace without disrupting operations.

TELUS Managed SSE provides a suite of intelligent, cloud-native AI security controls designed to help secure data in the age of AI. These include:

- **Shadow AI Discovery & App Control:** Provides identification of unapproved AI tools being used across the network, and gives administrators the ability to block unsanctioned AI tools.
- **Advanced Data Loss Prevention (DLP):** Provides detection of sensitive corporate data, PI, or intellectual property hidden inside unstructured, conversational prompts, to help prevent data leakage.
- **Data Masking & Anonymization:** Provides masking of sensitive information from a user's prompt before it leaves the corporate perimeter and hits an external AI model.
- **AI-Generated Phishing Detection:** Provides analysis of page rendering and text patterns to detect highly convincing, evasive phishing pages generated by adversarial AI.
- **Insecure Output Filtering:** Provides analysis of the responses generated by AI to ensure they don't contain malicious code.

A phased approach to network transformation.

TELUS helps to accelerate your security transformation by deploying core Palo Alto Networks SSE capabilities with Prisma Access including Zero Trust Network Access (ZTNA), Secure Web Gateway (SWG), and Cloud Access Security Broker (CASB) fortified with AI-driven security controls to protect your business as it evolves.

As of 2026, TELUS has expanded its ecosystem to offer Prisma SD-WAN, which integrates with Prisma Access to deliver a complete Palo Alto Networks SASE framework. This integrated offering is designed to help eliminate architectural complexity by consolidating disparate security and networking tools onto TELUS' secure national infrastructure, boosting security, optimizing performance, and delivering complete end-to-end support through a single trusted partner.

To support today's extended enterprise, we also offer Managed Palo Alto Networks Prisma Browser, a solution designed to extend zero-trust security to contractors and third-party vendors and to safeguard critical assets even on unmanaged, non-corporate devices.

Why TELUS with Palo Alto Networks.

Disjointed security and networking tools can generate frustrating latency and operational overhead. By unifying the Palo Alto Networks cloud-native SSE platform with Palo Alto Networks networking capabilities over TELUS' high-performance national infrastructure, enterprises can unlock low-latency secure access to critical applications and AI tools all while streamlining procurement under one contract and vendor management through a single accountable partner.

The TELUS advantage

Decades of frontline experience

Leveraging over 20 years of experience managing security for hundreds of Canadian organizations, we apply the same methodologies used to safeguard Canada's own national telecommunications infrastructure.

All-Canadian Security Operations Centre (SOC)

We provide 24x7[2] monitoring and response backed by highly skilled experts operating inside our state-of-the-art Canadian bilingual SOC.

A longstanding partnership

TELUS has a 15+ year relationship with Palo Alto Networks and is one of the largest MSSP partners in Canada. We have met the most stringent training requirements, making us one of the most certified partner in the country with over 50 certified Palo Alto Networks experts on staff.[3]

We don't just help you to safeguard your network, we are your long-term partner, working with you to adapt your defense and provide solutions designed to meet constantly evolving security needs.

Don’t let your network fall behind in the age of AI.

Reach out to a TELUS expert today to learn how our TELUS Managed cybersecurity services powered by Palo Alto can accelerate your AI transformation and defend your business against next-generation threats.

telus.com/Cybersecurity

1 The State of Generative AI 2025 © 2025 Palo Alto Networks, Inc.

2 Subject to power availability, network usage constraints, and other factors outside TELUS' control. See our Service Level Agreement for specific uptime guarantees and service exclusions.

3 Figures and partnership status verified by Palo Alto Networks as of April 2026.