RESEARCH BY

CIO ASSOCIATION OF CANADA

Navigating the AI PC Era

Cybersecurity Challenges and Innovations

SUPPORTED BY

DELL Technologies

intel vPRO

Welcome to the AI PC Era

A marketing team is suddenly able to produce dozens of creative campaign materials in a matter of minutes. A customer service agent receives a summary of last week's call transcripts that identifies common troubleshooting areas. Developers who worried about missing a release date are generating code that may finalize an app update ahead of schedule.

Innovations in artificial intelligence (AI) are unlocking near-limitless opportunities to transform the way organizations operate. Realizing the potential of these applications and platforms, however, depends on IT leaders being able to provision the hardware that's been purpose-built to run them in the most secure way possible. Enter the AI PC – and the challenge facing chief information security officers (CISOs) across Canada and beyond.

Unlike a traditional enterprise device, AI PCs run three compute engines. This not only includes the central processing unit (CPU) and a graphics processing unit (GPU) but a neural processing unit (NPU). Given the sustained, heavily-used workloads AI requires, the NPU allows a PC to operate with the right balance of low power and efficiency.

AI PCs represent a force multiplier in how organizations create content, collaborate and boost employee productivity. According to market research firm Gartner, AI PCs will represent 100% of enterprise purchases as quickly as 2026*.

As with any sea change in technology, of course, organizations need to ensure they simultaneously provide employees and customers what they want and IT departments what they need. The power, performance and the nature of data running on AI PCs makes them highly valuable assets – and therefore potentially bigger targets for cybercriminals.

The CIO Association of Canada (CIOCAN), working in partnership with Dell Canada and Intel of Canada, recently convened a group of CISO members to discuss the evolution of AI PCs and the security implications. This report is intended to combine their anonymized insights with guidance on how technology partners are collaborating to offer the level of data protection Canadian organizations need.

*Gartner Forecasts Worldwide AI Chips Revenue to Grow 33% in 2024, May, 2024

Cybersecurity Challenges in the AI PC Era

IT leaders have learned to be cautious as they integrate new technologies into their existing stack. No one can afford to allow the business benefits of innovation to come at the expense of an incident that leads to reputational damage, financial loss or other negative impacts. As revolutionary as AI PCs are, CISOs are mindful of the potential pitfalls as they prepare to adopt them.

As one CIOCAN member pointed out, organizations are already contending with phishing schemes, DDoS attacks and other threats on their device fleets. AI PCs may bring a lot of value to the enterprise, but some fear their capabilities could be equally well-used by rogue actors.

We could see the rise of advanced threats powered by large language models (LLMs), for example, where hackers learn to bypass voice authentication and facial recognition authentication.

"AI has the opportunity to greatly improve their capabilities and also open up new opportunities for them to enact attacks," the IT leader said. "It's going to allow threat actors to be able to do things in a shorter amount of time, and to discover new tech attack vectors that probably didn't exist before."

AI PCs are also being introduced at a time when CISOs are adapting to the use of AI across many different departments. Those responsible for regulatory compliance, governance and policies are playing catch-up with the way employees are using the technology. One CIOCAN member gave the example of developers using generative AI to write code and allowing an organization's large language model (LLM) to communicate with the open Internet.

"Until we can actually get some kind of homogeneity on how we want to approach data compliancy and privacy, it becomes next to impossible, the more jurisdictions your enterprise works in, to get a governing policy that actually complies across the entire enterprise," the IT leader said.

For IT departments specifically, the benefits of AI PCs are being weighed against a shift in how hardware and software workloads have been moving since the advent of cloud computing.

"We've been working for years to get people to keep their data on an area that we control – either cloud storage or some kind of network storage," another CIOCAN member said.

Running locally has many benefits, however, and AI PCs were designed to deliver a level of privacy that aligns with IT department expectations. CIOs and CISOs have many tools to protect the data within their organization, even if some workloads continue to run in the cloud.

It's also important to note that IT leaders see many upsides from AI adoption as well. CIOCAN members talked about the potential for the technology to improve data protection processes, for example, accelerate the time required to respond to security incidents and even get ahead of future threats.

Continued on next page

"AI is going to allow threat actors to be able to do things in a shorter amount of time, and to discover new tech attack vectors that probably didn't exist before."

CIOs and CISOs are also conscious of the need to align with business requirements, and in that sense, AI PCs represent the only way forward.

Based on the experience an end user is trying to drive, for example, existing compute approaches will lead to latency and other performance issues. With more people in organizations depending upon AI and LLMs, bandwidth limitations will quickly become an impediment. Scalability will become more challenging.

Perhaps most significantly as more organizations focus on sustainability, AI PCs offer a viable alternative to the excess energy usage and potential waste experienced running AI workloads.

All these challenges have created a catalyst for AI PC adoption – and for industry partners to find a best-in-class way to secure them.

Integrated Attack Surface Protection

What hasn't changed in the AI era is the need for a defense-in-depth approach to safeguarding organizational data. As rogue actors become increasingly sophisticated, CISOs need to know they are deploying hardware and software that work in tandem to provide multiple layers of protection, all the while providing intelligence that assists security operations teams in detecting and responding to future threats.

Intel, Dell and CrowdStrike have come together to provide this level of cybersecurity by leveraging the strengths of each of their respective technology capabilities.

Intel vPro

Many CISOs and CIOs are already familiar with the comprehensive security features of Intel vPro®, which builds in protection at the hardware level, BIOS/firmware, hypervisor, virtual machine (VMs), operating system and applications. Intel vPro uses AI-based threat detection to spot potential threats at the hardware-level. Intel vPro is also powered by Intel® Core™ Ultra processors, which means it has three compute engines.

In practice, of course, IT departments are often over-extended and struggle to keep systems current and avoid vulnerabilities. Intel vPro helps IT by offering the ability to provide seamless firmware updates and remotely manage fixes. This helps IT departments meet the security demands of organizations in Canada and elsewhere that have embraced hybrid work models.

No matter where an organization's workforce is located, Intel vPro helps IT departments to keep everyone patched and updated against the latest threats. Advanced AI-powered telemetry, meanwhile, includes device discovery solutions that allows IT to assess security posture and act accordingly. With the level of automation Intel vPro provides, CIOs and their teams could even turn ITOps into AIOps.

Dell commercial PCs

Having provided essential computing products to organizations around the world for decades, Dell has developed a three-pronged perspective on securing its PCs.

Continued on next page

This starts with what's "built in" through partnerships with market leaders such as Intel. This includes on-device telemetry capabilities that allow for real-time analysis and swift mitigation when attacks occur. Dell also defends against BIOS attacks through verification and by working with the Intel Management engine. It also equips each device with SafeID, a security chip that protects credentials and authenticates users.

Next is Dell's "built with" security, based on its SafeSupplyChain solution that can use a unique Secured Component Verification to check product integrity.

Finally, Dell offers "built on" security through 24x7 services and support, managed detection services and partnerships with organizations such as CrowdStrike.

CrowdStrike Falcon Insight XDR/EDR

As endpoints multiply across organizations in response to digital transformation and business growth, CrowdStrike's Falcon Insight XDR/EDR is designed to help IT security team see and understand suspicious activity in order to prevent malicious attacks.

Instead of focusing on evidence a data breach has occurred – otherwise known as an indicator of compromise (IOC), Falcon XDR/EDR uses hardware and telemetry data to target indicators of attack. This means security teams can look beyond the malware or exploits threat actors are using and instead learns their intent. Machine learning models trained on large data sets allow Falcon XDR to send AI-based IOA alerts that drive proactive data protection on AI PCs.

What integrated attack surface protection looks like in practice

This cross-industry partnership means Dell PCs built on Intel vPro come with Intel® Threat Detection Technology (Intel® TDT), which offers device-level telemetry that CrowdStrike's Falcon XDR/EDR then uses to defend against common attack scenarios.

Imagine an employee who innocently clicks on a link in an e-mail message distributed as part of a phishing campaign. This executes a payload that allows intruders inside a corporate network and potentially additional backdoors through a command-and-control server.

Traditional cybersecurity technology might detect this kind of fileless attack, but without any sense of the attackers' goals. Are they trying to steal data? Are they looking for a financial reward via ransomware? Or is this part of an advanced persistent threat that will penetrate deeper – into the corporate VPN?

By using the accelerated memory scanning algorithms of Intel TDT and its ability to offload processing to the Intel Graphics Technology integrated graphics processor, CrowdStrike can apply dynamic IOAs to the memory layer. This is on top of Intel's Control Flow Enforcement Technology and the BIOS and firmware defences Dell commercial PCs already provide. For example, system privileges can be restricted before attackers gain traction through Dell's SafeBIOS and Intel® System Resources Defense technology.

The integrated attack surface protection developed by Intel, Dell and CrowdStrike can also defend against foundational attacks and a growing number of other use cases.

The Results

Far from an additional headache for CISOs and CIOs, AI PCs are already being used to optimize security software.

By moving security capabilities down to the NPU and GPU, for example, the CPU is freed up to provide the performance and capabilities users require to do their work. At the same time, security vendors can take advantage of that CPU bandwidth to bring more capability from the cloud to the endpoint.

The outcome is a safer computing environment where security teams are less likely to find themselves operating in reactive mode, while employees are able to capitalize on all the value advancements in AI will bring to customers.

IT leaders are recognizing the promise of integrated attack surface protection as they learn more about it.

"I think ultimately the value comes down to the heightened ability to detect and respond based on wherever your endpoint is," one CIOCAN member said. "That gives you the leeway to move fast and mitigate against threats that are emerging before they actually reach your environment."

IT leaders are also looking at the impact of advanced protection on their teams, particularly given many have had to reduce headcount. Without advancements from trusted partners, they already realize their efforts to secure their organization's data will become more difficult than ever before.

"Static IOCs are next to useless nowadays, like if I'm getting something that's second third hand through a blog post, it's already done. It's already dead," another CIOCAN member said. "The staff I still have need to spend their time investigating substantive issues that actually matter. They can't be doing level one, level two analyst work. The greatest advantage for us as security practitioners is (this approach) takes care of that low level stuff, so our analysts can actually dedicate themselves to doing substantive investigative work."

"Static IOCs are next to useless nowadays, like if I'm getting something that's second third hand through a blog post, it's already done. It's already dead."

Conclusion

AI PCs are poised to become the standard computing devices for a modern workforce, but they need to roll out in a way that doesn't introduce organizations to greater risk of cyber threats.

At the same time, attacks will only continue to grow in scale and complexity as rogue actors make use of AI too. Organizations will not be able to depend on the heroics of individuals within the organization to thwart data breaches. Instead, they need to have that security capabilities built in and automated.

Partnerships such as the one between Intel, Dell and CrowdStrike illustrate how an integrated approach can give organizations the best of both worlds – AI PCs that allow organizations unprecedented levels of creativity and productivity, along with peace of mind that their data will remain safe.

Thank you

Our thanks to the panel of experts who contributed their knowledge and expertise to this paper. The panel included the following:

George Al-Koura, CISO, Ruby Life
Omid Hamed, Retired - vCISO
Paul Twigg, CTO, Digital Commerce Bank
Rob Milman, Information Security Officer, University of Prince Edward Island
Shaun Guthrie, SVP, Technology & eCommerce, Peavey Industries LP
Cara Wolf, CEO & CISO, Ammolite Analytx
Steve Biswanger, Retired - vCISO
Dee Saleh, Information Security Officer and Systems Analyst, Legal Aid Alberta
Mo Nozari, Founder & Head of Technology, Strategic Consulting Inc.
Derek Cullen, CIO, Stikeman Elliot LLP
Matti Pearce, VP - Information Security, Risk, and Compliance, Absolute Security
Howard Plato, Manager, Information Systems, Strathcona Resources Ltd.