2023 CANADIAN

CYBERSECURITY STUDY:
EMERGING ISSUES AND TRENDS

TABLE OF CONTENTS

ABOUT THIS STUDY

About This Study

This report presents the findings of *CDW's 2023 Canadian Cybersecurity Study: Emerging Issues and Trends*. The data provided in this report was obtained through a Canada-wide, cross-province and cross-industry survey, independently conducted by IDC Canada, of 553 IT security and risk & compliance professionals. All survey participants were screened for direct involvement in improving or managing their organization's IT security. Of the IT security respondents, 51.7 percent directly managed the IT function. Survey respondents were screened to represent organizations with a minimum of 15 full-time employees, with at least 10 percent of their total employees located in Canada.

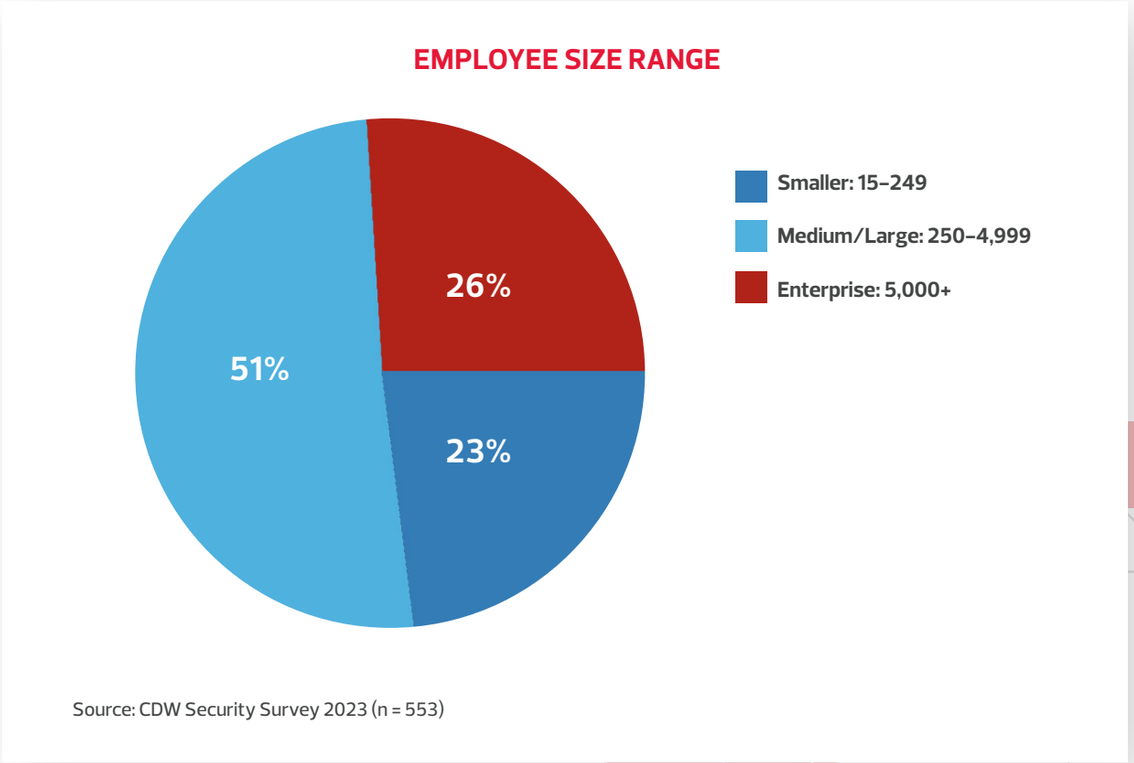
The survey was conducted from December 2022 to January 2023 by IDC Canada on behalf of CDW Canada. Appendix A shows a detailed description of the demographics and firmographics of the survey participants.

Organization Size Segmentation

In this report, CDW Canada classifies responding organizations as smaller, medium/large and enterprise organizations. The definition for each is based on its number of employees:

- **Smaller: 15–249 full-time employees located within Canada**
- **Medium/large: 250–4,999 full-time employees located within Canada**
- **Enterprise: 5,000-plus full-time employees located within Canada**

Chart A:



Source: CDW Security Survey 2023 (n = 553)

Introduction

As cyberattacks continue to disrupt our economy and society, it is no surprise that security has become a top concern for IT and business executives across Canada. The ever-growing complexity of today's IT environments has underscored the need to secure IT against the increasingly frequent and malicious nature of threats. The risks of data loss, service interruptions, infiltration and reputational impact are all top of mind for business and IT leaders in Canada as they seek to protect customer, employee and partner data and ensure the continuity of business operations.

As the Threat Landscape Grows, So Does the Risk to the Business

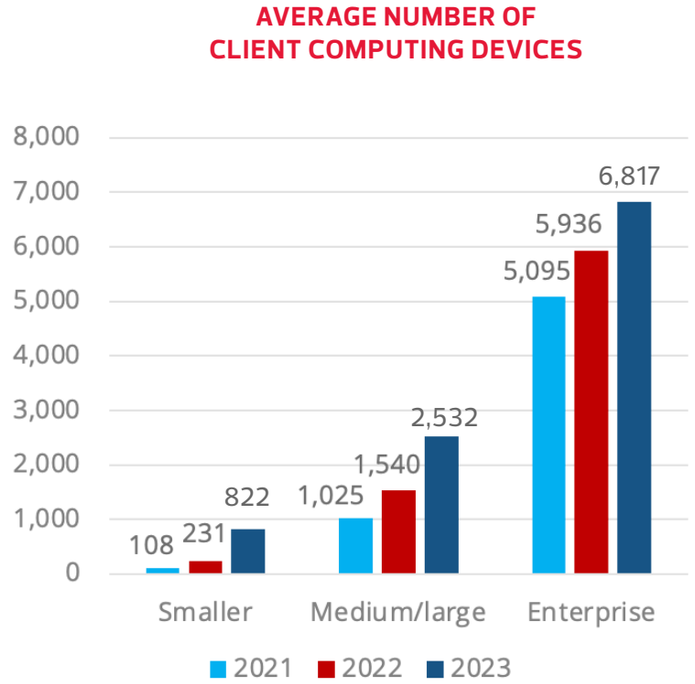
Expanding IT = Expanding Attack Surface

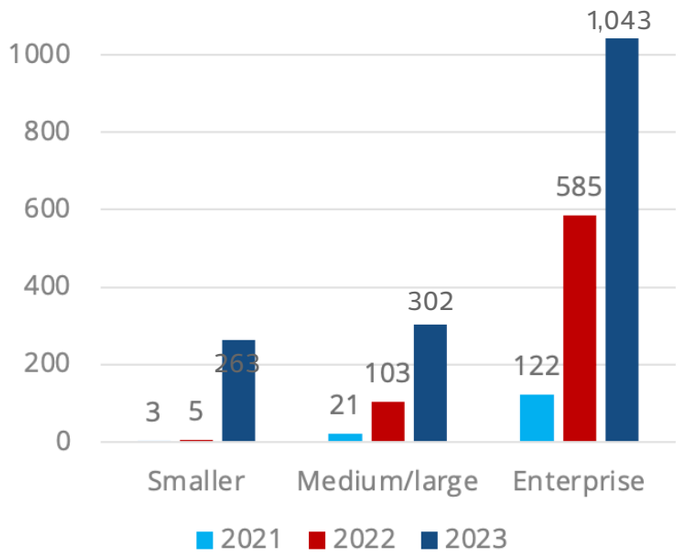
Post-pandemic, companies have experienced a rapid shift to hybrid work, digital services and custom-created application programming interfaces (APIs) and a rapid adoption of Internet of Things (IoT) devices. Many Canadian organizations are fast-tracking their public, hybrid and multicloud IT strategy. With the expansion of IT, data is being created, exchanged and processed at lightning speed.

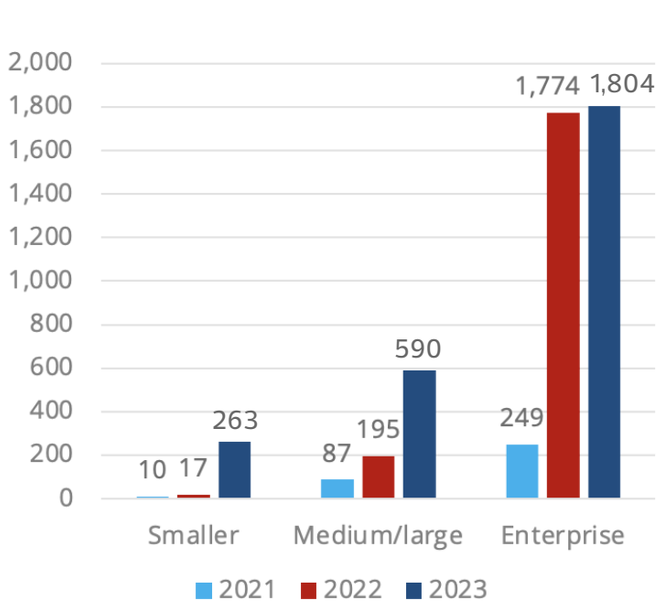
The Attack Surface of Canadian Organizations Continues to Expand

The attack surface of Canadian organizations is vast and encompasses Software as a Service (SaaS) applications, APIs, containers, virtual machines (VMs), storage systems, database appliances, network appliance endpoints and more. However, this study zeroed in specifically on analyzing the enormous growth of client computing devices, servers and IoT devices to represent organizations' expanding attack surface. Note how the number of these components used by smaller organizations has exploded.

Chart 1:





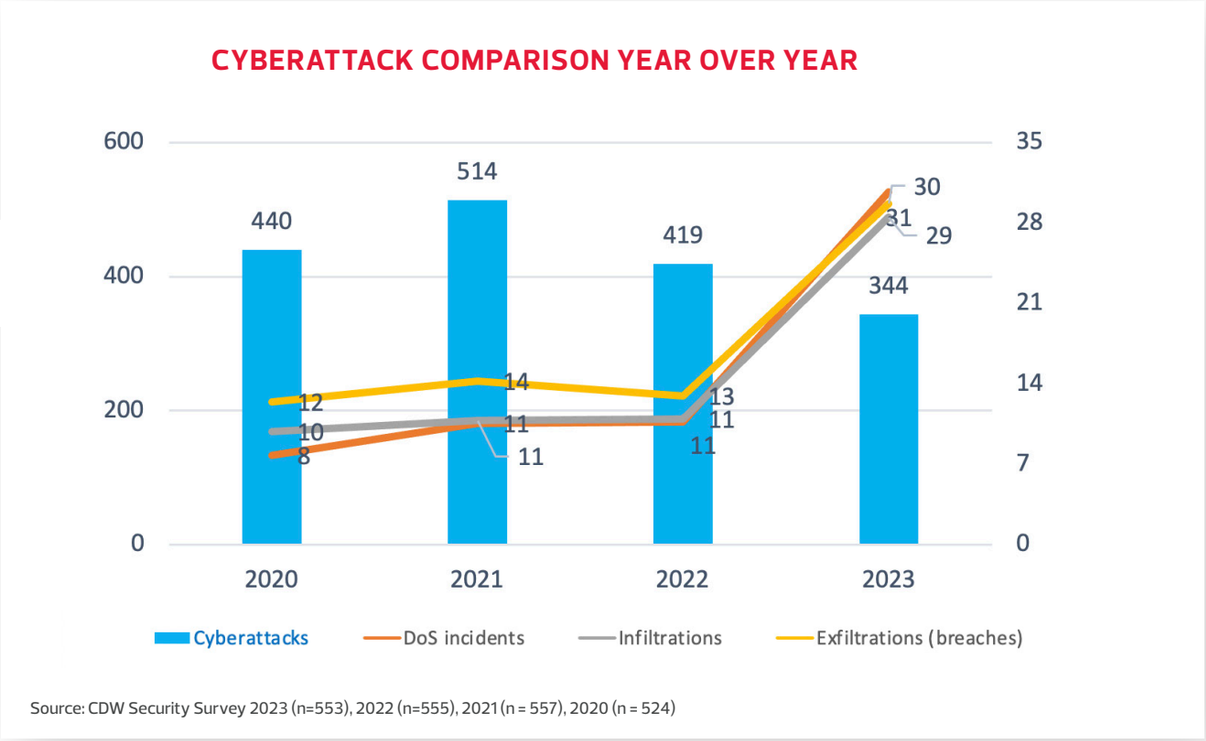


Client Computing includes PCs, laptops, smartphones and tablets
Source: CDW Security Survey 2023 (n = 553), 2022 (n = 555), 2021 (n = 557)

Number of Successful Cyberattacks Is Rising

The total number of cyberattacks saw a decline year over year; however, the number of successful incidents continues to trend upward. Specifically, a sharp uptick in exfiltrations (breaches) was reported in the study. For example, the number of breaches jumped from 13 in 2022 to 30 in 2023. Similarly, the number of infiltrations also increased, from less than 11 in 2022 to more than 28 in 2023.

Chart 2:



Source: CDW Security Survey 2023 (n=553), 2022 (n=555), 2021 (n = 557), 2020 (n = 524)

With cyberattacks now more sophisticated and effective than ever before, the infection rate has seen an increase, according to the 2023 study. This indicates that cyberattacks have a significantly better "hit rate" (number of attacks that are successful and become an incident) than in previous years. Across industries and organization size, 7–10 percent of all cyberattacks were successful. The highest hit rate was found in government and education.

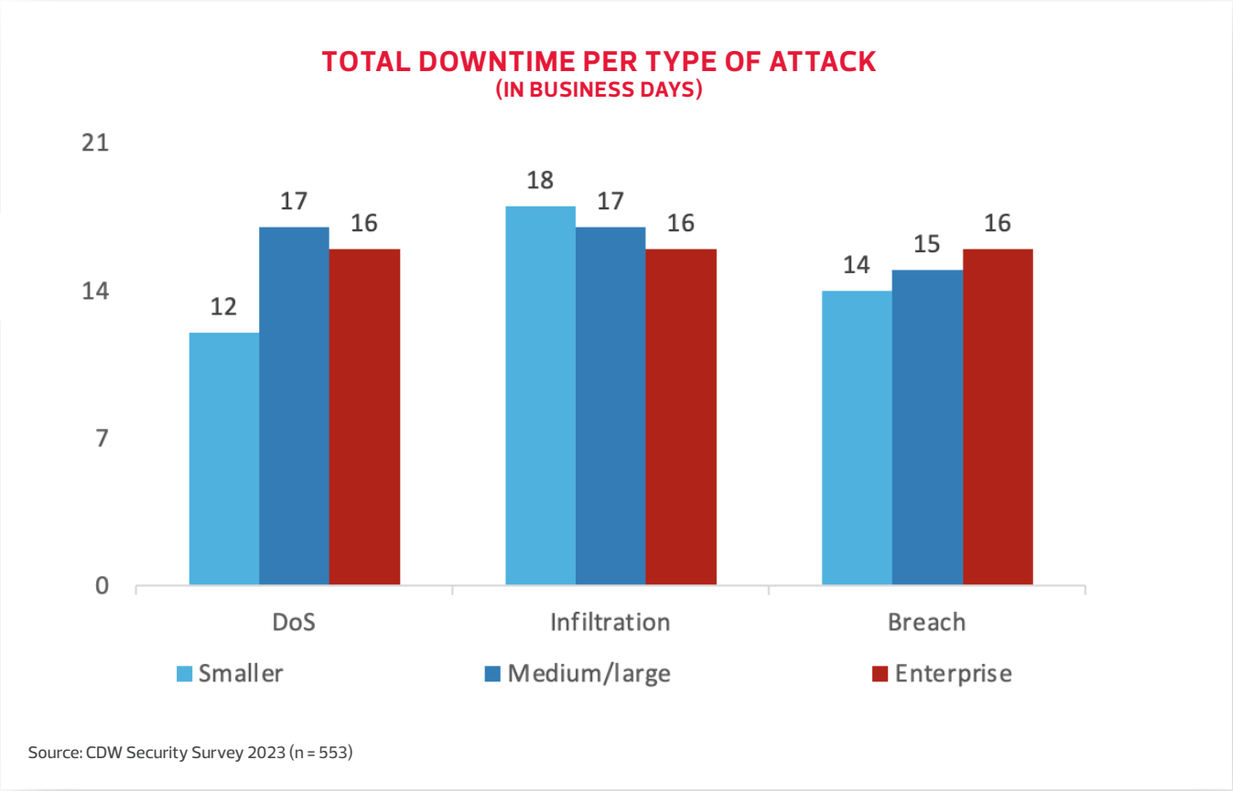
Table 1: Cyberattack Success Rate

Attack Type	Total	Industry						Size		
		Financial Service	Energy	Public Sector	Education	Healthcare	Other	Smaller	Medium/ Large	Enterprise
Denial of service (service interrupted specifically due to an attack)	8%	9%	6%	10%	11%	7%	7%	8%	7%	9%
Infiltration (attackers gained access to the organization's network/infrastructure/data but no data was exfiltrated)	7%	7%	5%	11%	9%	7%	7%	7%	6%	9%
Breach (data was exfiltrated)	7%	8%	5%	13%	9%	7%	7%	8%	7%	9%
Security incident in cloud	7%	6%	6%	8%	9%	6%	7%	6%	6%	9%
Average	7%	7%	6%	10%	10%	7%	7%	7%	7%	9%

Downtime Puts Pressure on the Business

Downtime resulting from cyberincidents affects both a company's reputation and its bottom line. Canadian firms across all business sizes reported average downtime of two weeks or more over a period of 12 months per each category of attack. While downtime related to denial of service (DoS) and infiltration remained the same in 2023, downtime related to breaches rose by one to four days, depending on business size.

Chart 3:



Source: CDW Security Survey 2023 (n = 553)

Downtime seems mostly independent of business size, although smaller organizations reported a sharp increase in infiltration attacks (the stealthy insertion of malware) at 18 days, compared with 11 days in 2022. Infiltration and DoS were the most cited types of attack related to downtime in 2023. Financial services and government reported more downtime than other industries for infiltration attacks.

Table 2: Downtime/Attack Ratio (X05/X04)

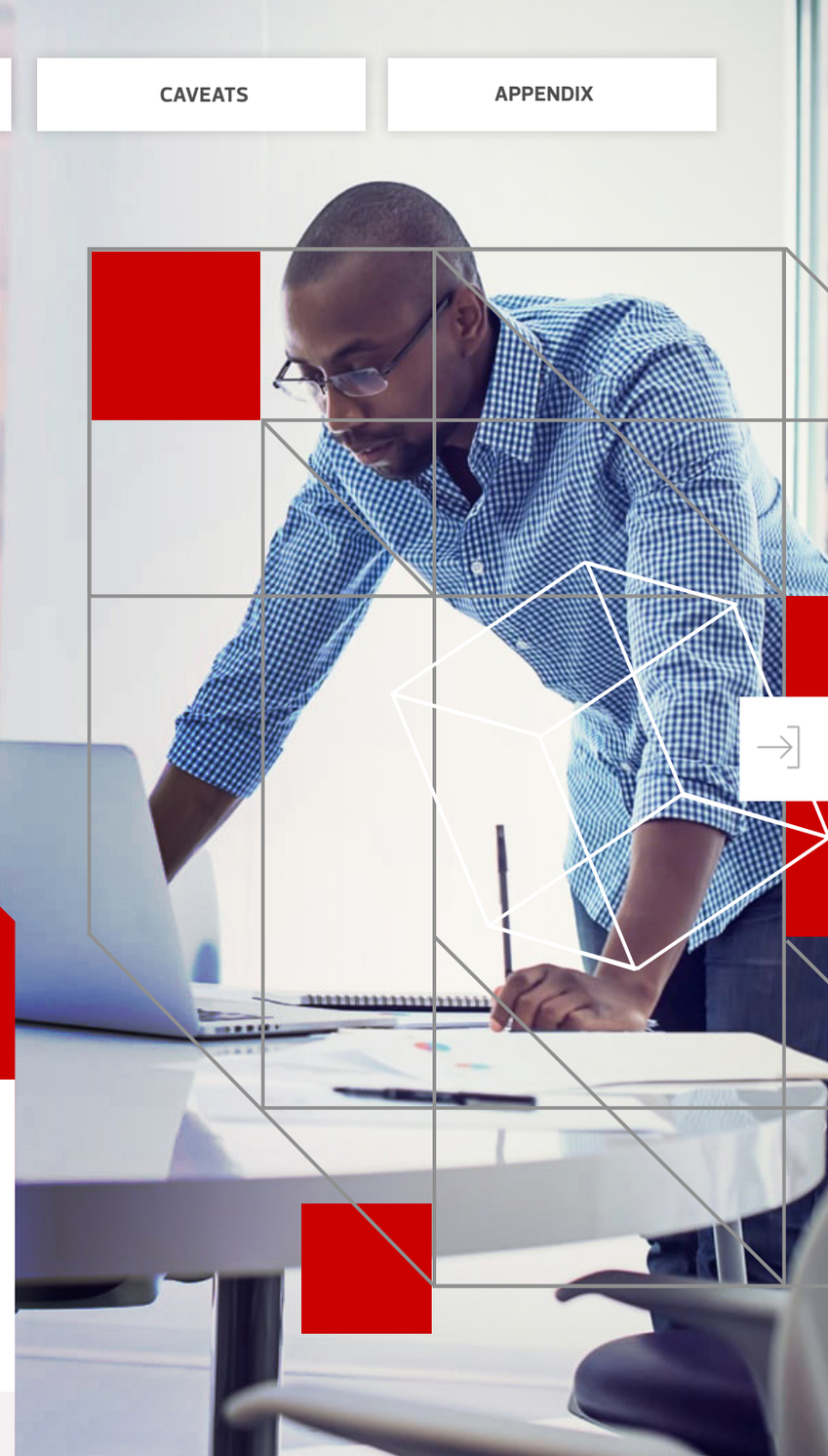
Downtime/Attack Ratio	Total	Industry						Size		
		Financial Service	Energy	Public Sector	Education	Healthcare	Other	Smaller	Medium/ Large	Enterprise
DoS	0.51	0.68	0.55	0.61	0.3	0.42	0.5	0.40	0.54	0.52
Infiltration	0.6	0.75	0.58	0.73	0.48	0.56	0.58	0.66	0.60	0.56
Breach	0.5	0.57	0.55	0.47	0.49	0.4	0.51	0.48	0.51	0.50
Cloud	0.39	0.43	0.24	0.54	0.33	0.34	0.42	0.38	0.38	0.41

KEY FINDINGS

FINDING 1:

For many Canadian organizations, zero-trust architecture is often confined to identity and access management — but zero trust encompasses a complete catalogue of capabilities.

While recognizing that zero-trust architectures are essential in the era of hybrid work, Canadian organizations tend to overlook an important principle of zero trust: assumption of breach. Understanding this reality will produce a renewed focus on threat detection and response.



Zero Trust Is Rapidly Gaining Traction as the Threat Landscape Evolves

Growth of Hybrid Work Has Expanded Potential Attack Surfaces

In the post-pandemic era, hybrid work arrangements have allowed workers to split their time between home and the office. Unfortunately, the growth of the hybrid workforce has expanded potential attack surfaces.

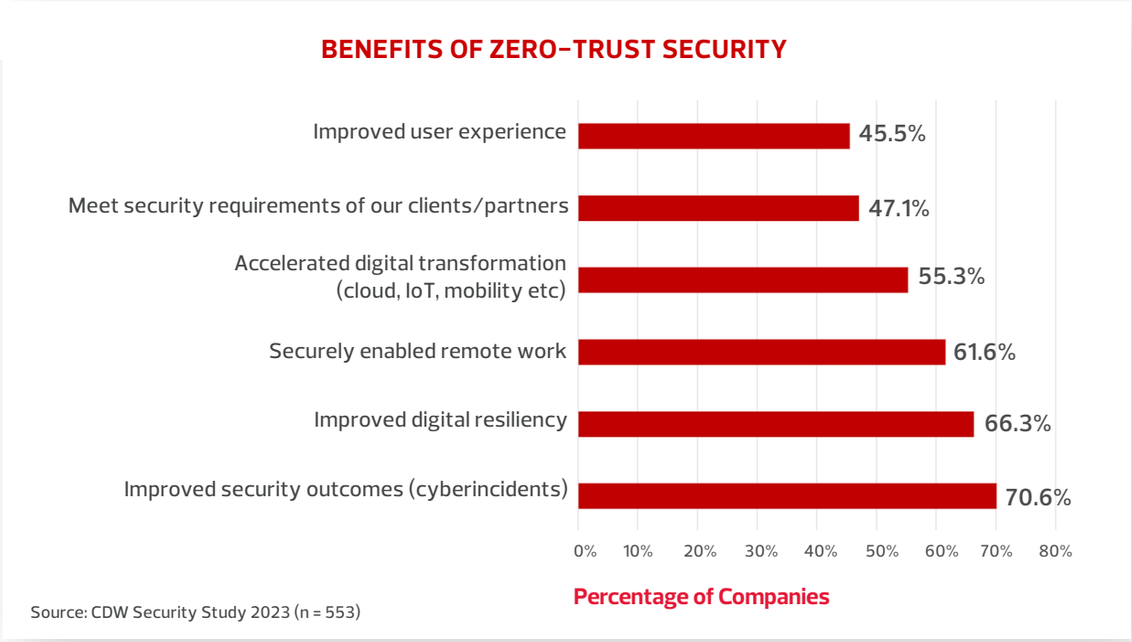
In recent years, Canadian organizations have made significant investments in digital transformation (DX) initiatives, with many that had previously lagged behind rapidly expanding their DX efforts during the pandemic. Why? Cloud services are ideal for business continuity and operational efficiency, supporting business innovation, hybrid work and increased mobility.

However, when users, data, devices and services are spread across multiple locations, perimeter-based security architectures are limited in their ability to protect critical systems from cyberattack. That is why the security principles of zero trust have rapidly gained traction. With zero trust, inherent trust is never granted automatically, and scalable architectures can be readily extended to devices and networks, enhancing visibility and control and improving threat detection and response.

Benefits of Zero Trust

Rising cyberattacks are a grave concern for Canadian organizations and a top driver of the adoption of zero-trust architectures. For 71 percent of Canadian organizations, reducing the number of security incidents is a top benefit they seek to realize through zero-trust initiatives. Sixty-six percent of respondents indicated that they believe zero-trust security architecture will make their organizations digitally resilient, while 61 percent believed it will make remote work more secure.

Chart 4:



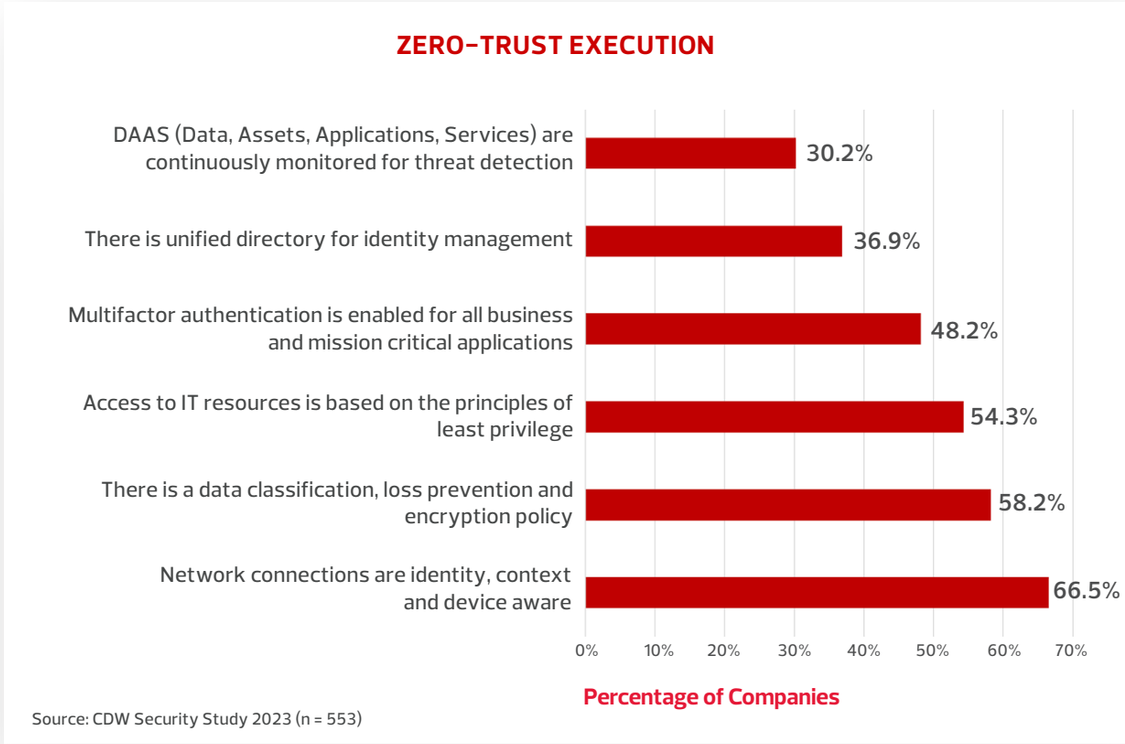
Source: CDW Security Study 2023 (n = 553)

Zero-Trust Policy Lagging Behind in Threat Monitoring

While Canadian companies clearly see the merit in zero-trust architecture, analysis of its execution shows that it is often heavily skewed in favour of identity and access management (IAM).

As organizations implement policies that support a zero-trust philosophy, 66 percent of Canadian organizations have network connections that are identity-, context- and device-aware. Another 58 percent have a policy for data classification, loss prevention and encryption, and 54 percent grant access to IT resources based on the principle of least privilege. However, when it comes to monitoring DAAS (data, assets, applications and services) for threat detection, Canadian organizations are falling short. Only 30 percent of respondents indicated that a policy for threat monitoring exists in their organization.

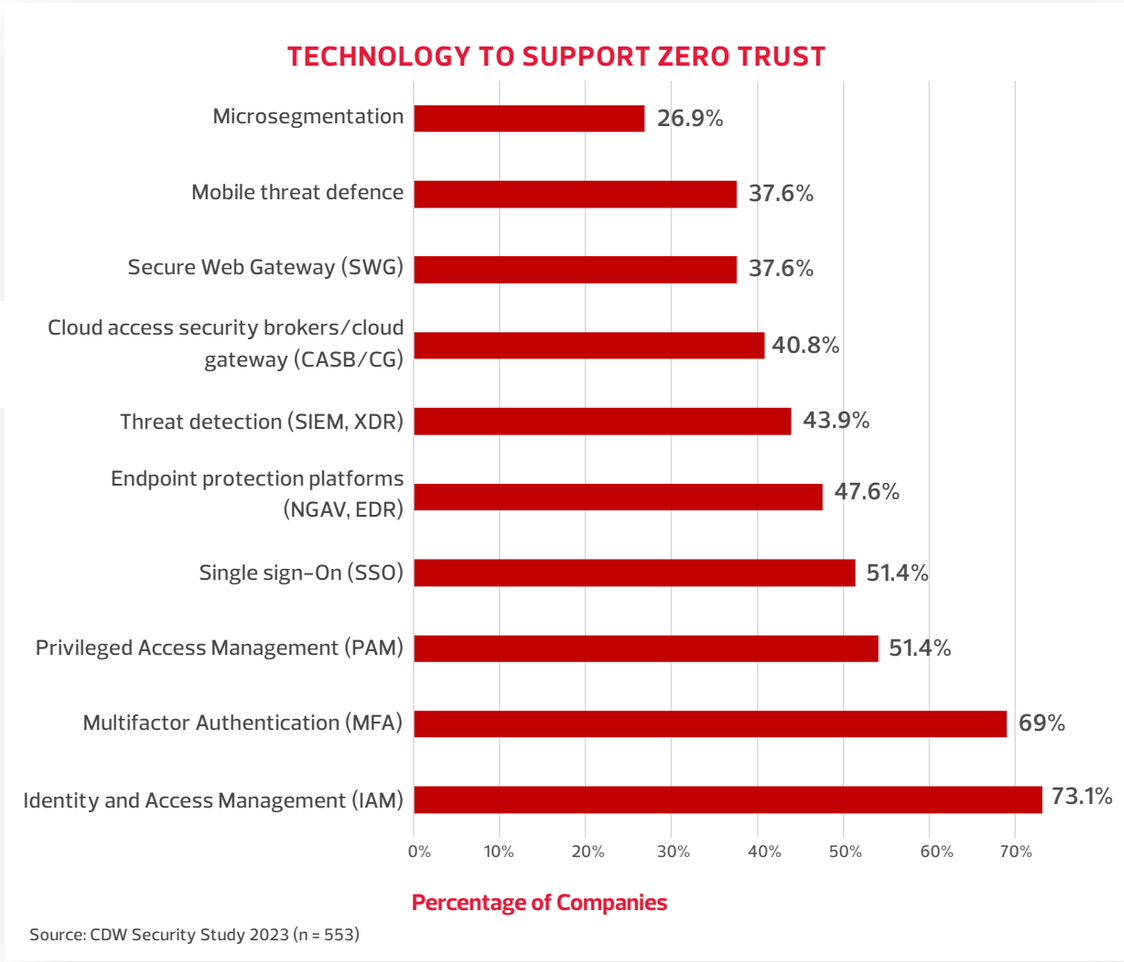
Chart 5:



Source: CDW Security Study 2023 (n = 553)

Similarly, when assessing technology investments to support zero-trust principles, the study showed that the leading technology deployments are identity and access management (73 percent), multifactor authentication (69 percent), privileged access management (54 percent) and single sign-on (51 percent). The adoption of threat detection and response tools such as security information and event management (SIEM) and extended detection and response (XDR) was only 44 percent.

Chart 6:



Source: CDW Security Study 2023 (n = 553)

Assumption of Breach Is an Essential Zero-Trust Principle

The core principles of the zero-trust philosophy are continuous verification, least-privilege access and assumption of breach. Canadian organizations have begun their zero-trust journey with IAM, which reflects the first two principles. However, assumption of breach is an equally important principle, one that focuses on threat detection and response instead of just threat prevention.

To maintain a proactive security posture that doesn't only react to security threats but proactively defuses them as soon as (or before) they begin, Canadian companies should increase their investments in threat intelligence; telemetry-based threat detection (network, cloud, endpoint, etc.); security analytics and artificial intelligence/machine learning (AI/ML) use cases; threat hunting; and security orchestration and automation.

FINDING 2:

The mean time to recover from a cyberincident for Canadian organizations is approximately 48 days.

The threat detection and response capabilities of Canadian organizations are falling short, tipping the scales in favour of adversaries.

Detection and Response Delays Give Cyberattackers Free Rein

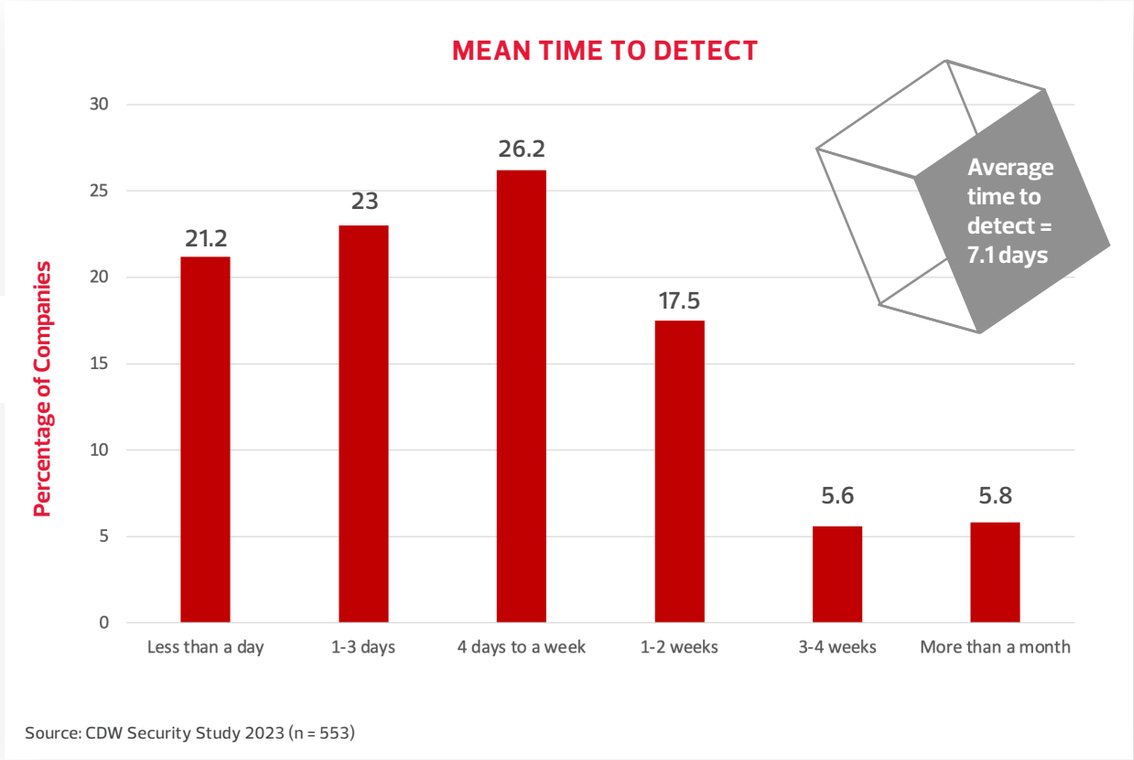
Costly Consequences

Cyberattackers try to access and steal personal, financial or intellectual data, or they attempt to disrupt business processes with ransomware and distributed denial of service (DDoS) attacks. With the increasing sophistication of tactics, techniques and procedures (TTPs), a data breach or another serious cyberincident has become more likely than ever before.

Any delay in detection and response times related to cyberattacks puts Canadian organizations at higher risk for regulatory fines, loss of customer trust and the cost of recovering from security incidents — at the expense of investments in IT growth initiatives that support business goals.

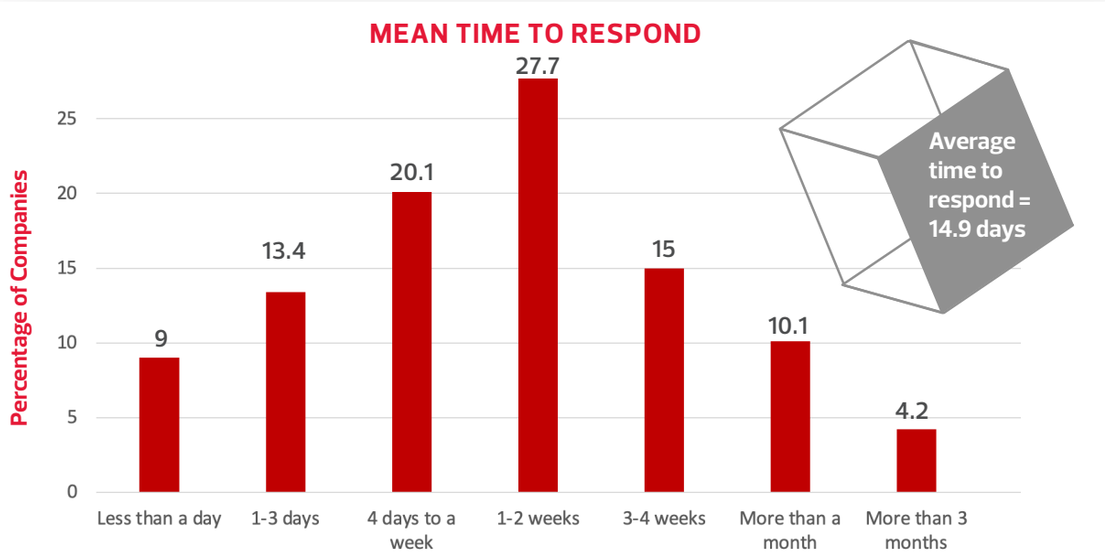
According to the study, the MTTD (mean time to detect) of a cyberincident for a Canadian organization was 7.1 days. About 29 percent of Canadian organizations took over a week to detect a cyberincident. About 57 percent of Canadian organizations took over a week to respond to a cyberincident, with a mean time to respond of 14.9 days. Coupled with a mean time to recover of 25.6 days, the total time needed by Canadian organizations for incident management was approximately 48 days. This amount of time offers attackers a significant window during which they can access valuable enterprise resources, and it significantly tips the scale in favour of these adversaries.

Chart 7:



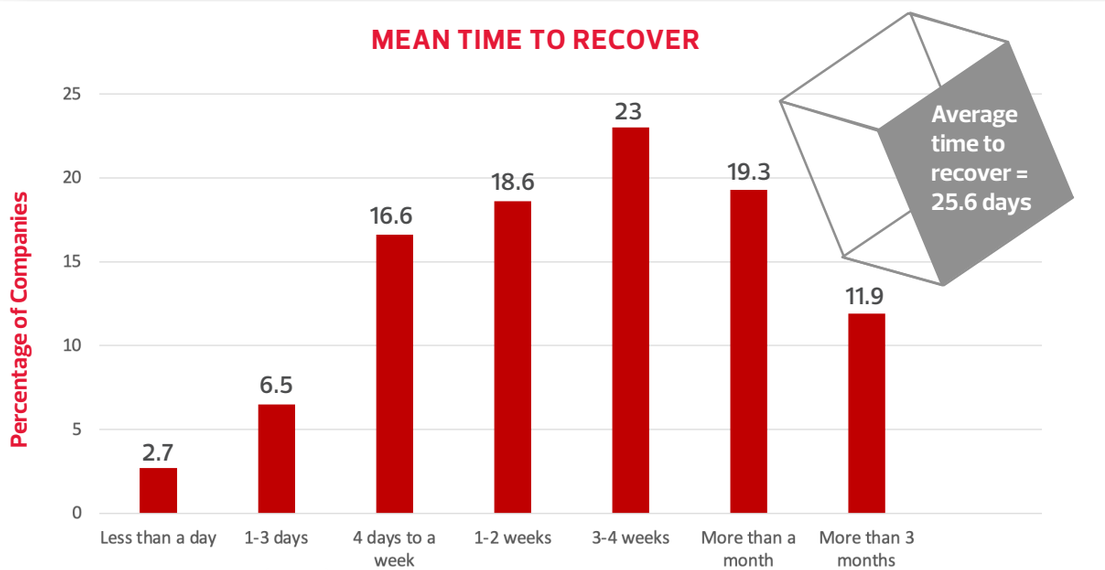
Source: CDW Security Study 2023 (n = 553)

Chart 8:



Source: CDW Security Study 2023 (n = 553)

Chart 9:



Source: CDW Security Study 2023 (n = 553)

Business Exposed to Risk and Loss

The slower the detection and response time, the greater the damage to the business and the more costly the resolution and recovery. This puts the business at risk for:

- **Detailed reconnaissance:** The longer the attacker stays in the network, the more time they have to identify and locate sensitive information, gather financial information for negotiation and make lateral moves.
- **Reinfection:** Given enough time, attackers will find ways to avoid detection or create mechanisms for re-entry (for example, the installation of back doors, password theft and more).
- **Evidence tampering:** Slow response time gives attackers a window of opportunity to remove evidence. This makes efficient recovery more difficult to achieve.
- **Recovery backlog:** Slow detection and response time leads to a cascading effect for resolution and recovery that can lead to backlogs, adding significant delay and costs to recovery.

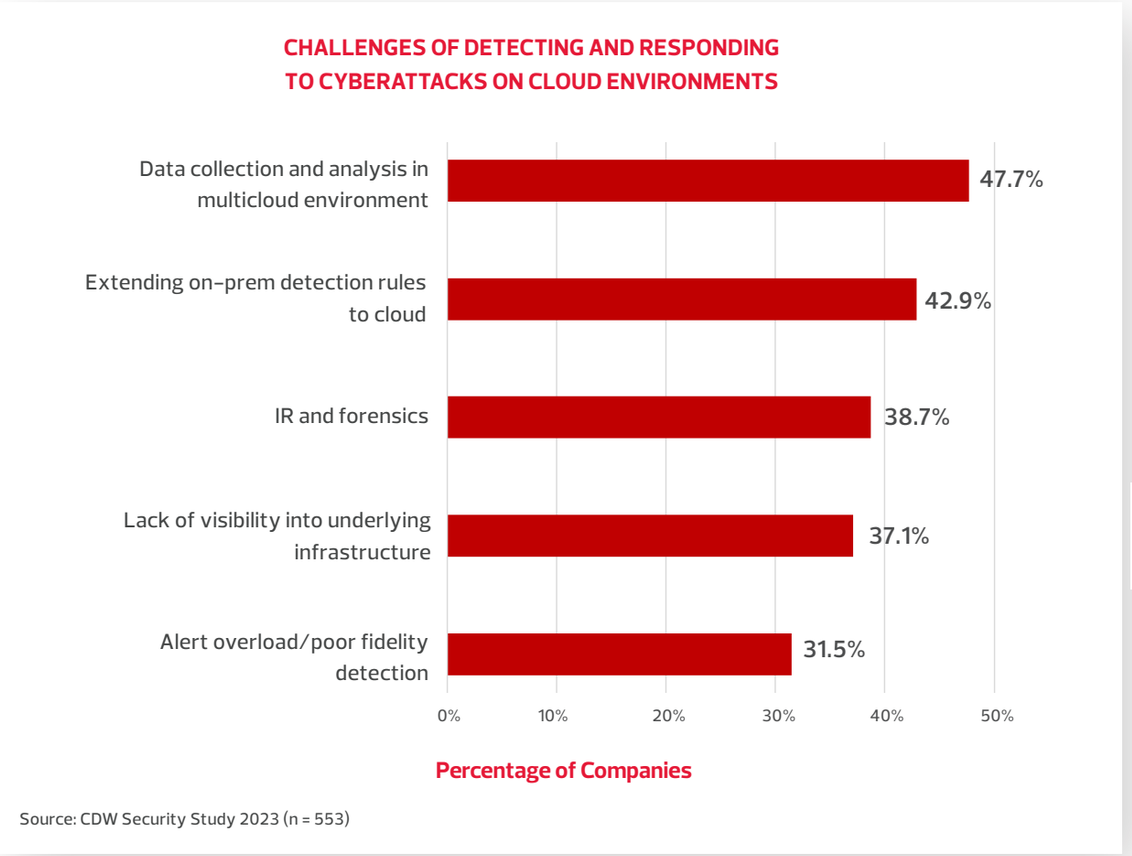
Cloud Adoption Is Complicating Threat Detection and Response

The expansion and proliferation of cloud services has been good for business, but it has further complicated the ability of Canadian organizations to detect and respond to threats. The study showed that the leading challenges for detection and response in the cloud environment include:

1. Security data collection and analysis (48 percent of respondents)
2. Extending on-premises detection rules to the cloud (43 percent)
3. Responding to incidents and forensics (39 percent)

The cloud has visibility and control restrictions that do not apply to on-premises infrastructure. Effective threat detection and response depends on a specialized set of skills, tools and processes that organizations should acquire to strengthen their overall threat detection and response program.

Chart 10:



Source: CDW Security Study 2023 (n = 553)

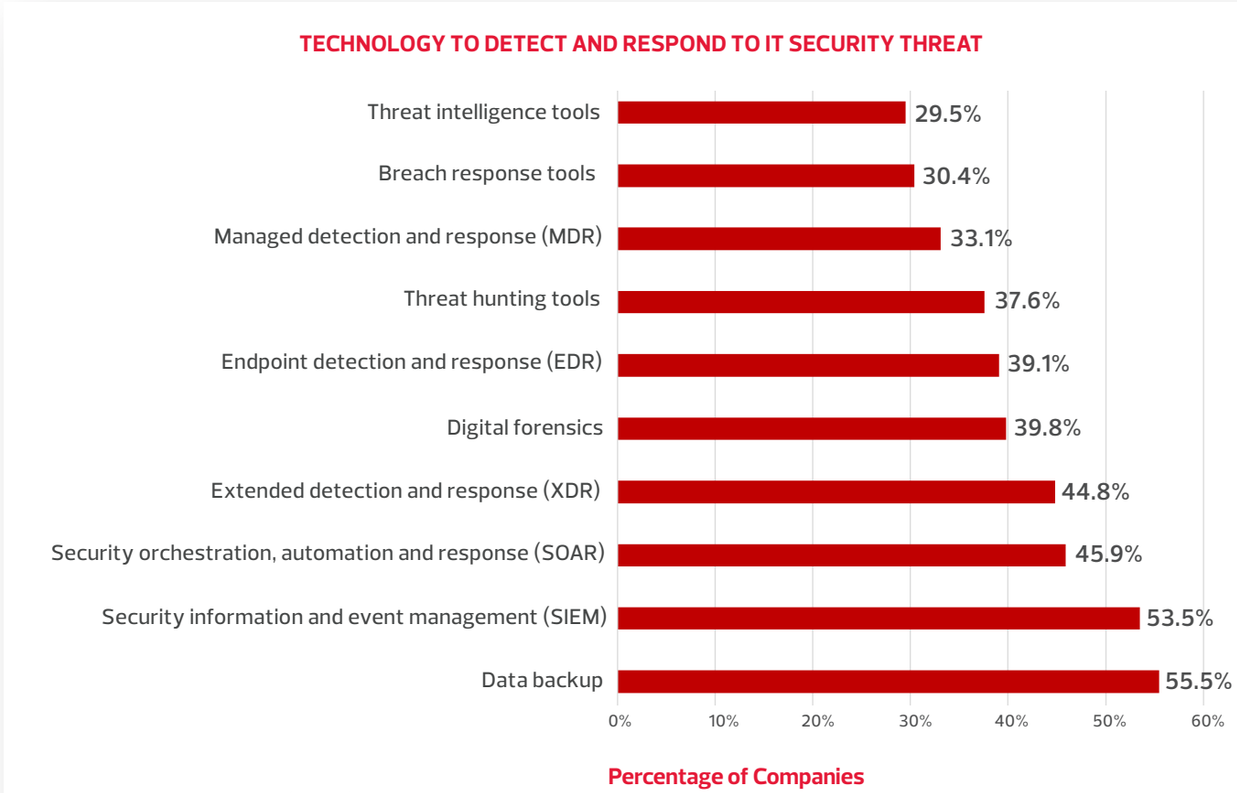
Traditional Security Responses No Longer Enough

Canadian organizations have invested in a myriad of security solutions in their efforts to deal with incidents faster and more efficiently. However, adoption rates for modern threat detection tools such as security orchestration, automation and response (SOAR), XDR, threat intelligence and threat hunting remain low.

To protect against modern threats, traditional log-based threat detection and manual response methods can only go so far. Without intelligence-based threat detection and automated and orchestrated response mechanisms, Canadian security teams will find it hard to tip the scales back in their favour.

However, it takes more than security solutions to reverse high dwell times. An incident response plan that outlines the policies and procedures to evaluate, contain and recover from a security incident is a good place to start.

Chart 11:



Source: CDW Security Study 2023 (n = 553)

FINDING 3:

The gap between cloud adoption by Canadian organizations and their efforts to secure it has manifested into a top cyber risk.

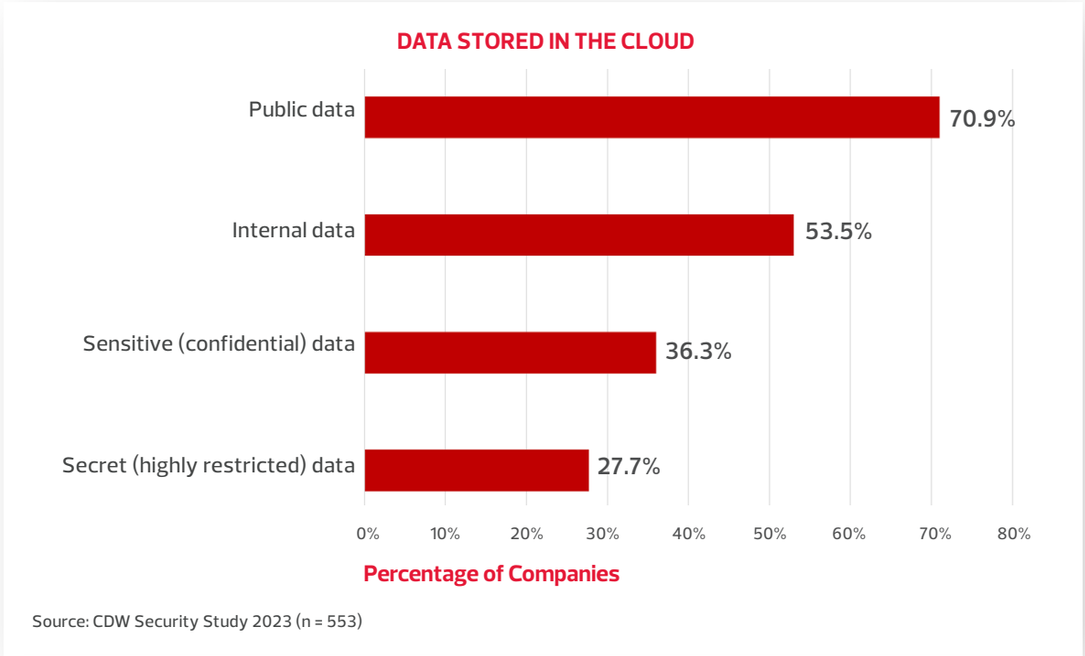
Public cloud environments are the IT components most directly affected by a security incident. The risk impact has increased significantly as more Canadian organizations rely on cloud for storing their private, sensitive and secret data.

It's Time to Close the Gap Between Cloud Adoption and Cloud Security

Securing Sensitive Data a Top Concern

Canadian organizations are leveraging cloud to store the bulk of their organizational data. Not surprisingly, the study shows that the top concern related to storing sensitive data in cloud is security. Seventy-one percent of Canadian organizations store their public data – press releases, marketing information, job descriptions – in a public cloud, while 54 percent store internal data such as employee handbooks and company-wide memos in a public cloud. We see the numbers start to taper off as the sensitivity of the data increases. For example, 36 percent store sensitive (confidential) data such as financial data in a public cloud, whereas only 28 percent store secret (highly restricted) data such as personally identifiable information (PII) and protected health information (PHI) in a public cloud.

Chart 12:

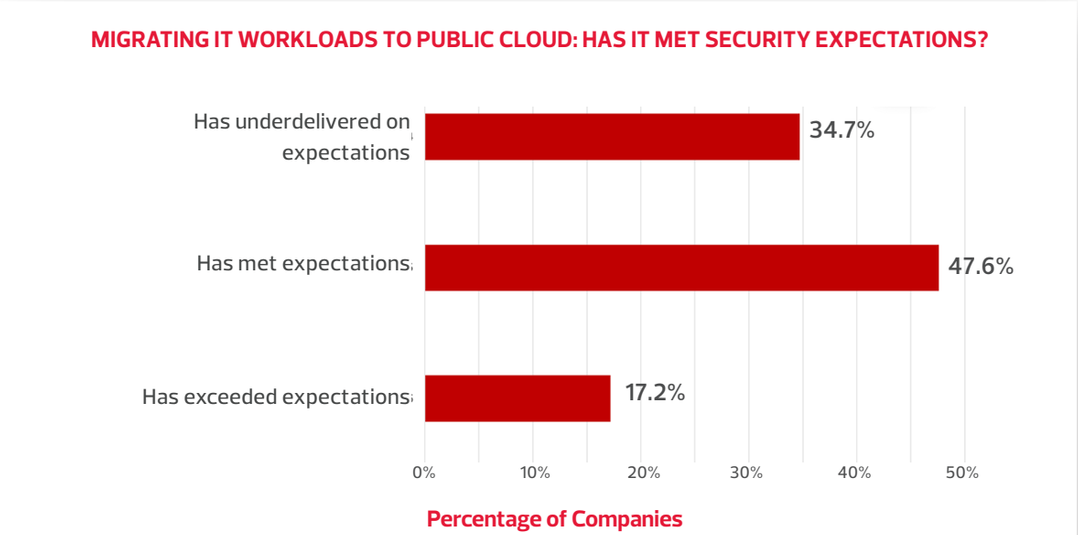


Source: CDW Security Study 2023 (n = 553)

Public Cloud Falls Short of Security Expectations for Many Organizations

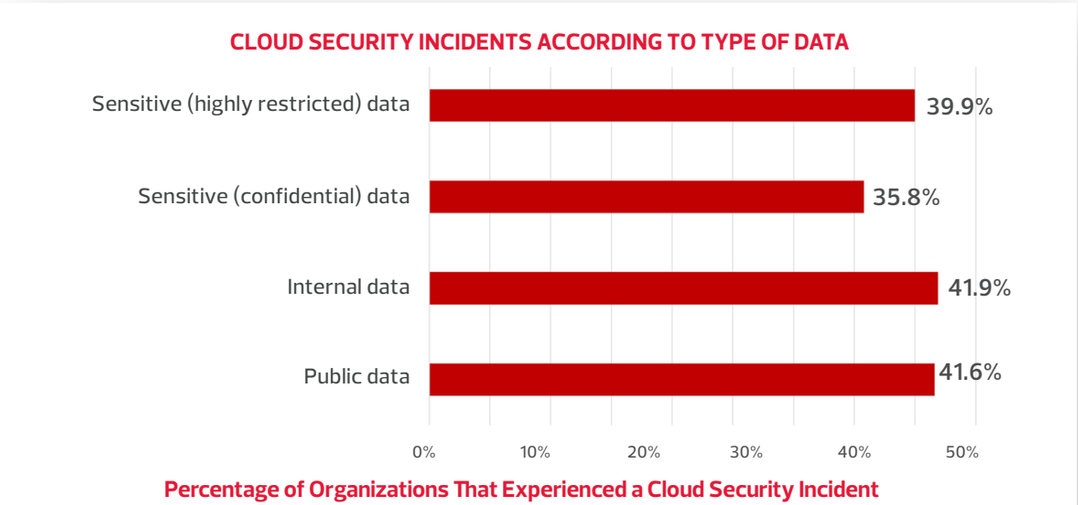
Overall, approximately 40 percent of respondents from Canadian organizations that store the above-mentioned categories of data in the cloud experienced a security incident in the cloud. Especially concerning is the fact that two in five organizations that store highly restricted data such as PII and PHI suffered cloud incidents. It is no surprise, then, that many Canadian organizations (35 percent) reported that public cloud did not meet their initial security expectations.

Chart 13:



Source: CDW Security Study 2023 (n = 553)

Chart 14:

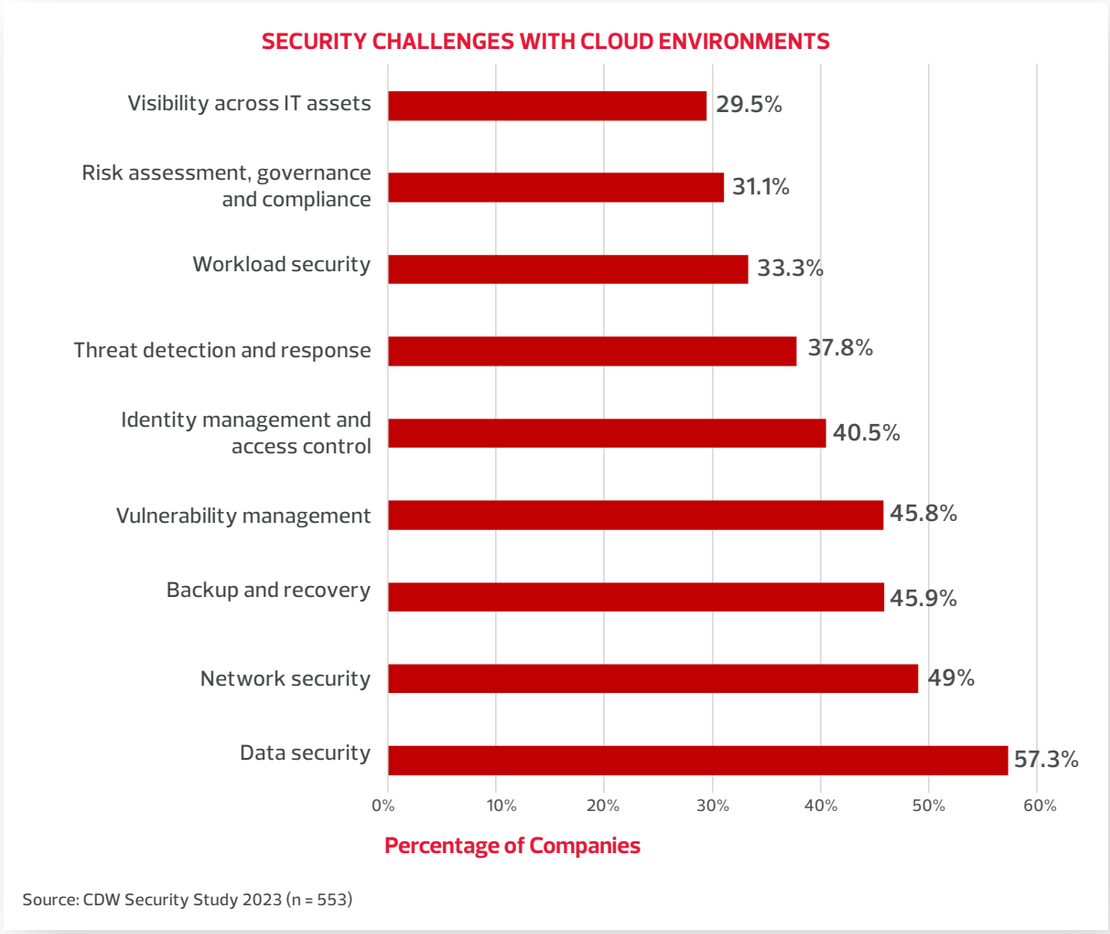


Source: CDW Security Study 2023 (n = 553)

Top Three Cloud Security Challenges

Cloud security may be particularly challenging due to its inherent business model. Not only is the responsibility of cloud security shared between the provider and the customer, but there is also low visibility and control over the underlying infrastructure. Canadian organizations reported that the top three challenges that made cloud security difficult were data security (57 percent), network security (49 percent) and backup and recovery (46 percent).

Chart 15:

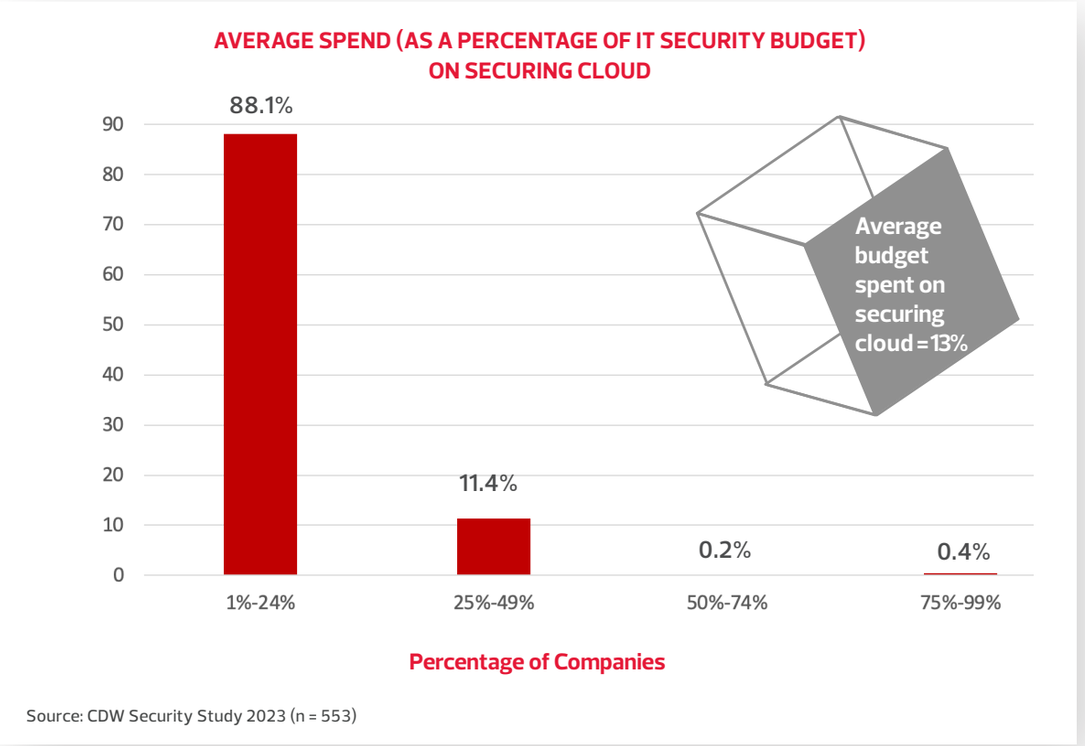


Source: CDW Security Study 2023 (n = 553)

The Cloud Is Under Attack and Organizations Are at Risk

Cloud environments have become the most attacked IT components, and the gap in cloud adoption and cloud security investment has manifested into a top cyber risk for many Canadian organizations. How can Canadian organizations close the gap between cloud adoption and cloud security? Determining the sensitivity of data in the cloud, identifying and assessing the potential risks, and understanding the shared responsibility model are all necessary steps for prioritizing investments and skill acquisition and development. The study showed that Canadian organizations spend, on average, only 13 percent of their security budget on securing cloud environments.

Chart 16:



Source: CDW Security Study 2023 (n = 553)

FINDING 4:

Rising cyberthreats are driving the need for security automation among Canadian organizations.

Canadian security teams view security automation as key to improving security team productivity and security outcomes for the organization.

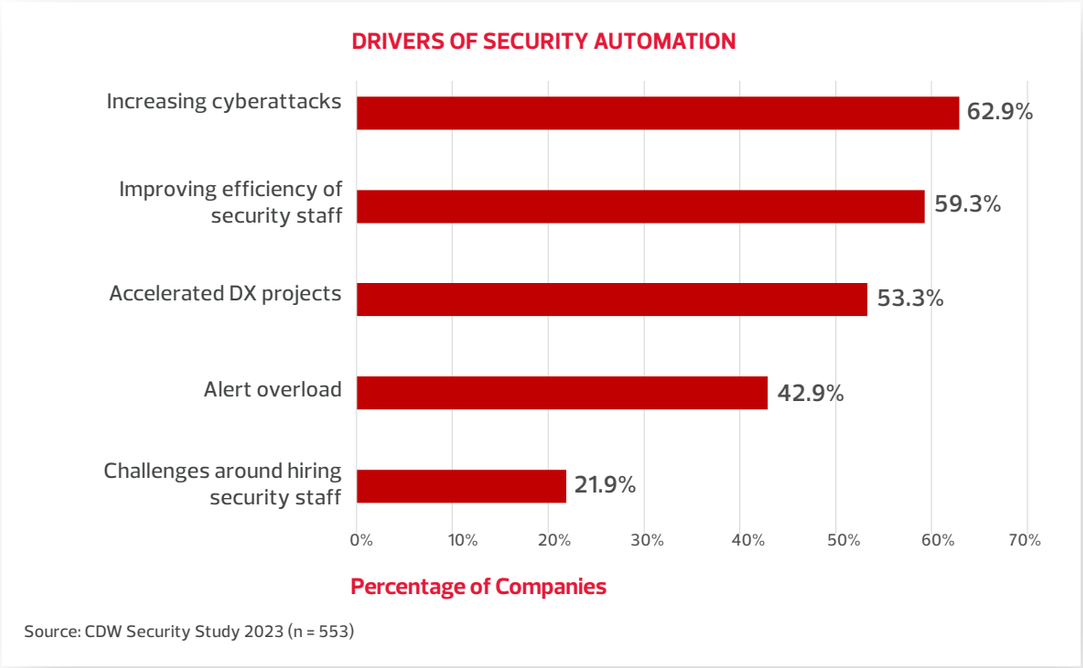
Rise in Cyberthreats a Key Driver for Increased Security Automation

Growing Adoption of Security Automation

New security architectures based on zero-trust principles and intelligence-based threat detection provide granular visibility into security events but can also create a significant amount of alert overhead for security teams. Many Canadian organizations have turned to security automation to enable high-fidelity detection, faster incident response and security agility.

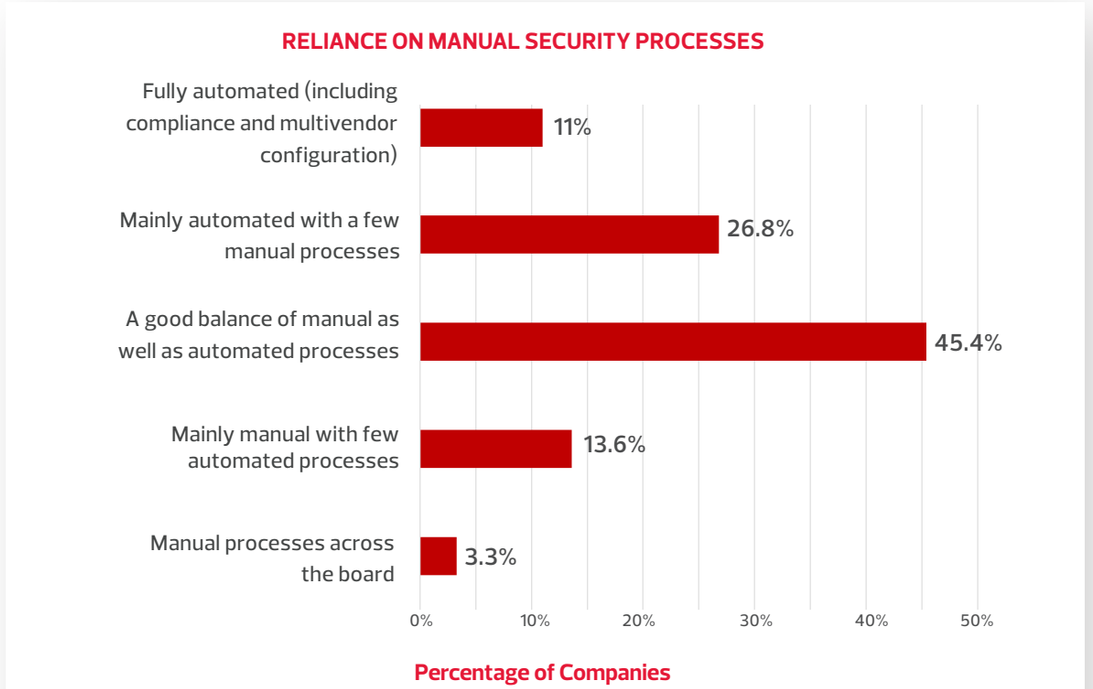
For 63 percent of Canadian organizations, rising cyberattacks are a leading driver of security automation. Fifty-nine percent see automation as a means to improving the efficiency of security staff. For example, automation use cases such as alert aggregation, enrichment and prioritization can significantly improve efficiency for Tier 1 and Tier 2 security operations centre (SOC) analysts, which frees up time for value-added activities such as investigations and threat hunting.

Chart 17:



Source: CDW Security Study 2023 (n = 553)

Chart 18:



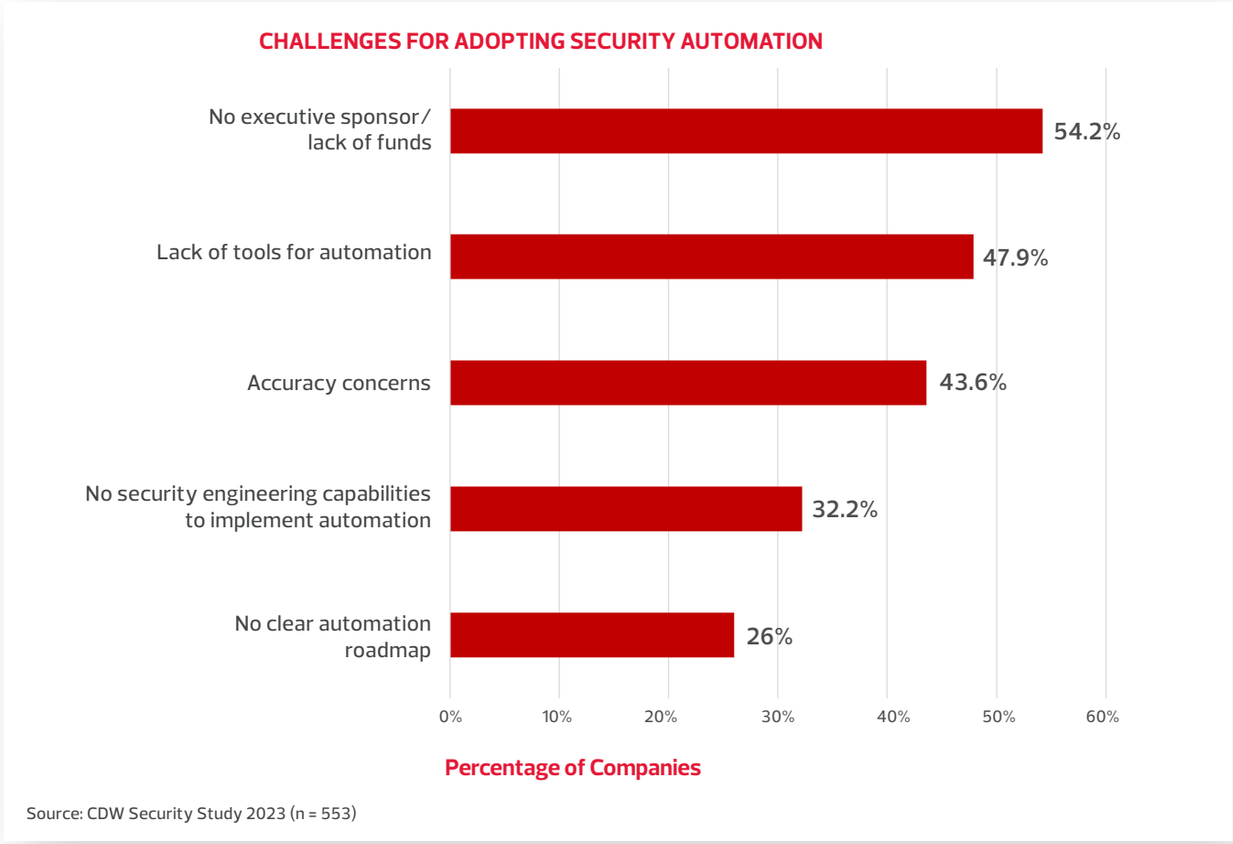
Source: CDW Security Study 2023 (n = 553)

Manual Security Processes Still Commonplace

Although most Canadian organizations have scrutinized and documented their security workflows to identify areas that could be automated, there is still a long way to go. While Canadian organizations have started their journey toward security automation, 62 percent still rely on manual security processes, according to the study.

Why do manual processes continue to be so prevalent? Canadian organizations face several key challenges as they seek to modernize their security. Budgetary constraints remain the top hurdle, followed by a lack of necessary tools for automation. Despite these and other challenges, organizations should strive to create a strategic plan for security modernization. With a long-term commitment to continuous improvement, organizations are likely to see quantifiable improvements to their security posture — and their ability to combat the growing threat of cyberattacks.

Chart 19:



Source: CDW Security Study 2023 (n = 553)

FINDING 5:

DevOps is now a leading software development methodology in Canadian organizations, paving the way for DevSecOps.

Organizations using DevOps that have also consistently invested in DevSecOps report lower levels of data breaches over time compared with those that have not.

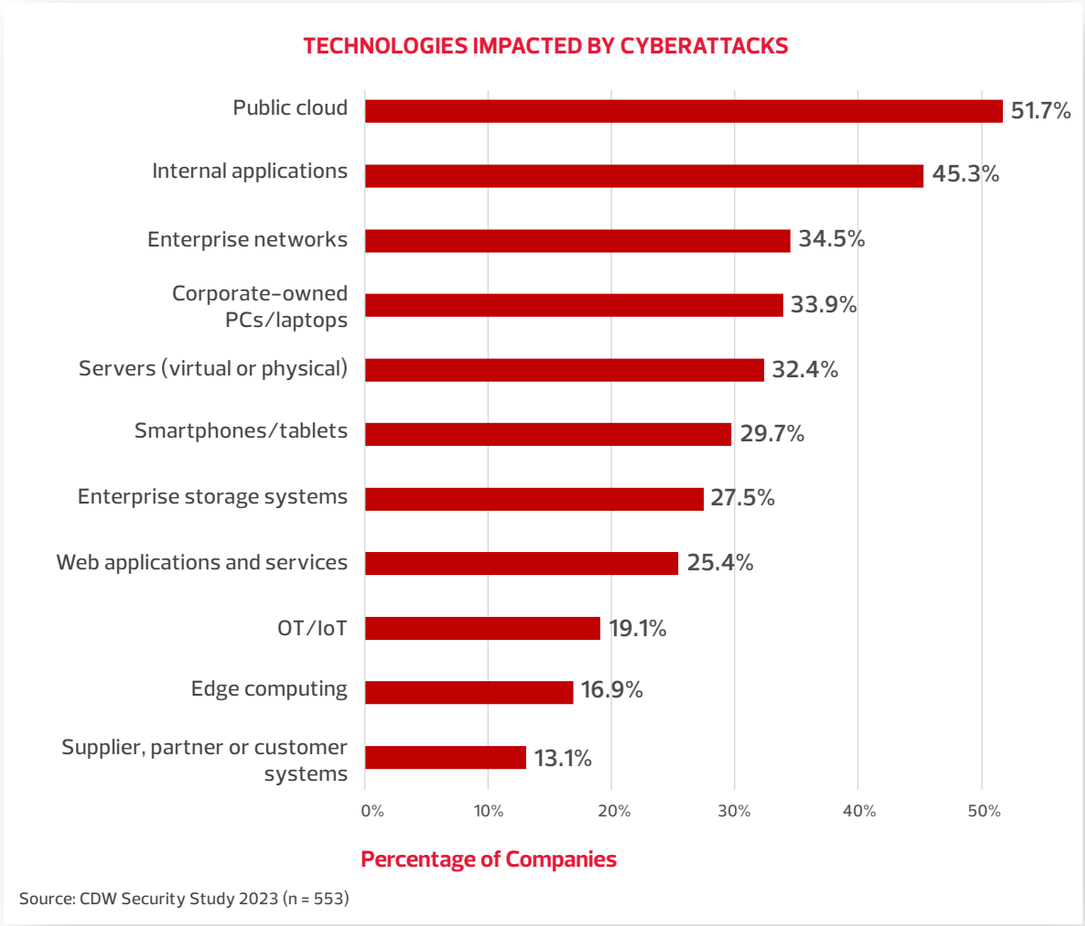
Secured Application Development a Top Priority for Canadian Organizations

Security Needed Throughout the Application Development Cycle

Most applications today are no longer part of a monolithic architecture. Thus, development teams do not have the luxury of the long development and testing cycles that were characteristic of the traditional waterfall software development lifecycle. Applications are now developed using microservices architectures, creating a need to integrate security concepts and security testing throughout the development cycle.

After public cloud environments, the IT components most affected by cyberattacks are internal applications. Collectively, this places "secured application development" among the top security concerns of Canadian organizations.

Chart 20:

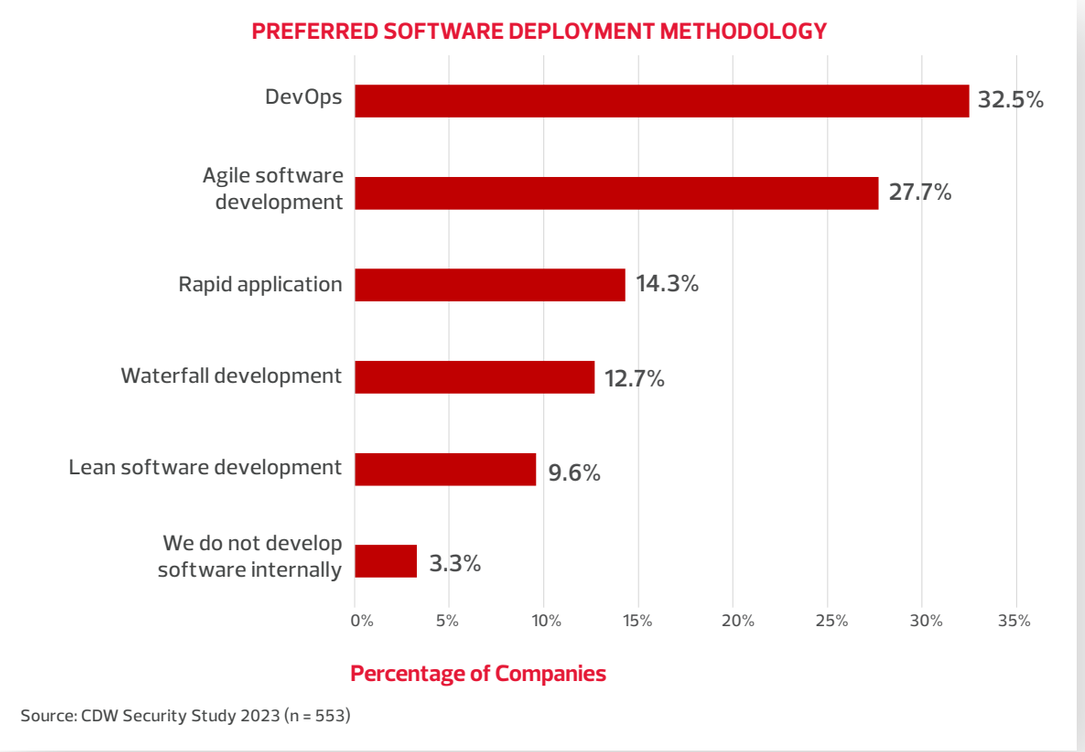


Source: CDW Security Study 2023 (n = 553)

DevOps Development Methodology Gaining Ground

According to the study, almost one third (32 percent) of Canadian organizations have adopted DevOps as their standard software development methodology. Since the inception of DevOps, software developers across Canada have embraced it to speed up the delivery process and facilitate communication between developers and IT operations teams. As a result, the development process has become increasingly iterative and inclusive.

Chart 21:



Source: CDW Security Study 2023 (n = 553)

DevSecOps Ensures Security Is "Baked in" to Application Development

A siloed approach to security can cause delays in development, effectively defeating the objective of DevOps. Consequently, some Canadian organizations have adopted DevSecOps to achieve fast and secure application development, with the collaboration between security teams and developers ensuring that security is "baked in" to application development. Security teams share knowledge about known threats, malware and vulnerabilities during the design phase, before those issues have a chance to snowball into larger problems post-delivery.

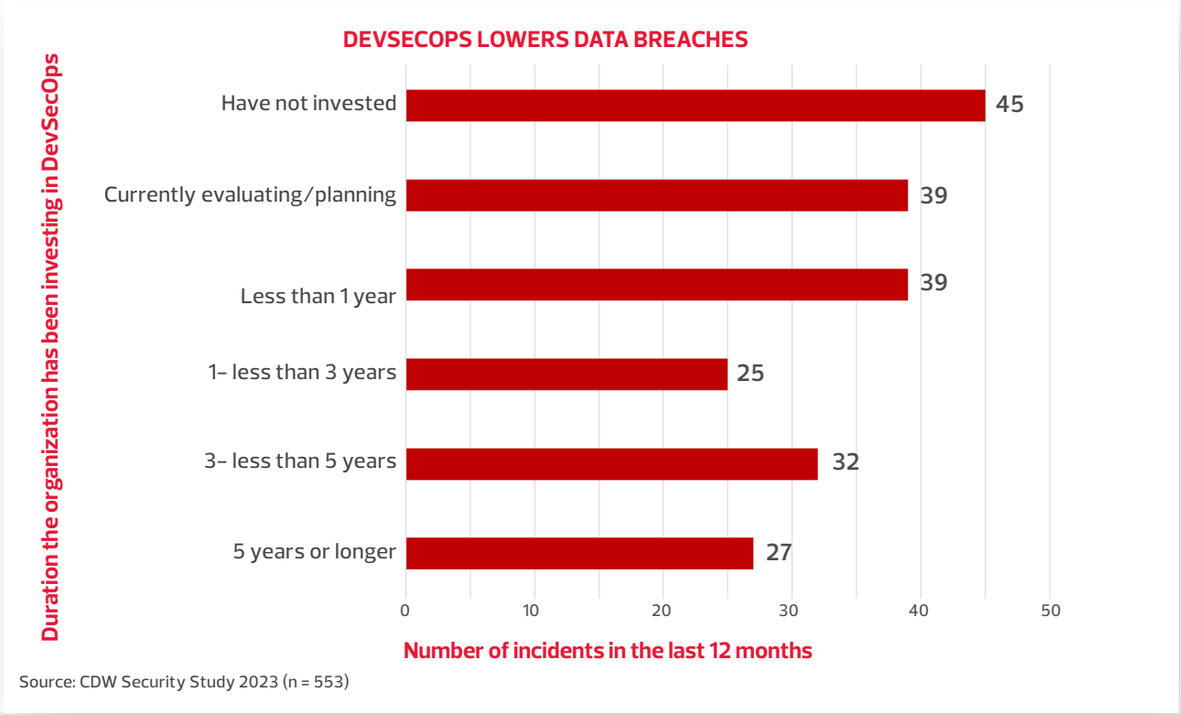
Automation Critical to DevSecOps

Automation empowers DevSecOps teams with more visibility and observability into the software development lifecycle, which is critical for solving security issues with minimal manual interference and delays. One example is automating security testing in the continuous integration (CI) process, such as container image screening and automated static application security testing (SAST) and dynamic application security testing (DAST).

DevSecOps requires a fundamental change to the organizational mindset. Building security into application development from end to end requires more than just new development tools: Many organizations may need to modernize the entire development environment, including source code repositories, container registries, the continuous integration/continuous delivery (CI/CD) pipeline, API management, operations management and monitoring.

Despite these challenges, it is worth the effort, as it significantly improves security outcomes. According to the study, the organizations using DevOps that have also invested in DevSecOps reported lower cases of data breaches over time compared with those that have not yet begun their DevSecOps journey.

Chart 22:



Source: CDW Security Study 2023 (n = 553)

FINDING 6:

Macroeconomic pressures and security skills gaps are both significant roadblocks to the digital maturity of Canadian organizations.

More than 60 percent of Canadian organizations say that the skills gap has reduced their ability to prevent security incidents. A significant percentage of Canadian organizations rely on external security service partners to face the storms of disruption.

Key Factors Affecting Digital Maturity: Macroeconomic Pressures and Security Skills Gaps

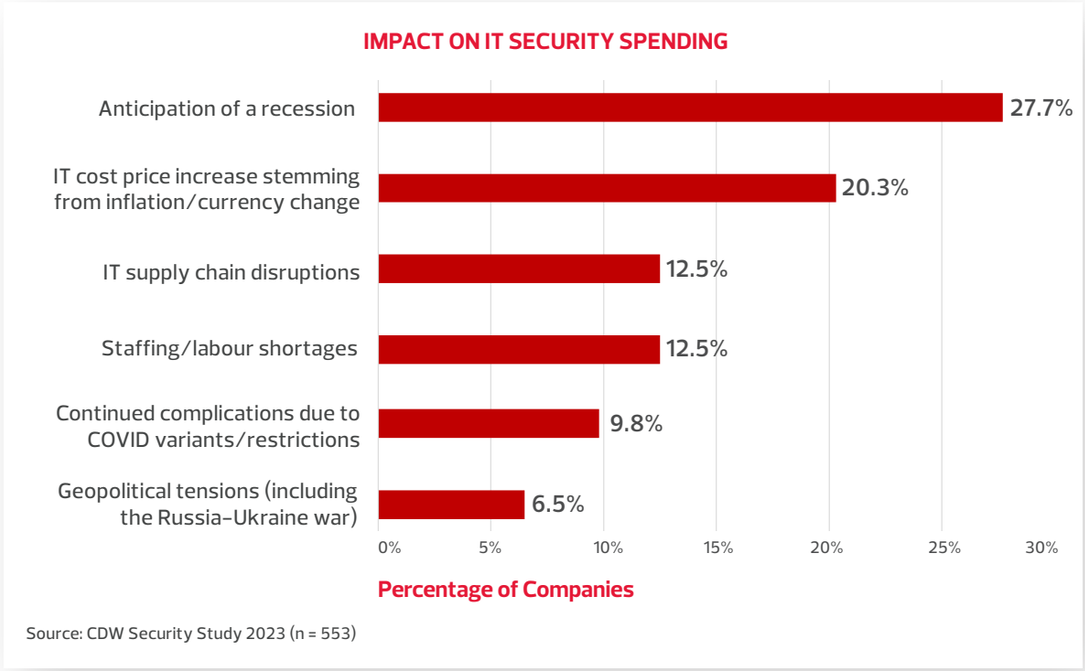
Skills Assurance a Top Priority

In an age when digital maturity drives business resilience, any hindrance to IT modernization reduces the organization's future growth and competitiveness. As greater numbers of security leaders are evaluated on the value they add to the business, it becomes increasingly important that CIOs and CISOs focus on skills assurance — i.e., making sure that skilled security personnel such as incident responders, SOC managers and governance, risk and compliance (GRC) specialists are available when the need arises.

A Strategic Approach to Security Spending

Our study found that 48 percent of Canadian organizations believe that two things will have the greatest impact on their security spending for 2023: a looming recession (28 percent) and rising inflation (20 percent). Geopolitical tensions such as the Russia–Ukraine war and possible complications due to COVID-19 variants now have little impact on security spending and are a concern only for 16 percent of Canadian organizations.

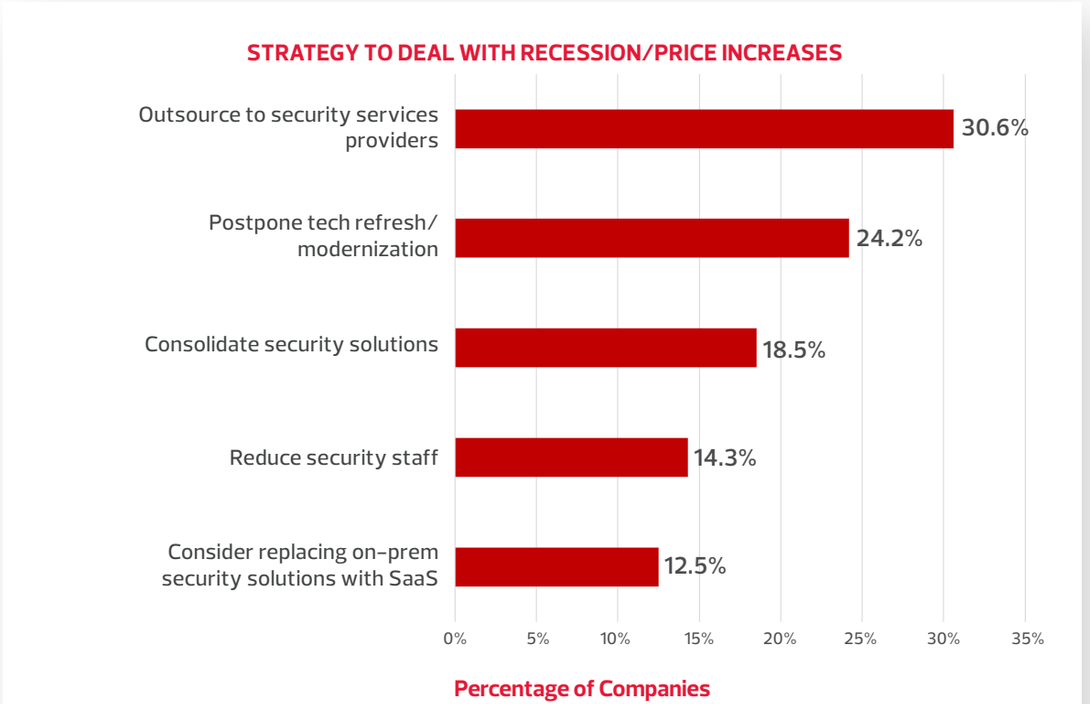
Chart 23:



Source: CDW Security Study 2023 (n = 553)

Thirty-one percent of Canadian organizations have turned to external security service partners to maintain and improve their security posture to combat the impact of macroeconomic triggers on their security spending, while 24 percent have postponed their security tech refresh and modernization initiatives.

Chart 24:



Source: CDW Security Study 2023 (n = 553)

Scarcity of Security Skills

Macroeconomic triggers are a significant hurdle facing organizations that want to improve their cybersecurity. Many Canadian organizations also find it challenging to hire and retain adequate security skills. Security architects (38 percent), cloud security professionals (35 percent) and SOC analysts (30 percent) were the top skills that Canadian organizations reported as being scarce within their organizations.

Chart 25:

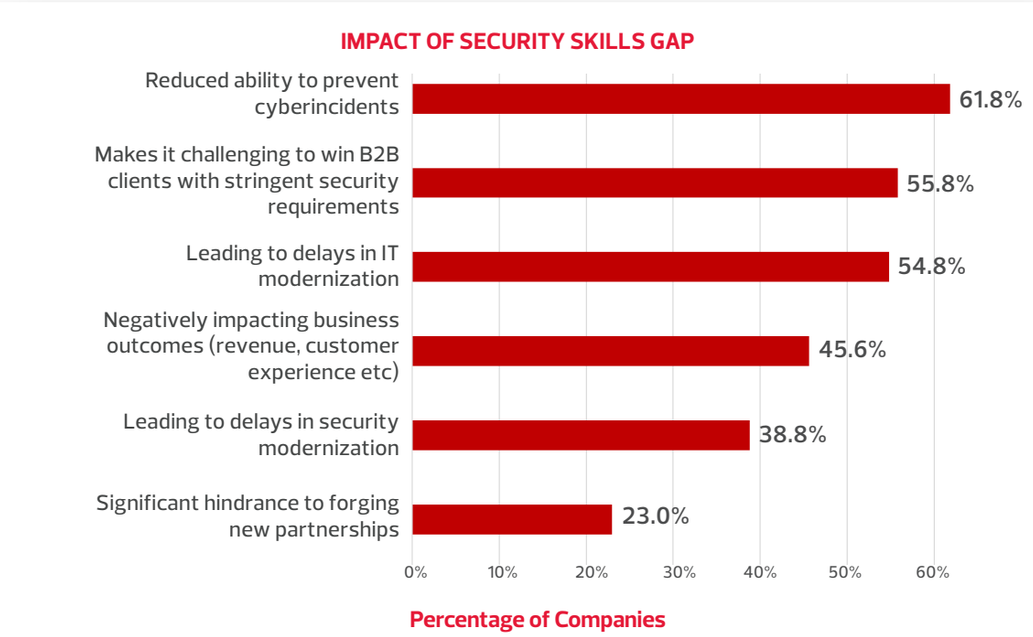
Source: CDW Security Study 2023 (n = 553)

Skills Gap: A Significant Challenge

Canadian security teams cannot guarantee that niche skills (such as incident response) would be available within their organization if a security incident were to take place at any given time. According to the study, the skills gap has led to a reduced ability to prevent security incidents for 62 percent of Canadian organizations.

The skills gap is a major hindrance to advancing Canadian organizations' digital maturity. For 56 percent of respondents, this hindrance has made it difficult to win business with partners that demand stringent security measures. For more than half of respondents (55 percent), the skills gap has led to delays in IT modernization.

Chart 26:



Source: CDW Security Study 2023 (n = 553)

RECOMMENDATIONS AND CALLS TO ACTION

I. Orchestrate, Then Automate

For years, Canadian organizations have managed cybersecurity in silos, with specific teams responsible for managing the components of network security, identity and access management, endpoint security, threat detection and response, and more. However, attackers do not view an organization's IT landscape in silos, and more often than not, the siloed approach works against the organization when it is facing a cyberattack.

Orchestration is the glue that makes the organization's entire security ecosystem work as one unit. Orchestration centralizes the management of the ecosystem and connects various tools through their input, output and APIs. This integration paves the way for automation, which can drive context gathering and the execution of certain tasks based on conditions met — thereby removing repeatable manual effort. Hence, organizations should always put orchestration before automation.

Security automation cannot be achieved through a project-based approach. Instead, security automation builds upon itself with the implementation of learnings from the previous iteration of threat detection, incident response and recovery.

The following recommendations will help drive successful security orchestration and automation:

- Create repeatable security workflows and document them. Organizations that rely heavily on manual processes often become dependent on "security heroes;" without them, security investigations and incident response are often chaotic and not repeatable. Standardization and documentation through the creation of consistent workflows are the first steps toward achieving security automation.
- Employ frameworks such as the Adversarial Tactics, Techniques and Common Knowledge (ATT&CK) framework to facilitate continuous asset monitoring and threat detection. These frameworks serve as a unifying taxonomy for different groups such as incident response teams, SOC analysts, threat hunters, IT teams and more.
- Automate processes to achieve the speed and agility needed in complex environments. Information and insights should be shared across the entire environment to make security truly scalable.
- Measuring is essential, as it allows for the creation of evidence-based learning processes. Measuring also helps transfer findings back to the learning processes, thereby transforming them and enabling the changes to be seen in action.

Organizations that lack the tools or expertise to effectively orchestrate their security ecosystem could invest in solutions, such as XDR, that offer out-of-the-box integration with popular security technologies or come pre-integrated with a security stack from the same vendor. Of course, organizations should evaluate the risk of vendor lock-in when investing in such technologies.

II. Operationalize Zero Trust

For many Canadian organizations, their zero trust strategy may fall short of delivering the security outcomes they expected at the outset of their zero trust journey. The problem lies with the excessive hype around the term itself, with almost every security vendor borrowing from the concept to brand its solution as a "zero trust enabler."

Zero trust requires a mindset change that can only be propelled across the entire organization when all stakeholders — executive leadership, IT teams and users — acknowledge that cyberthreats exist both inside and outside their IT environment and that users, devices and network components cannot be trusted implicitly based on their location within the network. This mindset change leads to the following assumptions, which are foundational for the zero-trust security model:

- Assume that any access request for IT resources may be malicious. Organizations need to strive toward continuous authorization.
- Assume that all devices and infrastructure inside the perimeter can be compromised. Thus, organizations should limit the blast radius with least-privilege access.

The following are recommendations and considerations for operationalizing zero trust within your organization:

- Define strategic goals and early wins. IT landscapes are no longer static, and any security architecture modernization should include long-term IT initiatives such as hybrid workplace, cloud services, e-commerce, IoT adoption, bring your own device (BYOD), etc. Since zero trust requires long-term leadership commitment, plan for early wins to maintain momentum. Early wins could include such things as improvements in compliance manager scores, a reduction in the number of security incidents, improvements in visibility and monitoring, and more.
- Find your own path to zero trust. Zero trust is not a collection of tools; rather, it is a set of principles for security and systems management. There is no defined path that works well for all organizations, as it will differ depending on each organization's unique landscape. Some organizations may start with segmenting their networks, some with microsegmentation in the data centre, and others with identity and access management.
- Remember, zero trust is only as good as its underlying security policies. Organizations should identify critical DAAS and all of the network paths that access them. Create and enforce security policies to secure them consistently across the IT environment (LAN, WAN, endpoints, mobile, cloud, etc.).
- Zero trust enables intelligence and telemetry-based threat detection. An important advantage of zero trust is that highly granular data — including authentication data, telemetry from endpoints and network, batch data from applications and more — is available for monitoring and threat detection. Enable security analytics that can consume and correlate all of this data for high-fidelity threat detection and prioritization for response.

When properly implemented, security architectures based on the principles of zero trust should be able to prevent, detect and contain security incidents effectively.

III. Incorporate Security Considerations in Your Cloud Migration Strategy

Cloud has steadily become the focal point of all IT innovation, and organizations that are lagging behind in their cloud transformation journey are putting speed of innovation, and thus competitive advantage, at risk.

However, the global pandemic pushed organizations to adopt cloud services with an often-hurried "lift and shift" of data, applications and networks, without having comprehensively assessed their unique privacy and security requirements. The mindset of "adopt first, secure later" that was prevalent during this time has proven to be very costly for many Canadian organizations that have since experienced cyberattacks on their cloud environments and a negative impact on their business operations and customer trust.

Security needs to be baked into cloud workload migration, and Canadian organizations should consider following the guidance to migrate to cloud securely:

- Identify and classify the types of data that will be stored in or used by cloud applications based on their sensitivity and governance requirements, as it could be subject to regulations such as the Payment Card Industry Data Security Standard (PCI DSS), HIPAA, etc. Complex third-party business requirements that access sensitive data through APIs further increase the risk of downstream policy violations. Security solutions such as cloud access security brokers (CASB) enable the enforcement of data security policies, prevent data loss and monitor for governance.
- Understand the shared responsibility model, as it could vary by cloud service provider (CSP). And define governance controls, the means to achieve full-scale visibility for monitoring and the requirement for threat detection and response capabilities before migration.
- Identify cloud APIs to extend data protection. For cloud services such as email or data storage, leverage the provider's APIs to extend existing data protection measures to those platforms for better access control and logging.
- Identify specialized tools for cloud security. The cloud is constantly changing, as cloud instances, containers and other units have life spans of mere seconds. In such environments, tools such as cloud security posture management (CSPM) make a significant difference in identifying configuration deviations from best practices/policy and in auto-remediation. Similarly, use cases for a CASB go beyond compliance and data security: It adds an additional layer for threat protection and can detect malware and other advanced threats, provide visibility into cloud application usage and support behavioural analytics.
- Secure cloud applications. In addition to endpoints and networks, cloud security relies heavily on application security. Security may be ignored for functionality during cloud application development. Make sure that cloud applications are tested for common vulnerabilities, or review the results of DAST and penetration testing of third-party cloud applications.
- Define policies and controls for acceptable cloud usage. Before migration, define policies for access control and authentication, end-to-end encryption, change management and security monitoring.
- Plan ongoing employee security awareness trainings for improved cloud security hygiene. Endpoints, applications and network connections are only as secure as the users operating them. Regular security awareness trainings are essential for cloud users to understand the risks of poor cloud security hygiene as well as best practices for securely using cloud services and data.

IV. Distribute Security Decisions at Speed and Scale with DevSecOps

DevSecOps, in theory, is a means to securing the software supply chain. It is built on the idea that security is everybody's responsibility; hence, to achieve the goal of secured application development, security decisions must be distributed across security, development and operations teams at speed and at scale — and automated wherever possible.

In a world of cyberthreats, security and development teams can no longer afford to work in silos. All stakeholders across the organization should actively work together to minimize software supply chain threats. Much like DevOps, there is an important cultural aspect to DevSecOps and software supply chain security that involves further breaking down silos so that development, operations and security teams can work together toward releasing software faster and more securely.

Recommendations include the following:

- Security and development teams should collaborate to identify software supply chain security gaps. All security weaknesses will need protection, but recognize that this will be an iterative process. Prioritize the next steps using an agile "weighted smallest job first" (WSJF) approach, considering the risk of delaying easy fixes while addressing harder problems.
- Leverage automation to prevent the loss of application development velocity. DevSecOps automation helps administer security controls throughout the development process without the need for manual intervention. Other areas that could benefit from automation due to enhanced visibility across the software supply chain are auditing and compliance reporting.
- Empower developers to remediate vulnerabilities. Self-service tools to remediate vulnerabilities without interacting with IT security teams significantly improve the speed of development and are key for cross-team skills development.

CAVEATS

There are inherent limitations to survey research that need to be carefully considered before drawing inferences from findings. The following items are specific limitations that are germane to most web-based surveys.

Nonresponse bias: The current findings are based on a sample of survey returns. We sent surveys to a representative sample of individuals, resulting in a large number of usable returned responses. Despite nonresponse tests, it is always possible that individuals who did not participate are substantially different in terms of underlying beliefs from those who completed the instrument.

Sampling frame bias: The accuracy is based on contact information and the degree to which the list is representative of individuals who are IT or IT security practitioners located in various organizations in Canada. We also acknowledge that the results may be biased by external events such as media coverage. We also acknowledge bias caused by compensating subjects to complete this research within a specified time period.

Self-reported results: The quality of the survey research is based on the integrity of the confidential responses received from the subjects. While certain checks and balances can be incorporated into the survey process, there is always a possibility that a subject did not provide accurate responses.

APPENDIX A: DETAILED SURVEY RESULTS

Demographics

A sampling frame of 1,689 Canadian IT security and risk & compliance professionals were selected to receive invitations to participate in this survey. All survey participants were screened for direct involvement in improving or managing their organization's IT security. The following table shows the returns, including the removal of certain participants based on screening and reliability checks. Our final sample consisted of 553 surveys, or a 32.7 percent response rate.

The survey firmographics and demographics are as follows:

Which of the following industry categories best represents the principal business activity of your organization?

	Total
Business/professional services (e.g., legal, accounting, engineering, architecture, etc.)	4.0%
Personal/consumer services (e.g., travel, beauty, personal training, dry cleaning, etc.)	3.6%
Construction	3.8%
Hospitality	3.4%
IT industry	6.3%
Not for profit	0.0%
Manufacturing	7.6%
Crown corporation or other publicly funded organization	0.0%
Education, K–12	2.4%
Education, college/university	6.7%
Financial services	9.4%
Government	9.6%
Healthcare	9.6%
Primary (e.g., agriculture, mining, forestry, etc.)	1.4%
Oil & gas or field services–related	3.8%
Retail	7.8%
Communications (e.g., cable and telecommunications services, etc.)	2.9%
Media (e.g., radio/TV broadcasting)	3.1%
Printing, publishing, etc.	2.7%
Transportation and warehousing	3.4%
Utilities	5.2%
Wholesale and distribution	3.3%

At your organization, do you play a role in or are you part of the following functions?

	Total
Directing the IT function	51.7%
Improving/managing IT security	100.0%
Setting IT priorities	53.7%
Managing IT budgets	38.0%

Is your company headquartered in Canada — and if so, which of the following areas is it headquartered in?

	Total
Western and Central Canada (BC, AB, SK, MB)	18.1%
Ontario	32.7%
Quebec	25.5%
Atlantic Canada (NB, NS, NFLD, PEI)	14.6%
North (Yukon/Northwest Territories/Nunavut)	9.0%

Which of the following best describes the department you work for?

	Total
C-level executive management, excluding IT	9.6%
C-level IT, including CIO/CTO/CSO/CISO	9.2%
IT/IS/MIS/data centre/IT security	68.0%
Legal/compliance/risk	13.2%

How many full-time employees does your organization have located within Canada?

	Total
15–24	5.6%
25–99	6.9%
100–249	10.8%
250–499	22.2%
500–999	14.3%
1000–4999	14.5%
5000 or more	25.7%

Which of the following ranges would your organization's annual revenue (or budget for government) fall under?

	Total
Less than $10 million	6.7%
$10 million–$25 million	9.8%
$26 million–$99 million	15.4%
$100 million–$499 million	26.6%
$500 million–$999 million	26.4%
$1 billion or more	15.2%

APPENDIX B: DEFINITIONS

Analytics: Using statistical analysis to discover and interpret patterns in data.

Application programming interface (API): Code that enables two software programs to communicate.

Artificial intelligence (AI): Mimicking the natural intelligence of humans using machine learning and statistical models.

Continuous delivery (CD): Automates the deployment of all source code changes to a testing or production environment after the build stage.

Continuous integration (CI): The practice of automating the integration of code changes from multiple developers into a single repository.

Denial of service (DoS): An attack in which multiple compromised systems are used to attack a single target. The flood of incoming messages to the target system forces it to shut down and denies service to legitimate users.

DevOps: Combines software development (Dev) and IT operations (Ops) to shorten the development lifecycle with continuous delivery and integration.

DevSecOps: Augmentation of DevOps; aims to automate integration of security at every phase of software development.

Endpoint detection and response (EDR): A type of cybersecurity control that continually monitors endpoints and has capabilities to respond to cyberevents and threats. EDR has two components: clients, which are installed on endpoints, and a centralized management console, which is usually used by security analysts.

Exfiltration: The unauthorized removal of data or files from a system by an attacker.

Identity and access management (IAM): A framework of security policies and technologies to ensure that the right users have access to an organization's IT resources.

Infiltration: Unauthorized access to any computer network or system resource, in which attackers gain access to an organization's network, infrastructure and/or data but no data is exfiltrated.

Microservices: Application architecture that structures an application as a collection of loosely coupled, fine-grained services communicating through lightweight protocols.

Multifactor authentication (MFA): Authentication using two or more different factors to achieve authentication. Factors include something you know (e.g., password/PIN), something you have (e.g., cryptographic identification device, token) or something you are (i.e., biometric authentication).

Personally identifiable information (PII): Information that, when used alone or with other relevant data, can identify an individual.

Security information and event management (SIEM): Network monitoring controls that may also provide log management capabilities. SIEM allows organizations to detect malicious activity on their networks.

Security orchestration, automation and response (SOAR): A group of security controls, usually managed using a single pane of glass, that aids analysts in responding to security threats. Depending on the implementation, a significant amount of artificial intelligence may be built into the solution, allowing low-level alerts and events to be responded to automatically without human intervention.

Shared responsibility model: A cloud security framework that dictates the security responsibilities of a cloud service provider (CSP) and its users to ensure accountability. How a CSP's versus a user organization's responsibilities are defined varies among CSPs and the services being provided (SaaS, PaaS, IaaS), so it is imperative that user organizations clearly understand what security responsibilities their CSP will take ownership of versus which responsibilities the organization will retain.

Single sign-on (SSO): An authentication scheme that allows a user to log in with a single ID and password to any of several related yet independent software systems. True single sign-on allows the user to log in once and access services without re-entering authentication factors.

Software as a Service (SaaS): A cloud-based software solution in which software providers deliver applications to users over the internet.

Static application security testing (SAST): Scans the source files of an application to identify security flaws in the code.

Telemetry: The automatic process of collecting data remotely that is created by systems through the use of agents and protocols — for example, network telemetry, endpoint telemetry, application telemetry, etc.

Threat intelligence: Threat information that has been aggregated, transformed, analyzed, interpreted or enriched to provide the necessary context for decision-making processes.

Virtual machine (VM): A virtual environment that functions as a virtual computer system with its own CPU, memory, network interface and storage, created on a physical hardware system (located off- or on-premises).

Extended detection and response (XDR): A consolidation of tools and data that provides extended visibility, analysis and response across endpoints, workloads, users and networks.

Zero-trust architecture: Unlike traditional perimeter security architectures, which trust all individuals and applications inside the perimeter, zero-trust architectures trust no one on either side. Identity and access management is a critical component of zero-trust architectures.

ABOUT CDW

CDW Canada is a leading provider of technology solutions for business, government, education and healthcare. CDW Canada helps customers achieve their goals by delivering integrated technology solutions and services that help customers navigate an increasingly complex IT market and maximize the return on their technology investment. Areas of focus include software, networking, unified communications, data centre and mobility solutions. CDW Canada is on the Channel Daily News Top 100 Solutions Provider list in Canada, and is a wholly owned subsidiary of Vernon Hills, Illinois–based CDW Corporation, a Fortune 500 company. For more information, visit www.CDW.ca.

ABOUT IDC CANADA

International Data Corporation (IDC) is the premier global provider of market intelligence, advisory services and events for the information technology, telecommunications and consumer technology markets. IDC Canada is part of a network of over 1100 analysts providing global, regional and local expertise on technology, industry opportunities and trends with more analysts dedicated to understanding the Canadian market than any other global research firm.

CDW PEOPLE WHO GET IT™

IDC

Research independently conducted by IDC Canada | Published June 2023