RESEARCH BY

CIO ASSOCIATION OF CANADA

Advancing Endpoint Security in the Hybrid, AI-Powered Era

SUPPORTED BY

DELL Technologies

intel vPRO

Introduction

While hybrid work models are creating opportunities to enhance employee experiences and drive greater productivity, IT leaders can be forgiven if they occasionally look back fondly on simpler times.

Less than twenty years ago, for example, many Canadian organizations were run using stationary PCs and desk phones. Security threats like malware could be distributed via a floppy disk, and basic intrusion detection software was enough to detect attempts to send suspicious files and other nefarious activities.

Today, IT leaders are charged with protecting an ever expanding security perimeter. This is thanks in part to the proliferation of technologies that allow work to happen almost anywhere. It's also the result of hybrid work policies that sanction employees to manage critical information remotely.

In practice, this means a sensitive corporate contract may be printed at an employee's home office. Marketers and sales staff could be working with customer data at a coffee shop over a public Wi-Fi connection. IT leaders might not have full visibility into where all their endpoints are, much less the risk of insider threats or external attackers.

Headlines about organizations issuing return-to-office mandates doesn't change the fact that within almost every sector, hybrid work models will continue to exist and even expand in some cases. At the same time, advancements in artificial intelligence (AI) are allowing hybrid employees to work with data in ways that are transforming businesses – and making them even more valuable targets.

The CIO Association of Canada (CIOCAN) – working in partnership with Dell Canada and Intel of Canada – facilitated a virtual gathering of IT leaders* to discuss how the hybrid era and AI is changing their outlook on endpoint security. This report captures the highlights of that conversation and points to integrated solutions that will help them offered a layered defense strategy to keep critical data secure.

*All CIOCAN member comments have been anonymized to protect personal privacy. Some comments have been lightly edited for clarity.

Challenges of Hybrid Work Models

Hybrid work models have often been treated as an HR issue. Should senior leadership teams trust employees to work productively outside the office? Will allowing hybrid work attract more of the best talent?

The reality is that hybrid work is just as much an IT issue, particularly as endpoint protection increases in complexity and the efforts of threat actors become more sophisticated.

As one IT leader in our virtual roundtable pointed out, the hybrid work model can create a "Goldilocks Effect" for those leading cybersecurity functions, in that they need to determine an approach to observing employee activity that's not too much or not too little based on the level of risk.

"If you have this hybrid model, you've automatically increased your attack surfaces, especially if you have a geographically dispersed workforce," the IT leader said. "You're complicating the monitoring; you're complicating the enforcement of rules among certain people."

Already, CISOs have spent years grappling with containing insider threats and fending off phishing schemes in the relatively controlled environment of a centralized office. The impact of hybrid work could mean significant extra effort for IT departments that have been overworked to begin with.

"You're trying not to overload your employees, and you're trying to maintain their performance and their productivity," the same IT leader added. "Decentralization is a very nice concept to talk about, but on the ground, it can be very difficult to achieve."

One of the problems is that much of the discussion around hybrid work models has focused on employee flexibility, while "endpoint security" may be an unfamiliar term to many of those participating. Another CIOCAN member used a hypothetical example of a team member who asks their employer to work from Europe. The employee might be able to do their job just as well from abroad, but that's not the only factor to consider in giving them the go-ahead. Security, data sovereignty and other factors all need to be addressed.

"We (in the CISO role) have to think about, okay, what are the laws there? How do we enable you to work, and how can you work in a more efficient manner without you having access to all the data in this uncontrolled fashion?" the CIOCAN member said. "We try to put solutions in place, but when we can't, it makes you look like the bad guy. There are tough decisions to make in order to keep everyone working in a safe environment."

The divide between users and IT threatens to grow even wider as AI tools become more pervasive within Canadian organizations. CIOCAN members pointed out that the initial shift to hybrid occurred during a public health crisis, when there was a push to simply "keep the lights on" in terms of network uptime and other everyday operations. This meant endpoint security has had to evolve as more of a follow-up activity.

AI, meanwhile, is fueled by data, which means hybrid employees have higher expectations around what they can feed into emerging solutions, regardless of where they're physically based.

"If you have this hybrid model, you've automatically increased your attack surfaces, especially if you have a geographically dispersed workforce."

Continued on next page

“(Employees) all decided that data democratization was the next best thing, and everybody wants access to everything, because everybody now is looking at these large language models or prototypes that they think will solve all their work problems,” one CIOCAN member said. “They may be getting blocked by their identity management system from getting access to certain kinds of information, but that doesn’t stop them from being creative and trying to fill those gaps.” In other words, employees may decide the path of least resistance is in attempting to workaround their IT department’s policies.

The result, in some cases, has been a level of exposure to cybersecurity threats that IT departments can’t take in on their own. In the worst-case scenarios, it’s those entrusting their data to an organization that have taken on the responsibility of providing early warning signs. It could be as simple as an invoice request that appears to be a phishing attempt.

“We are told about potential threats more often by our customer base than through the tools we use that are coming,” one IT leader said. “If people aren't scared, they're confident now to put their hand up if there isn't something that seems quite right, because in a lot of cases, the really good subversions work around your toolsets. They're socially engineered.”

Not only are threat actors well-versed in duping employees, hybrid models may revive age-old debates about the pros and cons of bring-your-own-device (BYOD) policies, another CIOCAN member said.

“I find that it doesn't matter how much control you have – there's still a big chance of data moving and ending up on personal devices,” the member said.

“I find that it doesn't matter how much control you have – there's still a big chance of data moving and ending up on personal devices.”

Integrated Solutions for Robust Security

Of course, many organizations have already invested in endpoint detection and response (EDR) solutions designed to monitor and mitigate malicious threats. The problem is that many IT leaders are now dealing with threats they are unable to see.

Fileless memory and firmware attacks, for example, can remain undetected by corporate IT departments as threat actors either turn off legacy EDR solutions or blend in with valid system processes. The future is one in which more of these attacks will circumvent traditional signature and behavior-based approaches, where software alone will not provide adequate intelligence.

The only way to prevent unauthorized parties from gaining privileged access is by using multiple, integrated layers of defence that extend beyond software-only security. A good example is the partnership between Intel, Dell, and CrowdStrike, which combine both hardware-based protection and software to disrupt the cybersecurity kill chain.

These co-engineered capabilities begin with Intel vPro®, which allows IT departments to remotely manage fixes and provide seamless firmware updates, and Intel® Threat Detection Technology (Intel® TDT) to spot the stealthiest attacks. This is on top of the protections offered via Dell commercial PCs with its built-in on-device telemetry features, its *SafeSupplyChain* solution that checks product integrity through a unique Secured Component Verification, plus 24x7 services and support.

Continued on next page

With CrowdStrike's Falcon Insight XDR/EDR, meanwhile, IT departments can perform clustering and similarity analysis of static file-based data that would be otherwise difficult to detect as malware. This is important given the rise of polymorphic malware that can mutate to change its appearance and morph its code at a rapid pace.

These integrated technologies can work together to mitigate the kinds of attacks keeping Canadian IT leaders up at night. Imagine a hybrid employee who innocently clicks on a Word document that launches a macro allowing an attack to set up a remote console and disable an organization's antivirus software.

This could normally lead to a "living off the land" attack, whereby threat actors use the system's own BIOS commands to allow placement of rootkit malware. When attackers cover their tracks and escalate privileges, trust in the entire PC trust stack can be compromised.

Using the Dell Trusted Device Console with Intel vPro probabilities, however, an admin would be given a BIOS indicator of attack alert. A quick look at the security assessment viewer would allow them to see the falling security score based on Intel Manageability Engine (ME) attestation and other security policy settings.

Dell devices can be configured in Crowdstrike's Falcon XDR and Falcon Discover console, giving that same admin visibility into attacks that happen below the OS that need to be remediated. Dell's Client Command Suite (DCCS), meanwhile, allows for remote management capabilities via Intel vPro© or through an integration with Microsoft System Center Configuration Manager (SCCM).

The machine affected by the rootkits can then get a new image and firmware as the admin uses using Intel® Active Management Technology (Intel® AMT). Intel firmware guard technologies on the device, meanwhile, ensure the reliability of the firmware updates.

Cross-Platform Security Considerations

Endpoint protection can become even murkier when you not only factor in hybrid work but the many different operating systems (OS) that are now part of the typical organization's computing environment. This not only includes Microsoft Windows but Android, Mac OS, iOS and more.

This means best-in-class endpoint protection needs to offer seamless cross-platform management based on a variety of endpoints. After all, sensitive data is being collected, managed and shared not only on PCs but smartphones, tablets and other devices.

CIOCAN members said, it all starts with being able to see what kind of devices employees are using, whether they are working in the office or not.

"If you have the highly disparate, highly unobservable endpoint fleet, you're going to be in a worse situation than if you have a highly observable, highly standardized endpoint fleet," one of the IT leaders said, adding that following a standard means organizations can enforce policies and assist employees amid the transition to hybrid work models.

This is one of the reasons why Intel and Dell have mapped their hardware features so IT departments can know how their organization's PCs contribute to the MITRE ATT&CK framework, which classifies and provides guidance on common cyberattacks and intrusion detection techniques that is used by security operations globally.

"If you have the highly disparate, highly unobservable endpoint fleet, you're going to be in a worse situation."

Future-Proofing Security Investments

The hardware and software protections provided by Dell, Intel and Crowdstrike not only address current threats but future risks as endpoints continue to spread based on hybrid work models. CIOCAN members said those capabilities need to be coupled with a laser focus on marrying security policies with training as employees take their work – and corporate data – with them outside the office.

One IT leader outlined an approach whereby their organization not only requires employees to use a corporately-issued and managed device but adhere to conditional access policies. For example, full access to data might be limited if the employee is working in a country where the organization had security concerns, or if they're working in what is considered a high-risk environment.

"(Employees) are free to use personal devices too and access data 365 days a year, but they can't do anything with what they see there, other than view and interact with it. They can't print it or download it," the IT leader said. "It may seem a bit heavy-handed, but it works for us."

The same CIOCAN member said their organization gets buy-in by publishing security awareness articles on the internal corporate Internet. These articles provide details on observed threats and how they work and encourage employees to share knowledge with family or those with whom they'll be working remotely. It's just one way to get ahead of tomorrow's threats.

Future-readiness is also about having a firm grasp of how you'll respond to threats or data breaches, another CIOCAN member said. Many incident response plans might have been initially developed prior to hybrid work models and should therefore be updated to acknowledge the new norms and increased risks the organization is facing as a result.

Hybrid work models aren't just providing remote access to employees, meanwhile, but many other third parties as well. Another IT leader said his organization is looking at what kind of policies and endpoint protection will be necessary to support the access provided to contractors, suppliers and even customers that access corporate data and applications.

Governance and Policy Implementation

Any investments Canadian IT leaders make in endpoint security need to be aligned with their organization's overall approach to data governance. This covers not only the way policies around data quality, integrity and stewardship are enforced in hybrid work environments but how data will be used to fuel AI platforms and tools.

Several CIOCAN members suggested that in many organizations, endpoints should be folded into an over-arching governance framework that ensures data creates business value, respects user privacy and helps achieve and maintain compliance with any applicable laws or regulations.

AI may be able to help in some areas that contribute to data governance, such as classifying and organizing information such as endpoint security policies and incident reports. However strong security will be essential to strong governance to keep critical details about an organization's performance and plans secret.

Continued on next page

One IT leader talked about his organization's stock price falling, for instance, when word got out about some bad news that was set to be announced.

"There are systems that can now find patterns in just the movement of information, or they make inferences based on publicly available information and build derived data sets that are completely outside of the scope of the standard data governance policies and practices right now," the IT leader said.

Of course, any data sources would need to be properly verified in order to ensure any inferences are accurate. This is clearly an area where manual efforts by humans alone will not suffice, another CIOCAN leader said.

"When you've got this dispersed environment, you want to really focus on being very consistent in enforcing and developing your policies. You want to be using a lot of automation and a lot of standardization too, because you have a much larger environment," the IT leader said. "Having things like hardware-based security is very helpful in that area."

Where humans do come in – and where they'll remain in the picture – is in how they analyze the results of automation. This can't happen in ad-hoc fashion, or where the accountabilities around security and governance become confused.

"Having those roles and responsibilities within your organization is key when you're setting up these frameworks," another IT leader said.

Another best practice that came out of the discussion was not to wait for enforcement situations to arise, either in terms of governance or security. Both kinds of policies should have run-throughs early on as technologies are brought in to help.

"Test, test, test," one CIOCAN member urged. "Validate that those controls work, and then really start leveraging, if you're not already, these integrated security controls and multi-layered security controls."

"When you've got this dispersed environment, you want to really focus on being very consistent in enforcing and developing your policies."

Conclusion

The one thing Canadian IT leaders can count on is that sophisticated threat actors are going to shift the signatures of their malware more often than ever before. They have every incentive to do so as data becomes a critical fuel for AI platforms, and as more organizations embrace the many benefits of hybrid work models.

Canadian CIOs are well aware that allowing hybrid work increases the potential attack surface for their organizations, and they're paying close attention. They're also trying to strike a delicate balance between assisting employees in working productively and collaboratively from outside the office while not losing sight of what's happening at the endpoint level.

As more IT leaders become aware of the integrated endpoint security capabilities such as those offered by Intel, Dell and Crowdstrike, they will be able to approach evolving needs and expectations around hybrid work with greater confidence. They'll also be able to stay one step ahead of issues such as cross-platform security and the need to future-proof their organization.

The most important thing to keep in mind is that hybrid work and AI have advanced and been adopted around the world at a speed that few would have ever been able to predict. That makes it all the more critical to make the right investments now. With the right tools to keep data secure CIOs can align with governance frameworks and ultimately make their organizations more successful.

Thank you

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

Sonny Sarai, Director, Information Security, Pattison Food Group

Sam Shabaani, Director, IT and Cyber Security, Svante

Dee Saleh, Security Officer and Systems Analyst, Legal Aid Alberta

Jassi Kaur, Head of IT and Security, Bulk Barn Foods Ltd.

Adam Fletcher, Director Technology Infrastructure and Operations, Concert Properties

Karl Galbraith, CISO, Galbraith & Associates

Tim Happychuk, Director & Chief Information Officer, CN/TransX Group of Companies

Kevin Kowal, Associate Director, ITSM, SAIT

Ross Ballendine, VP of IT, Trimac Corporation

Ian Calder, Manager, Information System & Technology, EfficiencyOne