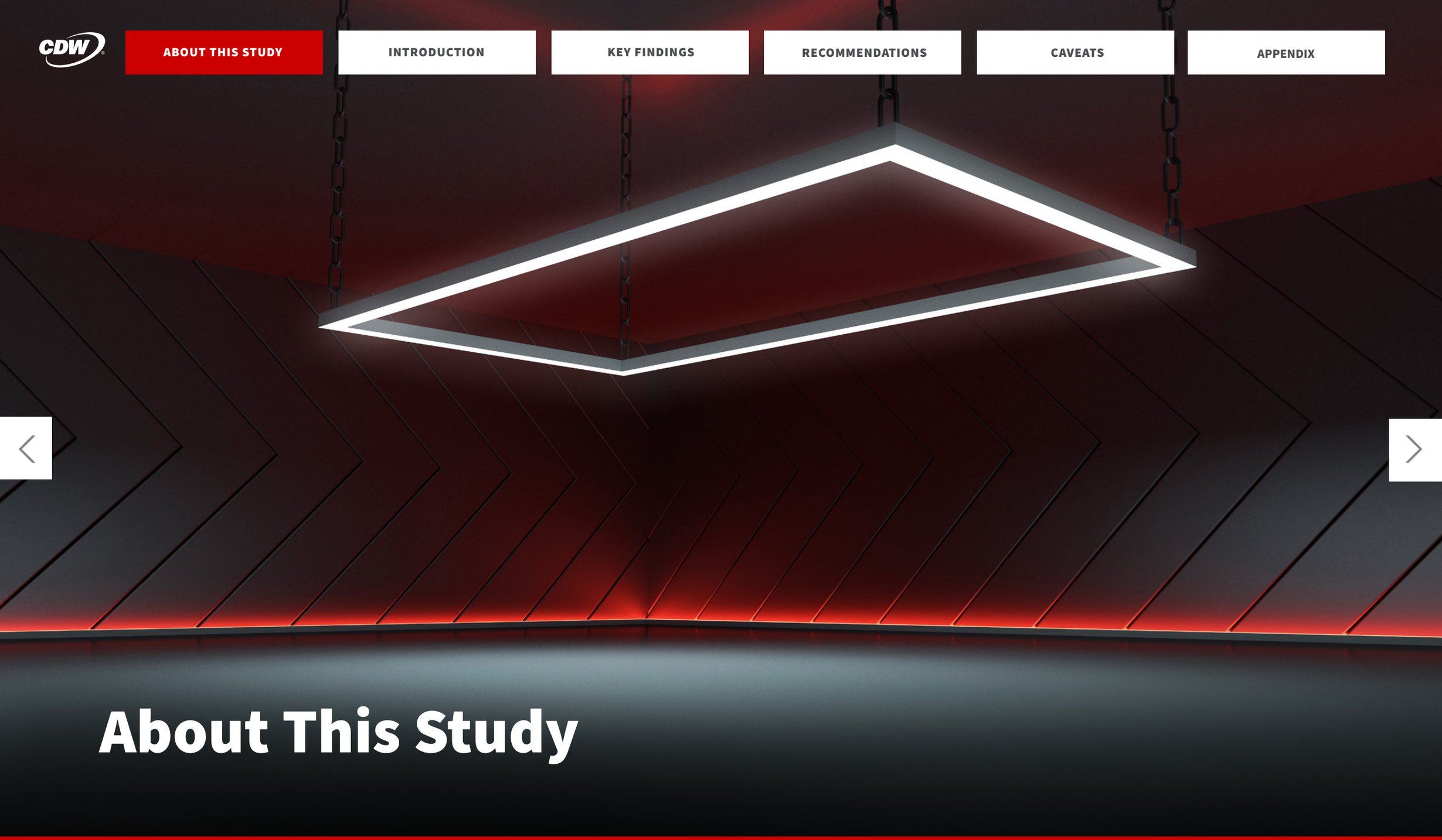
# Cybersecurity in Focus 2024:

## Trends, Threats and Strategies

# Table of Contents



# About This Study

## About This Study

This report presents the findings of the 2024 CDW Canadian Cybersecurity Study. The data provided in this report was obtained through a Canada-wide, cross-province and cross-industry survey, independently conducted by IDC Canada, of 706 IT security, risk and compliance professionals. All survey participants were screened for direct involvement in managing their organization's IT security. 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 November–December 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 small, medium and enterprise organizations. The definition for each is based on its number of employees:

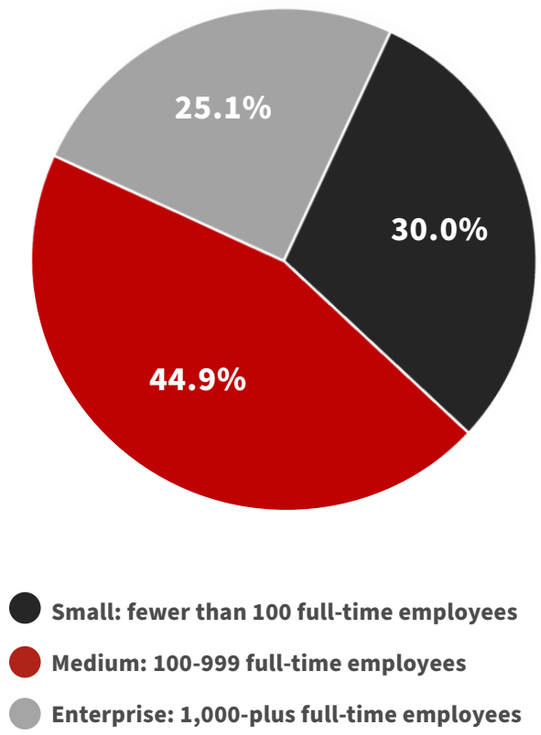
**Small: fewer than 100 full-time employees located within Canada**

**Medium: 100-999 full-time employees located within Canada**

**Enterprise: 1,000-plus full-time employees located within Canada**

**Chart 1:**

### Employee Size Segmentation




Source: CDW Security Survey 2024 (n = 706)

## Introduction

Cyberattacks are becoming increasingly sophisticated, effective and destructive. As Canadian business and IT leaders seek to protect their data and ensure business continuity, cybersecurity continues to be a top priority. Canadian organizations that adopt AI and machine learning technologies as part of a comprehensive cybersecurity strategy are better equipped to detect and respond to cyberattacks while addressing talent shortages and budget constraints.

## An Evolving Threat Landscape

### Attack Surfaces

The attack surface of Canadian organizations is vast and encompasses SaaS applications, APIs, containers, VMs, storage systems, database appliances, network appliances, endpoints and more. However, the study specifically analyzed the growth in user endpoints (PCs, laptops, smartphones and tablets), servers and IoT devices to demonstrate organizations' expanding IT attack surface.

**Table 1: Average Number of IT Devices**

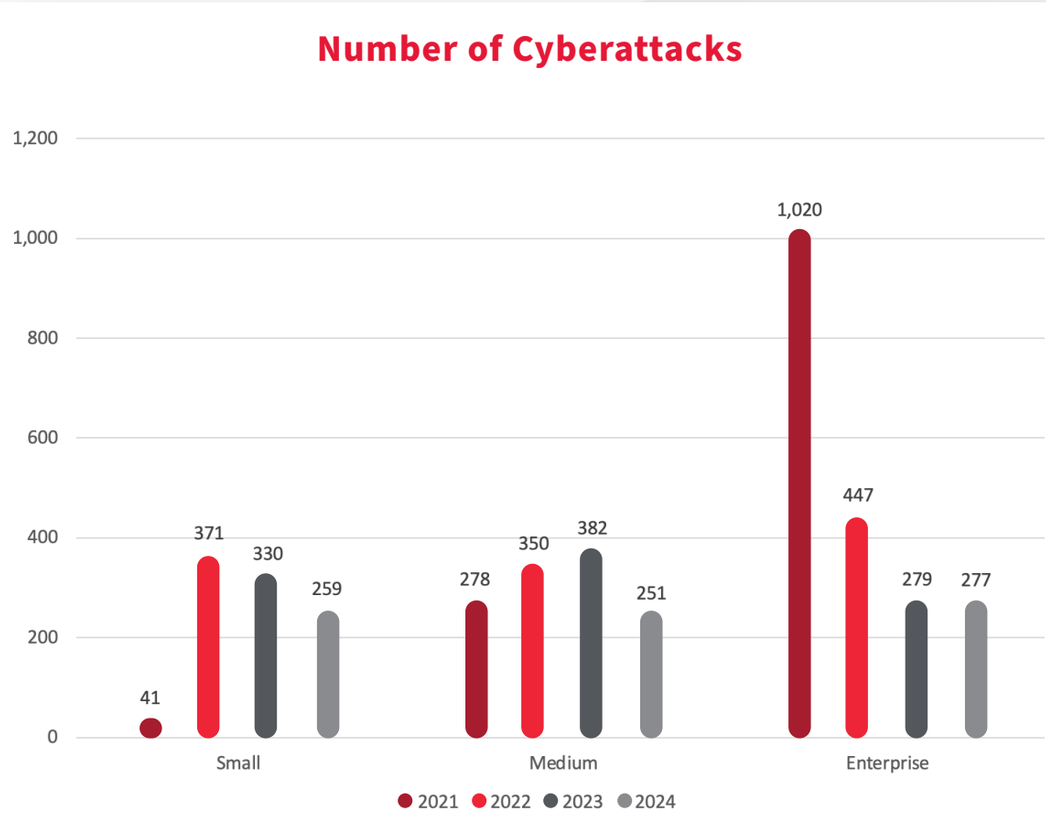
| | Size | 2021 | 2022 | 2023 | 2024 |
|---|---|---|---|---|---|
| Client Computing [PCs / laptops / smartphones / tablets] | Small | 108 | 231 | 822 | 48 |
| | Medium | 1,025 | 1,540 | 2,532 | 579 |
| | Enterprise | 5,095 | 5,936 | 6,817 | 5,978 |
| Servers | Small | 3 | 5 | 263 | 20 |
| | Medium | 21 | 103 | 302 | 137 |
| | Enterprise | 122 | 585 | 1,043 | 718 |
| IoT devices | Small | 10 | 17 | 263 | 205 |
| | Medium | 87 | 195 | 590 | 523 |
| | Enterprise | 249 | 1,774 | 1,804 | 1,159 |

Source: CDW Security Survey 2024 (n = 706), 2023 (n = 553), 2022 (n = 555), 2021 (n = 557)

## Infection Rates Rising

The number of cyberattacks saw a sharp decline for small and medium organizations compared with the 2023 study, while enterprises remained the same; however, the number of incidents remained flat.

**Chart 2:**




Source: CDW Security Survey 2024 (n = 706), 2023 (n = 553), 2022 (n = 555), 2021 (n = 557)

**Table 2: Number of Incidents**

| Denial of Service | | | | |
|---|---|---|---|---|
| Size | 2021 | 2022 | 2023 | 2024 |
| Small | 6 | 31 | 32 | 26 |
| Medium | 14 | 28 | 31 | 27 |
| Enterprise | 82 | 29 | 30 | 25 |

| Infiltration | | | | |
|---|---|---|---|---|
| Size | 2021 | 2022 | 2023 | 2024 |
| Small | 6 | 20 | 29 | 24 |
| Medium | 19 | 31 | 28 | 25 |
| Enterprise | 52 | 25 | 29 | 25 |

| Breach | | | | |
|---|---|---|---|---|
| Size | 2021 | 2022 | 2023 | 2024 |
| Small | 6 | 26 | 30 | 27 |
| Medium | 18 | 22 | 29 | 28 |
| Enterprise | 55 | 25 | 30 | 27 |

| Cloud Incident | | |
|---|---|---|
| Size | 2023 | 2024 |
| Small | 23 | 24 |
| Medium | 28 | 24 |
| Enterprise | 28 | 25 |

Source: CDW Security Survey 2024 (n = 706), 2023 (n = 553), 2022 (n = 555), 2021 (n = 557)

It is also worth noting that the attack rate increased in both the 2023 and 2024 studies, with a growing number of Canadian organizations indicating that they suffered security incidents in the last 12 months.

The number of cyberattacks trending down, while the number of incidents remained flat, indicates that cyberattacks had a significantly better "hit rate" (number of attacks that become an incident) than in previous years. In 2023, 7 to 8 percent of all cyberattacks became cyberincidents. In the 2024 study, this increased to 9 to 10 percent across industries.

Specifically, a sharp rise in denial of service (DoS) attack rate was reported for smaller organizations, from 34 to 46 percent.

**Table 3: Attack Rate**

| Denial of Service | | | | |
|---|---|---|---|---|
| Size | 2021 | 2022 | 2023 | 2024 |
| Small | 45% | 35% | 34% | 46% |
| Medium | 39% | 33% | 38% | 41% |
| Enterprise | 33% | 41% | 42% | 37% |

| Infiltration | | | | |
|---|---|---|---|---|
| Size | 2021 | 2022 | 2023 | 2024 |
| Small | 40% | 49% | 46% | 49% |
| Medium | 47% | 42% | 48% | 52% |
| Enterprise | 43% | 37% | 53% | 49% |

| Breach | | | | |
|---|---|---|---|---|
| Size | 2021 | 2022 | 2023 | 2024 |
| Small | 40% | 49% | 62% | 62% |
| Medium | 47% | 42% | 60% | 68% |
| Enterprise | 43% | 37% | 66% | 65% |

| Cloud Incident | | |
|---|---|---|
| Size | 2023 | 2024 |
| Small | 37% | 47% |
| Medium | 43% | 48% |
| Enterprise | 41% | 43% |

| Web Defacement | |
|---|---|
| Size | 2024 |
| Small | 25% |
| Medium | 24% |
| Enterprise | 21% |

Source: CDW Security Survey 2024 (n = 706), 2023 (n = 553), 2022 (n = 555), 2021 (n = 557)

## Smaller Organizations Experience More Downtime

Cyberincidents disrupt business operations and put sensitive data at risk – which affects both business reputation and the bottom line. Although downtime remained about the same overall in 2024 compared with the 2023 study, downtime related to breaches and cloud rose by one to three days in the 2024 study, depending on the business size. Canadian firms of all sizes reported total downtime of two weeks or more across most categories of attack.

Most notably, smaller organizations reported a sharp increase in downtime due to DoS attacks at 18 days, compared with 12 days in the 2023 study. Healthcare and government reported more downtime than other industries related to DoS attacks.

**Table 4: Downtime (Business Days)**

| Denial of Service | | | | |
|---|---|---|---|---|
| Size | 2021 | 2022 | 2023 | 2024 |
| Small | 4 | 16 | 12 | 18 |
| Medium | 6 | 14 | 17 | 18 |
| Enterprise | 41 | 13 | 16 | 16 |

| Infiltration | | | | |
|---|---|---|---|---|
| Size | 2021 | 2022 | 2023 | 2024 |
| Small | 3 | 11 | 18 | 14 |
| Medium | 11 | 19 | 17 | 15 |
| Enterprise | 30 | 19 | 16 | 15 |

| Breach | | | | |
|---|---|---|---|---|
| Size | 2021 | 2022 | 2023 | 2024 |
| Small | 3 | 13 | 14 | 16 |
| Medium | 7 | 11 | 15 | 15 |
| Enterprise | 18 | 12 | 15 | 14 |

| Cloud Incident | | |
|---|---|---|
| Size | 2023 | 2024 |
| Small | 9 | 12 |
| Medium | 10 | 13 |
| Enterprise | 11 | 13 |

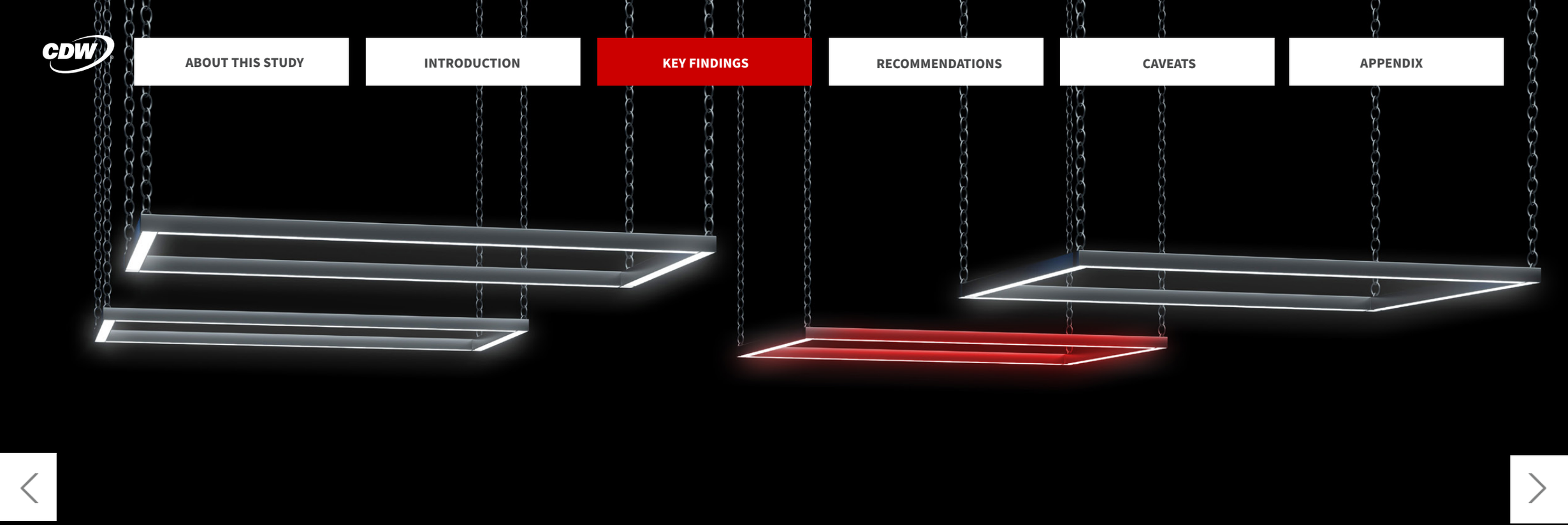
Source: CDW Security Survey 2024 (n = 706), 2023 (n = 553), 2022 (n = 555), 2021 (n = 557)

Compared with the 2023 study, average downtime per incident in 2024 has increased across industries and business sizes. For example, financial services experienced significantly more downtime per infiltration and cloud incident.

**Table 5: Downtime/Attack Ratio**

| Downtime/Attack Ratio | | Total | Financial Services | Energy | Public Sector | Education | Healthcare | Other | Small | Medium | Enterprise |
|---|---|---|---|---|---|---|---|---|---|---|---|
| 2023 | Denial of Service | 0.51 | 0.68 | 0.55 | 0.61 | 0.30 | 0.42 | 0.50 | 0.40 | 0.54 | 0.52 |
| | Infiltration | 0.60 | 0.75 | 0.58 | 0.73 | 0.48 | 0.56 | 0.58 | 0.66 | 0.60 | 0.56 |
| | Breach | 0.50 | 0.57 | 0.55 | 0.47 | 0.49 | 0.40 | 0.51 | 0.48 | 0.51 | 0.50 |
| | Security Incident in Cloud | 0.39 | 0.43 | 0.24 | 0.54 | 0.33 | 0.34 | 0.42 | 0.38 | 0.38 | 0.41 |
| 2024 | Denial of Service | 0.66 | 0.63 | 0.63 | 0.65 | 0.62 | 0.65 | 0.70 | 0.70 | 0.65 | 0.64 |
| | Infiltration | 0.60 | 0.54 | 0.61 | 0.63 | 0.62 | 0.61 | 0.58 | 0.58 | 0.60 | 0.61 |
| | Breach | 0.55 | 0.52 | 0.56 | 0.53 | 0.53 | 0.62 | 0.54 | 0.58 | 0.55 | 0.51 |
| | Security Incident in Cloud | 0.62 | 0.52 | 0.61 | 0.54 | 0.49 | 0.54 | 0.51 | 0.52 | 0.54 | 0.52 |

Source: CDW Security Survey 2024 (n = 706), 2023 (n = 553)



# Key Findings

# Finding 1:

## Canadian organizations are prioritizing security amidst declining IT budgets – accelerating a shift toward enhanced security maturity.

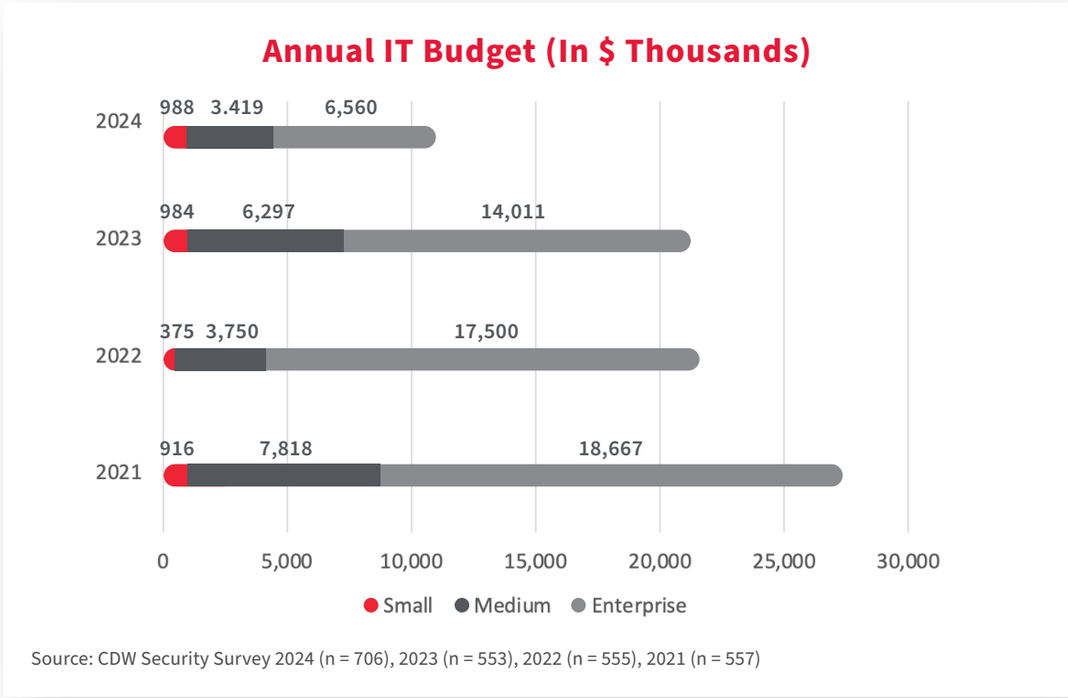
Amidst declining IT budgets, the security budget as a percentage of the overall IT budget has increased across industries and organization size, indicating a keen awareness that cyberthreats must be combated to reduce the potential impact on the business. Adopting security frameworks can be a helpful starting point toward improving an organization's overall security posture and maturity, by creating an environment that prioritizes the safeguarding of business assets against potential cyberimpacts.

## Security Spending Remains a Priority Amidst IT Cost-Cutting

### Accelerated Shift Toward Cost-Cutting

In the current climate of economic uncertainty, it is not surprising that Canadian firms are implementing cost-cutting measures and shifting toward more cost-effective technologies. Considering the anticipated recession and financial instability in 2024 and beyond, organizations have had to re-evaluate their spending priorities. As a result, IT budgets across Canada have declined when compared with the 2023 study.

**Chart 3:**




Source: CDW Security Survey 2024 (n = 706), 2023 (n = 553), 2022 (n = 555), 2021 (n = 557)

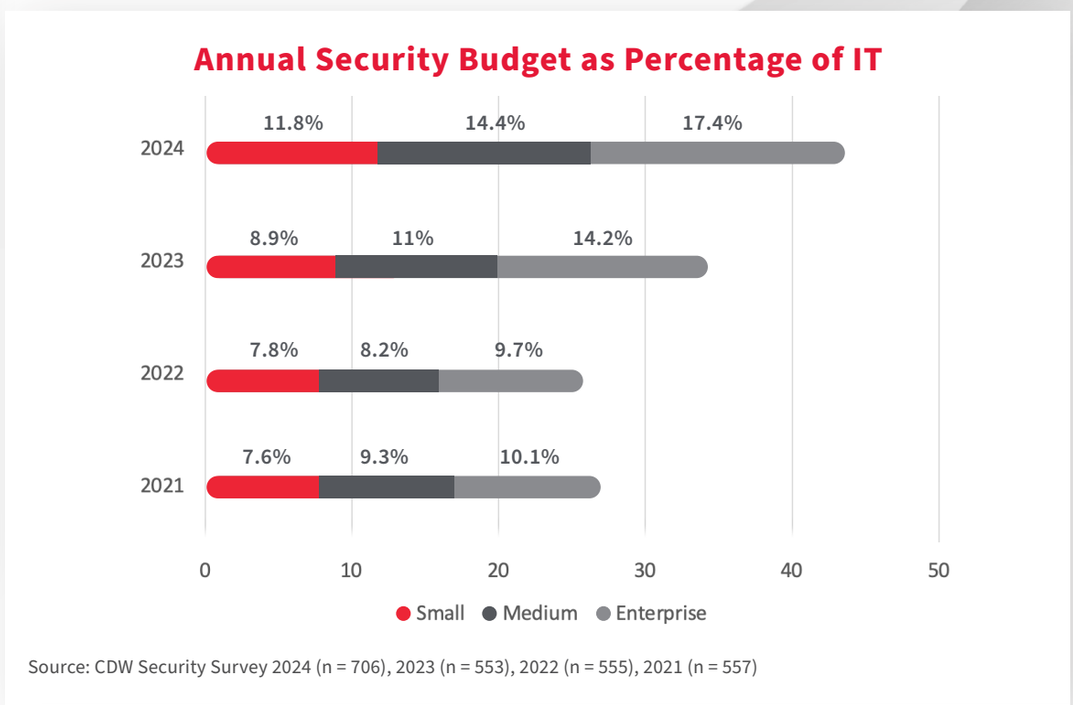
The study showed that IT budgets have declined significantly in medium and enterprise organizations but have seen a slight increase in small organizations. Overall, across Canada, IT budgets have declined in absolute terms by more than 50 percent and have also decreased as a proportion of revenue (or budget for government organizations).

## Security Spending Prioritized

The current environment of tightened budgets and increased cyberthreats makes it critical for organizations to have robust security measures in place to protect against current threats as well as proactively prepare for future risks by ensuring the resilience of the organization.

Despite budget constraints across the board, organizations continue to prioritize cybersecurity investments. According to the study, security budgets as a proportion of IT budgets have increased year over year for organizations of all sizes and across industries.

**Chart 4:**




Source: CDW Security Survey 2024 (n = 706), 2023 (n = 553), 2022 (n = 555), 2021 (n = 557)

## The Risks of Underfunded Security

While trying to do "more with less" can result in initial cost savings, it presents its own set of challenges. One major risk is the potential for increased exposure to cyberattack due to underfunded security measures. Although security spending as a percentage of the IT budget has increased, overall security budgets are down in absolute dollars. With less money available to spend on security, organizations may not be able to keep abreast of the latest threats and technologies, making them vulnerable to attacks.

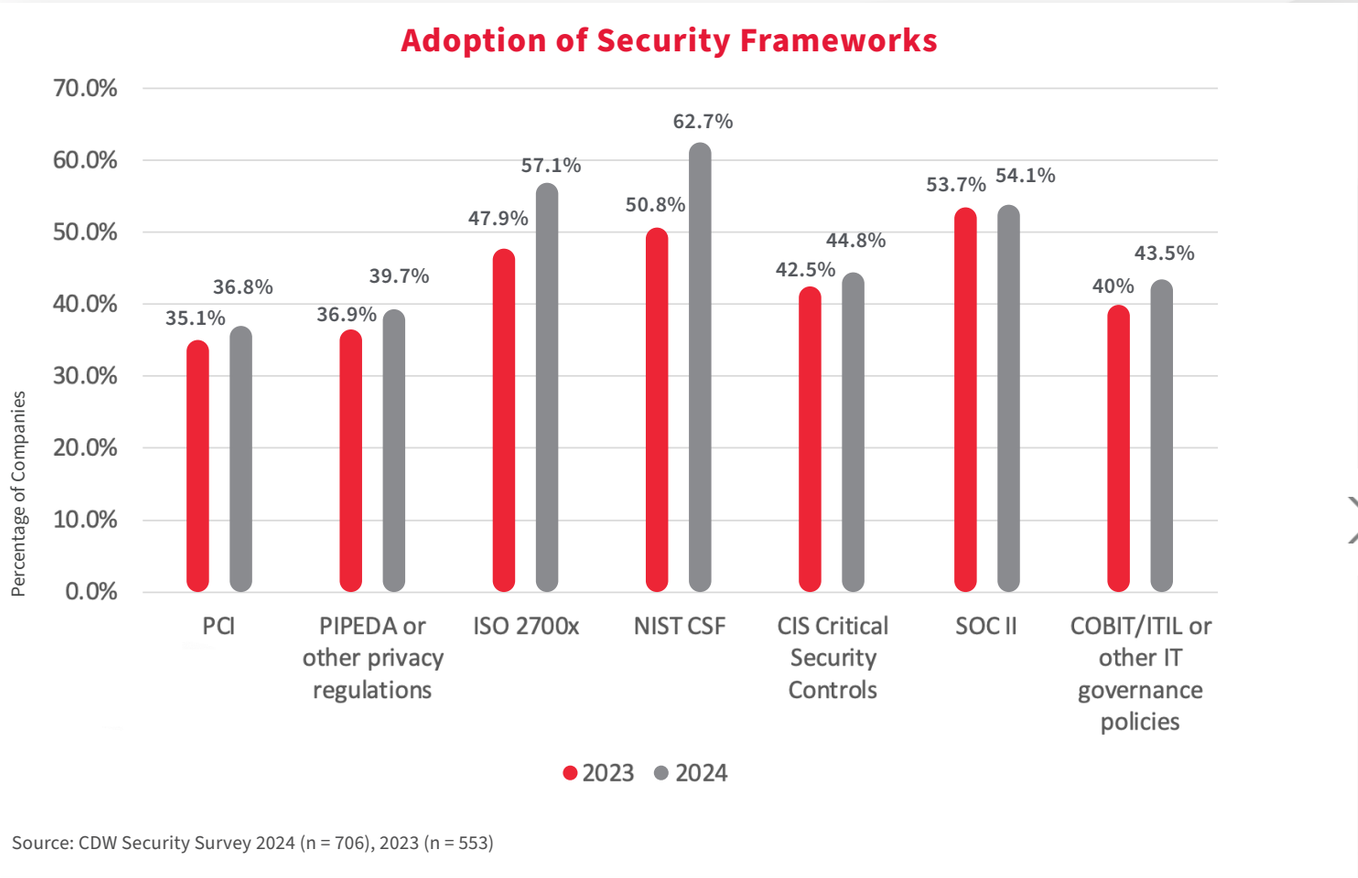
Furthermore, as depleted IT security team members contend with the continuous cycle of breach detection, response and recovery, they can experience physical and mental exhaustion, stress and decreased morale. Known as "breach fatigue," this can reduce the overall effectiveness of the security team by desensitizing them to the severity of breaches, which can lead to complacency and a lack of urgency when dealing with security incidents.

## Security Frameworks Are a Necessity

Adopting security frameworks such as NIST CSF, SOC 2 Type 2 and ISO2700x can be a helpful starting point to improve the security maturity of an organization. These frameworks provide a structured approach to managing cybersecurity risk and help stakeholders understand the cybersecurity program and its effectiveness. They also assist in prioritizing activities for improvement.

The study showed increased adoption of security frameworks – an important first step toward improving maturity. For example, the adoption of NIST CSF has jumped from 50.8 percent in 2023 to 62.7 percent in the 2024 study. Similarly, the adoption of ISO2700x increased from 47.9 percent in the 2023 study to 57.1 percent in the 2024 study. SOC 2 adoption also increased from 53.7 percent to 54.1 percent in the current study.

**Chart 5:**




Source: CDW Security Survey 2024 (n = 706), 2023 (n = 553)

# Finding 2:

## Canadian organizations focus on threat prevention in zero-trust strategies – but an equal emphasis on detection and response is required.

## Zero-trust access is just one aspect of a comprehensive zero-trust strategy

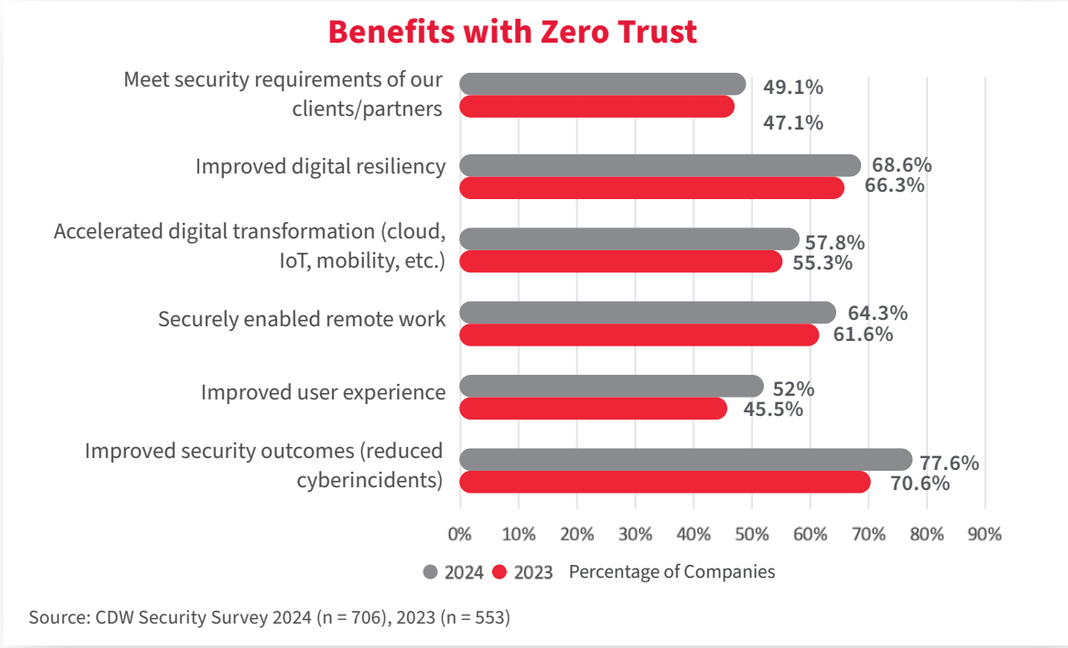
In the cloud era, zero-trust security has rapidly gained traction. However, while zero-trust access (ZTA) is an essential component of zero-trust security, it should not be the sole focus. Threat detection and response are equally important measures to ensure comprehensive security and to meet the long-term objectives of the zero-trust strategy.

**Benefits of Zero Trust**

Zero-trust security is a modern approach to security that is particularly beneficial for organizations that have invested in cloud services to support hybrid work, employee mobility and business innovation.

Based on the principle of "never trust, always verify," zero trust ensures that every user, device and network flow is authenticated and authorized before being allowed to access resources. 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.

**Chart 6:**




Source: CDW Security Survey 2024 (n = 706), 2023 (n = 553)

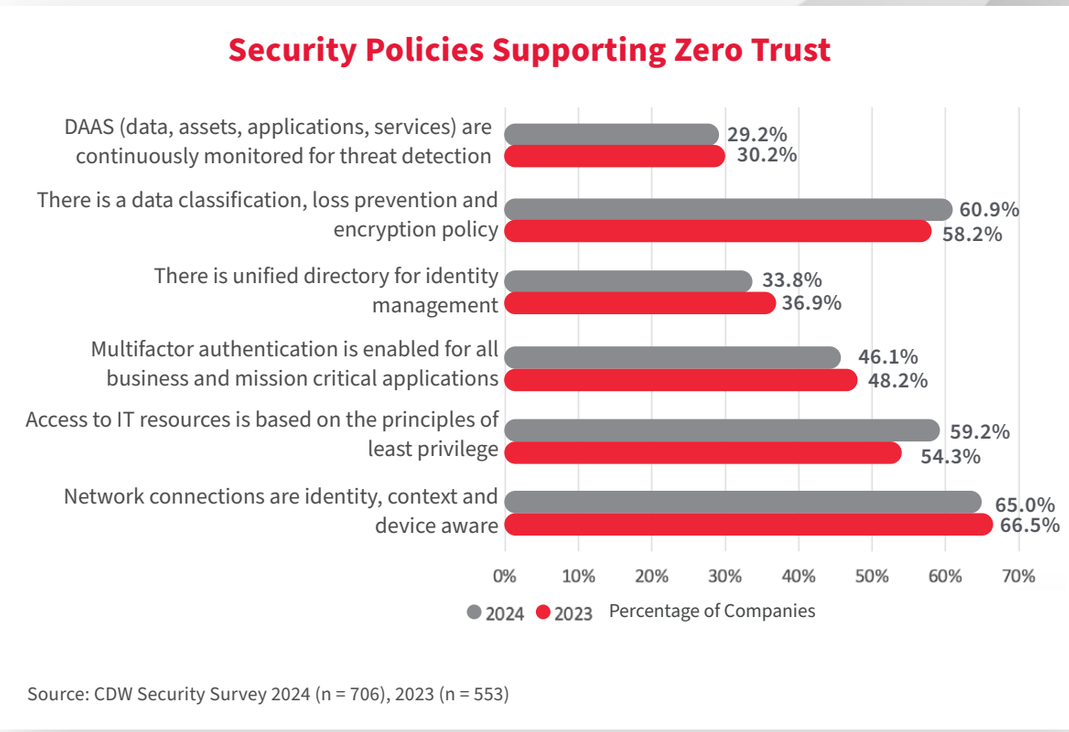
According to the study, organizations are increasingly realizing the benefits of zero trust. Respondents report improvements across every category surveyed – including security outcomes, user experience, remote work, digital transformation and more.

## Policies Supporting Zero Trust

Zero trust reduces the risk of data breaches by ensuring that only authorized users and devices can access sensitive data. It also improves visibility and control over network traffic, enabling organizations to detect and respond to threats more quickly.

However, when we look at incremental adoption of security policies that form the foundation of a zero-trust strategy and the technologies that constitute its operationalization, organizations have a long way to go to realize the second benefit.

**Chart 7:**



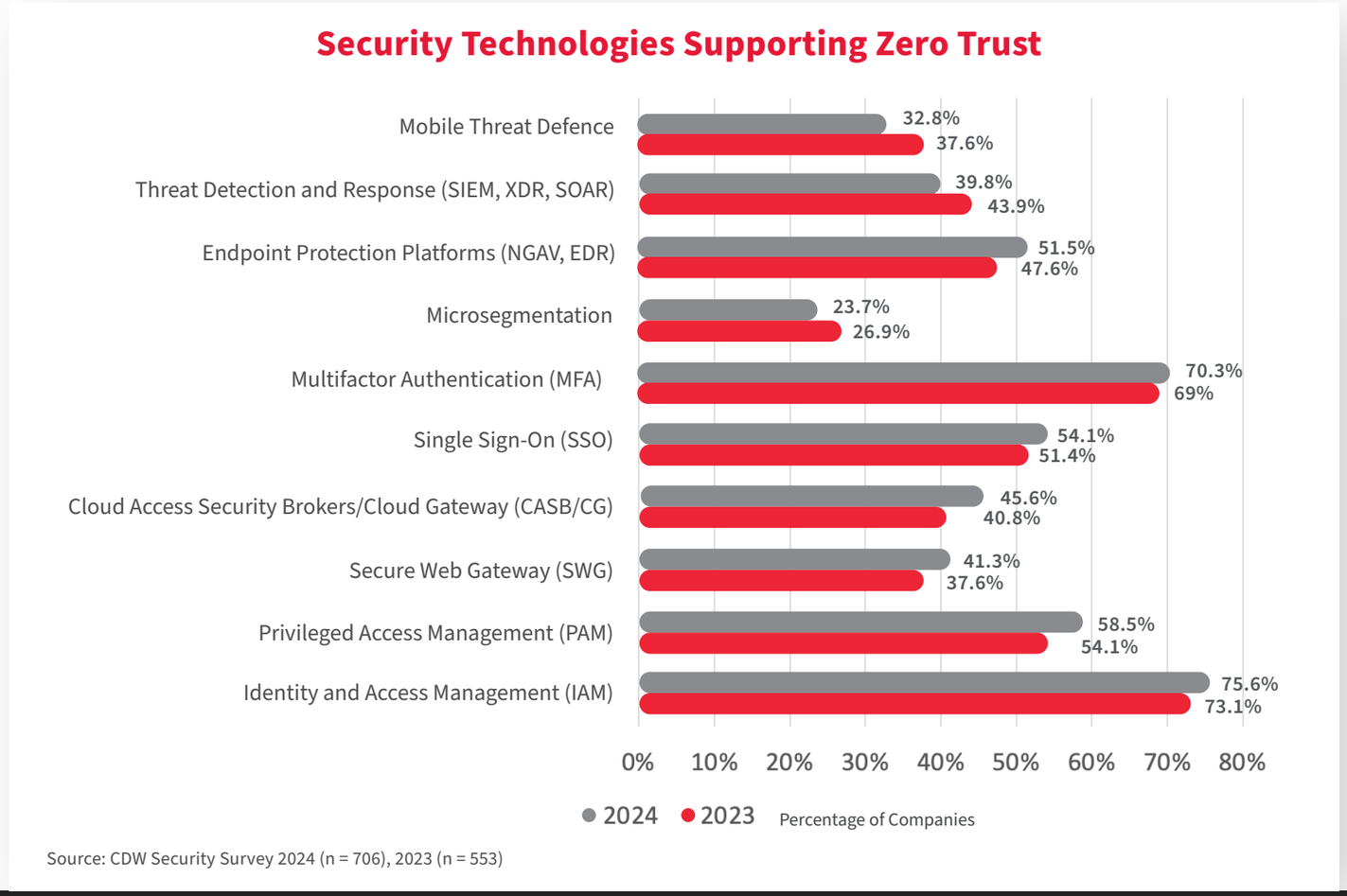

Source: CDW Security Survey 2024 (n = 706), 2023 (n = 553)

Compared with the 2023 study, there is little change to security policies supporting zero trust. Noteworthy is the fact that less than one third of organizations have a policy that mandates security monitoring for threat detection.

**Technologies Supporting Zero Trust**

The study showed that there is steady growth in the adoption of many security technologies supporting zero-trust network access, such as IAM, MFA, SSO, SWG and CASB. However, it is worrisome to note that adoption declined for threat detection and response technologies (SIEM, XDR, SOAR).

**Chart 8:**




Source: CDW Security Survey 2024 (n = 706), 2023 (n = 553)

If organizations focus solely on ZTA for threat prevention, without investing in threat detection and response, they may be missing a crucial part of the equation. ZTA is indeed a powerful set of technologies for preventing unauthorized access, but it doesn't address the full spectrum of potential threats.

For instance, an organization might have robust ZTA in place, but if an insider threat or a sophisticated phishing attack manages to bypass this barrier, the organization remains vulnerable. In such cases, the lack of a robust threat detection and response system can lead to significant damage.

Moreover, a focus on ZTA without threat detection and response can lead to a false sense of security. Organizations might feel they are well protected when, in fact, they are not. This can hinder their ability to achieve the long-term objectives of the zero-trust strategy, which includes maintaining a secure environment, protecting sensitive data and ensuring business continuity.

While ZTA is an essential component of zero-trust security, it should not be the sole focus. Threat detection and response are equally important to ensure comprehensive security and to meet the long-term objectives of the zero-trust strategy.

# Finding 3:

## Concerns about cybersecurity are hampering cloud adoption and emerging as a key barrier to fully realizing the benefits of the cloud.

Canadian organizations view public cloud environments as the most directly impacted component of a cybersecurity incident. Point solutions are not the answer. An effective approach for addressing gaps in security on public cloud must consider the entire cloud ecosystem, ensuring that all aspects of the cloud, from its design to its operation, are secure.

## Effective Cybersecurity Considers Entire Cloud Ecosystem

### The Cloud Is Under Attack

Canadian organizations understand the benefits of moving to public cloud, including the potential to:

1) Reduce IT costs by eliminating the need for expensive hardware and software
2) Enable scalability without investing in additional infrastructure
3) Ensure high availability and business continuity, as cloud services are often more reliable than on-premises solutions
4) Take advantage of enhanced security measures, as cloud providers invest heavily in security infrastructure and practices

Unfortunately, the move to public cloud, which accelerated during the pandemic, has not gone unnoticed by adversaries. Cyberattackers have adapted their tactics, techniques and procedures (TTPs) to target public cloud environments, recognizing the increasing reliance on these platforms for data storage and processing. They exploit the shared responsibility model of public cloud security, where the cloud provider is responsible for the infrastructure security, while the customer is responsible for the security of the data and applications.

### Cyberattacks Have Eroded Confidence in Cloud Security

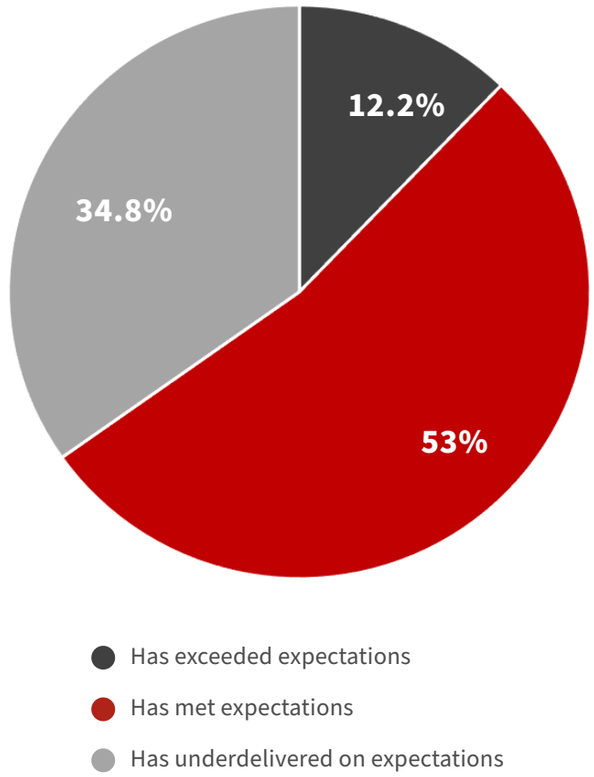
Market researchers have observed a variety of methods that attackers use to target the cloud:

1) By developing sophisticated phishing and social engineering tactics, they trick users into revealing their cloud credentials. This is known as "cloud jacking."
2) They have learned to exploit cloud-specific vulnerabilities, such as misconfigurations, to gain unauthorized access.
3) Ransomware attacks have been adapted to target cloud storage, leveraging the cloud's scalability to inflict maximum damage.
4) They have started to use cloud-based services as a launchpad for attacks, exploiting the cloud's computational power for cryptojacking.

Consequently, one in three Canadian organizations believe themselves short-changed on the security in cloud promise. According to the study, 35 percent of respondents do not feel that migrating their IT workloads to public cloud has met their security expectations.

**Chart 9:**

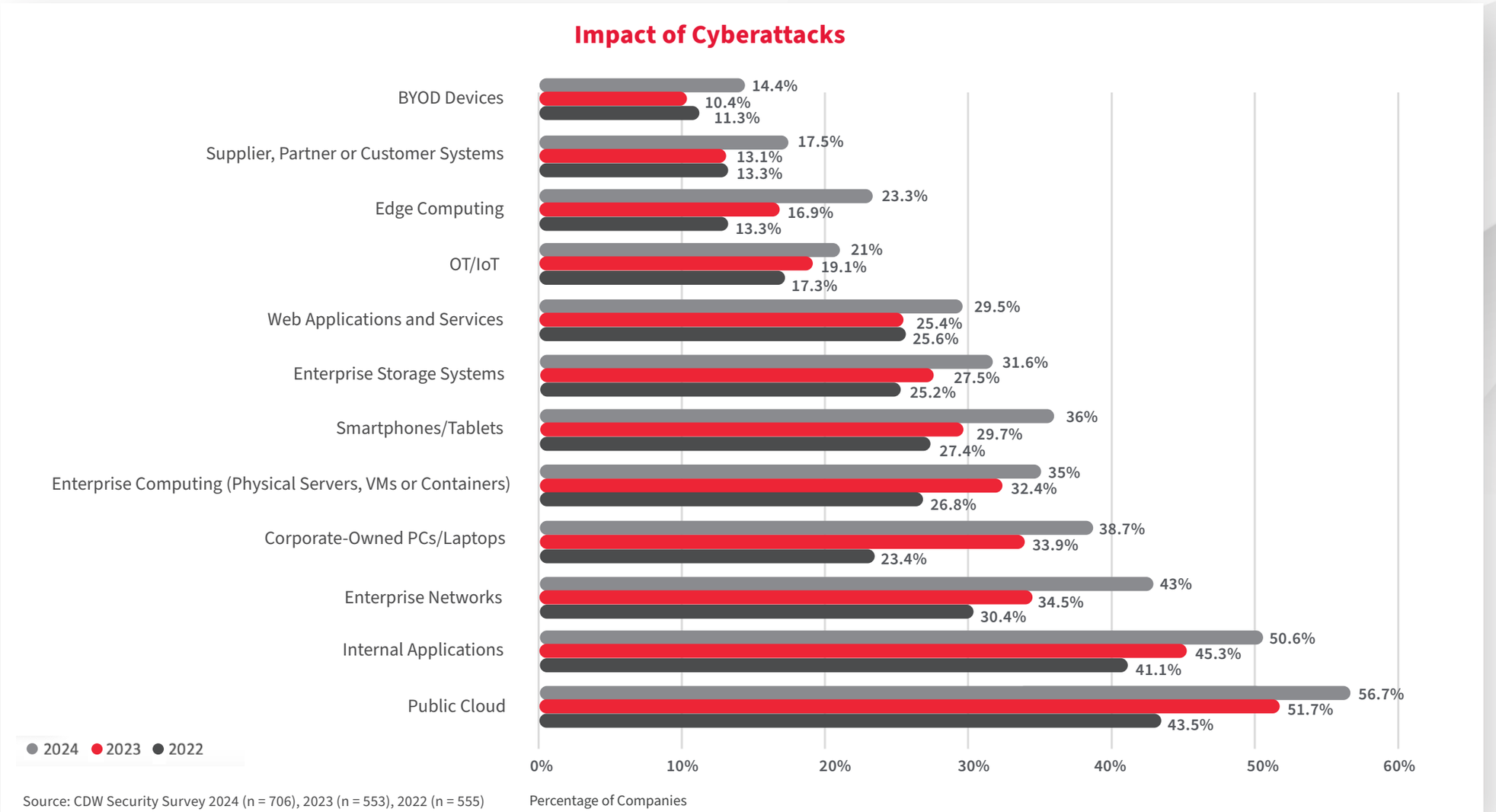
### Is Migration to Cloud Meeting Security Expectations?




Source: CDW Security Survey 2024 (n = 706)

For the last three consecutive years, many Canadian organizations have indicated that public cloud environments were the most directly impacted IT component resulting from a cybersecurity attack, when compared to other components. This concern continues to rise year over year. In the 2024 study, 56.7 percent of respondents pointed to public cloud, compared with 51.7 percent in 2023 and 43.5 percent in 2022.

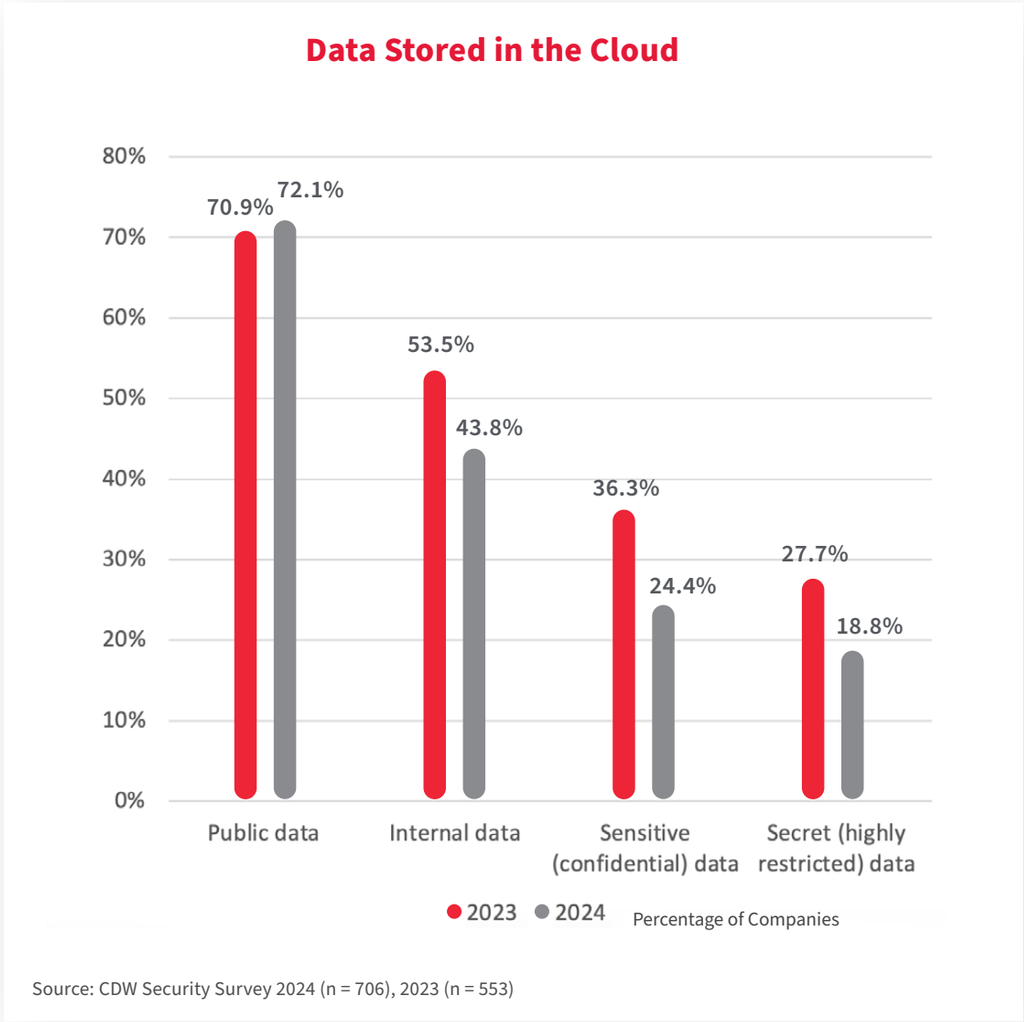
**Chart 10:**




Source: CDW Security Survey 2024 (n = 706), 2023 (n = 553), 2022 (n = 555)

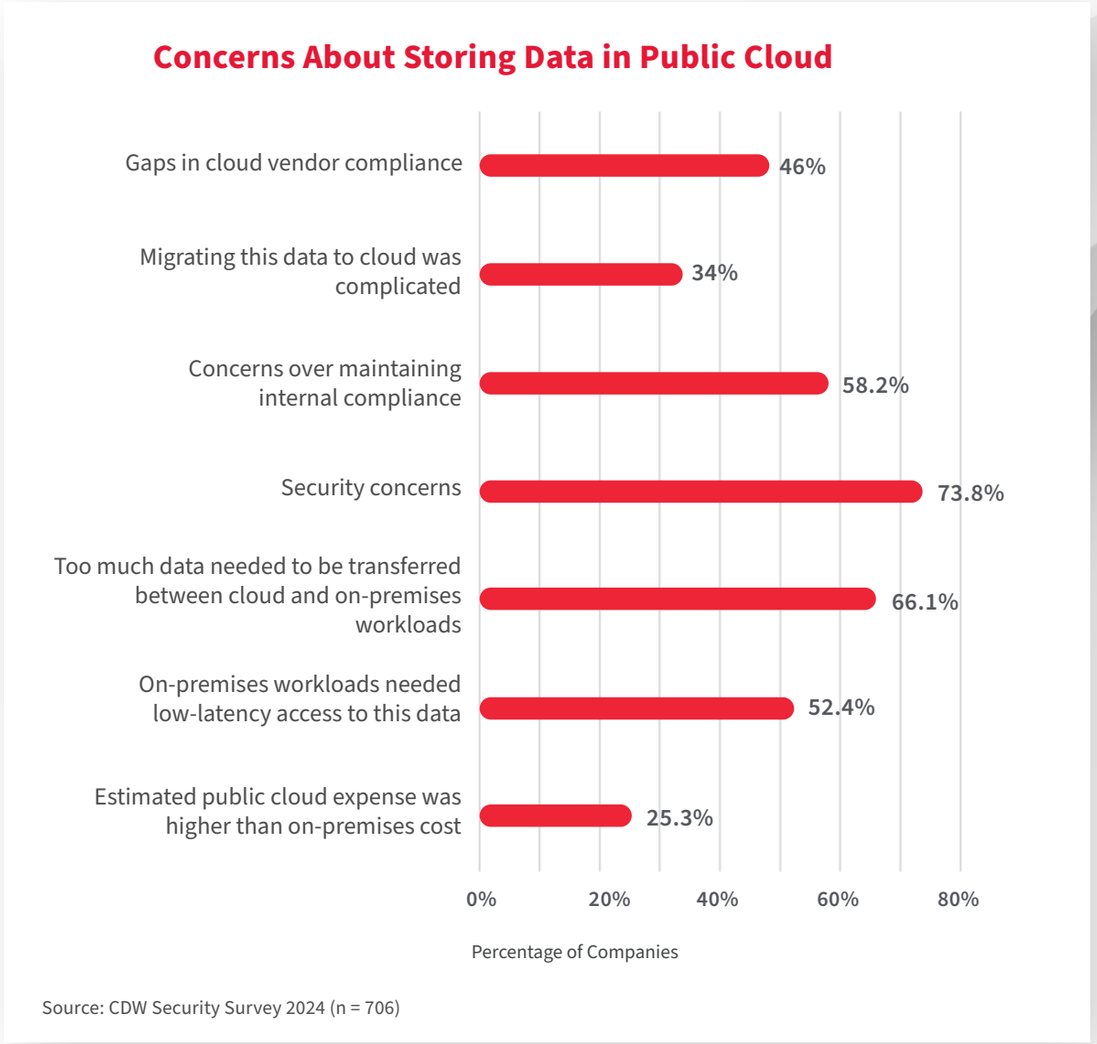
Compared with the 2023 study, fewer organizations stored their confidential and secret data in public cloud. The top reason cited by 74 percent of respondents in the 2024 study was concern about security.

**Chart 11:**




Source: CDW Security Survey 2024 (n = 706), 2023 (n = 553)

**Chart 12:**



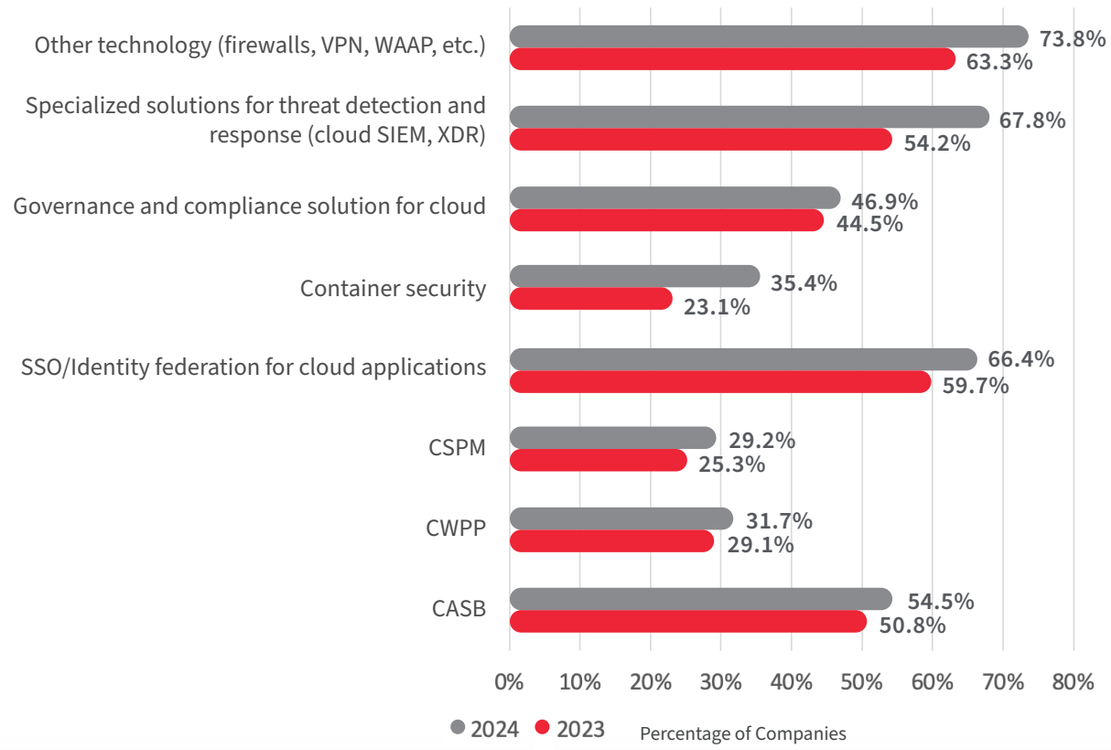

Source: CDW Security Survey 2024 (n = 706)

## Investment in Security Technology Has Not Improved Security Outcomes

In response to the growing public cloud security threat, Canadian organizations are investing more heavily in cloud security technology. Compared with the 2023 study, the adoption of cloud security technologies has grown. For example, investment in CASB, CWPP, CSPM and threat detection software has increased by between 2.5 to 13.6 percentage points.

**Chart 13:**

### Technologies to Secure Cloud Environments




Source: CDW Security Survey 2024 (n = 706), 2023 (n = 553)

Despite this investment in cloud security, the 2024 study data does not show a significant reduction in cloud security incidents compared with the previous study. Why? Investing in point solutions might not reduce security incidents because it addresses specific use cases rather than the broader cloud architecture. For example, CSPM, CASB for access control, firewalls for cloud and VPN for cloud all support a single use case, thereby leaving gaps in security. These solutions do not account for the dynamic and complex nature of cloud environments.

A more effective strategy should focus on niche cloud architecture and security skills, as well as workflows and processes. This approach considers the entire cloud ecosystem, ensuring that all aspects of the cloud, from its design to its operation, are secure. It also involves continuous monitoring and adaptation to changing threats, which is crucial in the ever-evolving landscape of cloud security.

# Finding 4:

## Canadian organizations that prioritize AI-enhanced functions can improve cybersecurity defences, streamline operations and address talent shortages.

ChatGPT has demonstrated that AI and machine learning (ML) can be effectively applied to a broad spectrum of use cases, including cybersecurity.

# AI/ML: Invaluable Tools in the Modern Cybersecurity Landscape

### AI Is User-Friendly and Intuitive

Prior to ChatGPT, AI adoption was largely confined to academic and research circles, with its applications limited to specific domains like computer vision and natural language processing. However, with the advent of ChatGPT, AI's potential became evident to a broader audience. With its ability to generate human-like text, ChatGPT has demonstrated the power of AI in a tangible, accessible way and sparked interest in potential applications of AI across various fields. It has demonstrated that AI can be user-friendly and intuitive – decisively dispelling previous misconceptions about AI being complex and inaccessible.

Moreover, the success of ChatGPT has led to increased funding and research in AI and machine learning. This is accelerating the development of new AI technologies and applications, which has fuelled interest in AI for Canadian businesses, creating a positive feedback loop.

### Large Enterprises Lead the Way in AI/ML Implementations

AI/ML are not new to cybersecurity, and many Canadian organizations already have use cases that are enhanced by them. According to the study, enterprise organizations are the most advanced, and the financial services industry leads the way with 37.5 percent reporting mature and advanced AI/ML cybersecurity implementations.

**Table 6: Adoption of AI/ML in Security**

| | Total | Company Size | | | Industry | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|
| | | <100 employees [Small] | 100-999 employees [Medium] | >1,000 employees | Financial Services | Energy | Government | Education | Healthcare | Other |
| **No implementation – There is no formal AI/ML strategy for cybersecurity and unsure about AI/ML capabilities of security solutions stack.** | 16.7% | 33.0% | 13.2% | 3.4% | 1.8% | 19.2% | 17.6% | 25.5% | 2.0% | 20.8% |
| **Beginner – A formal AI/ML strategy is being developed. Security solutions with out-of-the-box AI/ML capabilities are being adopted.** | 29.3% | 43.9% | 28.1% | 14.1% | 12.5% | 42.3% | 34.3% | 39.2% | 20.8% | 28.0% |
| **Developing - A formal AI/ML strategy is in place and have already implemented some AI/ML technologies.** | 31.7% | 17.9% | 38.2% | 36.7% | 48.2% | 25.0% | 23.5% | 24.5% | 48.5% | 29.4% |
| **Mature – AI/ML strategy is established, and AI/ML technologies are well-integrated in our cybersecurity defences.** | 15.3% | 5.2% | 15.1% | 27.7% | 17.9% | 13.5% | 18.6% | 10.8% | 13.9% | 16.0% |
| **Advanced - A well-established, deeply integrated AI/ML strategy leverages AI/ML across cybersecurity functions.** | 6.9% | 0.0% | 5.4% | 18.1% | 19.6% | 0.0% | 5.9% | 0.0% | 14.9% | 5.8% |

Source: CDW Security Survey 2024 (n = 706)

## A Cost-Effective Approach

AI and ML are crucial in cybersecurity implementations, thanks to their ability to analyze vast amounts of data rapidly, identify patterns and predict future threats. They can also adapt to evolving IT landscapes and threats and, despite significant initial investment, can operate with limited resources, making them invaluable in the face of increasing threats, budget shortages and fast-evolving IT landscapes.

The study showed that AI/ML for IT security is a priority for many Canadian organizations, especially enterprise organizations. Industries in this category that indicate the most interest in using AI/ML for security are financial services and healthcare.

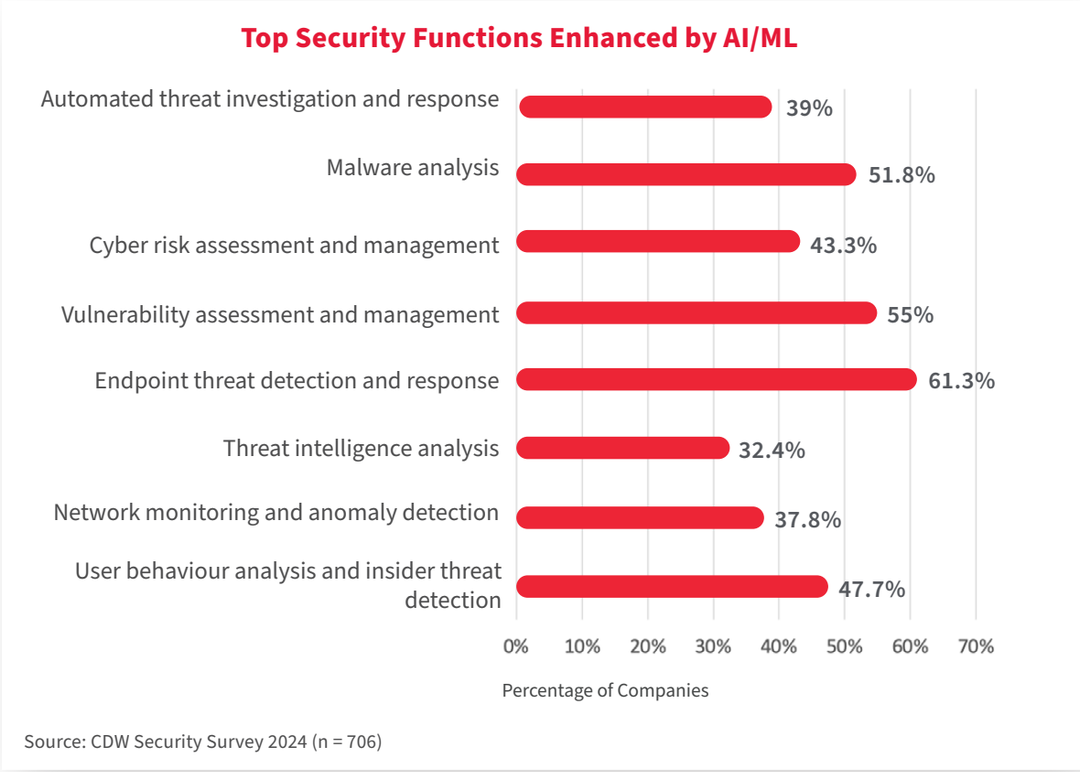
**Table 7: Priority of AI/ML Within Organizations**

| | Total | Company Size | | | Industry | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|
| | | <100 employees [Small] | 100-999 employees [Medium] | >1,000 employees | Financial Services | Energy | Government | Education | Healthcare | Other |
| High Priority (Strategic Focus) | 18.3% | 13.7% | 15.5% | 28.8% | 28.6% | 11.5% | 18.6% | 11.8% | 18.8% | 19.5% |
| Moderate Priority (Operational Focus) | 42.2% | 38.2% | 40.7% | 49.7% | 44.6% | 44.2% | 31.4% | 38.2% | 51.5% | 43.3% |
| Low Priority (Exploratory Stage) | 29.3% | 30.7% | 35.3% | 16.9% | 23.2% | 28.8% | 29.4% | 40.2% | 25.7% | 28.0% |
| Not a Priority (No Current Plans) | 9.8% | 16.5% | 8.2% | 4.5% | 3.6% | 15.4% | 20.6% | 7.8% | 4.0% | 8.9% |

Source: CDW Security Survey 2024 (n = 706)

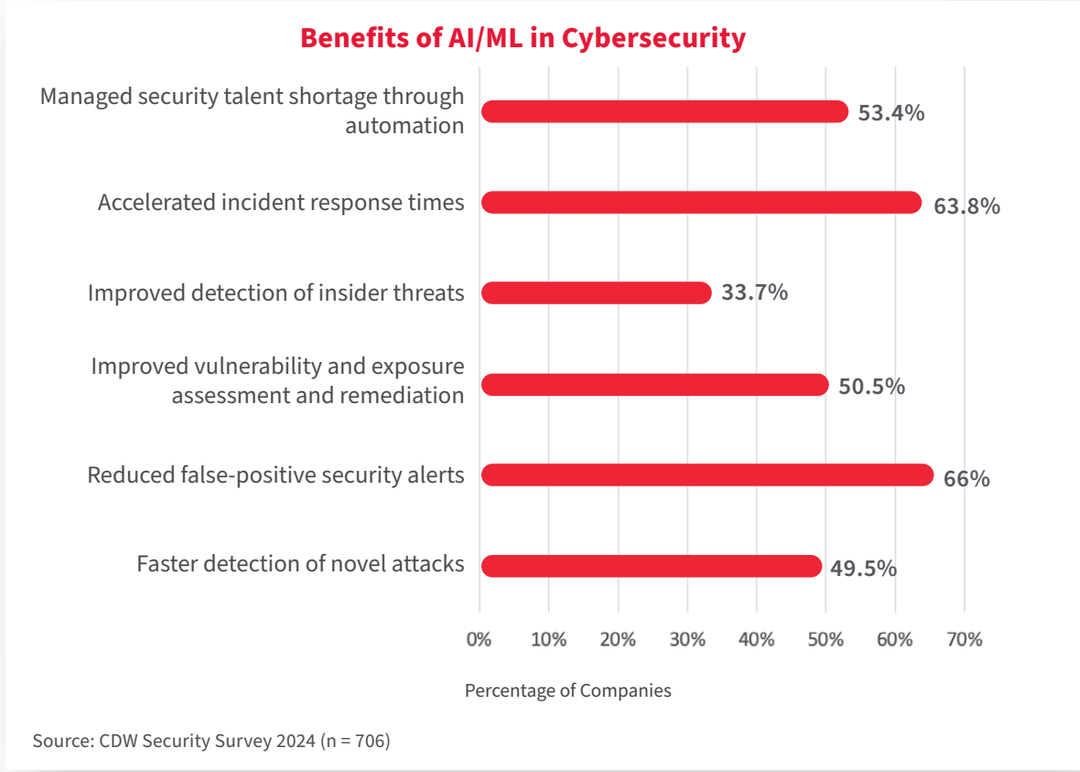
According to the study, the cybersecurity functions most enhanced by AI/ML are EDR at 61.3 percent, vulnerability assessment and management at 55 percent and malware analysis at 51.8 percent.

**Chart 14:**




Source: CDW Security Survey 2024 (n = 706)

**Chart 15:**




Source: CDW Security Survey 2024 (n = 706)

## Benefits of AI/ML in Cybersecurity

According to the study, AI and ML are beneficial when incorporated into cybersecurity operations. The top-cited benefits are:

1) Significantly reducing false positive alerts, improving the efficiency of security operations by focusing on real threats

2) Improving incident response times by automating threat detection and response processes, allowing for quicker remediation

3) Managing talent shortages through automation, enabling security teams to handle larger workloads without needing to hire additional staff

In short, not only can AI/ML enhance security, but it can also streamline operations and address talent shortages in cybersecurity.

# Finding 5:

## Canadian organizations acknowledge potential adversarial threats amidst growing use of AI/ML within cybersecurity.

AI and ML are making cybercriminals more formidable than ever before, necessitating robust AI-based defences in cybersecurity. A comprehensive AI strategy helps to ensure that defensive AI is used effectively and responsibly against adversarial AI.

# Combat Adversarial AI with Defensive AI

### Impact of Adversarial AI

AI and ML can empower cyberattackers by enhancing their ability to exploit vulnerabilities and evade detection. Cybercriminals can use AI to automate the process of finding vulnerabilities by increasing their efficiency and reach. In addition, AI can be misused to create sophisticated phishing and social engineering tactics, making it harder for victims to recognize fraudulent activity. Furthermore, ML can help attackers adapt their tactics in real time, learning from their successes and failures to refine their strategies.

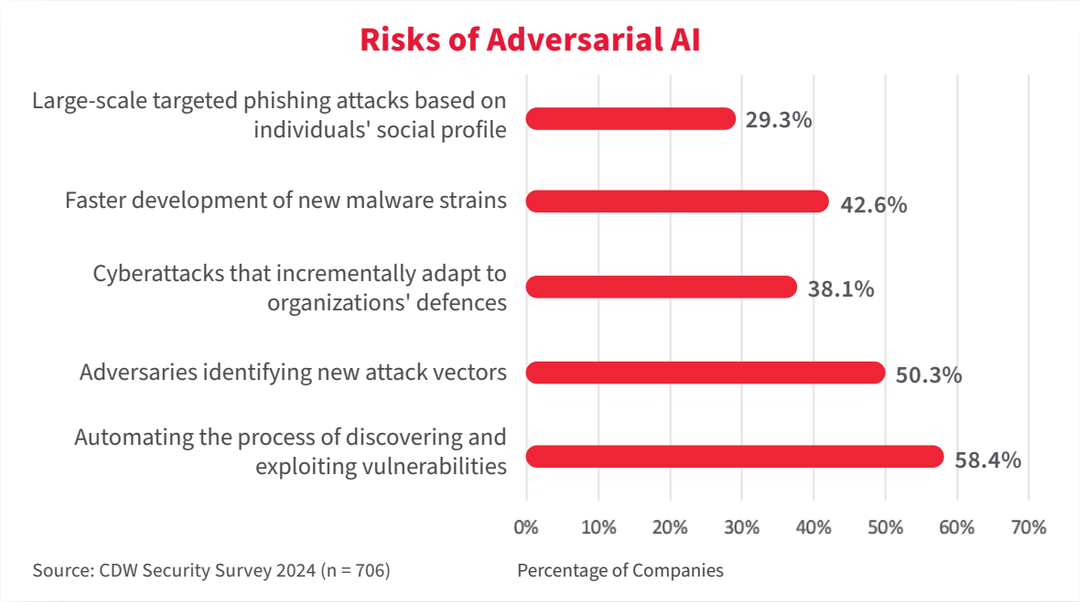
The 2024 study showed that Canadian organizations have grave concerns about the risk of AI empowering their adversaries. The top three risks cited include giving cyberattackers the ability to:

1. Automate the process of discovering and exploiting vulnerabilities (58.4 percent)

2. Identify new attack vectors (50.3 percent)

3. Speed up development of new malware strains (42.6 percent)

**Chart 16:**

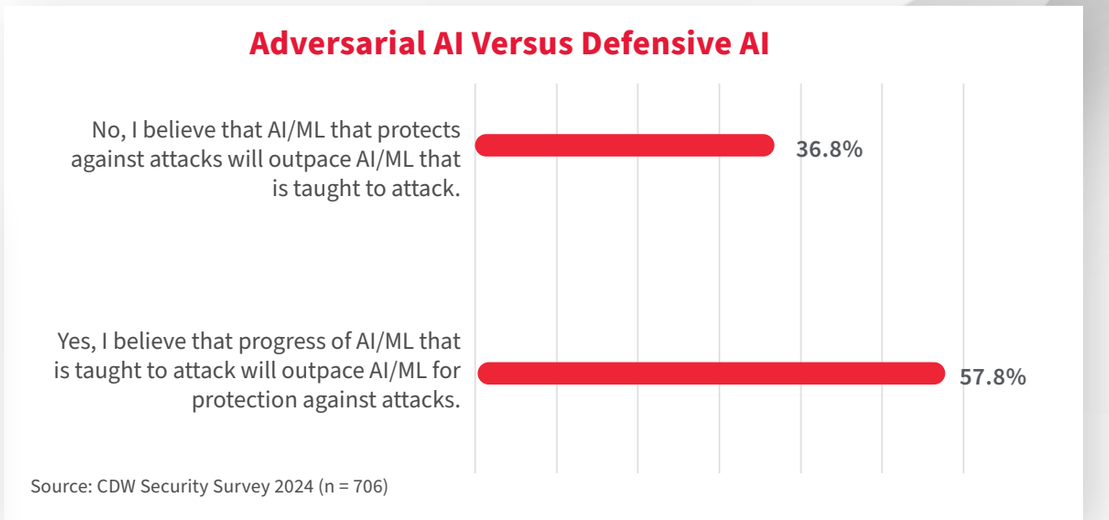



### Adversarial AI Versus Defensive AI

The combination of AI and ML can make cybercriminals more formidable, necessitating robust AI-based defences in cybersecurity. While AI could empower the adversaries, AI can also be used by cybersecurity teams to enhance their defences. It can help in real-time threat detection and response, automating the process of identifying and neutralizing threats. AI can also be used to predict potential threats based on historical data and patterns, enabling proactive security measures.

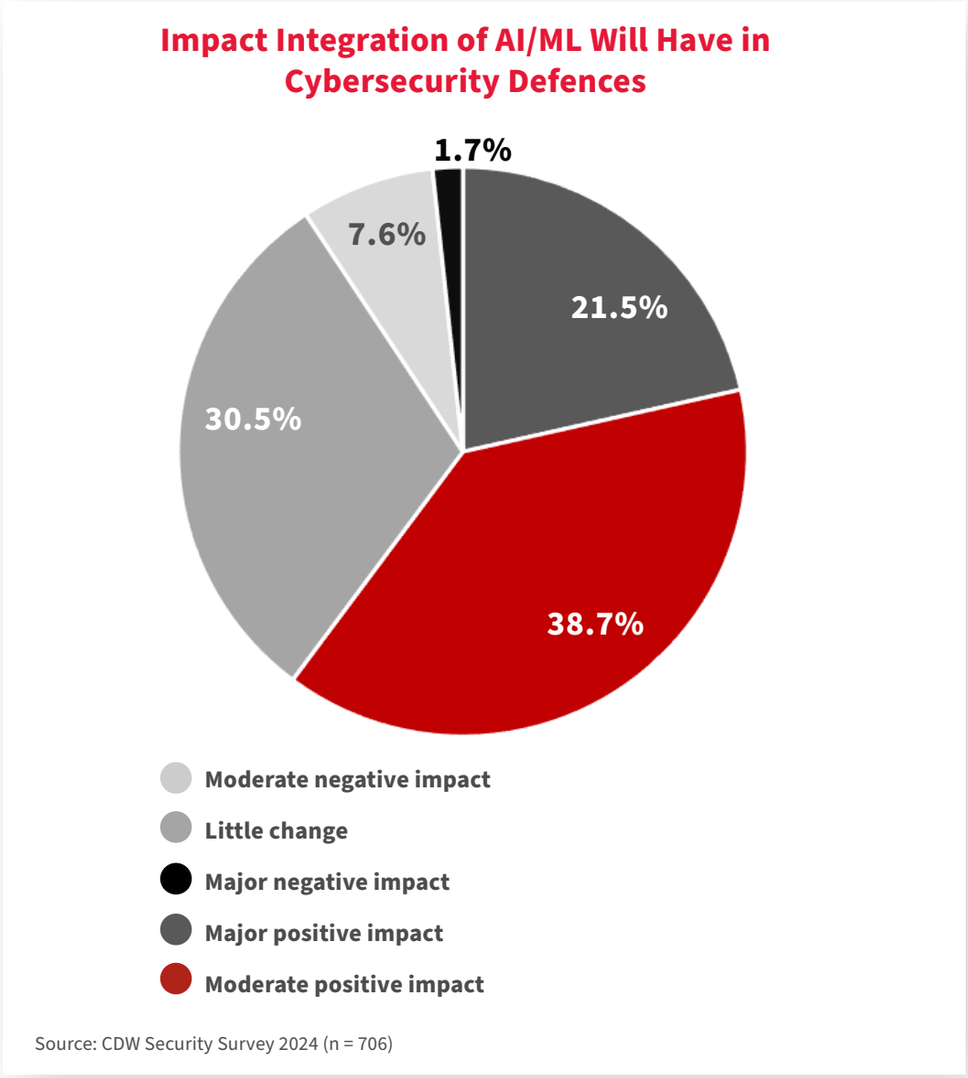
Thus, AI can be a double-edged sword in cybersecurity, serving both offensive and defensive roles. However, Canadian organizations believe that AI may slightly tip the scale in favour of adversaries. A majority of survey respondents believe that the development of adversarial AI/ML will outpace the development of defensive AI/ML that protects against attacks (57.8 percent).

**Chart 17:**



A total of 60.2 percent of Canadian organizations anticipate that AI will have significant positive impact on cybersecurity over the next two years.

**Chart 18:**




Source: CDW Security Survey 2024 (n = 706)

### AI Policy Is a Necessity

Organizations that embrace AI and ML technologies can significantly enhance their cybersecurity posture. Yes, there are risks, but the benefits of AI and ML in cybersecurity are too substantial to ignore. Their ability to automate threat detection and response, predict potential threats and manage talent shortages make AI and ML invaluable tools in the modern cybersecurity landscape.

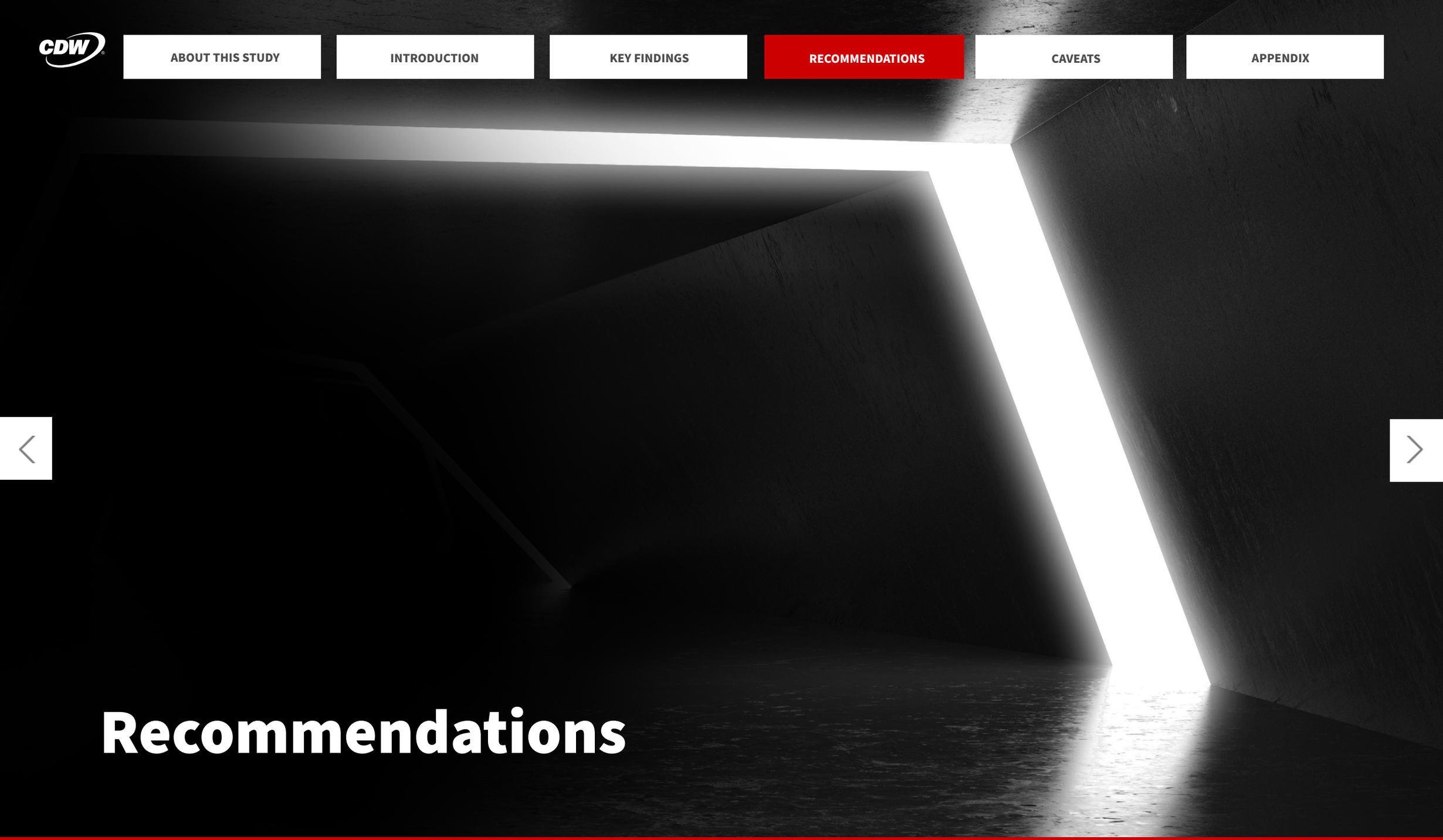
AI in cybersecurity is just one component of a comprehensive AI policy that covers all aspects of AI use within the organization. Aligning with their business goals and context, an organization-wide AI policy should outline the organization's stance on AI, including its use, management and ethical considerations. It should also define roles and responsibilities, ensuring that all members of the organization understand their part in implementing and maintaining the AI strategy. This will ensure that AI is used effectively and responsibly across the organization.

According to the study, while 59.3 percent of all Canadian organizations are working toward creating a security policy regarding the use of AI, small businesses are lagging behind at 39.2 percent, while enterprise organizations are leading the way at 78 percent.

**Table 8: AI Policy in Place**

| | | Company Size | | |
|---|---|---|---|---|
| | Total | <100 employees [Small] | 100-999 employees [Medium] | >1,000 employees [Enterprise] |
| Yes | 59.3% | 39.2% | 62.5% | 78.0% |
| No | 36.0% | 54.7% | 32.2% | 20.3% |

Source: CDW Security Survey 2024 (n = 706)



# Recommendations

## I. Prioritize Detection and Response within Zero Trust

By implementing advanced technologies, fostering a proactive response culture and consistently updating policies, enterprises can ensure comprehensive security and resilient operations in the face of evolving cyberthreats.

For improved threat detection and response within zero trust, organizations must consider:

- **Developing a comprehensive understanding of zero trust.** Recognize that zero trust extends beyond preventing unauthorized access. Acknowledge the importance of detecting and responding to various threats, including insider threats, advanced phishing attacks and diverse cyberthreats.
- **Implementing advanced detection technologies.** Deploy advanced technologies like next-generation firewall (NGFW), security information and event management (SIEM) systems and extended detection and response (XDR). Leverage these technologies to identify unusual activities or behaviours that might indicate potential threats within the network.
- **Establishing a well-defined response plan.** Develop a robust response plan outlining steps for isolating affected systems. Conduct thorough investigations to identify the root cause of the threat and implement measures to prevent similar incidents in the future.
- **Conducting regular monitoring and updates.** Emphasize the dynamic nature of cybersecurity. Regularly monitor and update security measures to stay abreast of emerging threats and evolving technologies, ensuring continuous adaptability.
- **Scheduling frequent security policy reviews and updates.** To maintain their effectiveness and relevance, ensure policies align with changes in IT infrastructure, business operations and the evolving threat landscape.

Although ZTA is a pivotal aspect of a holistic zero-trust security strategy, it should not monopolize the focus. Equally crucial are robust threat detection and response mechanisms. Organizations should prioritize all these areas to fortify their security posture and achieve the long-term goals of the zero-trust strategy.

## II. Strengthen Cloud Confidence

- **Navigate the cloud security terrain.** To embark on a secure cloud journey, IT and security leaders must first understand the intricacies of the cloud security landscape. This involves grasping the shared responsibility model, where the cloud service provider (CSP) shoulders the responsibility for the security of the cloud, while the customer is tasked with ensuring security in the cloud. This dual awareness includes a detailed understanding of the security controls provided by the CSP and a clear comprehension of the necessary implementations on the customer's end.
- **Fortify with best practices.** The security frameworks that organizations adopt can also guide security leaders to secure their cloud services by helping them to identify and assess the risk that cloud services pose to the organization and providing a structured approach to risk identification, risk analysis, risk response and risk monitoring. This risk-based approach is paramount for a resilient cloud security posture and requires establishing stringent access controls, ensuring regular system updates and deploying encryption for data at rest and in transit. Furthermore, establishing a comprehensive identity and access management (IAM) system will ensure that only authorized individuals gain access to sensitive data, further strengthening overall security.
- **Master cloud monitoring tools.** Operationalizing cloud security requires a nuanced understanding of various cloud monitoring tools. These tools, ranging from basic log analysis to advanced threat detection systems, form the backbone of effective security measures. IT and security leaders must familiarize themselves with the functionalities and limitations of each tool, ensuring proper use for optimal security outcomes.
- **Forge alliances with security experts.** Recognizing the complexity of cloud security, IT and security leaders may find collaboration with external security partners to be a strategic move. These partners bring specialized expertise in cloud security, providing invaluable support to navigate the intricate cloud environment. Collaborating with external experts fills skill gaps and enhances cloud security proficiency.

## III. Create a Comprehensive Strategy for AI in Security

- **Develop an overarching strategy.** As the first step toward leveraging AI for security, this strategy should outline the goals for AI adoption, the resources required and the timeline for implementation. It should also consider the potential challenges and risks associated with AI adoption and how they can be mitigated.
- **Establish policies and governance for AI use.** Business, IT and security leaders should institute policies that outline the standards for AI use, including how AI should be used, who can access it and how its use should be monitored. Governance should also be established to ensure that AI is used in a manner that is consistent with organizational goals and legal requirements.
- **Invest in AI training for IT and security staff.** This includes training on the basics of AI, how to use AI tools, how to interpret AI results and how to respond to AI-identified threats. By equipping staff with this knowledge, IT and security leaders can ensure that AI is used effectively and efficiently.
- **Implement AI security solutions.** By implementing solutions such as AI-powered threat detection systems, incident response systems and risk assessment tools, IT and security leaders can enhance their ability to detect and respond to security threats.

However, security leaders will have to establish their own policies on what is an acceptable level of AI that can be adopted by their department, based on the following key considerations:

- **Understanding the technology:** AI-based security solutions can be complex and challenging to understand, and security leaders should evaluate how well they understand the functioning of these solutions.
- **Ensuring data privacy and security:** This could involve protecting sensitive information from unauthorized access, ensuring that the data is accurate, up to date and more.
- **Maintaining data integrity:** Maintaining the integrity and accuracy of the data used by these solutions is foundational to the effectiveness of these solutions. Organizations will need a high level of data governance to ensure AI models' data integrity.
- **Ensuring the effectiveness of security measures:** A challenging endeavour, this may involve regularly testing and updating these measures.
- **Balancing the cost of the solution with its potential business benefits:** These solutions will require initial investment, as well as ongoing management and improvement, leading to high total costs of ownership that can be assessed using a cost-benefit analysis.
- **Ensuring the availability of the necessary resources:** Ensuring that the necessary resources, such as data, AI models and people, are available could be challenging. It is advisable for organizations to evaluate their capability to sustain such solutions.

Leveraging AI for security involves developing an overarching strategy, establishing policies and governance, investing in AI training, implementing AI security solutions and monitoring and evaluating AI performance. By following these recommendations, IT and security leaders can effectively leverage AI within their security, enhancing their ability to detect and respond to security threats.

## IV. Conduct Security Assessment and Implement an Effective Security Framework

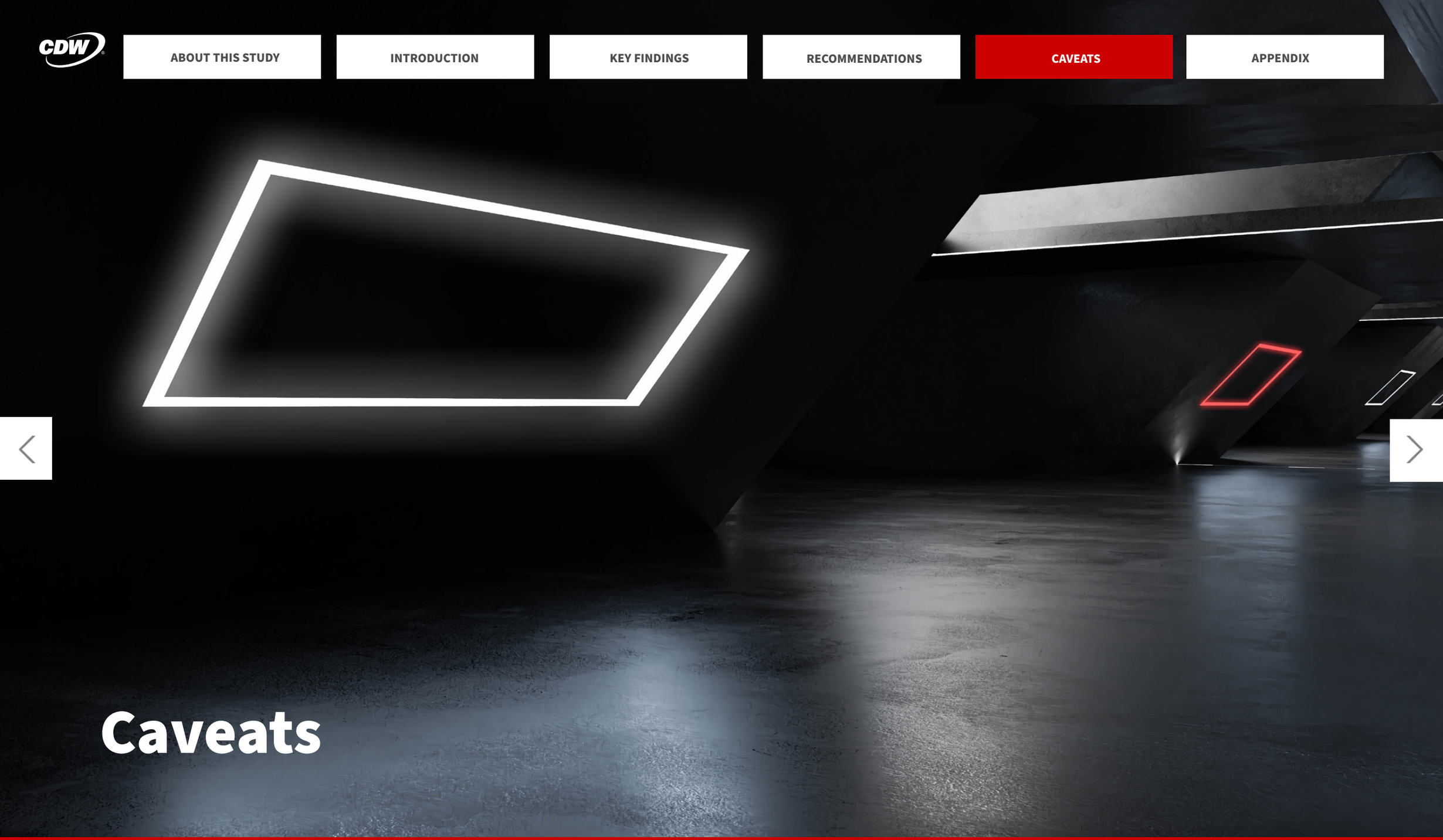
- Enhancing security maturity also requires understanding the current risk landscape. A comprehensive risk and security assessment can help identify areas of vulnerability and potential security risks. This assessment should cover all aspects of your IT infrastructure, including hardware, software, networks and personnel. The goal of this assessment is to provide a clear, objective picture of your organization's current security posture. It will help you identify areas that need improvement and prioritize your security initiatives.

**Key components of a comprehensive assessment include:**

- **Assess value of assets.** Establish a standardized process to assess the informational value of assets, considering factors such as financial implications, legal consequences, competitive significance, recreation feasibility, impact on revenue/profitability, operational importance and potential reputational damage.
- **Create an asset inventory.** Identify and prioritize assets by collaborating with business users and management to compile a comprehensive list, including details such as software, hardware, data criticality and security controls, using a risk matrix to simplify prioritization based on critical risks and potential impact on security posture.
- **Assess the threats.** Identify and assess a range of cyberthreats, including hackers, malware, human errors, adversarial threats, unauthorized access, information misuse, data leaks, loss of data and service disruptions; and establish a robust and regularly tested incident response plan to ensure prompt and effective responses by security teams.
- **Conduct security testing.** Identify and mitigate potential weaknesses in your organization's security by conducting vulnerability analysis and security testing.
- **Evaluate and implement security measures.** Evaluate existing controls and implement new measures, both technical (e.g., encryption, next-generation firewall, two-factor authentication) and non-technical (e.g., security policies, physical mechanisms). Classify them as either preventive or detective to minimize the probability of threats or vulnerabilities impacting the organization.
- **Prioritize risks.** Risks should be prioritized according to factors such as organizational policies, reputational damage, feasibility, regulations, effectiveness of controls, safety, reliability, organizational attitude toward risk and tolerance for uncertainty. Determine corrective measures that can be promptly developed for high-risk scenarios, within a reasonable period for medium risks, and evaluate whether to accept or mitigate low-risk situations.

Once cyber risks are assessed and documented, they can be effectively managed through a cybersecurity framework such as NIST CSF or ISO 2700x that provides a structured approach to managing cybersecurity risk by setting up necessary security controls and measures, helping stakeholders understand the cybersecurity program and its effectiveness.

While budget constraints may pose challenges, they do not have to prevent organizations from improving their security maturity. By conducting a thorough risk and security assessment and adopting a security framework, organizations can enhance their security posture and ensure the resilience of their operations.



# Caveats

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

# Appendix A: Detailed Survey Results

# Appendix A: Detailed Survey Results

**Demographics:** A sampling frame of 10,332 Canadian IT security, risk and 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 706 surveys, or a 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.) | 3.7% |
| Personal/Consumer Services (e.g., Travel, Beauty, Personal Training, Dry Cleaning, etc.) | 2.4% |
| Construction | 3.1% |
| Hospitality | 2.5% |
| IT Industry | 4.8% |
| Not for Profit | 0.0% |
| Manufacturing | 6.4% |
| Crown Corporation or Other Publicly Funded Organization | 0.1% |
| Education K-12 | 5.1% |
| Education College/University | 9.3% |
| Financial Services | 7.9% |
| Government | 14.4% |
| Healthcare | 14.3% |
| Primary (e.g. Agriculture, Mining, Forestry, etc.) | 1.1% |
| Oil & Gas or Field Services Related | 3.1% |
| Retail | 6.1% |
| Communications (e.g., Cable and Telecommunications Services, etc.) | 1.8% |
| Media (e.g., Radio/TV Broadcasting) | 2.4% |
| Printing, Publishing, etc. | 1.6% |
| Transportation and Warehousing | 3.3% |
| Utilities | 4.2% |
| Wholesale and Distribution | 2.1% |

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

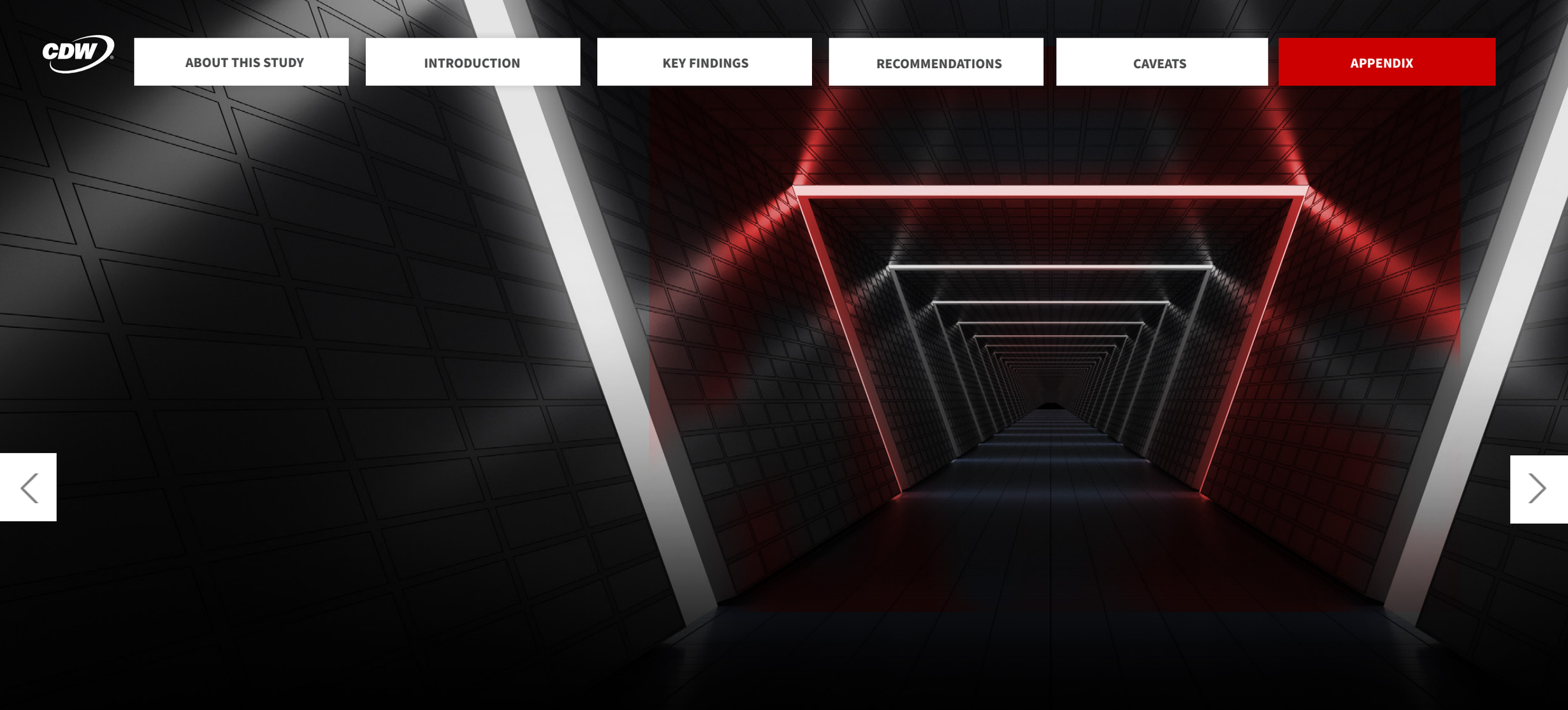
| | Total |
|---|---|
| Directing the IT function | 43.6% |
| Improving/managing IT security | 100% |
| Setting IT priorities | 46.2% |
| Managing IT budgets | 37% |

**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) | 16.4% |
| Ontario | 30.9% |
| Quebec | 24.1% |
| Atlantic Canada (NB, NS, NFLD, PEI) | 17.8% |
| North (Yukon / Northwest Territories / Nunavut) | 7.1% |
| Not Headquartered in Canada | 3.7% |

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

| | Total |
|---|---|
| C-Level Executive Management Excluding IT | 9.2% |
| Line of Business Management Excluding IT | 3.8% |
| C-Level IT Including CIO/CTO/CSO/CISO | 7.2% |
| Finance/Accounting | 4.8% |
| IT/IS/MIS/Data Centre/IT Security | 62.9% |
| Legal/Compliance/Risk | 12.0% |



# Appendix B: Definitions

**Application Program Interface (API):** An application programming interface (API) is code that enables two software programs to communicate.

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

**Cloud Access Security Broker (CASB):** On-premises or cloud-based security policy enforcement point that is placed between cloud service consumers and cloud service providers to combine and interject enterprise security policies as cloud-based resources are accessed.

**Cloud Workload Protection Platform (CWPP):** A unified cloud security solution that offers continuous threat monitoring and detection for cloud workloads across different types of modern cloud environments.

**ChatGPT:** An artificial intelligence (AI) chatbot that uses natural language processing to create humanlike conversational dialogue.

**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.

**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.

**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. Attackers gain access to an organization's network, infrastructure and/or data, but no data is exfiltrated.

**ISO 2700x:** A series of best practices to help organizations improve their information security.

**Machine Learning (ML):** Machine learning is a branch of artificial intelligence (AI) and computer science that focuses on the use of data and algorithms to imitate the way that humans learn, gradually improving its accuracy.

**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 (e.g., biometric authentication).

**NIST Cybersecurity Framework (CSF):** Provides comprehensive guidance and best practices that private sector organizations can follow to improve information security and cybersecurity risk management.

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

**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 services provider (CSP) and its users to ensure accountability. How CSPs versus a user organization's responsibilities are defined varies between CSPs and the services being provided (SaaS, PaaS, IaaS), so it is imperative that user organizations clearly understand what security responsibilities their CSPs will take ownership of versus responsibilities the organization will retain.

**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.

**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.

**Service Organization Control Type 2 (SOC 2):** A cybersecurity compliance framework designed to ensure that third-party service providers store and process client data in a secure manner.

**Tactics, Techniques and Procedures (TTPs):** Describes the patterns of behaviour, specific strategies and threat vectors used by malicious actors to execute a cyberattack.

**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 No. 1 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.

**Research independently conducted by IDC Canada | Published April 2024**