



Aligning cybersecurity with market dynamics and customer needs

Bell

IN ASSOCIATION WITH



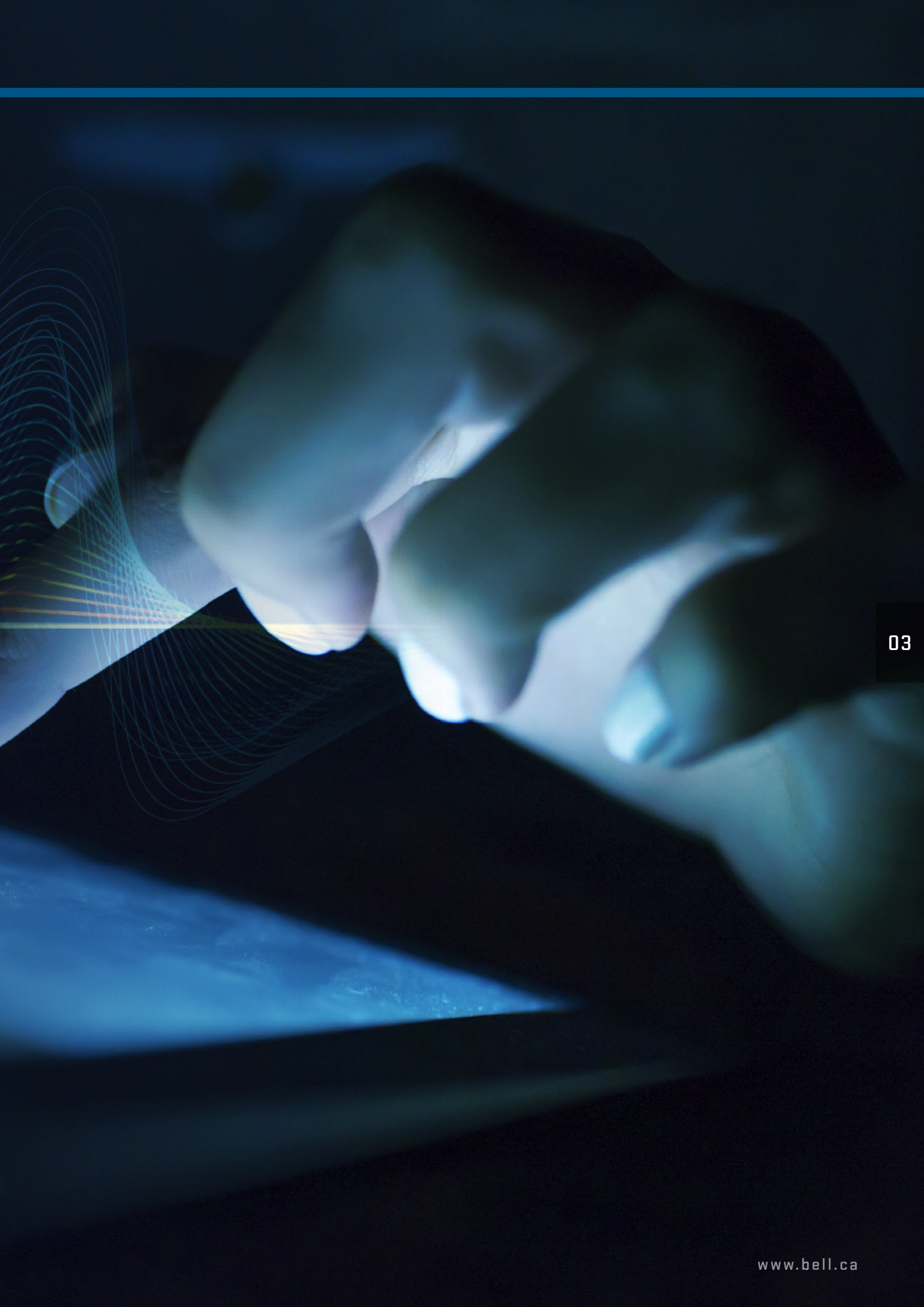
Check Point
SOFTWARE TECHNOLOGIES LTD



Bell

**Bell: a leader
in cybersecurity
with its finger
on the pulse**

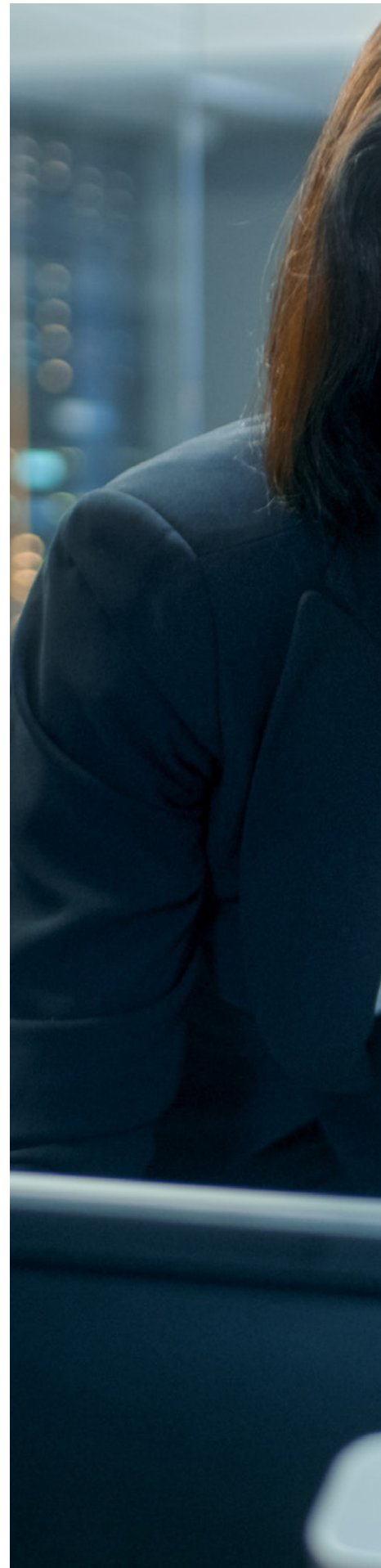
02



Bell has become a leader in Canadian cybersecurity, leveraging a customer-centric mentality and a powerful appreciation for market dynamics

As Canada's largest telecommunications network, Bell is also a leader in the country's cybersecurity space. "We have been recognized as a cybersecurity leader by firms such as IDC (International Data Corporation), and we're supporting both private and government customers on multiple levels," says Dominique Gagnon, General Manager of the Cybersecurity Practice at Bell. The breadth and depth afforded by the network is combined with cutting-edge technologies and an adaptable strategy, affirmed by a constant finger on the pulse.

Gary Miller, Cybersecurity Strategist at Bell, with a long history in the space and extensive business management experience, says that agility and a customer-centric strategy are vital to Bell's success. "What we do is shaped by listening to our customers and taking into account their needs," he says. "It's a circular process – one that requires us to be in tune with how the market is evolving and how these changes are impacting our customers."



A woman with dark hair and a blue lanyard leans over a woman with curly hair who is looking at a computer monitor. They are in a server room with blue lighting and server racks in the background.

\$23.4bn

Approximate
revenue

1880

Year founded

52,790

Approximate number
of employees

05

“We have been recognized as a cybersecurity leader by firms such as IDC (International Data Corporation), and we’re supporting both private and government customers on multiple levels”

Dominique Gagnon,
General Manager, Cybersecurity
Practice, Bell

When looking at changing market dynamics, Gagnon says that he sees five major trends that are impacting Canadian businesses.

Cybersecurity is top of mind for executives, with Canadian businesses investing more in cybersecurity each year. Yet, as Miller says: “The market for cybersecurity solutions is chaotic. Everyone claims to have the silver bullet, and Canadian organizations need guidance to sort through the noise. Since the costs and consequences of not getting it right are greater than ever, Bell’s primary





CLICK TO WATCH: 'BELL IS A RECOGNIZED LEADER IN SECURITY, COMMITTED TO PROTECTING BUSINESSES AND THEIR CUSTOMERS'

07

security objective is helping our customers enhance their foundational cybersecurity,” he says.

Traditional reactive approaches to cybersecurity are no longer sufficient as cyber attacks become more sophisticated, targeted and persistent. Instead of just protecting the network perimeter, Gagnon says that modern threats necessitate proactive internal protections. “Businesses recognize that they must evolve their approach and assume the perimeter has been breached. It’s a matter of being able to proactively detect the attacker, trip the response

and kick them out. It’s how fast you can achieve this, not just how well you can prevent them from getting in.”

As businesses are adopting more cloud-based applications and hosting more workloads in the cloud, it is critical to ensure that layers of protection are built in. “We are helping decentralize our customers’ approach to security, by facilitating secure, cloud-based environments across the country,” says Gagnon.

Businesses are also connected like never before thanks to the convergence of the Internet of Things (IoT), Operational

WELCOME TO THE FUTURE OF CYBER SECURITY

Check Point Infinity is the first consolidated security across networks, cloud and mobile, providing the highest level of threat prevention against both known and unknown targeted attacks to keep you protected now and in the future.

[LEARN MORE](#)



Check Point[®]
SOFTWARE TECHNOLOGIES LTD

CLOUD • MOBILE • THREAT PREVENTION

COMPLEXITY BREEDS INSECURITY •

The rapid digital transformation of business is placing ever-increasing demands on security. IT operations and security are in the midst of a major disruptive period and we are seeing unprecedented breadth of threats; cyber-attacks carried out as large-scale, multi-vector mega attacks that can inflict major damage on businesses and their reputation.

What's more - the velocity of attack evolution is outpacing the level of security that businesses have deployed - this is a problem. The level of security deployed by businesses cannot be behind the level of attacks coming at them.

There are many reasons security infrastructures have evolved to be behind the daily level of attacks. The most obvious is that attackers have no constraints - they can create and push the envelope, even recklessly, in developing new and advanced techniques. Businesses of course, have change control procedures, budgets, compliance and myriad other operational constraints to which they must adhere thus restraining security advancement. Another is the traditional check box method of building a security infrastructure whereby a specific security technology is deployed to defend against a specific type of attack or to protect a specific type of application. This binary, mono-vision approach, aka "best of breed", was effective in earlier generations when attacks were one-dimensional but today's attacks are anything but that - they are multi-dimensional, multi-stage, multi-vector and polymorphic.

YESTERDAY'S SOLUTIONS NOT UP TO TODAY'S CHALLENGES •

Unfortunately, while security technology proliferates and customers require more advanced IT functionality to support capabilities like big data analytics, hyper connectivity, IoT convergence and automation ... effective security architectures are very rare. This creates complexity, increases risk and drives up costs.

Take for example, the widespread move to the Cloud and adoption of Software Defined Wide Area Networking (SD-WAN). While connecting branch offices directly to the internet greatly improves agility and reduces costs, it also significantly increases security risks. Digitalization of operational and industrial systems increases the attack surface and the risk of cyber-attacks on critical and Industrial Control Systems (ICS) infrastructures. The sheer scale of growth in the area of IoT presents its own significant risks when managing policy.

WHERE THE CYBER SECURITY MARKET MUST GO •

True comprehensive protection requires a new, holistic approach to assessing and designing security; it requires an architected approach that does not rely on detection alone, prevents attacks before they happen. The solution must combine effective prevention technology, unified security policy, and an operational model that is realistic to implement across today's IT environment within a reasonable staffing and budget level.

The goal is to defeat all attacks across all possible vectors in a cohesive and unified way.

Check Point Infinity is the only security architecture that uniquely combines multiple security functions into a single, unified threat prevention solution to protect all of your IT assets - perimeter, data center, virtual, clouds, mobile devices and beyond - against all known, previously unknown and zero-day attacks.

The simple, business-oriented management interface reduces complexity, making it easier to deliver security and compliance within a constrained staff and on budget. Infinity helps organizations deliver agile yet secure IT, which can adapt to, and enable business as requirements change.

Through advanced threat prevention, business-oriented policy management, and cloud-based threat intelligence, Infinity delivers a solid foundation for a sustainable, effective risk management strategy.

1-800-429-4391

www.checkpoint.com



Check Point
SOFTWARE TECHNOLOGIES LTD



10

Technology (OT) and the proliferation of endpoints. With increasing numbers of applications, devices and endpoints connected every day, exposure is growing from a cybersecurity perspective. “Organizations are under great pressure to ensure that these new points of vulnerability are protected,” he says.

And finally, organizations have recognized the need for better control over what they see and how they see it. The challenge now is adopting, managing and integrating advanced capabilities, like enhanced detection

“Our approach has been to integrate different technologies’ capabilities to offer the best solution structure to our customers”

Dominique Gagnon,
General Manager, Cybersecurity
Practice, Bell





and response and SIEM platforms (security incident and event monitoring), in order to enhance visibility and control. Organizations need the right strategy and support to filter through the immense quantity of data and insights generated by these advanced solutions, in order to act upon urgent alerts and proactively hunt for threats.

As one of Canada's largest technology solutions and integration providers, Bell is well equipped to help customers navigate these market dynamics, supporting their needs at every turn. "Our approach has been to integrate

11


EXECUTIVE PROFILE

Dominique Gagnon

Dominique Gagnon is the General Manager of the Cybersecurity Practice at Bell, with over 25 years of practical and educational experience in IT. Prior to Bell, Dominique was the VP Consulting Services at CGI, managing the government vertical and leading the Canadian Cyber Security Center of Excellence Sales, Delivery and Operations. Dominique has expertise in P&L management, business engineering, strategic engagement management and infrastructure management with a focus on cybersecurity. He has negotiated, implemented and managed numerous large outsourcing contracts and led transformations and transitions for several large organizations. Dominique also served for 12 years in the Canadian Armed Forces.







“We look at network traffic metadata and apply it to a set of threat feeds and internal Bell data models to identify potential threat traffic targeting particular verticals or customers in Canada”

Dominique Gagnon,
General Manager, Cybersecurity Practice, Bell

Securing Your Cloud Strategy, Without the Complexity

Digital transformation promises to increase agility and scalability, but today's businesses face growing complexity when moving to the cloud.

Organizations must manage multiple tools and devices, protect against advanced threats, monitor increased bot activity, and deliver flawless digital experiences - all with limited budget and resources.

How do you get all of the benefits of the cloud, without the complexity?

The answer is at the edge.

By leveraging the Akamai Intelligent™ Edge Platform with a trusted cloud security advisor like Bell, you can adopt the cloud strategy that best supports your business goals and simplify your operations, while maintaining security and performance.

Find out 5 ways to make your cloud strategy pay off



Intelligent Security Starts at the Edge

“We aren’t talking to our customers about the latest tools and technologies, we’re talking to them about their foundational business needs and how security is core to them”

—
Gary Miller,
Cybersecurity Strategist, Bell

the capabilities of different technologies to offer the best solutions to our customers and address the challenges these five trends present,” explains Gagnon. “A key element is to make sure that, wherever possible, we don’t throw away our customers’ previous investments, but rather maximize their value through effective integration. The goal is simplified security rather than simple security.” Miller elaborates that this provides layers of protection that form a wider, simpler whole. “Traditionally, we’ve always talked about security-in-depth,” he says. “We’re seeing this manifest even more today as we look

15

EXECUTIVE PROFILE

Gary Miller

Gary Miller is a Cybersecurity Strategist at Bell. For more than 20 years, Gary has been assisting governments and organizations around the world shape appropriate and practical cybersecurity strategies to support their changing objectives. Gary has held senior executive positions, within international businesses leading corporate security functions and cybersecurity business units. He has successfully launched new cybersecurity products and businesses, consulted with governments on national cybersecurity strategy and policy, and is a frequent speaker on strategic cybersecurity issues.



at what an organization like Bell can provide. We have an end-to-end security approach and we can integrate the appropriate tools to provide customers with visibility from the edge to the core of their enterprise network.”

The advent of widespread virtual networks is also changing the cybersecurity industry. “Virtual networks provide a more agile and sophisticated way for customers to deliver network services. While every telecommunications provider is being impacted by virtual networks, providers who don’t have the scale and necessary technologies can really leave their clients vulnerable,” says Gagnon. “Bell is adapting our strategy to protect edge-based deployments for our virtual network services. And leveraging cloud-based services to support a broader, decentralized approach to security.”

The power of Bell security solutions is amplified by data-driven insights. Bell has developed a platform called CTI (Cyber Threat Intelligence) which leverages, with the approval of its customers, the breadth of its network to build intelligence on threats and threat





vectors specific to the Canadian environment. The process, as explained by Gagnon, doesn't collect data but instead recognizes and assesses network trends. "We look at network traffic metadata and apply it to a set of threat feeds and internal Bell data models to identify potential threat traffic targeting particular verticals or customers in Canada," he says. "What's happening in the network gives us an awful lot of insight into where issues are popping up. We collaborate with our customers to get further into their dataset for added insights, but in a general sense, we aren't gathering transmitted data, just the directional metadata, traffic patterns and so on."

These operations exist outside of the customers' network environment, but Bell is hard at work to bring these advanced detection capabilities to its customers. "We're investing in bringing Big Data to the customer's environment so that they can leverage the technology and threat intelligence to better detect what's happening within their own network," says Gagnon. "We're working with analytics partners to add such capabilities to the platform and provide

those benefits to the customer. That's where the future is." For Miller, CTI adds vital speed to the process of threat detection and response, along with the capacity to handle growing volumes of data. "There's a reality, particularly as we move to OT, that we're now getting more structured and unstructured data. We normalize all of these highly diverse and voluminous datasets, apply advanced analytics, AI and automation to filter through this massive volume and isolate the most critical and impactful things.



PARTNERS

Check Point and Akamai

"Check Point and Akamai are both important partners for Bell. They're leaders in their respective fields, and through those partnerships we can bring that expertise to our customers," says Dominique Gagnon, General Manager of the Cybersecurity Practice

at Bell. "We always look for organizations that align with our objectives: helping to clarify, simplify and integrate cybersecurity management to address operational liability and efficiency. These are two organizations that are highly aligned to our aims."



19

That is the value of Big Data for the future of cybersecurity.”

Ultimately, the customer is top of mind for Bell. Whether it’s filtering through the noise, managing SIEM environments, enabling virtual networks, or fortifying internal security in addition to perimeter control, Bell credits its deep understanding of the security landscape for its cybersecurity success. “We are very deliberate in the choices we make and continually engage with our customers every step of the way,”

enthuses Miller. “By bringing cybersecurity to the forefront, we have fundamentally changed the narrative. We aren’t talking to our customers about the latest tools and technologies, we’re talking to them about their foundational business needs and how security is core to them.” ■

Bell





Bell

Bell Canada

Montreal, Canada

T 1 800 668-6878

www.bell.ca