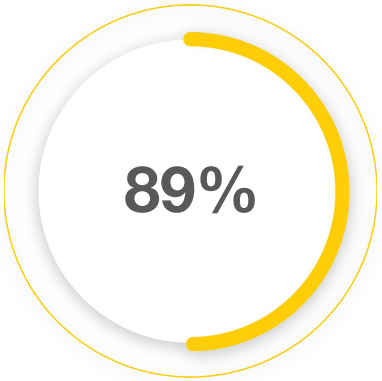
The AI Paradox:
Securing the Next Generation of K-12 Education

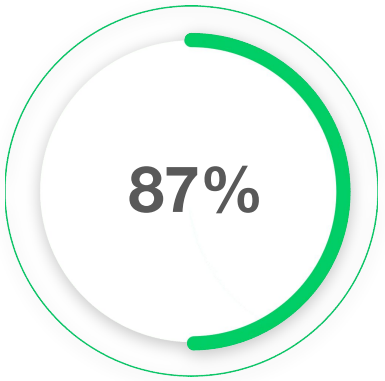
Ashley Anderson | DSM, Public Sector - Western Canada
November, 2025

Education + AI | it's in the Numbers

60% of teachers have **incorporated AI** into their regular teaching routines.



89% of students **admit to using ChatGPT** for homework assignments. With many stating it's their "first instinct" for assignment and project work.

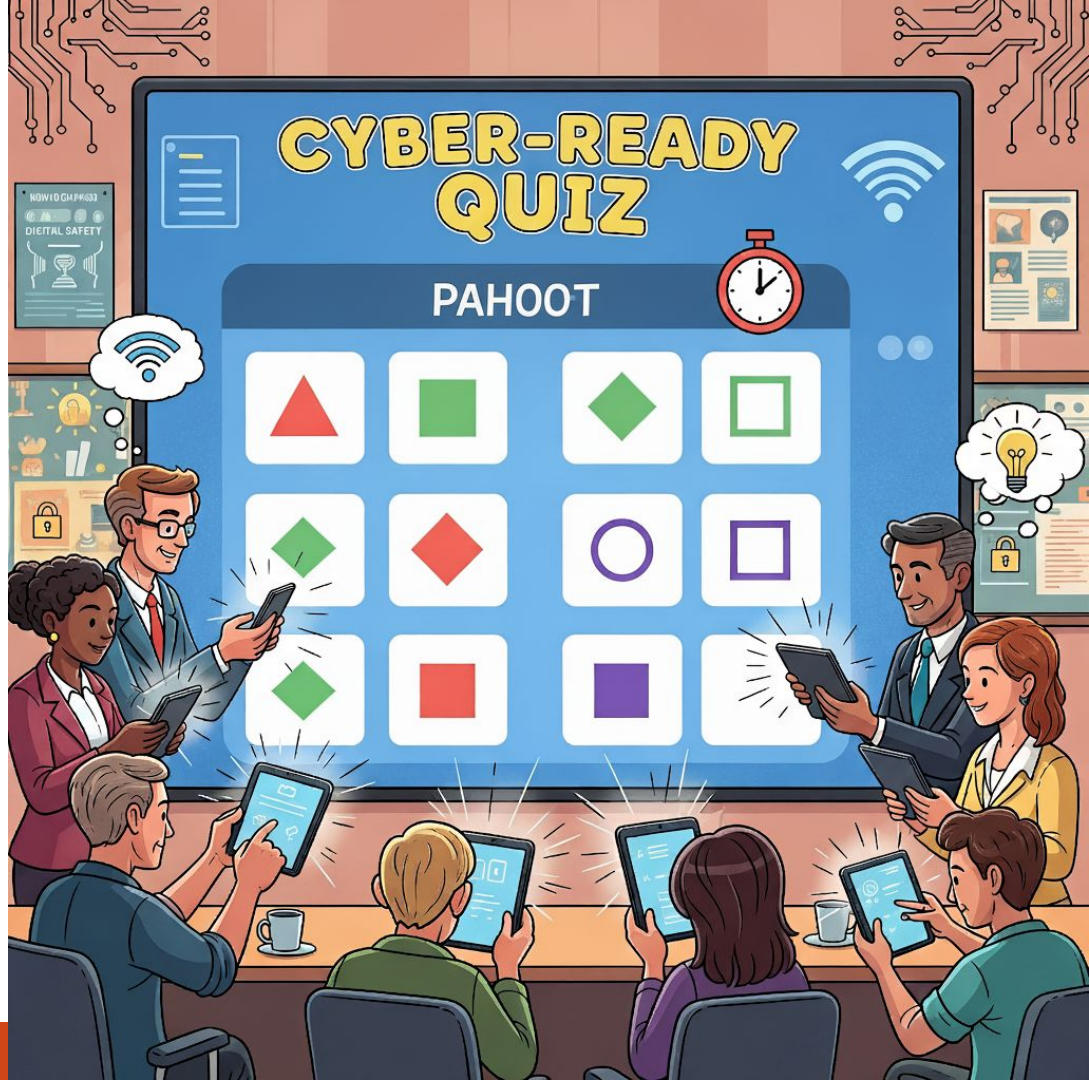


87% of organizations reported **being targeted by an AI cyberattack in the last year**.

Common AI-powered attacks include phishing (37% of AI breaches) and deep fakes (35% of AI breaches).

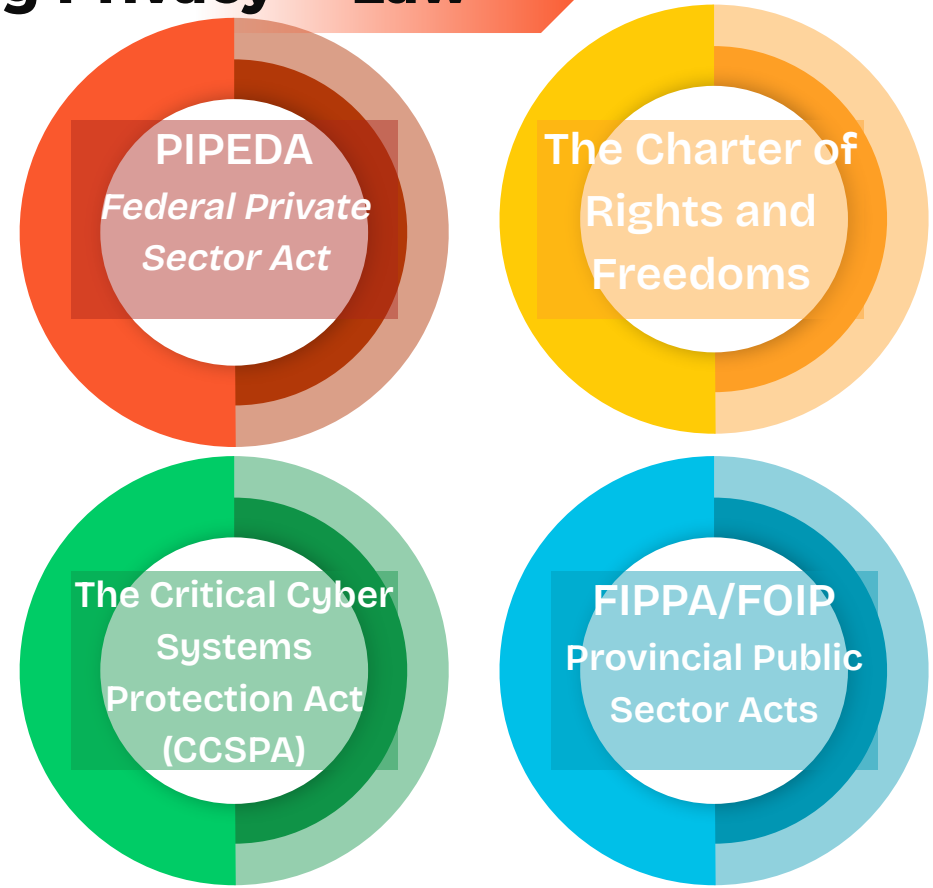
Cybersecurity for K-12 Leaders: Are you ready, British Columbia?

- Welcome K-12 leaders to this essential session.
- We will use this totally unique “PAhoot” Quick (you guessed it, for Palo Alto…and we will have a hoot
- This quick quiz assesses your organization's cyber-readiness.
- Learn about your school district's current knowledge around security posture.



Question 1: The Governing Privacy Law

In most Canadian provinces, the law that directly governs public school board's collection, use and disclosure of student and staff personal information (PII) is:



Question 1: The Governing Privacy Law

Public school boards in Canada are generally considered public bodies. This means **they fall under provincial privacy legislation like the Freedom of Information and Protection of Privacy Act (FIPPA) in Ontario and BC, or FOIP in Alberta.** The federal PIPEDA primarily applies to private sector organizations and private schools. This is a critical distinction for compliance and policy development.

Question 2: Third Party Liability

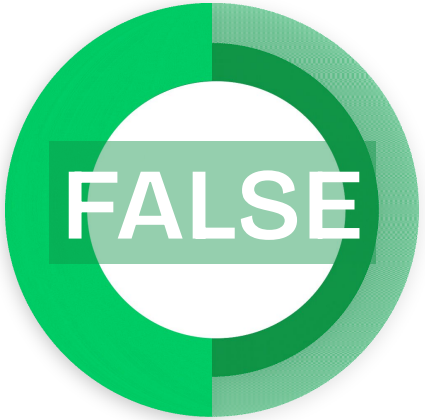
True or False?

If a data breach occurs through a third-party vendor (like a student information system or learning app), the school board is not liable because they don't technically own the software of cause the breach.

Question 2: Third Party Liability

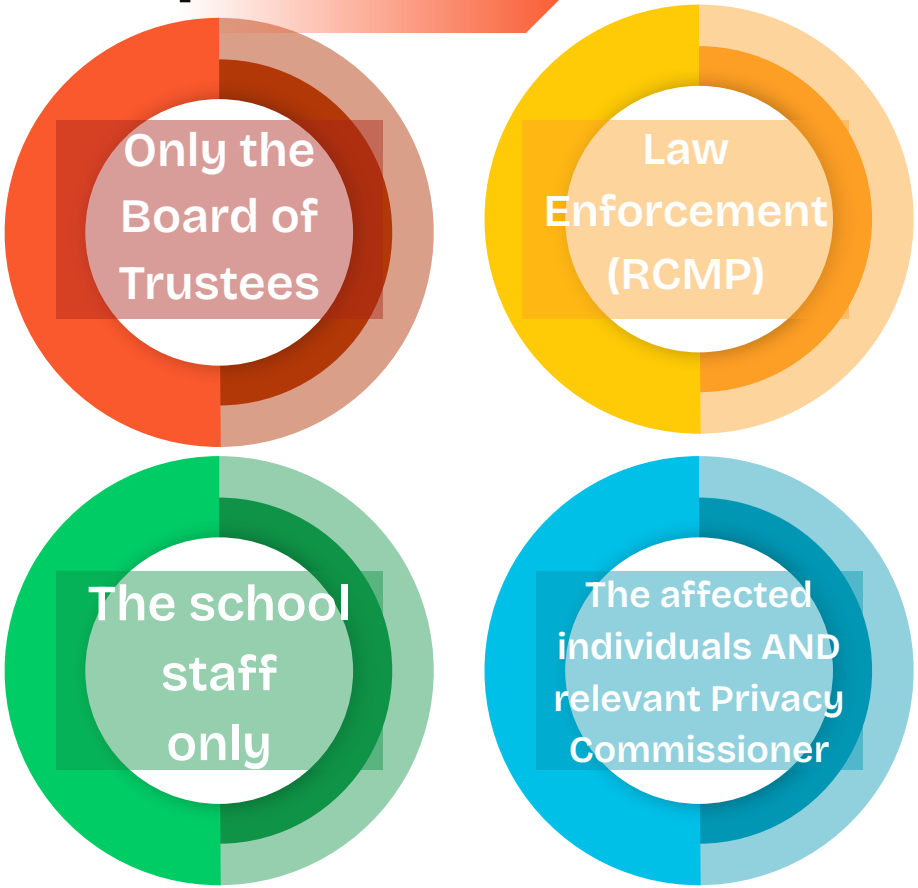
False

In Canada, **school boards remain accountable for the Personal Identifiable Information (PII) that is 'in their custody or control,' even if a vendor technically stores or processes it.** High-profile breaches involving vendors (e.g., PowerSchool affecting many boards) highlight that school leaders must demonstrate they had 'reasonable measures' and robust oversight in place for all third-party service providers. Due diligence in vendor contracts is key!



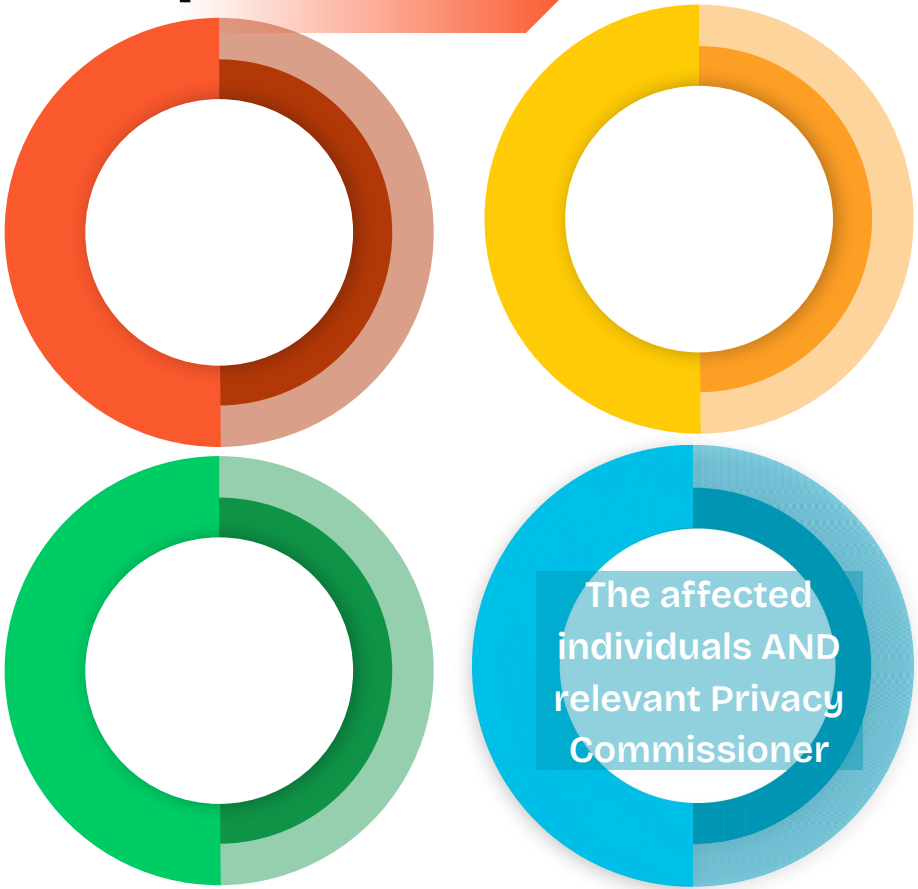
Question 3: The Required Response

Under Canadian privacy principles, when a data breach occurs at a school board, an administrator's first legal obligation is to notify:



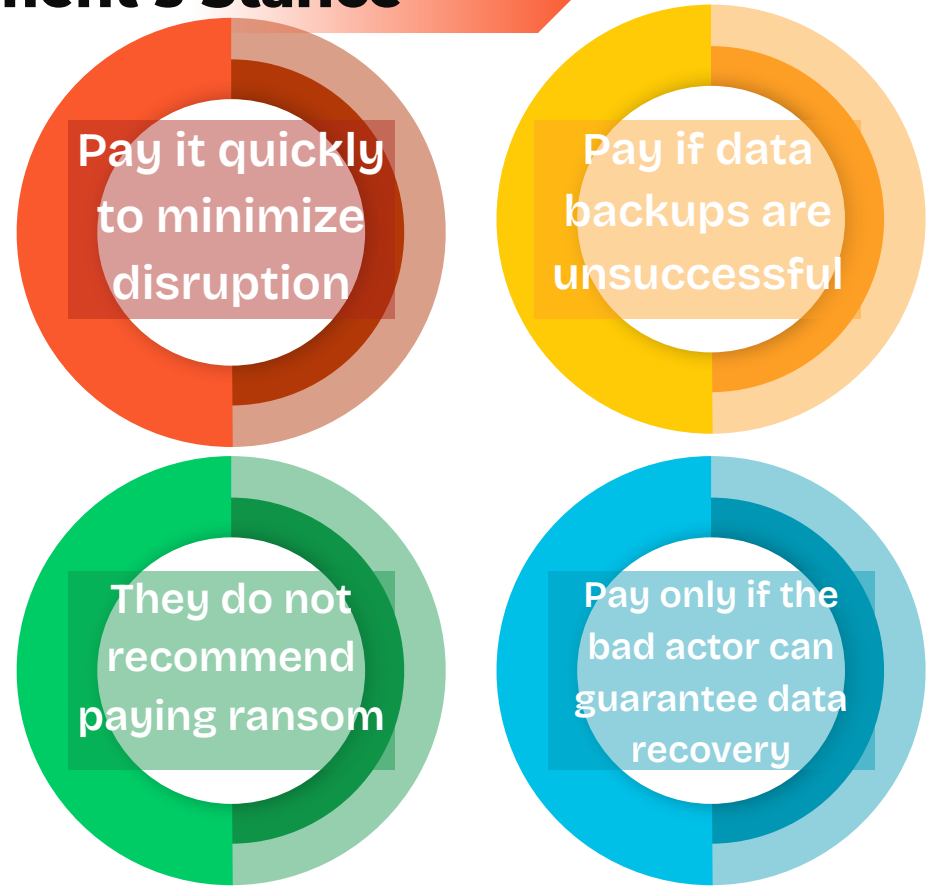
Question 3: The Required Response

The immediate legal obligation in Canada is to **notify the individuals whose data was compromised (students/staff/parents) and the relevant provincial or federal Privacy Commissioner.** This is especially crucial if the breach creates a **Real Risk of Significant Harm (RROSH)**. Proactive communication and compliance with these notification requirements are fundamental to Canadian breach accountability.



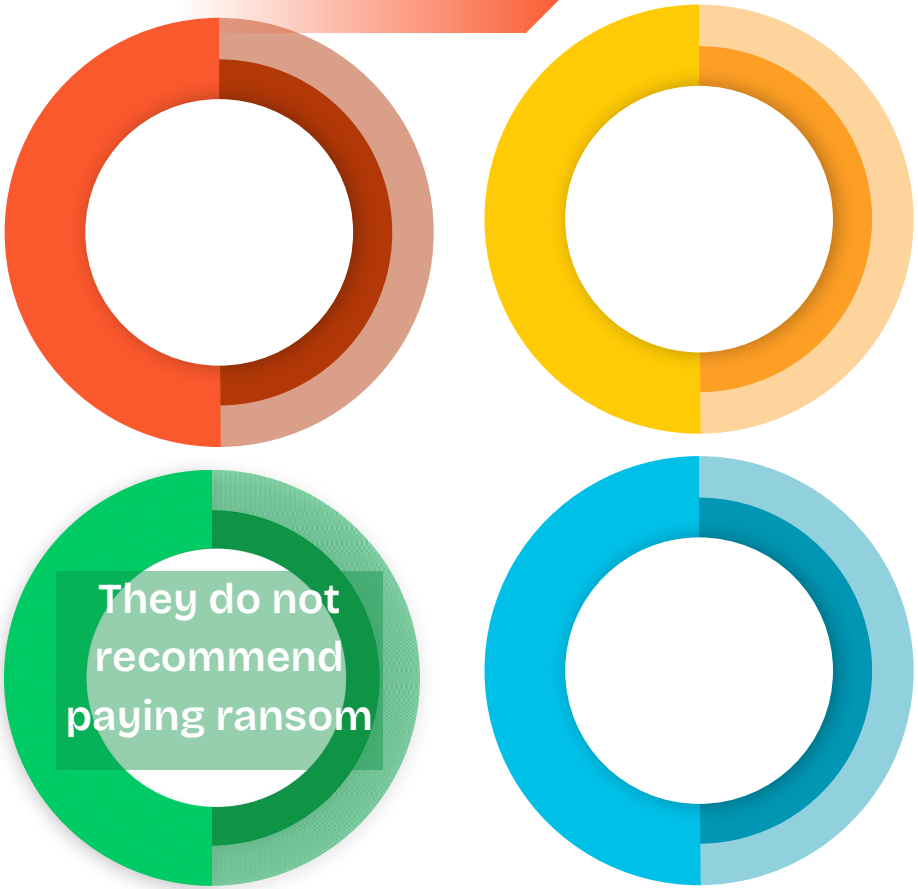
Question 4: The Government's Stance

What is the official recommendation of the Canadian Centre for Cyber Security, and the Government of Canada, regarding paying a random to cybercriminals during a ransomware attack?



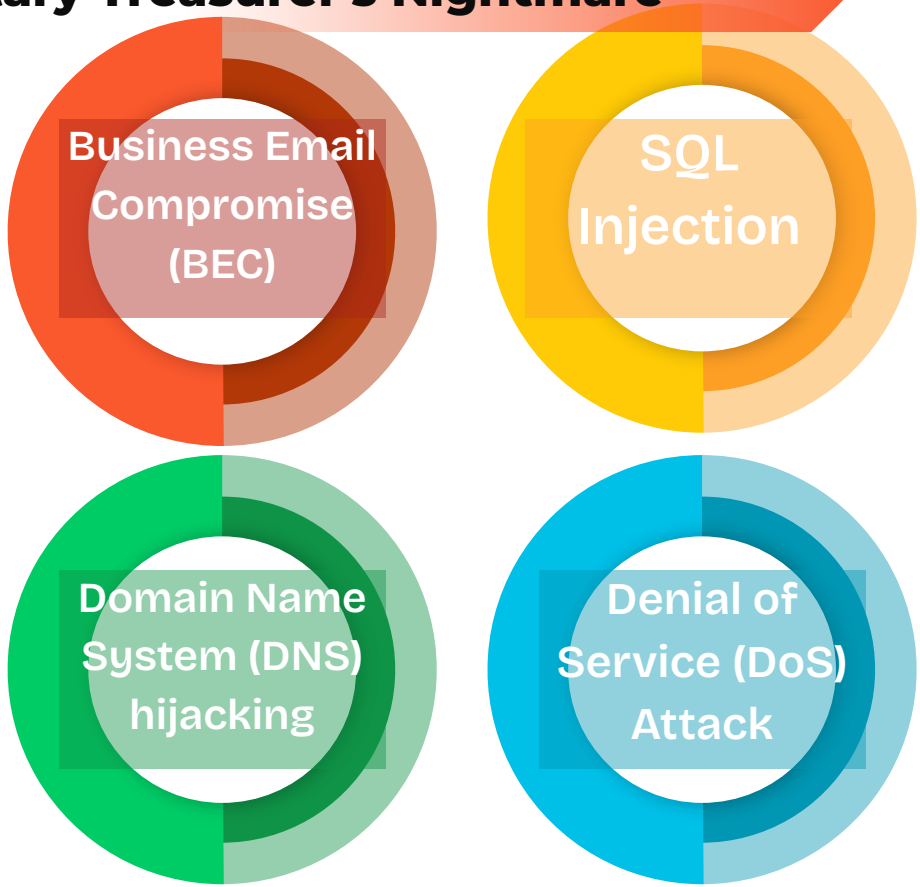
Question 4: The Government's Stance

The official stance of the Canadian Centre for Cyber Security is to not pay the ransom. **Paying fuels criminal activity, marks you as a potential repeat target, and offers no guarantee that your data will be returned or systems unlocked**. For school leaders, the focus must be on robust preventative measures and a tested **Incident Response and Recovery Plan** to restore systems without resorting to paying criminals.



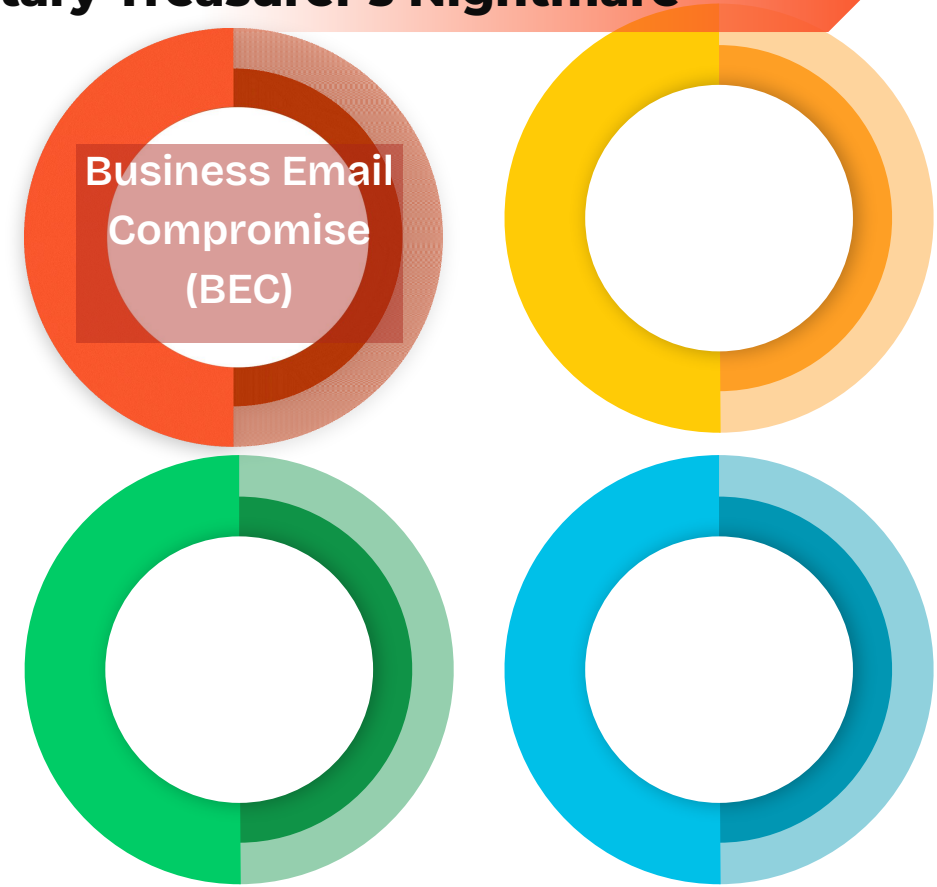
Question 5: The CFO / Secretary Treasurer's Nightmare

Which common cyber attack specifically targets the Business Office, and involved finance staff members being tricked into making unauthorized wire transfers to an attacker (without involving ransomware?)



Question 5: The CFO / Secretary Treasurer's Nightmare

Business Email Compromise (BEC) is a sophisticated, non-technical fraud. An attacker, **often impersonating a Superintendent, CFO, or trusted vendor, sends an urgent, fraudulent email to a finance team member** requesting an immediate wire transfer. It bypasses technical network security by exploiting administrative processes and human trust. For CFOs and Secretary Treasurers, this makes **continuous, realistic staff training on awareness & controls absolutely critical.**



Key Takeaways (from our PAhoot) for our K-12 Leaders:

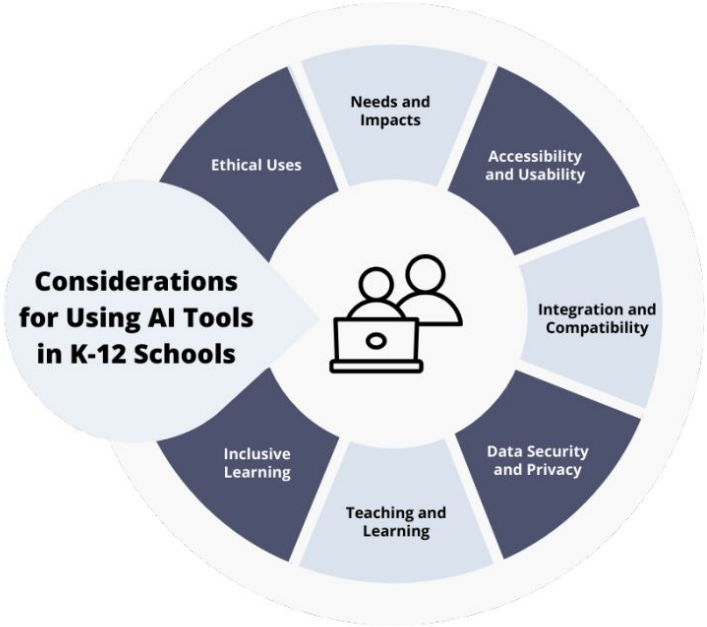
- Cybersecurity is a **governance and financial risk** issue, not just an IT problem.
- Understanding **Canadian privacy laws** (FIPPA/FOIP) is paramount.
- **Vendor oversight** and **Incident Response Plans** are critical.
- **Human error** (e.g., phishing) remains the top threat.
- **Ongoing staff education** is your best defense.

Call to Action:

Let's continue too work together to build cyber-resilient school environments!

GOOD NEWS! AI Is Already Here and Helping

- Students currently use AI tools for daily schoolwork
- Teachers leverage AI for planning lessons and grading automation
- Rapid adoption of AI brings both great opportunities to innovate and augment.
- BC is ahead of the curve! [Publishing Considerations for using AI tools in K-12]



Source: Consideration for Using AI Tools: Ministry of Education and Child Care

School boards

School boards may find the following sections of this document particularly relevant to their roles:

- Ethical Uses
- Needs and Impacts
- Accessibility and Usability
- Integration and Compatibility
- Data Security and Privacy

School district leaders

District leaders may find the following sections particularly relevant to their roles:

- Ethical Uses
- Needs and Impacts
- Accessibility and Usability
- Integration and Compatibility
- Data Security and Privacy
- Teaching and Learning
- Inclusive Learning

School leaders

School leaders may find the following sections particularly relevant to their roles:

- Ethical Uses
- Needs and Impacts
- Teaching and Learning
- Inclusive Learning

Teachers

Teachers may find the following sections particularly relevant to their roles:

- Ethical Uses
- Teaching and Learning
- Inclusive Learning

AI Is Benefiting Attackers

in the Same Ways It Benefits Education

AI is reshaping attacker productivity

4X the number of new attacks/day[1]

2024	2025
2.3M	8.95M

The time to carry out a ransomware attack is down >100X[2]

Before AI	After AI
48 hrs	25 min

Exposure issues are now real time

1/3

of new vulnerabilities exploited in <24 hours[3]

Sources: 1. PANW data, 2. Unit 42 develops agentic AI attack framework, 3. The Hacker News Q1 2025 CVE analysis

paloalto NETWORKS

And it’s in the News…

CBC

Cyberattacks can take entire school networks out. It’s time to pay more attention to them, experts say

Cyberattacks can derail day-to-day operations in every single school
integrat ide networks and endanger the vast...

K-12 Dive

Ransomware attacks in education jump 23% year over year

Education was the fourth
a report from C -targeted sector during the first half of 2025, according to

The Macdonald-Laurier Institute

Canada’s schools are sitting ducks for cybersecurity attacks: Paul W. Bennett in The Hub

The recent PowerSchool cyber attack highlights just how vulnerable students' personal
is to theft.

K-12 Dive

Data breach reporting lags in education sector, study finds

The sector reportedly takes an average of 4.8 months to report attacks — higher than for business, government and healthcare.

May 15, 2025

Cybercrime Magazine

Cybercriminals Get An A+ In Hacking K-12 Schools

Ransomware attacks on K-12 schools are projected to increase by 86 percent in 2021. That's right. 86 percent.

Aug 3, 2025

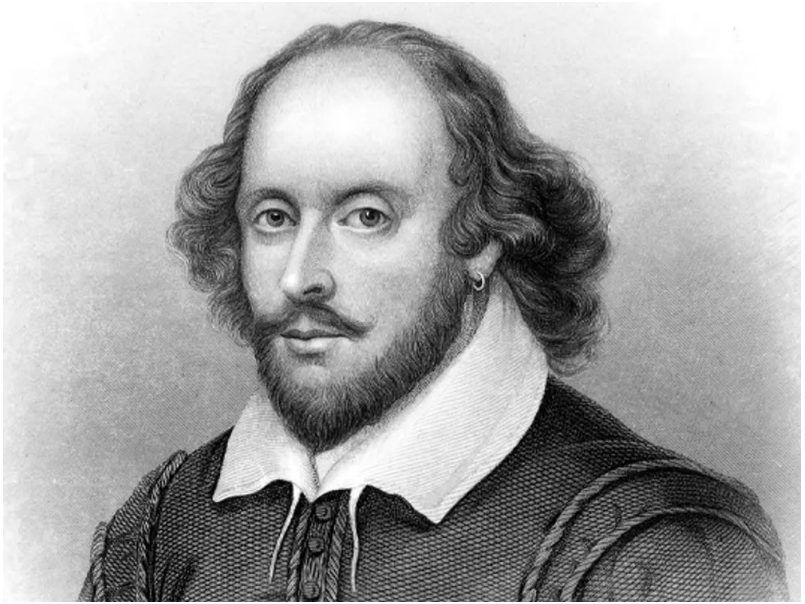
Common K-12 Challenges

- Limited school budgets constrain cybersecurity staff resources
- K-12 systems have a vast and complex attack surface
- Critical school operations cannot tolerate any downtime
- Small IT teams face automated, AI-powered attacks 24/7

Alert Fatigue: What does this mean for IT Teams?

- Traditional security tools generate massive amounts of alerts.
- Low-confidence alerts force teams to chase false positives all day.
- Manual correlation of security data is inefficient and slow.
- Overwhelmed teams often miss the critical threat amongst the noise.

An unlikely relationship



Fight AI With AI

- The only effective defense against automated AI attacks is AI
- Transition to an AI enabled security platform
- Stop manually managing alerts and start automating defense
- Equip small teams with a powerful virtual 24/7 security analyst or managed services
- Focus on buying a smarter tools, not just more security tools.. Sometimes less is more!

What's Needed to Secure GenAI App Adoption

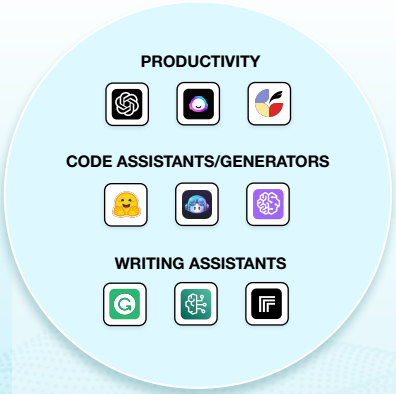
Challenges

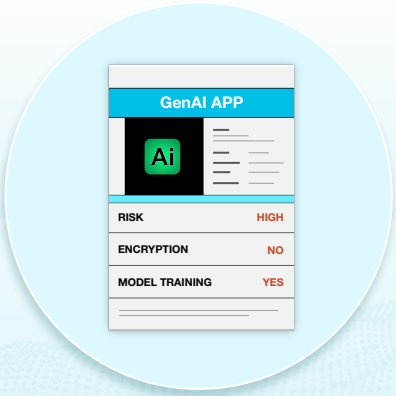
Democratization of AI app creation has led to sprawl of insecure apps.

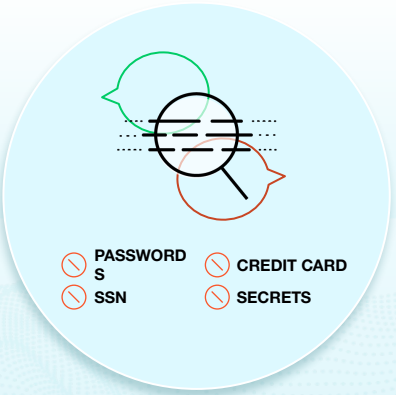
AI apps store, learn, and reiterate data.

AI apps ingest unstructured inputs and generate diverse outputs.

Rapidly evolving, powerful apps are readily accessible through marketplaces.







Comprehensive GenAI app catalog that keeps pace with the boom.

Visibility into AI apps that train on data.

Granular data controls with context-aware ML based detectors.

Ability to protect against threats in GenAI responses.

Visibility and control of 3rd-party AI plugins.

Detect plugins with excessive permissions.

Solutions

paloalto NETWORKS | PRISMA

Data Security is Key

Secure Enterprise Browsers are allowing students, teachers and administrator to control where and how their sensitive data is accessed and used

Consolidated DLP practices are allowing for schools to apply protections across their data in transit, in use, and at rest.

Utilization of current technologies with a “data mindset” has other K-12 Districts ahead of the curve.

AI Access Security to Enable Safe AI Adoption

Real-time visibility of AI usage

View what AI apps are used and by whom.

Access control

Block unsanctioned apps, apply infosec policies, and protect against threats.

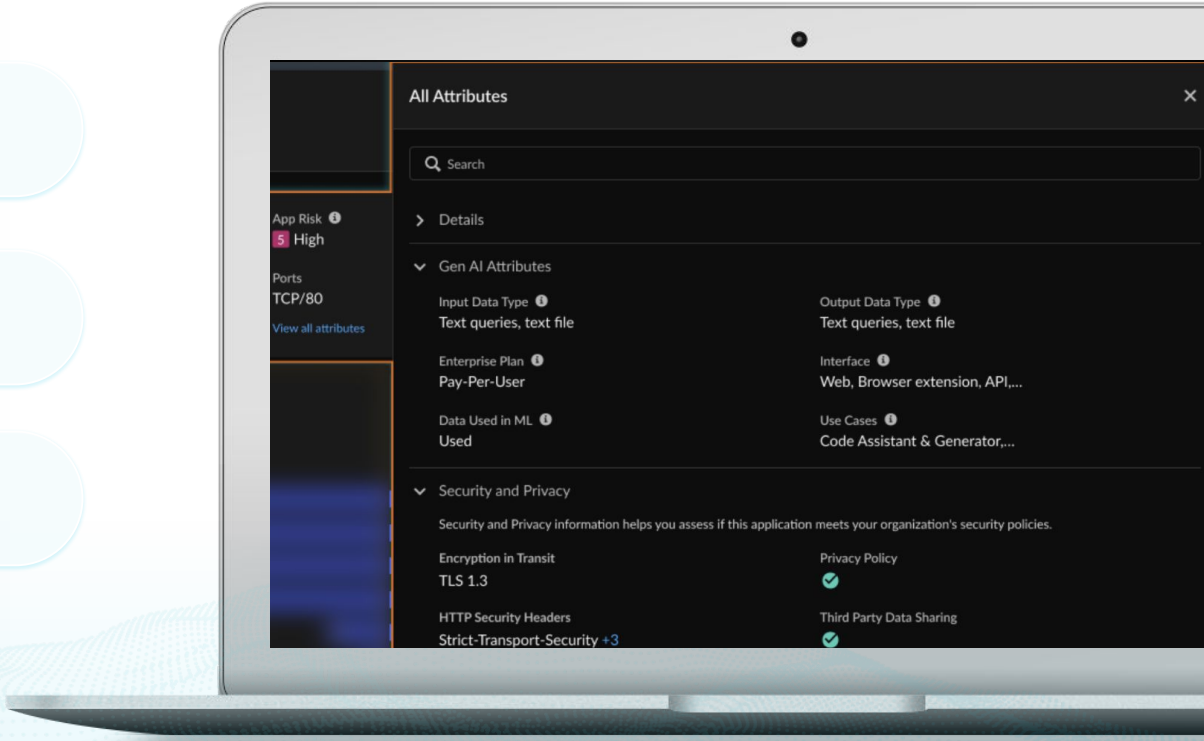
Comprehensive data protection

Scan what data, secrets, and IP are shared.

paloalto NETWORKS | PRISMA

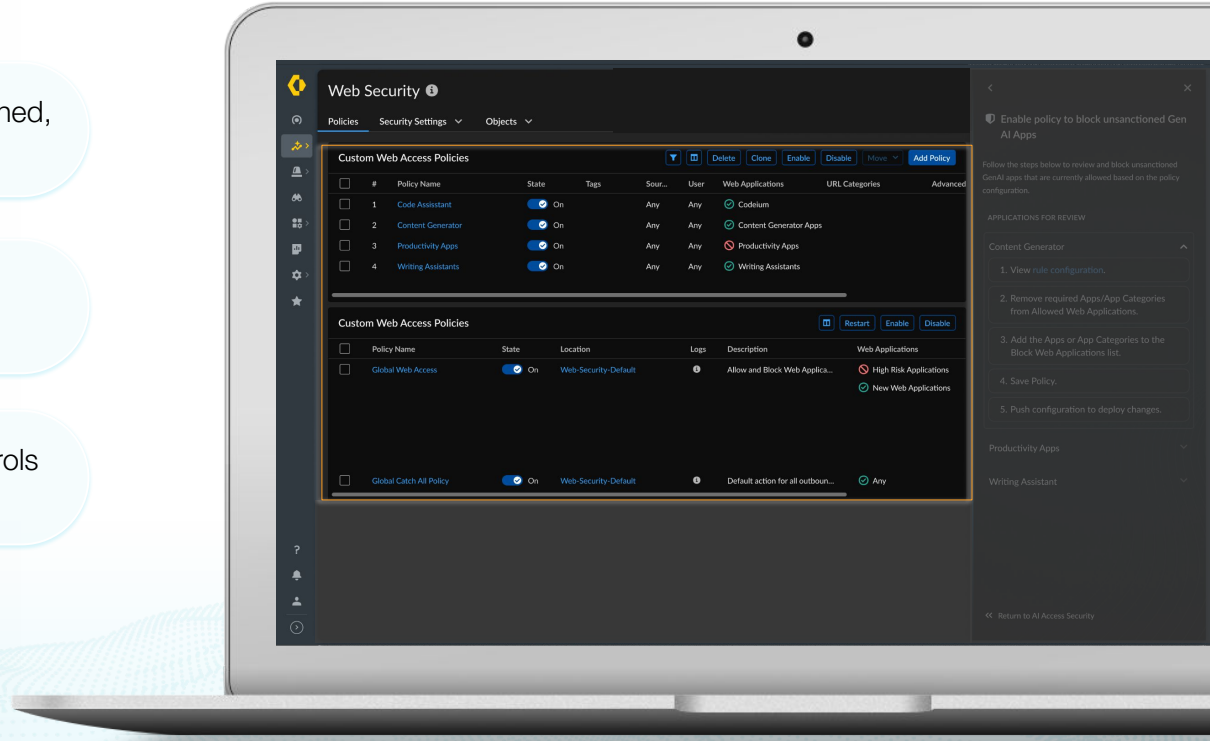
Step 1 Visibility Into AI Apps

- Discover **GenAI app** usage across different use cases.
- Detailed catalog of **1K+ GenAI** applications.
- In-depth visibility into **60+ application attributes**.



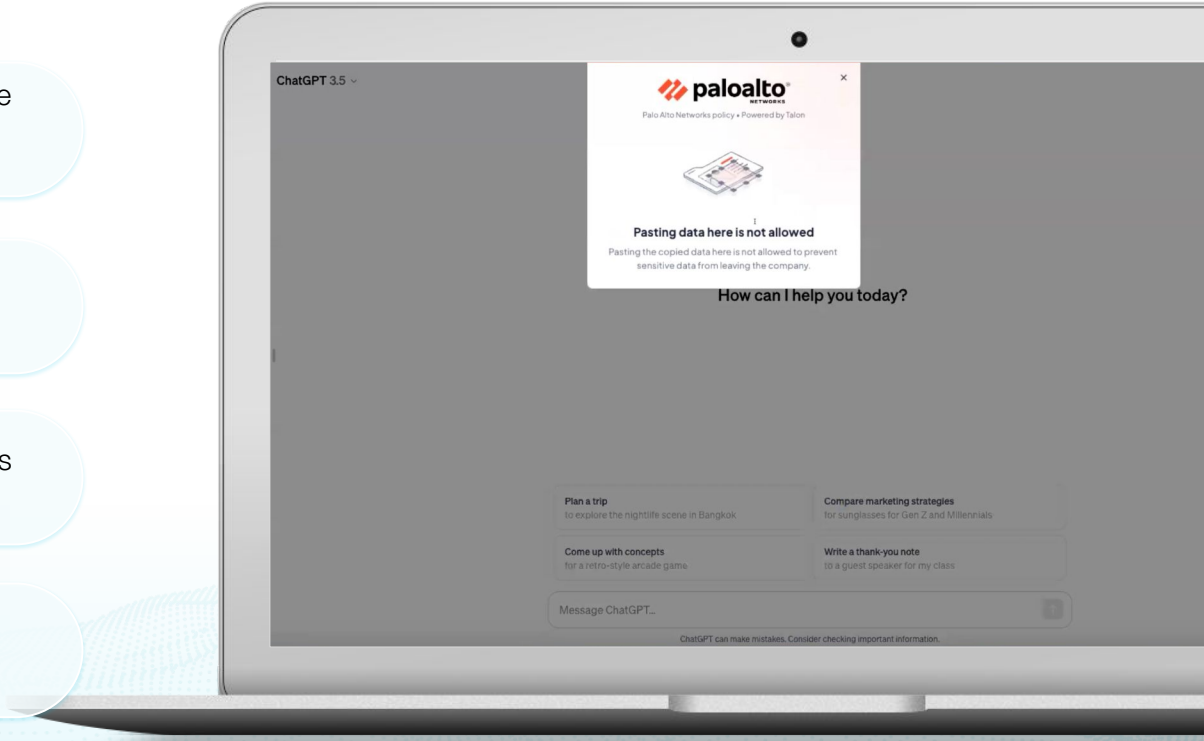
Step 2 Classification and App Access Controls

- **Classify applications** across sanctioned, tolerated, and unsanctioned.
- Get tailored **visibility and control measures** for each use case.
- Set up robust application access controls with **OOTB best practice policies.**



Step 3 Data Access Controls

- Utilize LLM powered and context-aware ML models to classify data across **300+ categories**.
- Set up **contextual inline policies** to prevent sensitive data exfiltration to GenAI apps.
- **End-user coaching** via Prisma Access agent and browser integrations.
- Visibility into encrypted traffic directly through **Prisma Access Browser**.



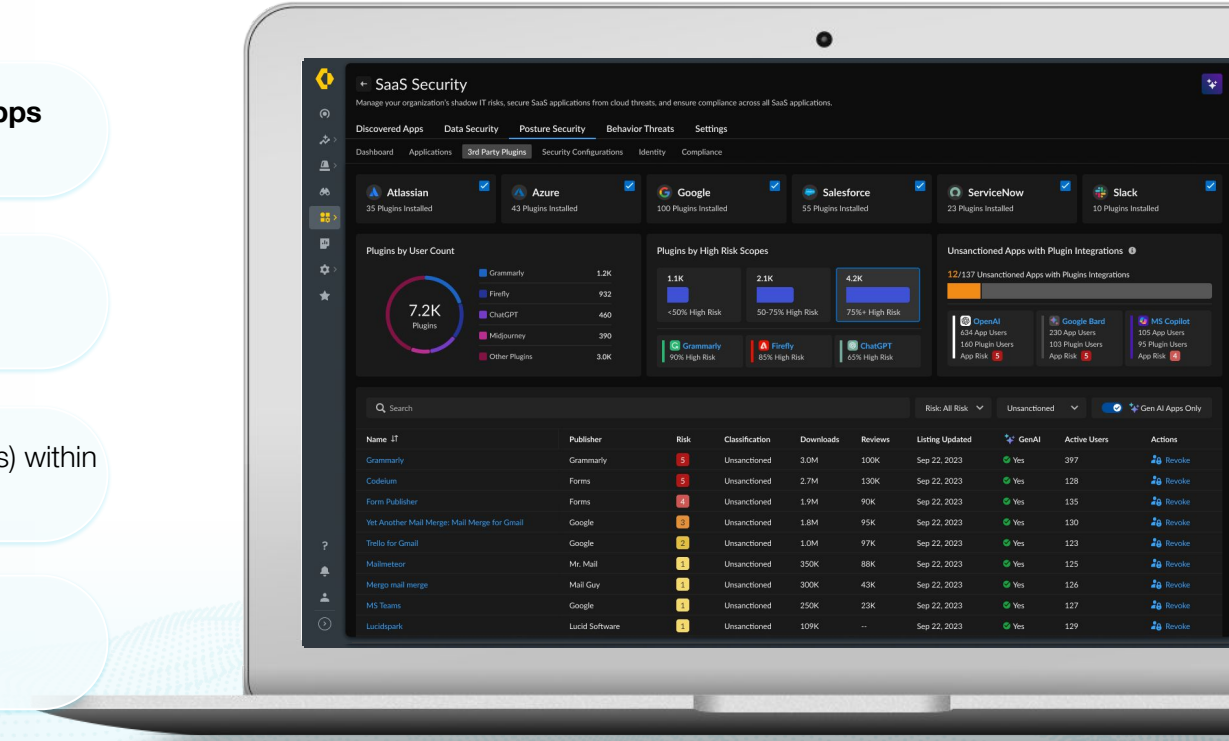
Step 4 Security Controls

Uncover interconnected GenAI apps within SaaS marketplaces.

Identify, monitor, and remediate **unauthorized AI bots**.

Detect threats (malicious URLs, files) within GenAI app responses.

Monitor and maintain **GenAI app posture** for compliance.



Step 5 Continuous Risk Monitoring

Review app adoption and usage insights across **GenAI app categories**.

Comprehensive report on GenAI app usage, risks, security, and compliance.

Contextual recommendations to strengthen security controls for GenAI apps.

Key Questions to Ask

- How much visibility do we have on our environment?
- What tools do you have right now that can be enabled to be more effective against AI?
- What are the repetitive, mundane security tasks that could be automated?
- How much time is spent on manual alert investigation?
- Do our security tools provide a single view of the entire attack?
- What percentage of critical threat response is automated?

How Can We Help?

PANW Canada x K-12 British Columbia

You're already a customer, and we'd love to help!

BC Education Trusted Cybersecurity Partner

- Neil Armstrong, Solutions Consultant - narmstrong@paloaltonetworks.com
- Ehsan Mafi, Resident Engineer - emafi@paloaltonetworks.com

BC Education Incident Response Partner (In partnership with Focused Ed) - Unit 42

In addition, we can also provide guidance with:

- Endpoint protection, Security, Analytics, Security Operations, Managed Response, Security Assessments & Proactive Services
- **FREE** Cybersecurity Education and Activities for K-12 Students and Staff
- Proper Data-Security to enable AND secure the use of AI Applications and Tools, SAFELY.

Teaching Safe Cyber Practices with Cyber A.C.E.S

Our goal is to demystify cybersecurity through interactive learning and equip youth ages 5-18 with resources to have a safe online experience, become good digital citizens, and maybe even pursue careers in cybersecurity.

By participating in **Cyber A.C.E.S.**, students will learn cybersecurity basics like how and why they should physically secure their technology, whom they're talking to online, and the permanence of information on the Internet.

Lessons are designed so they can be facilitated by anyone, regardless of their knowledge level, with each module tailored to a specific age group.

Lesson Roadmap

	Ages 5-7	Ages 8-10	Ages 11-13	Ages 14-15	Ages 16-18
Responsible Connectivity	Physical Security	Passwords	Secure Connectivity	User Authentication & Connections	Password Overload & Fatigue
Privacy	Tracking Online	Digital Footprint	Personal Information Sharing	PII, Terms and Conditions	Reverse Social Engineering
Communication	Who Are You Talking To?	Information Sharing/ Phishing	Verifiable Postings	Online Scams & Fact vs. Fiction	Guarding Your Digital Self
Digital Citizenship	Inclusion	Interactions and Bullying	Navigating Social Media	Copyright & Protecting Original Work	Digital Literacy and Ethics

https://start.paloaltonetworks.com/cyber-aces.html

1

Ensure student safety

Specialized features tailored to education-specific needs help maintain a safe online learning environment for students and ensure compliance with internet usage policies and data privacy.

2

Enable continuity of education

Advanced threat detection and prevention capabilities safeguard against various cyber threats— such as malware, ransomware and phishing attacks—to prevent interruption of education.

3

Overcome workforce challenges

Leverage AI and ML to automate monitoring and response activities, making it easier to operate at machine scale and overcome workforce, time, and effort limitations.

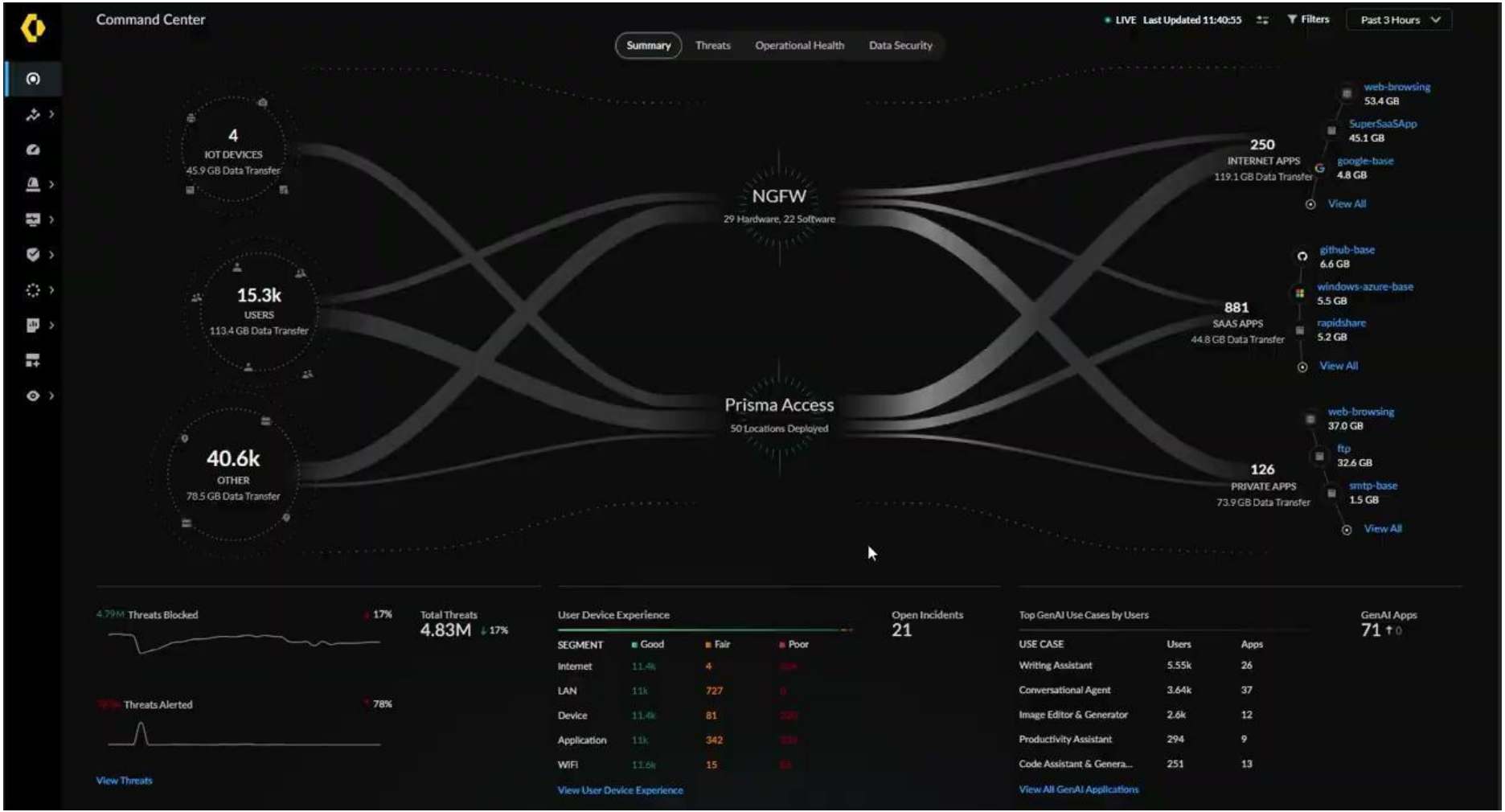
4

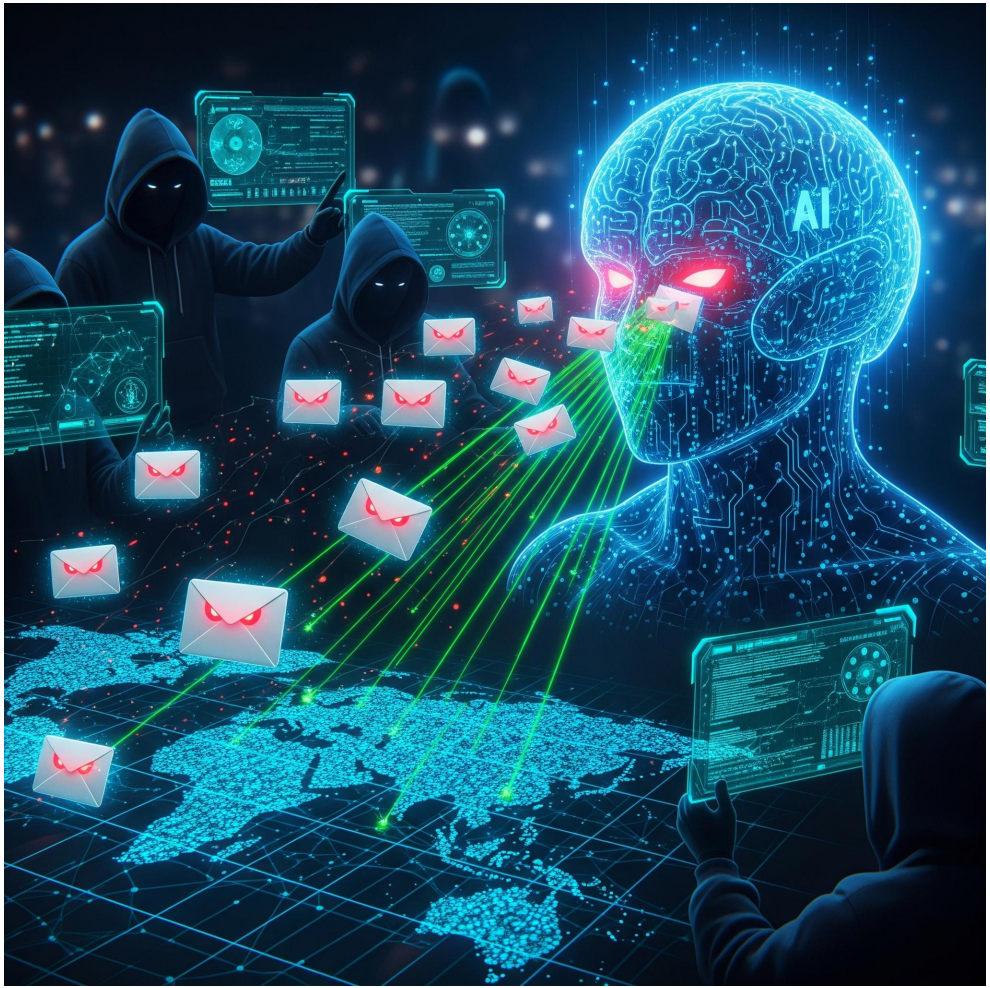
Optimize investments

Palo Alto Networks' single-platform approach reduces the complexity of creating and managing policies, simplifies integration with existing technologies, and enables automation—decreasing both capex and opex.

Thank You

paloaltonetworks.com





AI Cyber Attack Threat

- AI makes cyberattacks cheaper, faster, and much more effective
- Attackers weaponize AI to create hyper-realistic phishing emails
- Automated attacks scan networks at speed, finding vulnerabilities
- AI rapidly sifts through stolen data to find high-value targets

What is AI Enabled Defense Anyways?

- How do you use AI today?
  - LLMs: Chat GPT/Gemini?
    - Searching enormous data sets instantaneously
  - Learning Tools: Maps, Banking & Thermostats
    - Recognize patterns & anomalies
  - Virtual Assistants: Siri & Alexa
    - Help you stay on task, focus, and not miss anything