Canadian Cybersecurity Trends

Bridging Strategy, Technology, Artificial Intelligence and Human Expertise

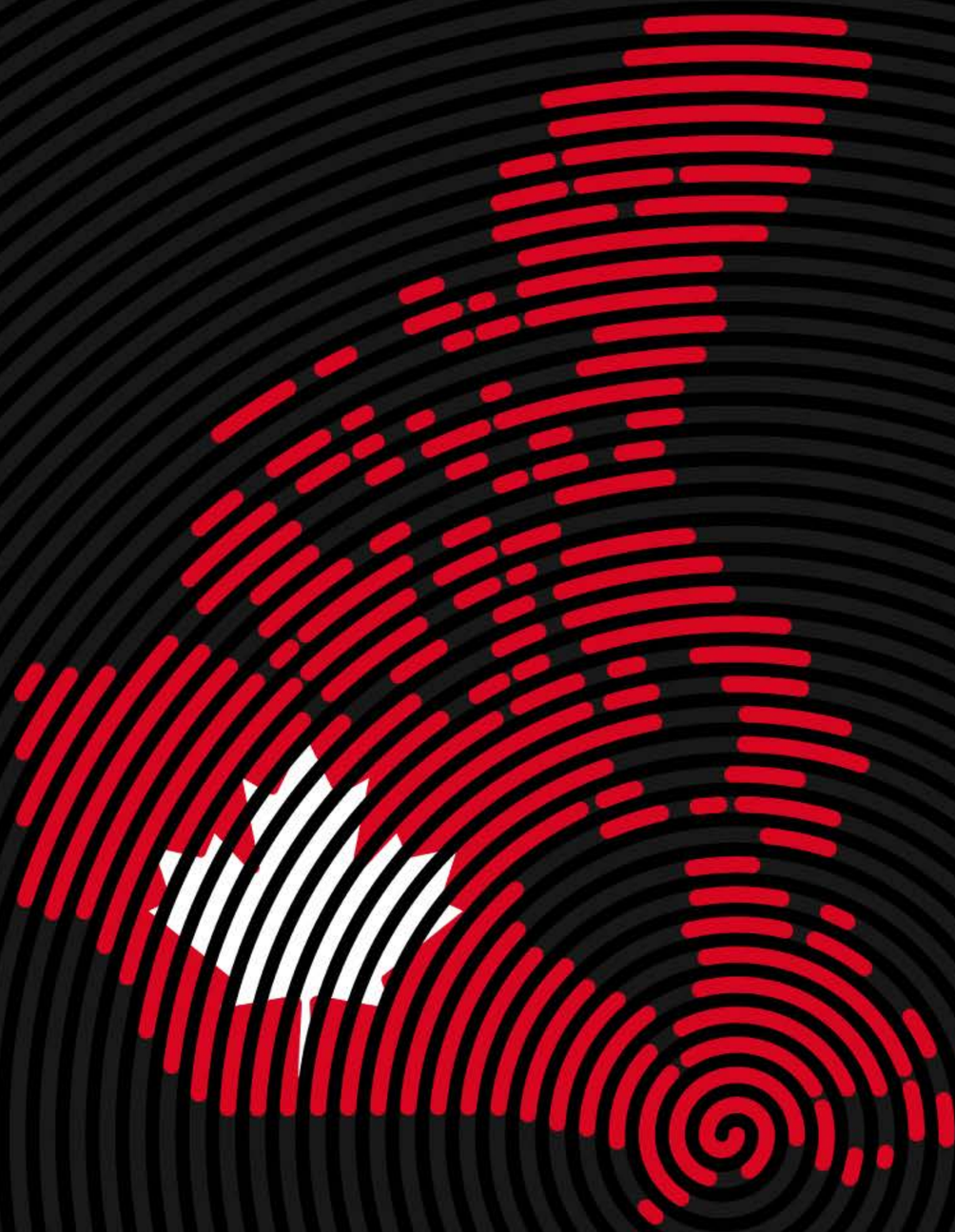


Table of Contents

About this Study

Over the past few years, the IT landscape has demonstrated trends of both contraction and expansion, reflecting the dynamic nature of today's IT environments. Our study specifically analyzed the growth in user endpoints (PCs, laptops, smartphones and tablets), servers and IoT devices over the years to illustrate the ongoing expansion of the IT attack surface.

This study presents the findings of the 2025 CDW Canadian Cybersecurity Study. The data provided in this study was obtained through a Canada-wide, cross-province and cross-industry survey, independently conducted by IDC Canada, of 704 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 2024 by IDC Canada on behalf of CDW Canada. Appendix A shows a detailed description of the demographics and firmographics of the survey participants.

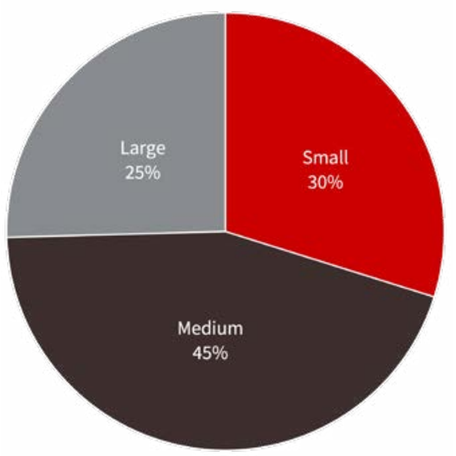


Figure 1: Employees in Canada

Organization Size Segmentation

For the purposes of this study, CDW Canada classifies responding Canadian organizations as small, medium and large 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
- **Large:** 1,000-plus full-time employees located within Canada

Introduction

Canadian Threat Landscape

This study explores the evolving cybersecurity landscape in Canada, focusing on key trends, challenges and strategies that organizations are adopting to strengthen their defences. Drawing on extensive survey data, the report examines critical areas such as the challenge of operationalizing zero trust, the impact of security testing for visibility, barriers to the adoption of AI, the rise of advanced threat detection technologies and the role of MDR services in bridging skills gaps.

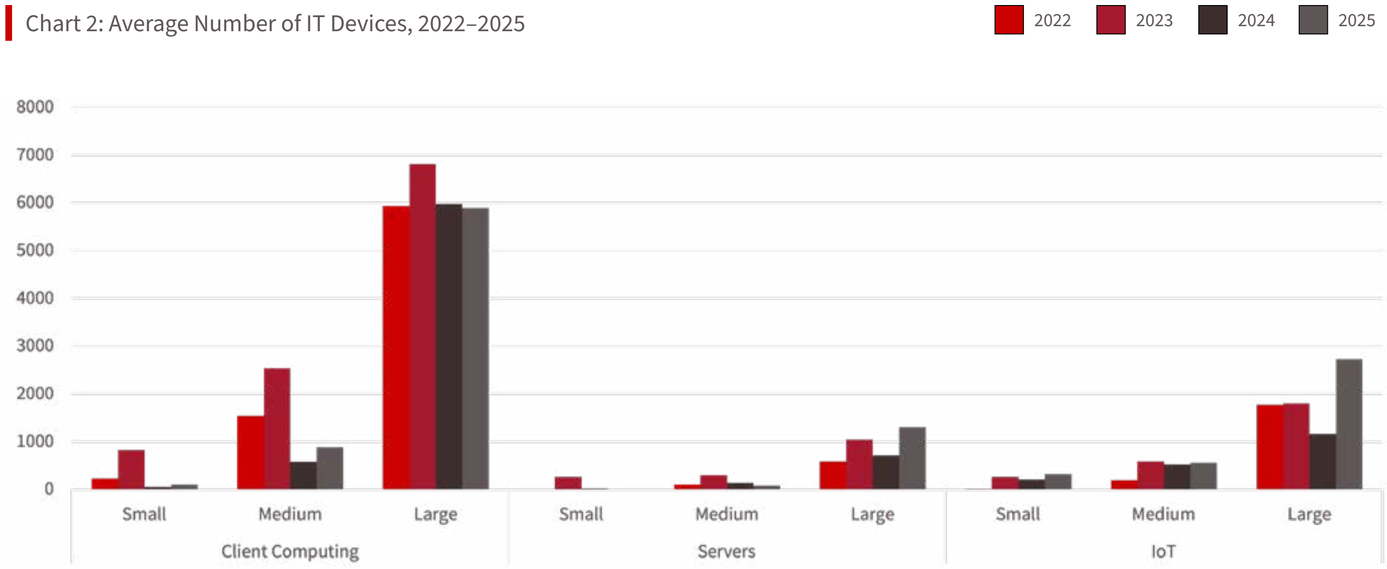
Each finding sheds light on how Canadian organizations are navigating complex security environments, leveraging new technologies and addressing operational bottlenecks to mitigate risks. The insights and recommendations provided aim to equip IT practitioners with actionable guidance to enhance their cybersecurity maturity and resilience in an ever-changing threat landscape.

The Dynamic Attack Surface

The attack surface of Canadian organizations is vast and increasingly dynamic, encompassing SaaS applications, APIs, containers, VMs, storage systems, database appliances, network appliances, endpoints and more. Over the past few years, the IT landscape has demonstrated trends of both contraction and expansion, reflecting the dynamic nature of today's IT environments. Our study specifically analyzed the growth in user endpoints (PCs, laptops, smartphones and tablets), servers and IoT devices over the years to illustrate the ongoing expansion of the IT attack surface.

This matters because as organizations adopt new technologies and scale their operations, the size and complexity of their attack surfaces continue to grow, posing significant challenges for security teams striving to manage and secure these environments effectively.

Chart 2: Average Number of IT Devices, 2022–2025



Client Computing	2022	2023	2024	2025
Small	231	822	48	99
Medium	1,540	2,532	579	880
Large	5,936	6,817	5,978	5,892

Servers	2022	2023	2024	2025
Small	5	263	20	7
Medium	103	302	137	76
Large	585	1,043	718	1304

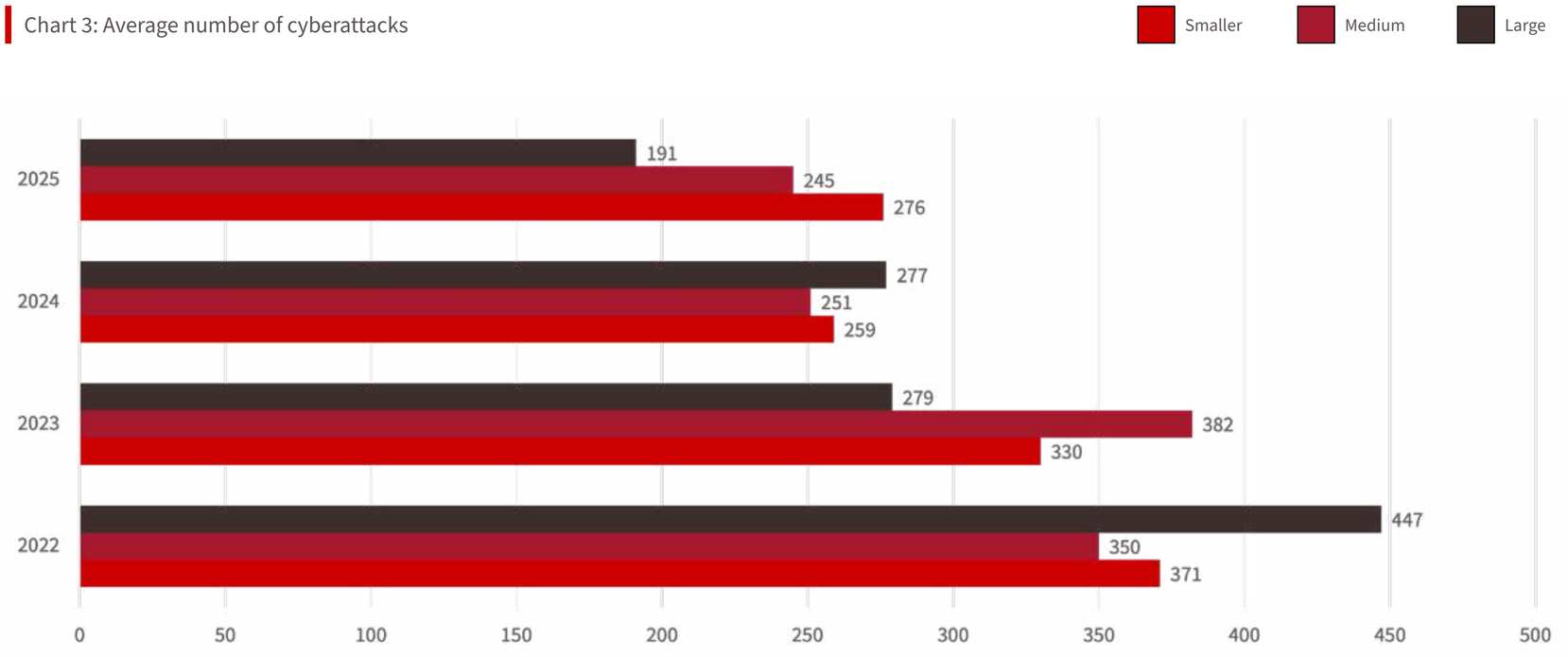
IoT	2022	2023	2024	2025
Small	17	263	205	319
Medium	195	590	523	556
Large	1,774	1,804	1,159	2,727

Cyberattacks, Incidents and Downtime

For the second year in a row, Canadian organizations have reported a decline in the number of cyberattacks year-over-year. However, infection rates remain high, with 86.5 percent of respondents in 2024 indicating a security incident in the past 12 months. The overall attack-to-incident success rate has increased, indicating that cyberattacks are becoming more successful and harder to prevent.

Average Number of Cyberattacks by Organization Size

Chart 3: Average number of cyberattacks



Cyberattacks: Large organizations experienced a sharp decline in attacks, with numbers falling from 447 in 2022 to 191 in 2025.

For smaller organizations, attack numbers slightly increased from 259 in 2024 to 276 in 2025.

Smaller and medium-sized organizations saw relatively consistent attack rates compared to 2024.

Infection Rates Across Categories of Cyberincidents

Denial of Service (DoS): Infection rates for DoS incidents remain steady across all organization sizes, with medium organizations showing a slight increase from 41 percent in 2024 to 43 percent in 2025.

Infiltration: Infiltration rates grew for smaller organizations, reaching 50 percent in 2025, while large organizations saw a decline to 28 percent in 2025.

Breach: Breach infection rates decreased slightly across all organization sizes, with large organizations reporting a drop from 65 percent in 2024 to 50 percent in 2025.

Cloud Incident Rates: Cloud-related infection rates show an upward trend across smaller organizations, increasing from 47 percent in 2024 to 50 percent in 2025, while large organizations remain steady at 41 percent.

Web Defacement Incidents: Small organizations saw an increase in web defacement incidents from 25 percent in 2024 to 28 percent in 2025, while rates for larger organizations remained flat.

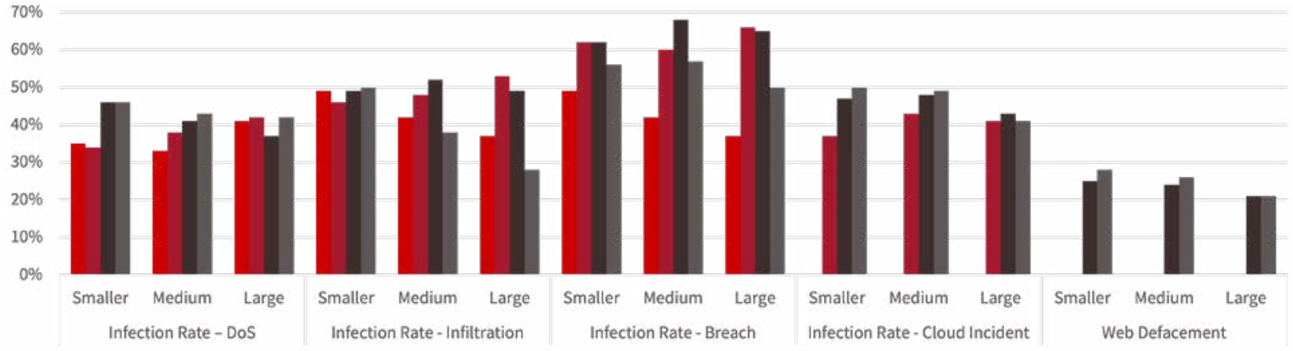


Chart 4: Infection Rates Across Categories of Cyber Incidents

Infection Rate – DoS	2022	2023	2024	2025
Smaller	35%	34%	46%	46%
Medium	33%	38%	41%	43%
Large	41%	42%	37%	42%

Infection Rate – Infiltration	2022	2023	2024	2025
Smaller	49%	46%	49%	50%
Medium	42%	48%	52%	38%
Large	37%	53%	49%	28%

Infection Rate – Breach	2022	2023	2024	2025
Smaller	49%	62%	62%	56%
Medium	42%	60%	68%	57%
Large	37%	66%	65%	50%

Infection Rate – Cloud Incident	2023	2024	2025
Smaller	37%	47%	50%
Medium	43%	48%	49%
Large	41%	43%	41%

Web Defacement	2024	2025
Smaller	25%	28%
Medium	24%	26%
Large	21%	21%

Cyberattack Success Rate

While the total number of cyberattacks and infection rate is declining, the success rate of attacks (incidents resulting from attacks) is increasing. Canadian organizations are experiencing 20-25 incidents annually across categories like DoS, infiltration, breaches and cloud incidents.

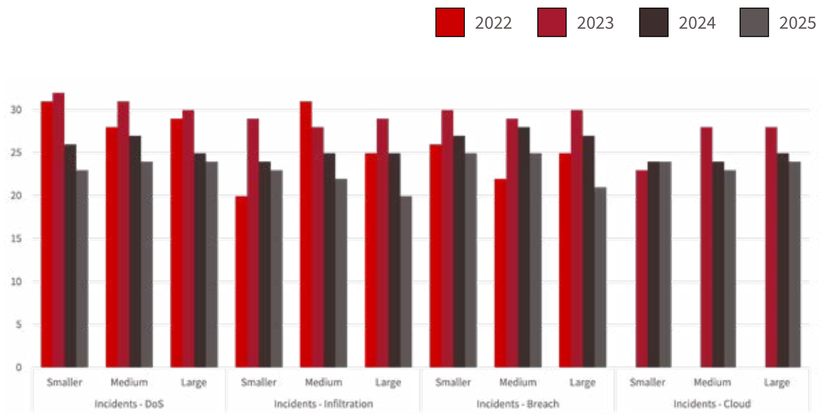
Chart 5: Number of Incidents Across Categories

Incidents – DoS	2022	2023	2024	2025
Smaller	31	32	26	23
Medium	28	31	27	24
Large	29	30	25	24

Incidents - Breach	2022	2023	2024	2025
Smaller	26	30	27	25
Medium	22	29	28	25
Large	25	30	27	21

Incidents – Infiltration	2022	2023	2024	2025
Smaller	20	29	24	23
Medium	31	28	25	22
Large	25	29	25	20

Incidents - Cloud	2022	2023	2024	2025
Smaller	-	23	24	24
Medium	-	28	24	23
Large	-	28	25	24



DoS Incidents: Medium organizations saw a slight decrease from 27 in 2024 to 24 in 2025.

Infiltration Incidents: A decline across all sizes of organizations, with small organizations reporting a drop from 24 in 2024 to 23 in 2025.

Breach Incidents: Breach incidents remained consistent for small organizations at around 25 in 2025, while larger organizations experienced a decline to 21 incidents.

The combination of a decline in attack numbers but consistent incident rates indicates that cyberattacks have become more targeted and effective, particularly against small and medium-sized organizations.

Downtime and Downtime per Incident

Downtime caused by cyberincidents remains significant but has shown improvement for some incident types. However, downtime per incident continues to grow, particularly for breaches and cloud incidents, highlighting the increasing complexity of incident resolution and lack of resilience in IT systems.

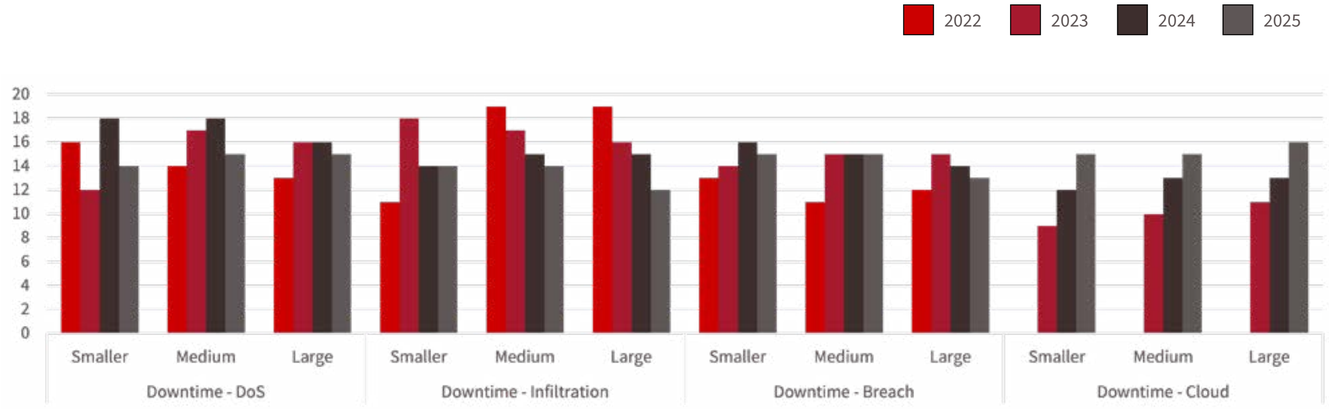
Chart 6: Average Downtime, 2022-2025 (Days)

Downtime – DoS	2022	2023	2024	2025
Smaller	16	12	18	14
Medium	14	17	18	15
Large	13	16	16	15

Downtime – Infiltration	2022	2023	2024	2025
Smaller	11	18	14	14
Medium	19	17	15	14
Large	19	16	15	12

Downtime - Breach	2022	2023	2024	2025
Smaller	13	14	16	15
Medium	11	15	15	15
Large	12	15	14	13

Downtime - Cloud	2022	2023	2024	2025
Smaller	-	9	12	15
Medium	-	10	13	15
Large	-	11	13	16



DoS Downtime: Small organizations saw a drop in downtime for DoS incidents, from average of 18 days in 2024 to 14 days in 2025.

Infiltration Downtime: Remained flat for small and medium organizations at an average of 14 days.

Breach Downtime: Small organizations experienced consistent downtime at 15 days on average, while large organizations improved from an average of 14 days in 2024 to 13 days in 2025.

Cloud Downtime: Small organizations faced increased downtime for cloud incidents, growing from 12 days on average in 2024 to 15 days in 2025.

Downtime per Incident Has Grown Significantly Year-Over-Year

Breaches: Up by 10 percent, with small organizations seeing a three percent increase.

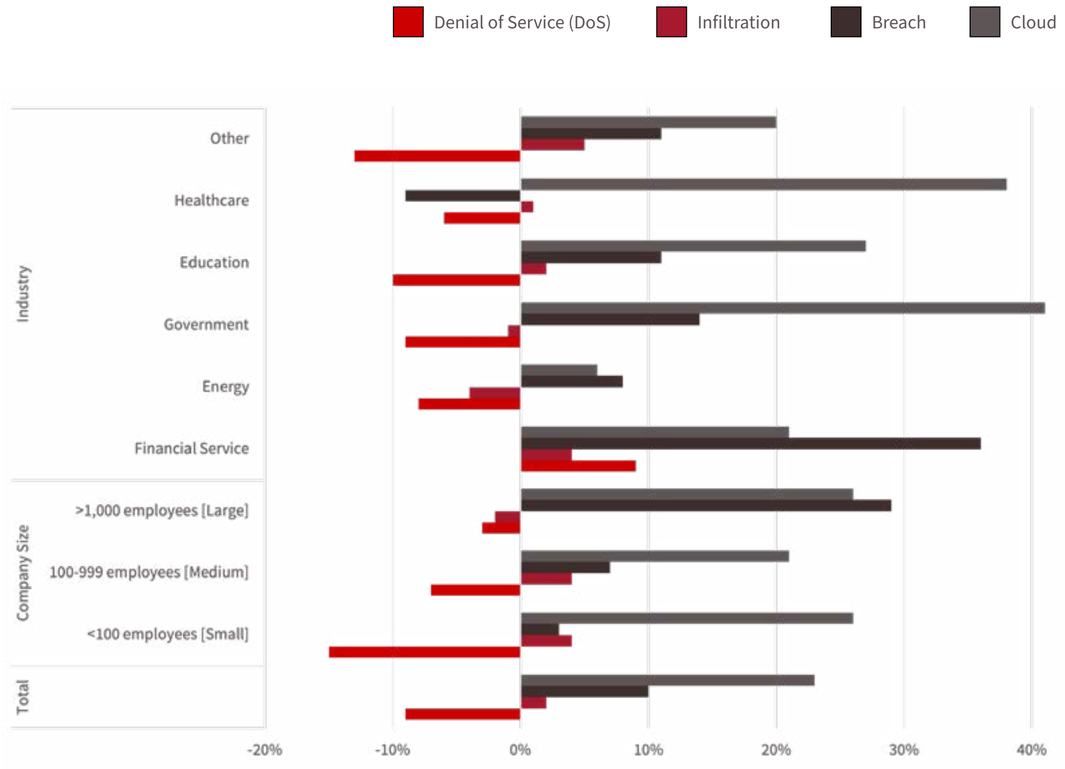
Cloud Incidents: Up by 23 percent, particularly affecting government (+41 percent) and healthcare (+38 percent) sectors.

Chart 7: Downtime per Incident YoY Increase (%)

Downtime by Industry Size	DoS	Infiltration	Breach	Cloud
Financial Service	9%	4%	36%	21%
Energy	-8%	-4%	8%	6%
Government	-9%	-1%	14%	41%
Education	-10%	2%	11%	27%
Healthcare	-6%	1%	-9%	38%
Other	-13%	5%	11%	20%

Downtime by Company Size	DoS	Infiltration	Breach	Cloud
Small	-15%	4%	3%	26%
Medium	-7%	4%	7%	21%
Large	-3%	-2%	29%	26%

Downtime YoY	DoS	Infiltration	Breach	Cloud
Total	-9%	2%	10%	23%



Maturity of Canadian Cybersecurity Programs

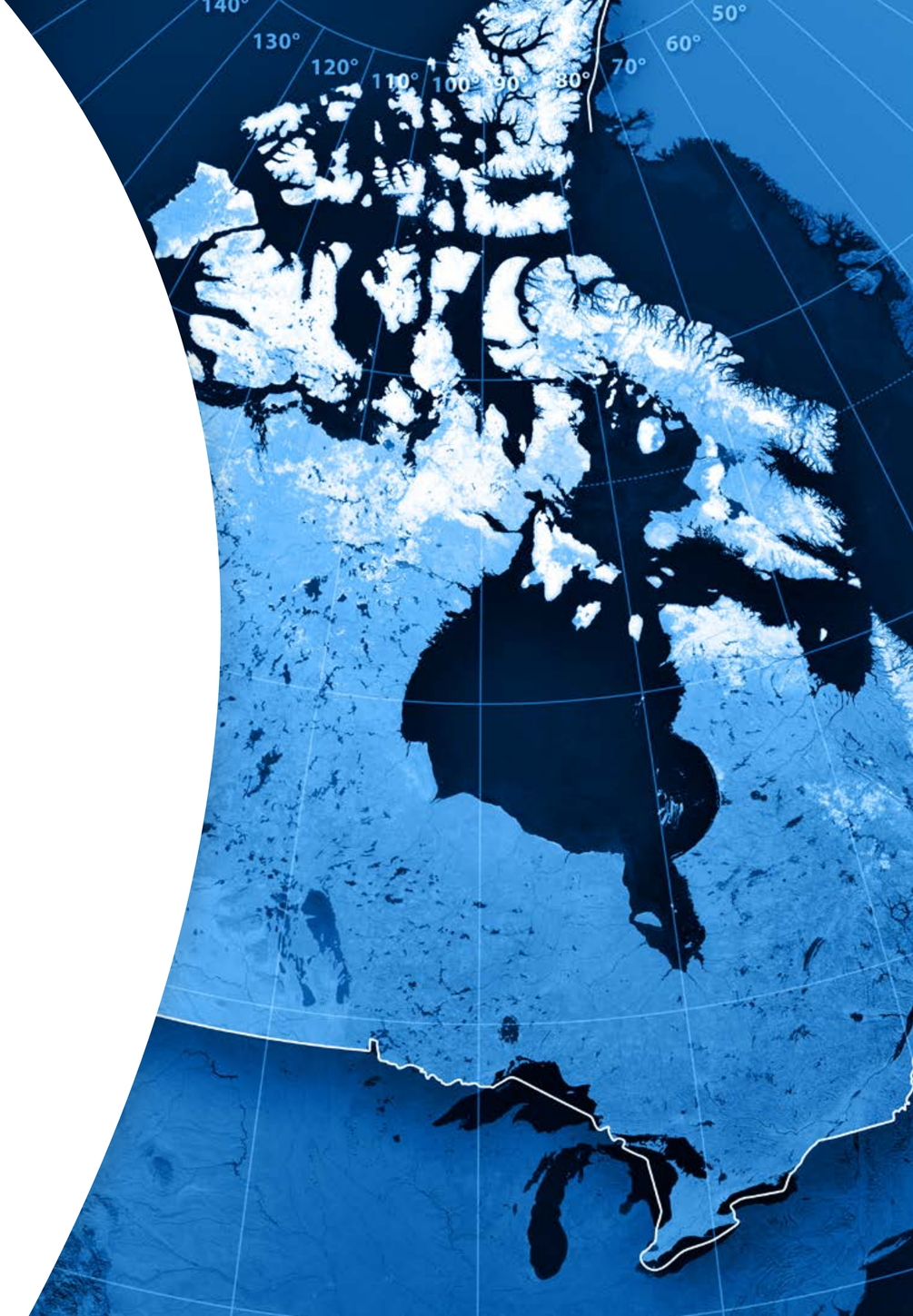
As part of the 2025 CDW Canadian Cybersecurity Study, respondents were asked to rate their organizations' maturity across ten critical cybersecurity domains, as well as their overall cybersecurity capabilities. The following groupings are listed in order, from least mature to most mature, to help organizations benchmark their current cybersecurity posture:

- Asset and Configuration Management
- Security Governance and Compliance
- Identity and Access Management
- Data Protection and Privacy
- Human Resources/Insider Threat Management
- Network Security
- Cloud Security
- Incident Detection and Response
- Business Continuity and Resilience
- Supplier and Third-Party Security

The results revealed a strong correlation between domain-specific maturity ratings and the overall maturity of an organization's cybersecurity program.

This correlation allowed us to group respondents into four distinct categories of increasing maturity: **Reactive Defence, Foundational Protection, Operational Resilience and Strategic Security.**

We will refer to these maturity categories throughout the study when analyzing key findings, to help illustrate how cybersecurity practices and outcomes vary depending on an organization's maturity level.



How the Maturity Groupings Are Defined

We categorized organizations into four cybersecurity maturity levels based on their processes, policies and alignment with industry standards:

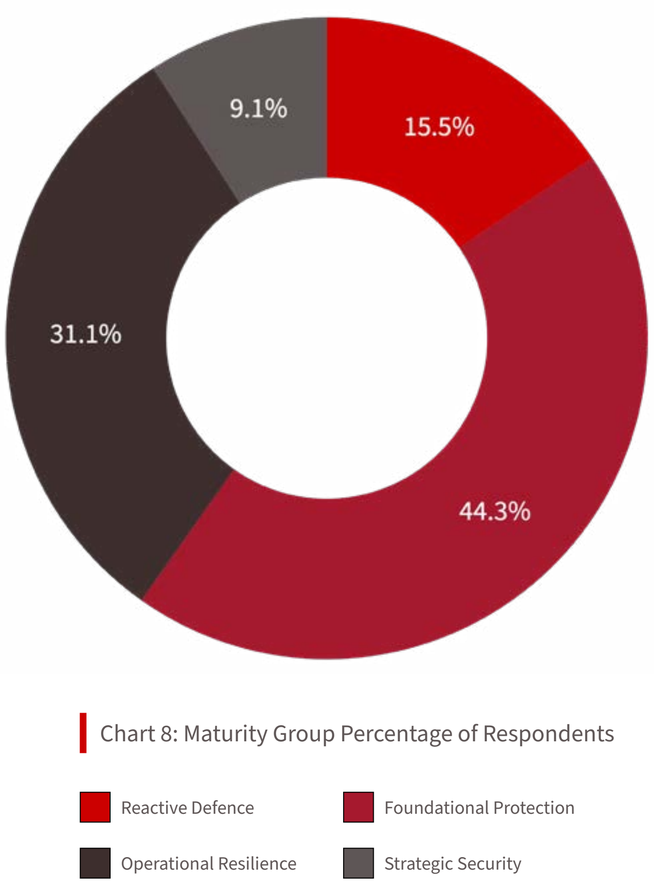
Reactive Defence: Organizations in this group have minimal or ad hoc cybersecurity processes. Their efforts lack structure, with limited documentation and inconsistent practices, leaving significant gaps in their security posture.

Foundational Protection: These organizations have established documented policies and identified process owners. They have started aligning with industry standards but face challenges in achieving consistency and scalability across their cybersecurity programs.

Operational Resilience: Organizations in this category have well-established processes that are consistently applied and aligned with recognized industry standards. They conduct regular compliance checks and periodic reviews to ensure program effectiveness.

Strategic Security: This group represents the highest level of cybersecurity maturity. Their processes are fully automated, continuously improved and regularly audited. These organizations prioritize measurable security outcomes and resilience, demonstrating a proactive approach to cybersecurity.

This maturity-based segmentation provides valuable insights throughout the study, highlighting the contrasts between organizations at different stages of their cybersecurity journey. It offers a framework for identifying areas of strength and improvement, enabling organizations to benchmark themselves and plan their next steps toward achieving optimized security.



Key Finding 1

GenAI Adoption Stalls

Canadian Organizations Struggle with Privacy, Skills and Technical Challenges, Leaving GenAI Largely in the PoC Stage

Generative AI (GenAI) holds transformative potential in automation, decision-making and innovation, reshaping industries worldwide. However, Canadian organizations face significant challenges in progressing from proof-of-concept (PoC) to full production. The study reveals that, on average, Canadian organizations conducted 17 GenAI PoCs between 2023 and 2024, yet only 28.2 percent of these PoCs transitioned into full production. This low conversion rate highlights the barriers that stall GenAI adoption and prevent organizations from fully realizing its benefits.

Barriers to GenAI Adoption

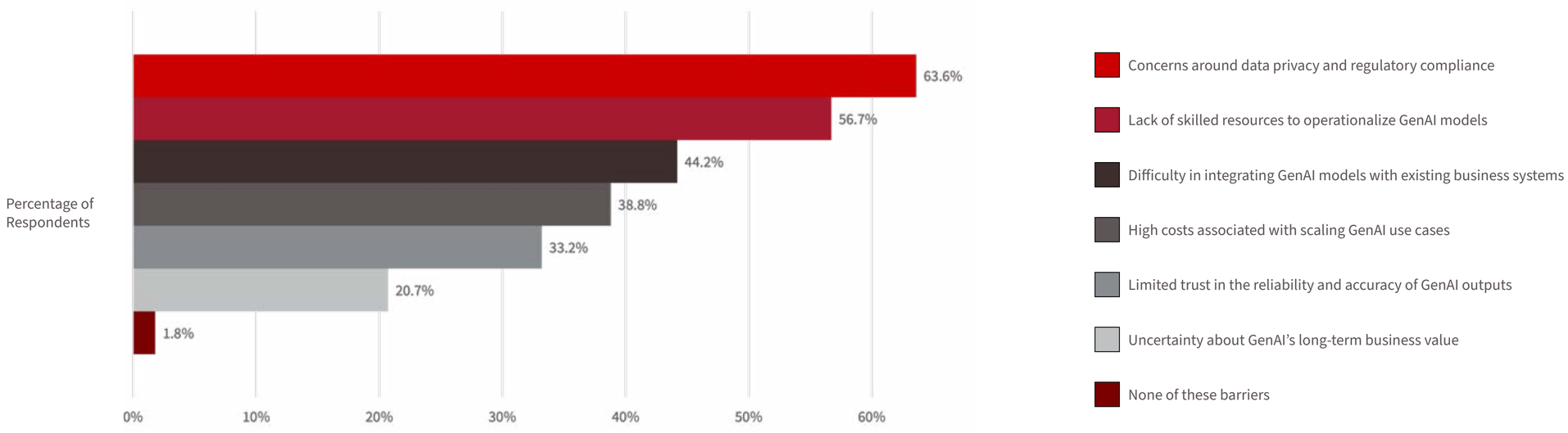
Privacy and Compliance Concerns

Data privacy and regulatory compliance were cited as the primary business barriers to moving GenAI use cases beyond the PoC stage (chart 9). Organizations, especially in regulated industries, are wary of exposing sensitive data during training and operationalization. These concerns hinder the broader adoption of GenAI models, limiting their integration into critical business processes.

Skills Gap in Operationalizing GenAI

The lack of skilled resources to develop, deploy and manage GenAI models remains a critical obstacle (chart 9). Without in-house expertise, many organizations struggle to operationalize AI initiatives effectively, resulting in stalled projects and unmet goals.

Chart 9: Barriers preventing GenAI use cases to move from PoC stage to full production



Technical Challenges

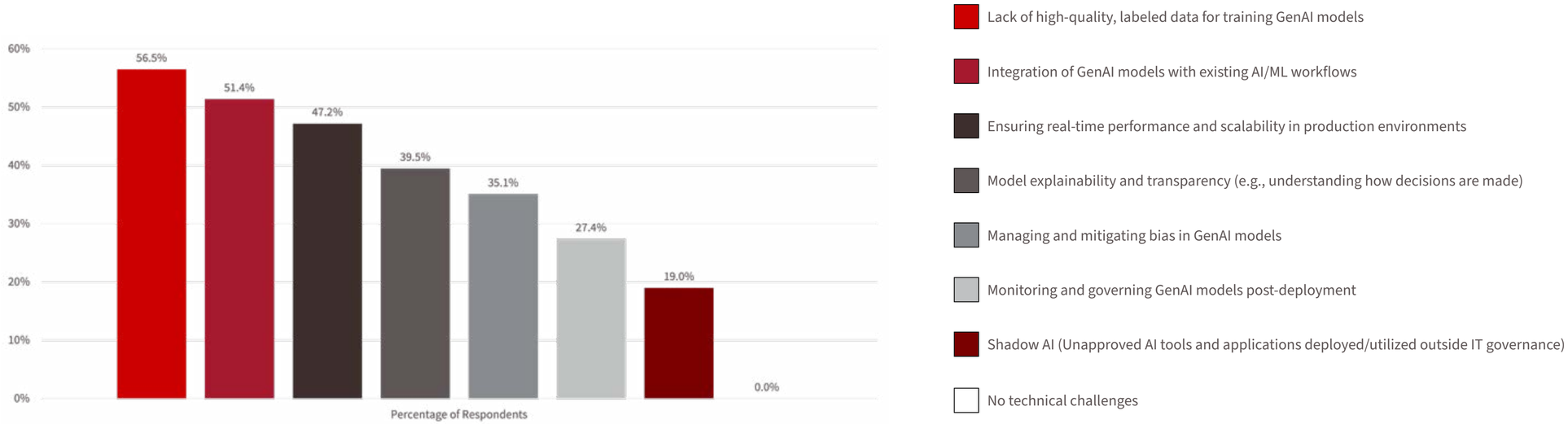
Survey respondents identified the following technical challenges as the most significant hurdles (chart 10):

- **Lack of High-Quality Labeled Data:** Poor data quality limits the accuracy and reliability of GenAI models, making them less effective in real-world applications.
- **Integration with Existing AI/ML Workflows:** Complex IT environments and legacy systems create difficulties in embedding GenAI models seamlessly.
- **Real-Time Performance and Scalability:** Ensuring that GenAI models operate efficiently at scale remains a significant challenge for many organizations.

Additional Barriers

Organizations also highlighted high costs associated with scaling GenAI use cases and limited trust in the reliability and accuracy of GenAI outputs. Concerns over potential biases and errors further deter organizations from advancing AI projects into production. (chart 10)

Chart 10: Technical challenges when implementing GenAI

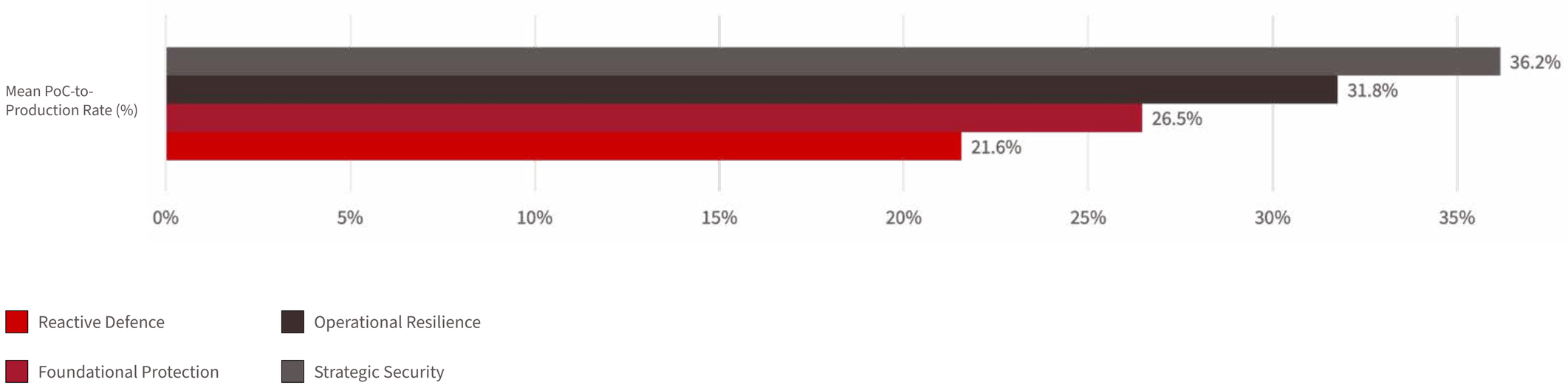


The Role of Maturity in AI Adoption

Organizations with mature security programs demonstrate higher rates of PoC-to-production transitions for GenAI use cases. The study shows that organizations in the “Strategic Security” maturity category convert 36.17 percent of PoCs into production on average, compared to just 21.56 percent for those in the “Reactive Defence” category.

Improved maturity enables organizations to address technical and operational challenges through better data governance, advanced technology integration and resource allocation. Mature programs also foster trust in AI outputs, helping organizations align AI initiatives with broader business goals more effectively.

Chart 11: Maturity Group Average PoC-to-Production Rate (%)

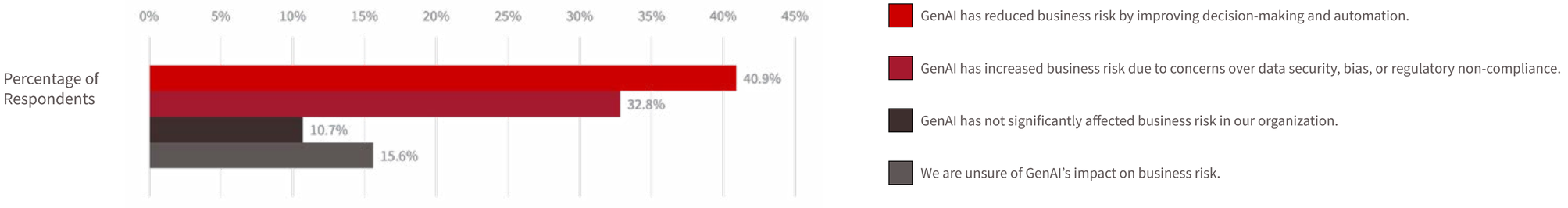


Impact on Canadian Organizations

The slow adoption of GenAI is limiting Canadian organizations' ability to harness its full potential for decision-making, automation and innovation. While 41 percent of respondents reported that GenAI has reduced business risk by improving decision-making and operational efficiency, 33 percent expressed concerns about increased risks due to data security, bias and regulatory non-compliance (chart 12).

These barriers – combined with technical challenges such as poor-quality data and integration difficulties – prevent organizations from scaling GenAI solutions and achieving competitive advantages.

Chart 12: Impact of GenAI on business risk



Conclusion

Organizations need to see the slowdown in GenAI adoption as a potential opportunity. By improving data governance frameworks, building internal AI capabilities and focusing on scalable, reliable solutions, organizations can not only accelerate the transition from PoC to production, but also overcome barriers holding organizations back, such as data governance, identity and access management, security integration and skills gaps. This is necessary work that strengthens the overall security and IT foundation. These hurdles highlight longstanding security and technical debt – issues that need to be addressed not just for AI, but for the long-term resilience of organizations.

By tackling these foundational challenges, organizations can move beyond PoCs with confidence, ensuring that AI is deployed responsibly, securely and at scale. The work being done today to align security, compliance and business objectives will ultimately enable organizations to leverage AI's full potential while minimizing risk. The delay may be a necessary step toward sustainable AI adoption and a healthier security posture overall.

Key Finding 2

Security Testing Pays Off

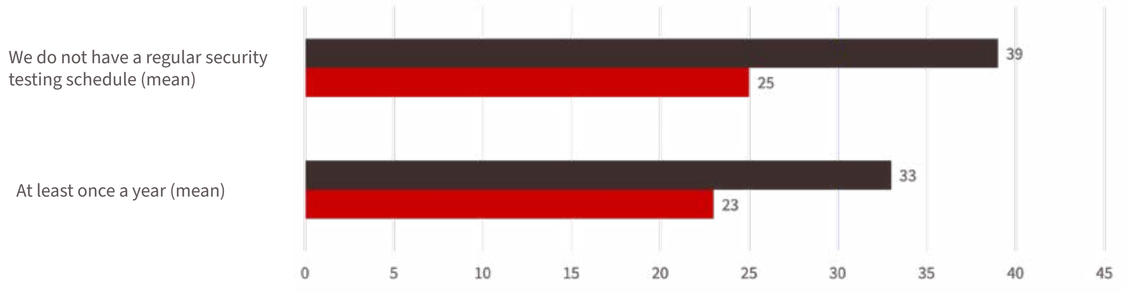
Annual Testing Reduces Breach Risk, Helping Canadian Organizations Reduce Serious Security Incidents

Security testing has consistently proven to be one of the most effective tools in reducing the risk of cyberbreaches and preventing significant security incidents. Organizations that conduct security testing (penetration testing/attack simulation) at least once a year are better equipped to identify vulnerabilities before they can be exploited. The survey reveals that organizations that perform annual security testing report fewer infiltration incidents (23 incidents on average) and fewer breaches (33 incidents on average) compared to those without regular testing schedules, who report 25 and 39 incidents, respectively. This demonstrates the tangible impact of security testing on mitigating risks and enhancing preparedness.

Chart 13: Frequency of security testing cross tabbed with average number of infiltration and data breach security incidents experienced by Canadian organizations

Infiltration (attackers gained access to the organization's network/infrastructure/data but no data was exfiltrated)

Breach (data was exfiltrated)



The Effectiveness of Penetration Testing

Penetration testing remains a cornerstone of effective security programs. According to the study, 61 percent of respondents indicated that penetration tests uncovered vulnerabilities that could have prevented past incidents, while 81 percent identified issues that could avert significant future breaches. Notably, no respondents considered penetration testing ineffective, underscoring its critical role in uncovering security gaps and fortifying defences.

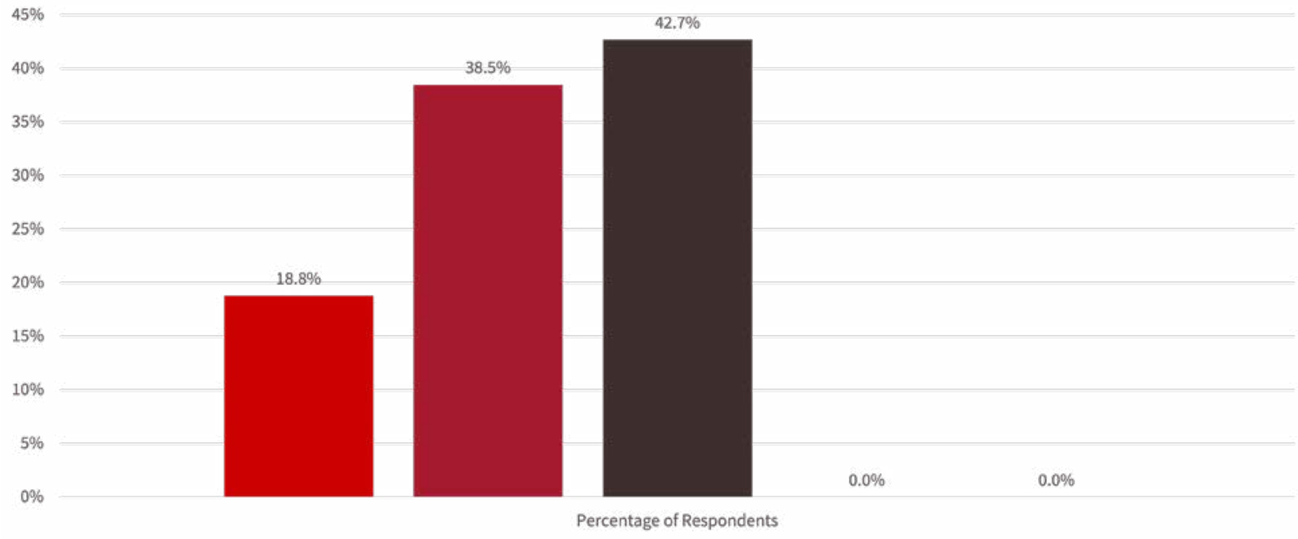


Chart 14: Effectiveness of penetration testing in uncovering vulnerabilities that prevent serious incidents

Yes – past incidents only

Yes – future potential incidents only

Yes – both past and future incidents

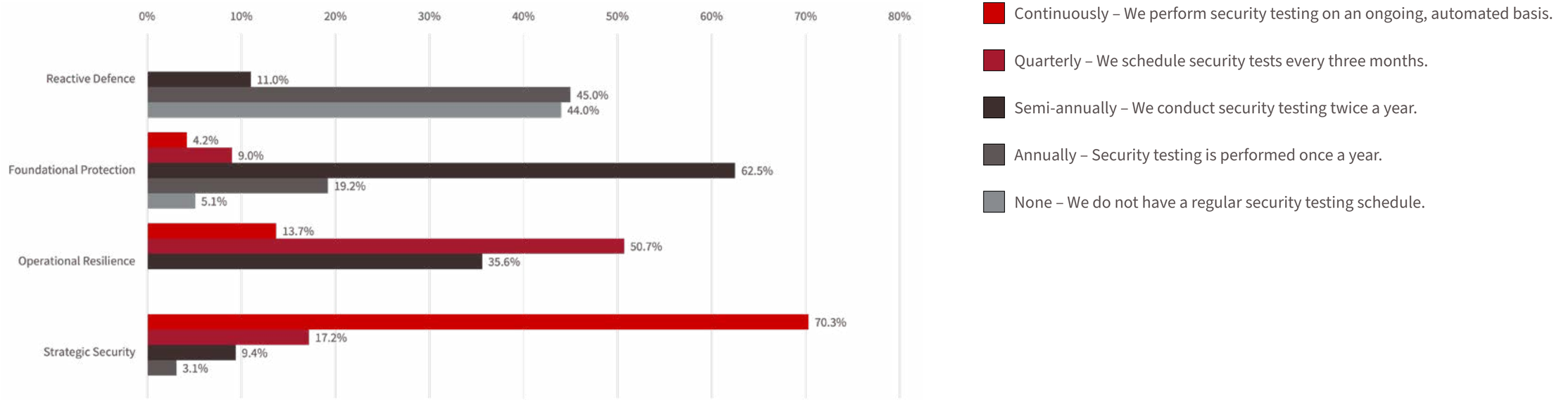
No

Not Sure

Continuous Testing: A Goal of Mature Security Programs

Continuous security testing and validation are key goals of mature security programs. The data shows that 70.3 percent of organizations in the “Strategic Security” category perform ongoing, automated testing, compared to just 13.7 percent in the “Operational” group and 4.2 percent in the “Foundational Protection” group (chart 15). Organizations conducting continuous testing can proactively detect and address vulnerabilities in real time, enabling them to adapt to modern, dynamic threat environments. By integrating security testing into agile and DevOps practices and leveraging automation, these organizations reduce reliance on manual processes, enhance efficiency and address risks earlier in the software lifecycle. This approach is critical for building resilience in today’s fast-paced cybersecurity landscape.

Chart 15: Frequency of security testing by cybermaturity



Cloud Security Testing: The Lagging Frontier

Despite nearly 100 percent cloud adoption in Canada, many organizations lag in evolving their security testing practices for cloud environments. Only 45.6 percent of respondents indicated that they use cloud-specific security testing tools and methodologies tailored to their environments. Instead, 27.6 percent continue to apply the same testing methods used for on-premises systems, while 21.4 percent rely solely on cloud service providers' built-in security testing tools (chart 16). This lack of comprehensive cloud-specific testing increases risks in cloud-native and hybrid IT infrastructures.

Moreover, the study reveals that public cloud environments are the most impacted IT components due to cyberincidents, with 60.5 percent of respondents in 2025 reporting that their cloud environments were affected. This marks a steady increase from 43.5 percent in 2022, highlighting the urgent need for more robust cloud security testing practices.

Chart 16: Approach to cloud security testing

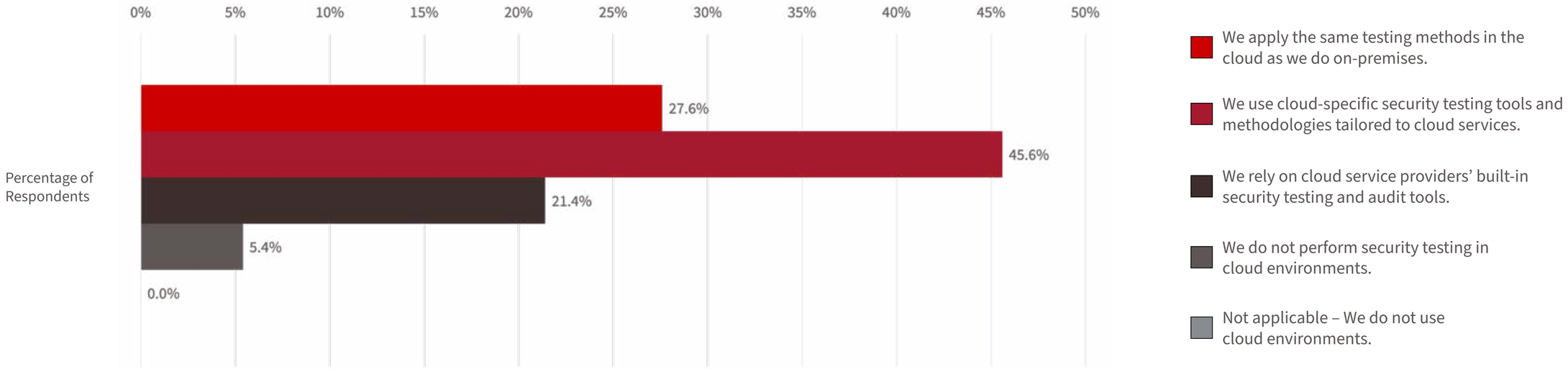
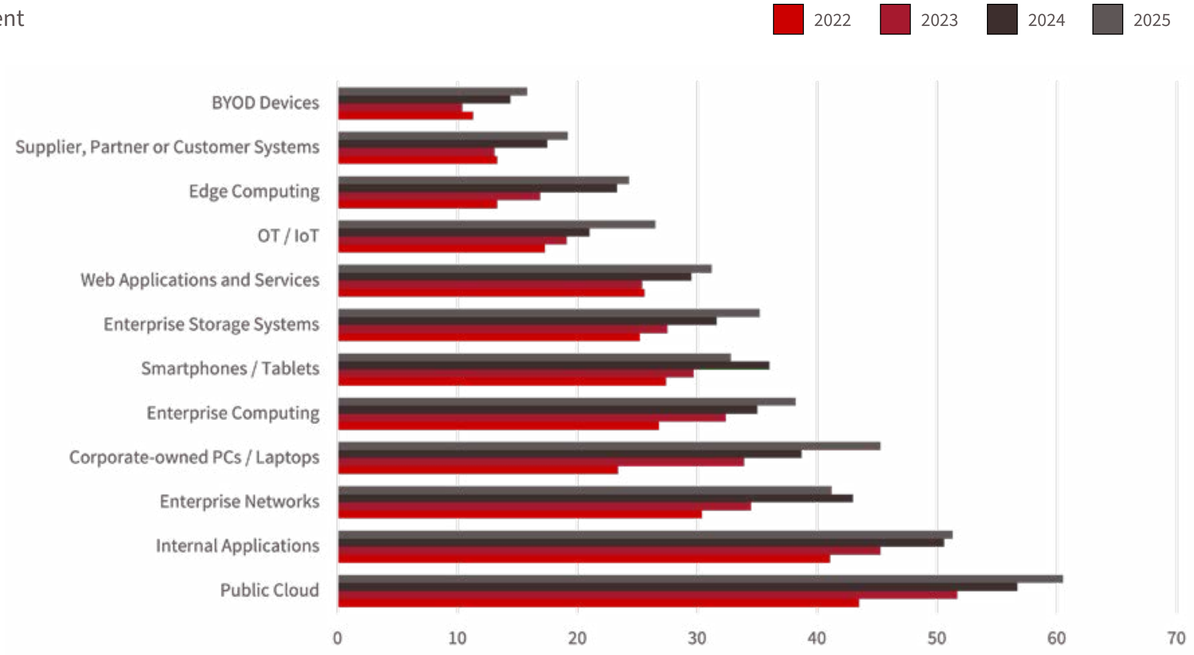


Chart 17 – Percentage of Respondents Reporting Impact to IT Components Following a Cyberincident

	2022	2023	2024	2025
Public Cloud	43.5	51.7	56.7	60.5
Internal Applications	41.1	45.3	50.6	51.3
Enterprise Networks	30.4	34.5	43	41.2
Corporate-owned PCs / Laptops	23.4	33.9	38.7	45.3
Enterprise Computing	26.8	32.4	35	38.2
Smartphones / Tablets	27.4	29.7	36	32.8
Enterprise Storage Systems	25.2	27.5	31.6	35.2
Web Applications and Services	25.6	25.4	29.5	31.2
OT / IoT	17.3	19.1	21	26.5
Edge Computing	13.3	16.9	23.3	24.3
Supplier, Partner or Customer Systems	13.3	13.1	17.5	19.2
BYOD Devices	11.3	10.4	14.4	15.8



Conclusion

Regular security testing has clear benefits for Canadian organizations, directly reducing breach risks and improving incident prevention. Organizations conducting annual or continuous testing are better prepared to identify and address vulnerabilities, strengthening their overall security posture. However, the slow adoption of cloud-specific security testing practices leaves significant gaps in protecting increasingly hybrid environments. To handle today's dynamic threat landscape effectively, organizations must embrace continuous, automated security testing tailored to their unique IT infrastructures, particularly in cloud environments. This evolution is critical to mitigate risks and ensure resilience in a rapidly changing cybersecurity landscape.

Key Finding 3

Detection and Response Get a Boost

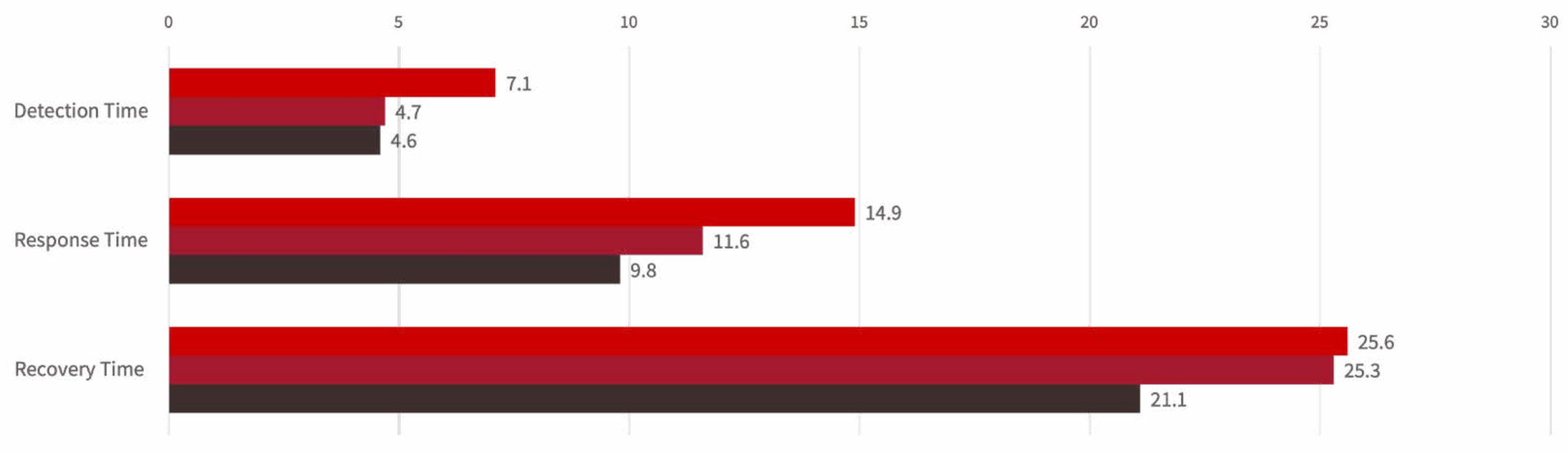
Canadian Security Teams Adopt Advanced Threat Detection Technologies, Driving Steady Improvements in Response Times

Effective threat detection, response and recovery are critical performance indicators for measuring the success of cybersecurity programs. The survey reveals that Canadian organizations are making steady improvements across all three areas, driven by the increased adoption of advanced threat detection technologies. Organizations are reporting meaningful reductions in the time it takes to detect, respond to and recover from cyberincidents.

The average time to detect cyberattacks has improved from 7.1 days in 2023 to 4.6 days in 2025, while response times have dropped significantly from 14.9 days in 2023 to 9.8 days in 2025. Similarly, recovery times have improved from 25.6 days in 2023 to 21.1 days in 2025.

These trends indicate a growing effectiveness in managing cyberthreats, allowing organizations to mitigate attacks faster and minimize operational disruptions. However, the trend is reversed for small organizations, which experienced an increase in detection times from 4.0 days in 2024 to 6.8 days in 2025, along with longer response and recovery times compared to medium and large organizations.

Chart 18: Average time to detect, respond and recover in number of days

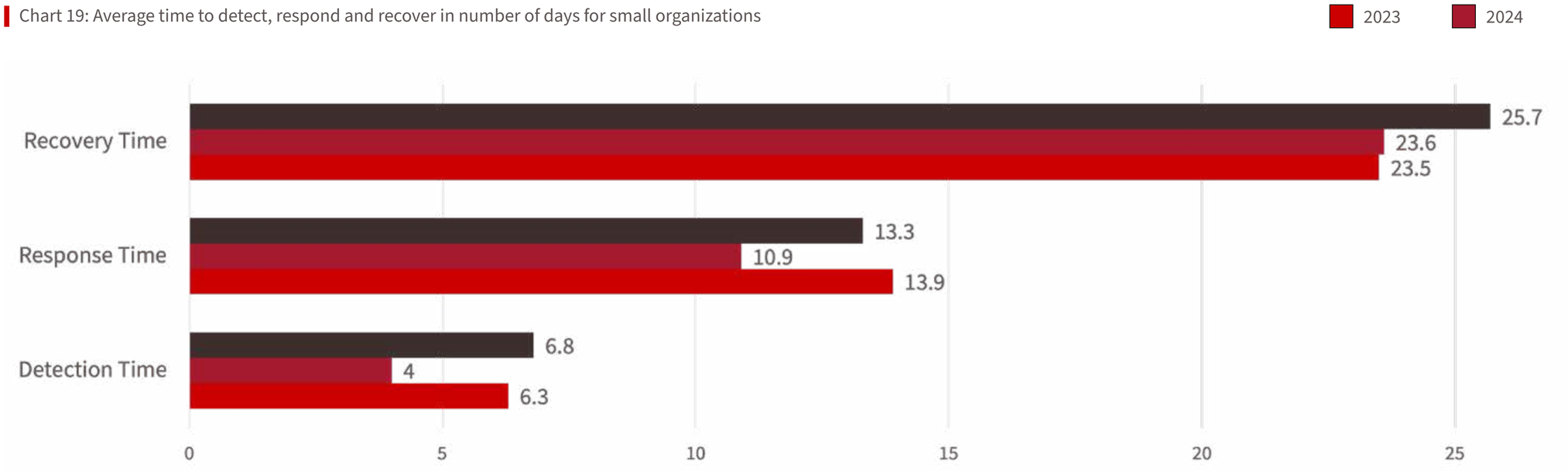


Challenges for Small Organizations

While larger enterprises are improving, small organizations (less than 100 employees) face increasing challenges in reducing detection and response times. Several factors contribute to this disparity, including:

- **Limited Incident Response Capabilities:** Small organizations often lack dedicated SOCs or security teams, relying on general IT staff with limited cybersecurity expertise, leading to delayed threat detection and response.
- **Budget Constraints and Competing Priorities:** Cybersecurity investments compete with other IT needs, limiting access to advanced security tools, personnel and automated threat response solutions.
- **Lack of Cybersecurity Awareness and Training:** Without structured security awareness programs, employees are more susceptible to phishing and social engineering attacks, increasing the likelihood of undetected threats.

Chart 19: Average time to detect, respond and recover in number of days for small organizations



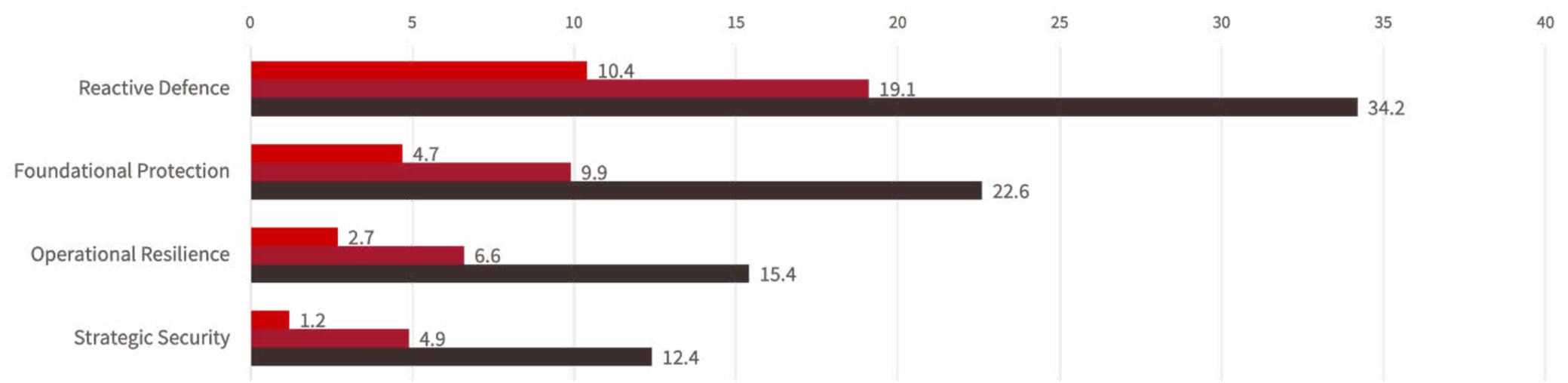
Security Maturity is a Game-Changer

The maturity of an organization's security program has a direct impact on its ability to detect, respond and recover from cyberincidents as expected. But the study shows that organizations in the Strategic Security category (our top category) detect cyberthreats nearly 10 times faster than those in the Reactive Defence (our least mature group) category (1.2 days vs. 10.4 days). The same trend applies to response and recovery times.

Mature security programs benefit from:

- Well-defined incident response processes that enable faster mitigation.
- Proactive threat detection using multilayered defence strategies.
- Advanced automation and analytics, allowing teams to react to threats in real time.

Chart 20: Average time to detect, respond and recover in number of days by cybersecurity maturity



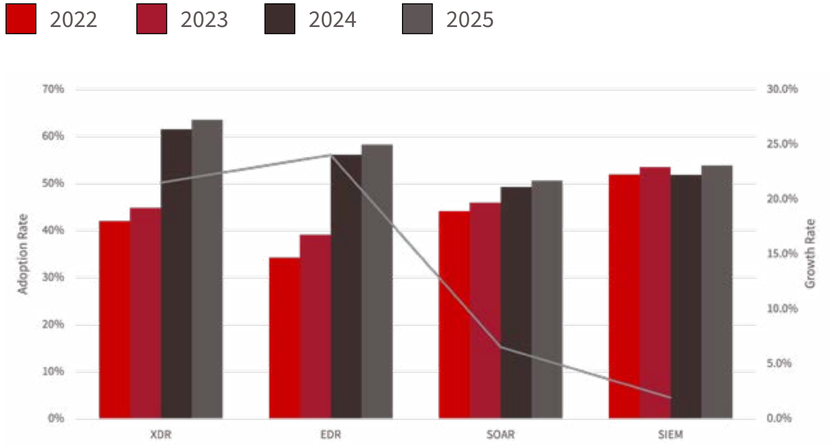
Growth in Adoption of EDR and XDR Technologies

The adoption of newer endpoint detection and response (EDR) and extended detection and response (XDR) technologies is outpacing traditional security solutions such as security information and event management (SIEM) and security orchestration, automation and response (SOAR).

Key Adoption Trends:

- XDR adoption increased from 42.0 percent in 2022 to 63.5 percent in 2025, reflecting 21.5 percent growth over four years. The sharpest jump occurred between 2023 and 2024, where adoption surged from 44.8 percent to 61.5 percent.
- EDR adoption grew from 34.2 percent in 2022 to 58.2 percent in 2025, a 24 percent increase. This growth highlights a strong shift towards endpoint-centric detection and response capabilities.
- SIEM adoption has remained relatively flat, increasing only 1.9 percent from 2022 (51.9 percent) to 2025 (53.8 percent), indicating a slower adoption curve compared to EDR and XDR.

Chart 21: Adoption rate of key detection and response technologies



Technology	2022	2023	2024	2025	Growth (2022-2025)
XDR	42.0%	44.8%	61.5%	63.5%	21.5%
EDR	34.2%	39.1%	56.1%	58.2%	24.0%
SOAR	44.1%	45.9%	49.2%	50.6%	6.5%
SIEM	51.9%	53.5%	51.8%	53.8%	1.9%

Conclusion

The steady improvement in detection, response and recovery times reflects the growing effectiveness of Canadian organizations in managing cyberthreats. The adoption of XDR and EDR is playing a pivotal role in these advancements, enabling organizations to detect and respond to threats faster than before. However, the widening gap between large and small organizations highlights a critical disparity in cybersecurity capabilities. To bridge this gap, small organizations must invest in modern security technologies and strengthen their incident response capabilities. By prioritizing security maturity and leveraging automation, Canadian organizations can further enhance their ability to mitigate threats, reduce downtime and improve overall cyber resilience.

Key Finding 4

Zero Trust in Theory, Shortfalls in Practice

Canadian Organizations Find It Challenging to Translate Strategy and Assessments into Actionable Progress

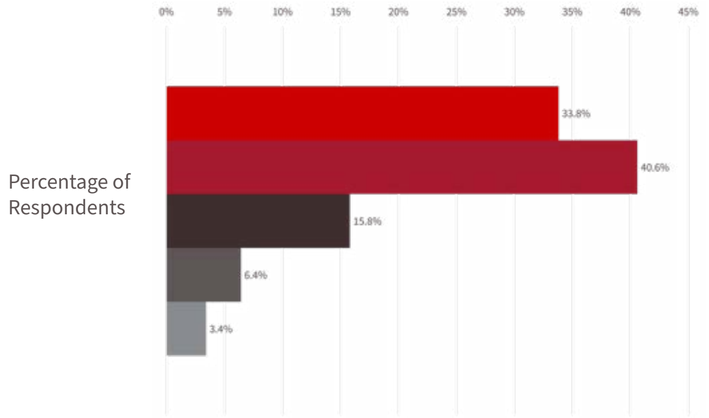
Zero trust has emerged as a cornerstone of modern cybersecurity strategies, emphasizing the principle of “never trust, always verify.” While its adoption has gained momentum across Canadian organizations, operationalizing zero trust remains a significant challenge. According to the survey findings, many organizations struggle to translate high-level zero-trust strategies and maturity assessments into actionable steps that drive tangible progress. This disconnect leaves critical gaps in security architecture, undermining the very principles zero trust is designed to enforce.

Challenges in Operationalizing Zero Trust

Gaps Between Strategy and Implementation

A significant proportion of organizations face challenges in bridging the gap between strategy and implementation. Transitions from assessment to execution often fail to define clear policy, technical or procedural initiatives, leaving security teams unsure how to advance their zero-trust journey. The disconnect between strategic and operational teams is often driven by resource constraints, competing priorities and a lack of shared understanding of business risk. These challenges can slow progress on security initiatives and make it difficult to effectively address vulnerabilities.

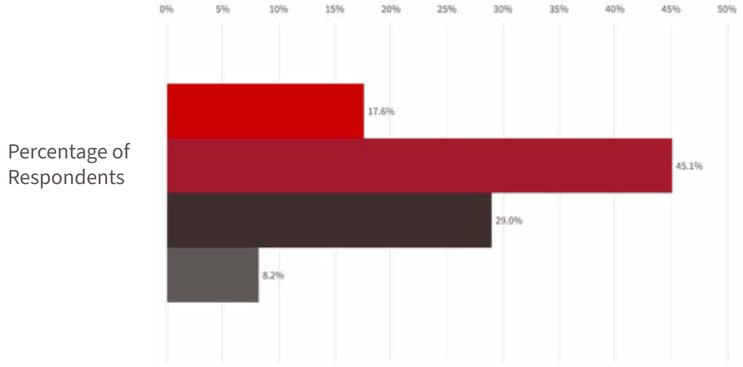
Chart 22: Zero trust strategy to implementation



From Paper to Execution or Shelfware Security

According to the survey findings, 63 percent of Canadian organizations struggle to translate high-level zero-trust strategies into actionable technical requirements (chart 22). Furthermore, while 37 percent of organizations conduct zero-trust maturity assessments, they find the resulting reports impractical or too abstract to guide action, with another 45 percent indicating that parts of the reports are useful but require additional efforts to fully translate into technical requirements (chart 23). This disconnect leaves critical gaps in security architecture, undermining the principles zero trust is designed to enforce.

Chart 23: Operational handover after cybersecurity maturity assessment

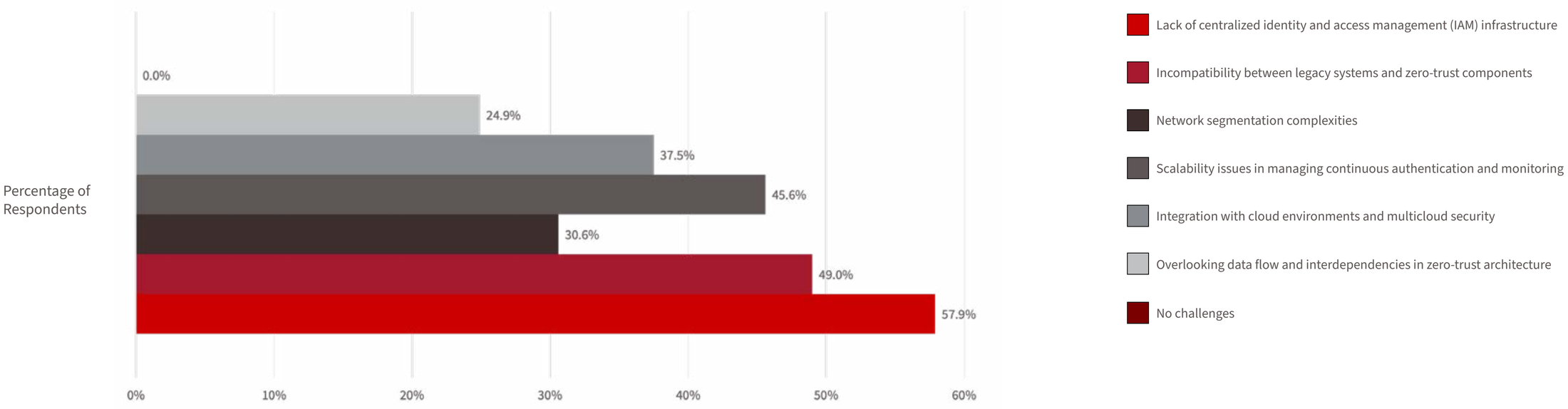


Zero Trust Gridlock - Architectural Challenges

Architectural hurdles represent another major barrier to operationalizing zero trust (chart 24). Key challenges include:

- Identity and Access Management (IAM): Misaligned IAM systems remain a primary concern for 58 percent of respondents, hindering the ability to enforce zero-trust principles effectively.
- Integration with Legacy Systems: Hybrid IT environments complicate the integration of modern zero-trust solutions, with 49 percent of organizations citing this as a significant hurdle.
- Scalability Issues: Expanding zero-trust principles across diverse systems and geographies poses challenges for 46 percent of organizations, further straining their implementation efforts.

Chart 24: Architectural challenges when implementing zero trust



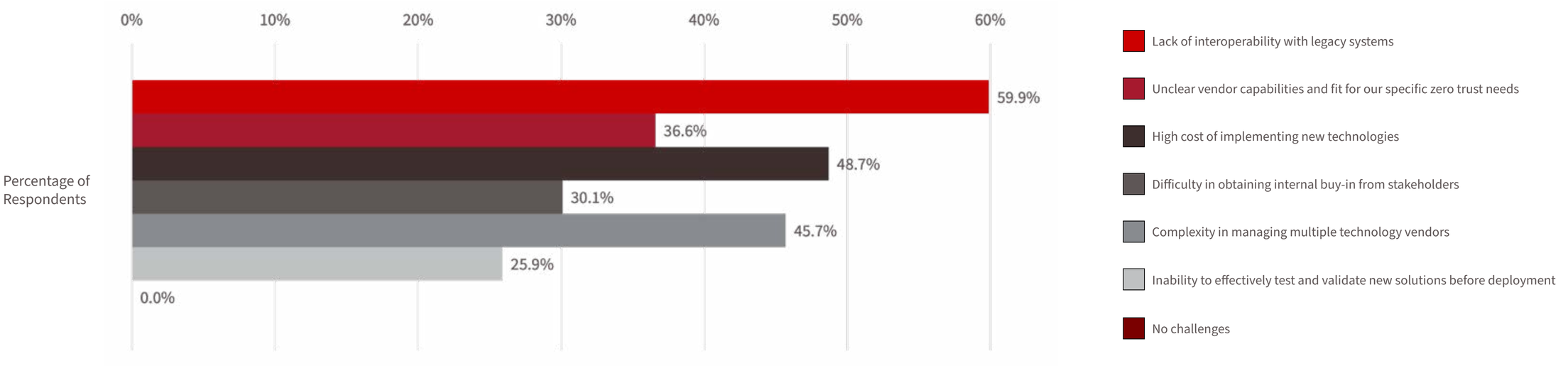
New Tech, Old Problems: Adopting New Technologies

Organizations face additional obstacles in implementing the technical backbone required for zero trust. The survey highlights several top concerns (chart 25):

- Lack of interoperability with legacy systems
- High costs associated with new solutions
- The complexity of managing multiple technologies across vendors

These challenges complicate the integration of zero-trust principles into existing IT environments, slowing progress and increasing operational strain.

Chart 25: Challenges when adopting new technologies for zero trust

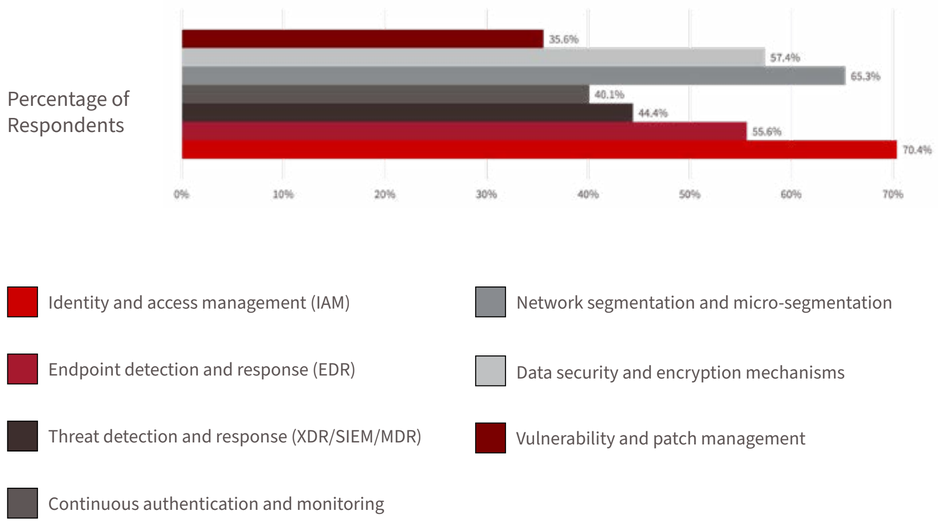


Not Cookie-Cutter Security: Customization Needs for Progress

A one-size-fits-all approach to zero trust fails due to the unique organizational structures, IT environments and compliance requirements faced by different organizations. To achieve meaningful progress, organizations must customize their zero-trust initiatives to align with their specific objectives and risk profiles. Key areas requiring customization include (chart 26):

- **Identity and Access Management (IAM):** Organizations need granular access policies and adaptive authentication mechanisms tailored to their environments.
- **Network Segmentation:** Implementing micro-segmentation without disrupting existing workflows remains a significant challenge.
- **Data Security and Encryption:** Varying data environments across organizations demand customized workflows to secure sensitive information.
- **Patch Management:** Ensuring real-time updates and proactive vulnerability management requires tailored solutions.

Chart 26: Components of zero trust that require most customization



These areas highlight the need for targeted solutions that address the specific needs of each organization while maintaining zero-trust principles.

Conclusion

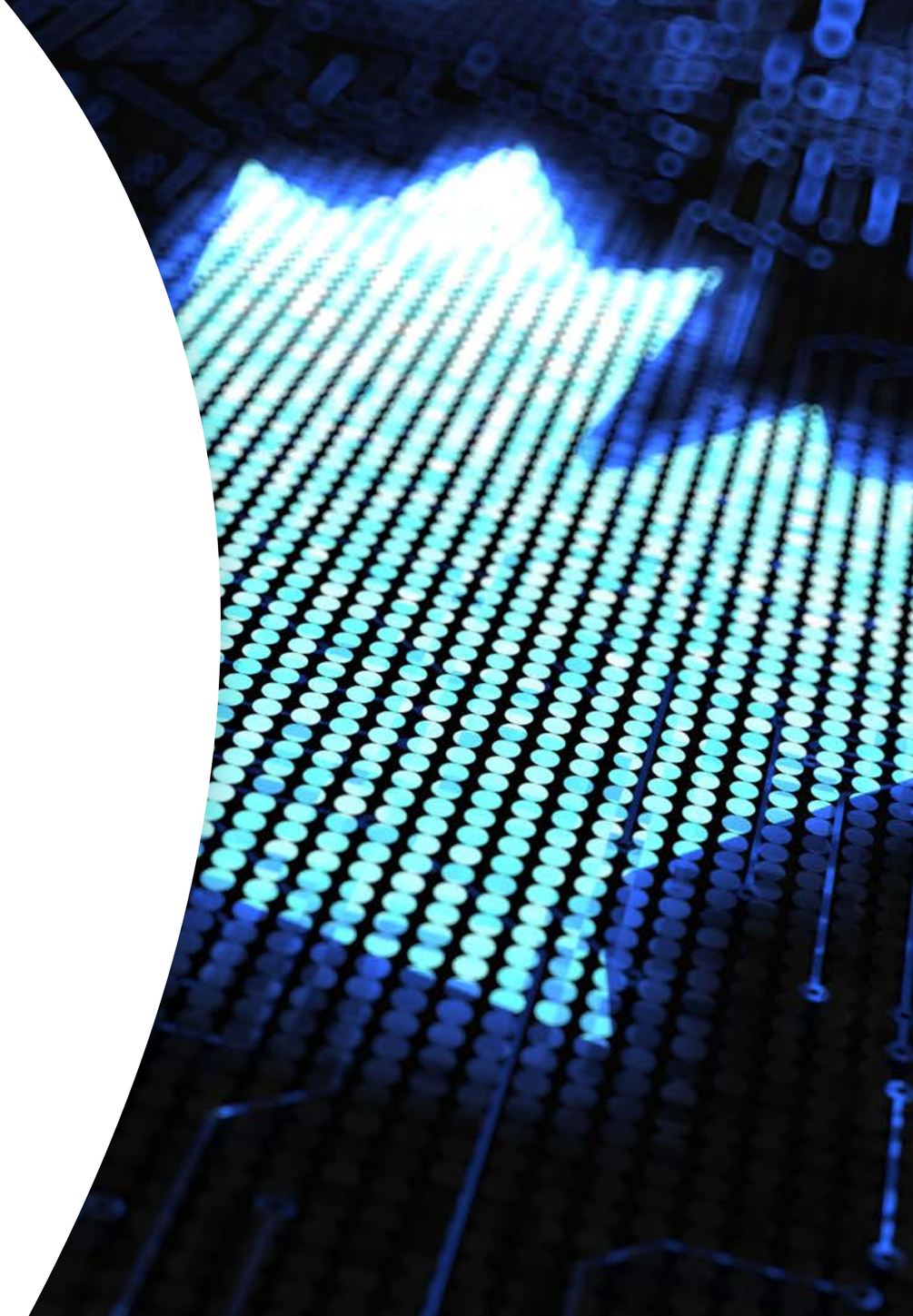
Organizations don’t have to adopt zero trust, but those who do see a lot of positive security outcomes. As we mature along with zero trust, we see that these challenges in operationalizing it have significant implications for Canadian organizations, leaving them vulnerable to cyberthreats and operational inefficiencies. Gaps in areas such as identity management, network segmentation and patch management increase security risks, while difficulties in adopting new technologies and managing vendor complexity hinder progress. The fragmented technology landscape and lack of actionable guidance amplify these issues, making collaboration with vendors and tailored solutions critical. Addressing these gaps is essential for organizations to enhance their cybersecurity posture and fully realize the benefits of zero trust.

Key Finding 5

Preventing Breaches and Accelerating Response

Canadian Organizations Turn to MDR Providers for Enhanced Threat Detection and Response Capabilities

Managed detection and response (MDR) services are becoming a cornerstone of cybersecurity strategies for Canadian organizations. With evolving cyberthreats and increasing pressure on internal security teams, organizations are seeking proactive, managed solutions to enhance their detection, response and remediation capabilities. The survey reveals that 41 percent of Canadian organizations have already adopted MDR services, while another 37 percent plan to adopt them in the near future, reflecting a clear recognition of their value in modern security programs.



Key Drivers of MDR Adoption

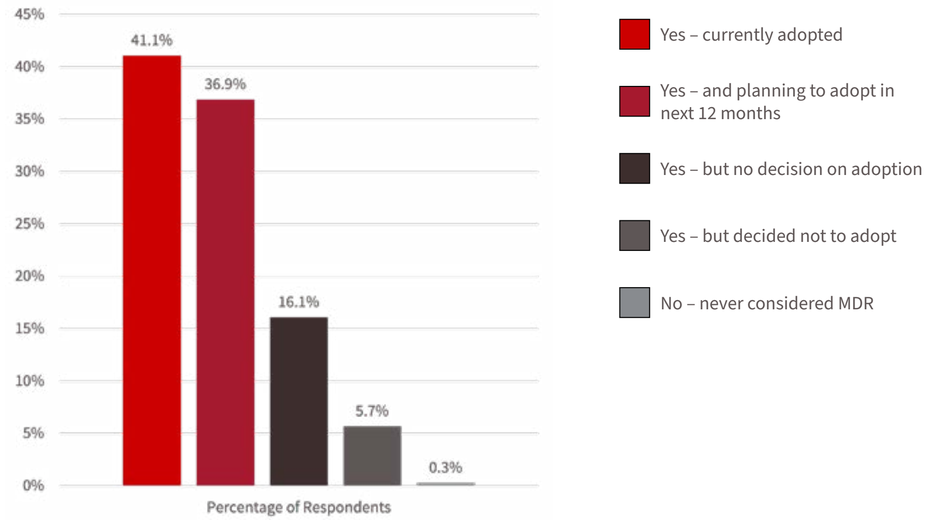
Organizations are increasingly turning to MDR services to strengthen their security posture. The top three drivers of MDR adoption include:

- Preventing and mitigating security breaches
- Improving incident response times
- Enhancing threat visibility and reporting

In addition to these primary drivers, several secondary factors are influencing MDR adoption:

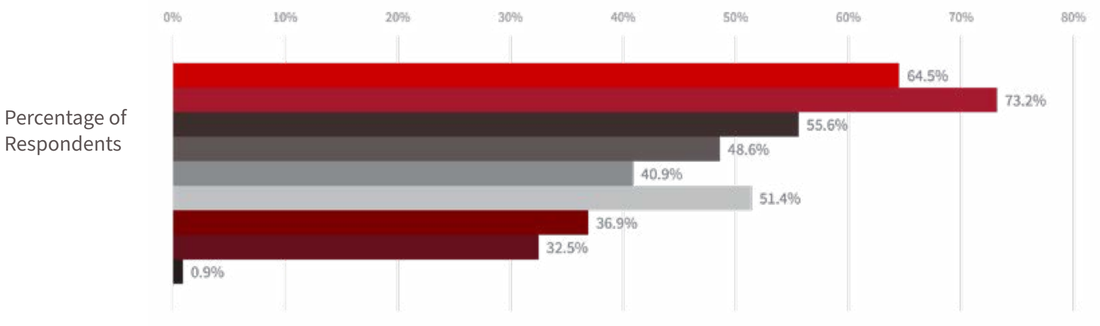
- Ensuring compliance and regulatory alignment
- Reducing operational burdens on internal teams
- Enabling continuous improvement of security posture

Chart 27: Adoption rate of MDR by Canadian organizations



Interestingly, cost savings did not rank among the top five reasons for MDR adoption, indicating that Canadian organizations prioritize security outcomes and resilience over cost reduction when evaluating MDR services. This signals a value-driven approach, where the focus is on improved security effectiveness rather than short-term financial savings.

Chart 28: Reasons for MDR adoption



The Role of Technology and Human Oversight

Leveraging GenAI to Bridge the Skills Gap

MDR providers are increasingly integrating GenAI-driven automation to reduce reliance on internal security teams, addressing the ongoing cybersecurity skills shortage. AI-powered tools enable:

- Faster threat detection and response by automating key processes
- More efficient remediation through predictive analytics and AI-driven incident management
- Reduced manual workload on security analysts, allowing them to focus on high-priority threats

Human Oversight Remains Critical

Despite advances in AI-driven threat detection, human expertise remains essential in cybersecurity operations. The study reveals that 53 percent of respondents believe that even though GenAI has boosted automation, human oversight is still necessary for most tasks. Security professionals provide:

- Contextual analysis of threats that AI alone cannot fully interpret
- Validation of AI-driven alerts to reduce false positives
- Strategic decision-making in incident response and risk management

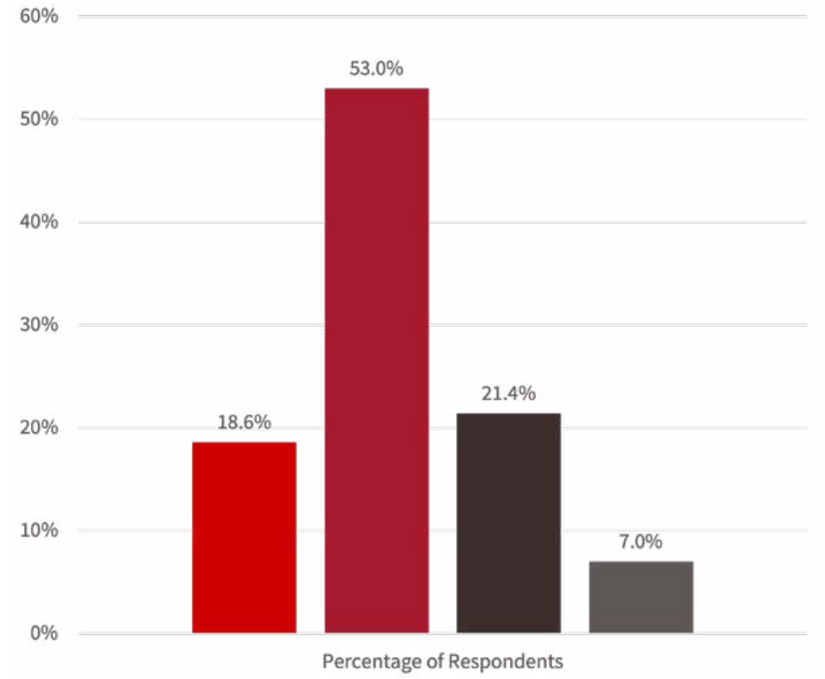


Chart 29: The extent to which GenAI has delivered the intended benefit of high automation and reduced human dependence

- Fully delivered – We have significantly reduced human intervention for routine security tasks.
- Partially delivered – Automation has increased, but human oversight is still necessary for most tasks
- Slightly delivered
- Not delivered

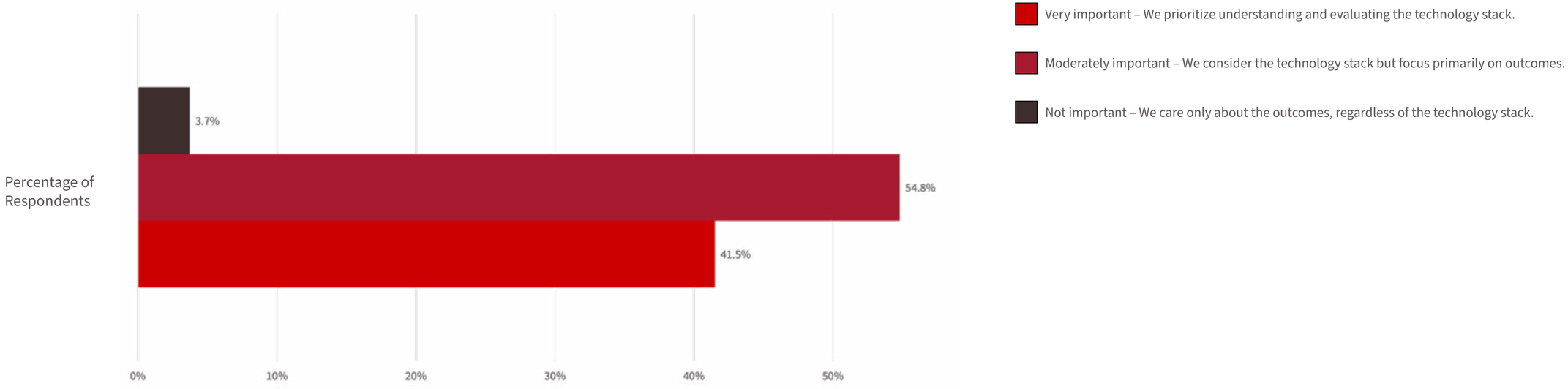
Focus on Outcomes Over Technology Stack

While MDR providers leverage various underlying technologies such as SIEM, EDR and XDR, organizations are shifting their evaluation criteria toward service outcomes rather than specific technology stacks. Nearly 55 percent of respondents state that while the technology stack is reviewed, it is not the primary decision factor. Instead, they focus on:

- Risk reduction
- Faster detection and response
- Overall security improvements

Only 41.5 percent of respondents consider the technology stack a key factor in MDR provider selection, highlighting the increasing importance of service quality over specific tools.

Chart 30: Importance of underlying technology stack while selecting the MDR provider



Measuring MDR Effectiveness

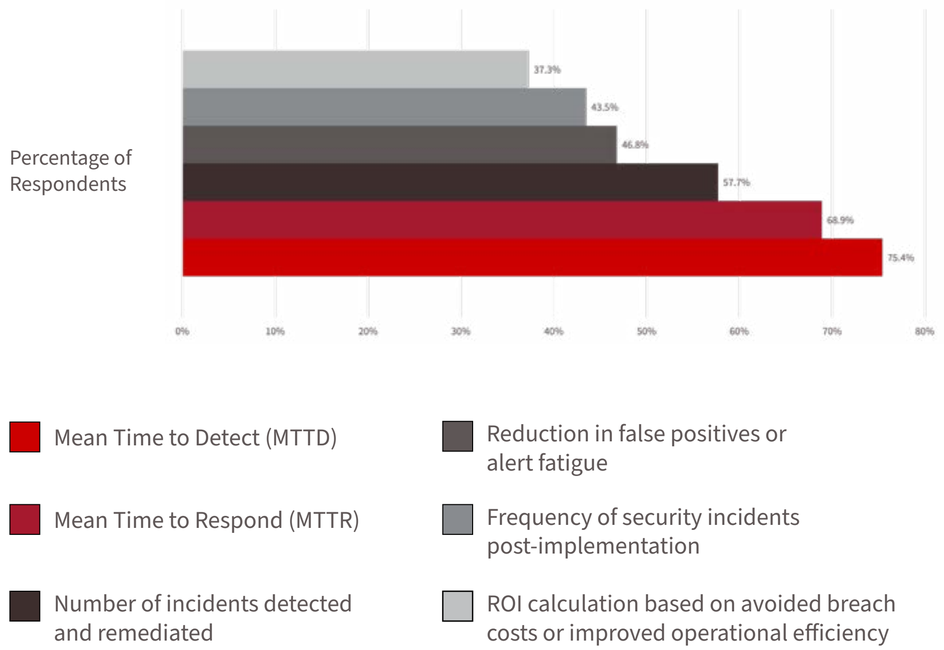
Organizations use several key performance indicators (KPIs) to assess MDR service effectiveness. The top three metrics include:

- Mean Time to Detect (MTTD): Measures how quickly threats are identified
- Mean Time to Respond (MTTR): Assesses the speed of incident containment and resolution
- Number of Incidents Detected and Remediated: Evaluates the impact of MDR services in stopping threats

Additional secondary metrics used by organizations include:

- Reduction in alert fatigue, as MDR services help security teams manage overwhelming volumes of security alerts
- Frequency of incidents before and after MDR adoption, demonstrating improvements in security outcomes

Chart 31: Metrics used by Canadian organizations to measure effectiveness of MDR service



Conclusion

The growing adoption of MDR services reflects a strategic shift among Canadian organizations to enhance their security capabilities and address resource constraints. It is the expectation of Canadian organizations that by integrating GenAI, MDR services will improve threat detection and response speeds, helping organizations mitigate risks more effectively. However, it is also the expectation that human oversight remains crucial for ensuring accuracy, context and reliability, particularly in handling complex security incidents. The shift toward outcome-driven evaluations over technology stack preferences further emphasizes the importance of service quality and measurable improvements rather than just technical specifications. This combination of advanced technology, strategic metrics and expert-driven security operations positions MDR as a critical enabler of mature cybersecurity programs in Canada.

Canadian Security Study

Recommendations

Zero Trust, Zero Excuses: Turn Strategy into Action

Zero trust has matured as a truly foundational cybersecurity strategy, but many organizations struggle to operationalize it effectively. Despite conducting zero-trust maturity assessments, organizations often find the results too abstract to guide implementation, leaving security teams without a clear roadmap. Legacy system constraints and lack of hands-on expertise further slow progress, making zero trust an ambition rather than an actionable framework. To bridge the gap between strategy and execution, organizations need a structured, systematic approach that transforms zero-trust principles into measurable security improvements.

Essential Guidance:

- **Build an End-State Design:** Establish a clear zero-trust framework that aligns security controls with business priorities, risk management and operational needs, serving as the foundation for implementation.
- **Develop Clear Implementation Roadmaps:** Convert zero-trust strategies to step-by-step action plans, assigning clear responsibilities and milestones to security teams to deliver against the end-state design.
- **Data and Application Classification:** Provide a view of data and how it's presented to users (via applications). This creates a clear role based access control (RBAC) strategy in providing information on a need-to-know basis and how to build a zero-trust validation process.
- **Conduct System Compatibility Audits:** Identify legacy system limitations that hinder zero-trust implementation and create a compensating control or an integration roadmap with vendor-supported solutions.
- **Leverage IAM Solutions:** Deploy adaptive identity and access management (IAM) controls that enable granular, context-aware access restrictions aligned with zero-trust principles including RBAC.
- **Upskill Security Teams:** Provide practical training to security teams on zero-trust enforcement mechanisms, including micro-segmentation, continuous authentication and policy-based access control against: data, application, network, device and identity pillars in the organization.

The zero-trust approach needs to go beyond being a theoretical framework – it also needs to be a practical security model that requires structured execution and continuous adaptation. Organizations that focus on implementation, training and infrastructure readiness will gain the full benefits of a zero-trust-driven security approach.

Penetration Testing: Moving to Proactive, Perpetual Protection

Annual security testing has proven its effectiveness in reducing breach risks, but organizations are now realizing that point-in-time testing is no longer enough. With evolving cyberthreats, continuous security validation is necessary to detect and remediate vulnerabilities in real time. Cloud environments, in particular, require specialized testing methodologies due to their dynamic, multitenant architectures. By automating penetration testing, embedding it into DevOps pipelines and leveraging cloud-native security testing tools, organizations can shift from reactive assessments to proactive protection.

Essential Guidance

- Automate Testing Processes: Implement continuous security testing frameworks that integrate automated vulnerability scanning, red teaming and attack simulations into routine security operations.
- Validate Cybersecurity Controls and Detection: Move beyond traditional network penetration tests and adopt cloud-native security testing approaches that account for serverless functions, object and secret storage, API security and containerized workloads.
- Integrate Testing into DevOps: Embed security tests into CI/CD pipelines, ensuring that every software deployment undergoes automated vulnerability assessments before production.
- Validate Controls through Purple Team Exercises: Conduct collaborative purple team engagements involving security operations teams to actively test and validate detection tools, security controls and incident response playbooks. This ensures that your technology is correctly configured, your staff can effectively utilize security solutions and your security operations are ready to respond effectively during real incidents.
- Collaborate with Security Providers: Work with specialized security firms or MDR providers that offer on-demand penetration testing, red teaming and attack surface management tailored to evolving threats.

Security testing must become an ongoing, automated process that evolves alongside cyberthreats. By integrating security testing into daily IT operations, organizations can stay ahead of attackers and fortify their defences in real-time.

From Chaos to Control: How Mature Security Programs Accelerate AI

Generative AI (GenAI) initiatives typically begin in the proof-of-concept stage, which provides organizations with a valuable opportunity to proactively address security, integration and operational challenges. Rather than viewing the PoC phase as a roadblock, organizations should leverage this phase to resolve foundational issues such as security debt, integration complexity and skills shortages. Addressing these challenges not only accelerates successful GenAI adoption but also significantly strengthens overall cybersecurity posture and organizational resilience.

Essential Guidance

- Resolve Security Debt Early: Prioritize foundational security practices – including asset visibility, vulnerability management and robust data governance – to ensure AI initiatives are built on secure, reliable infrastructure. Addressing security debt proactively reduces risk across the entire organization, not only within AI projects.
- Adopt Privacy-Preserving Techniques: Employ federated learning, differential privacy or encryption methods during AI training and deployment to protect sensitive data. These approaches reduce data exposure risks, enhancing privacy across all data-driven processes.
- Invest in Comprehensive Training Programs: Develop structured AI and cybersecurity upskilling programs for teams, emphasizing AI model governance, secure data handling, ethical AI deployment and threat detection. This broader skillset benefits organizational security posture beyond AI initiatives.
- Simplify Workflow Integration: Partner closely with AI and cybersecurity vendors to integrate new tools seamlessly into existing business workflows, minimizing disruption and increasing operational efficiency across the organization.
- Focus on Data Quality: Establish stringent data governance measures to ensure accuracy, integrity and bias mitigation in training data. High-quality data practices enhance decision-making, reduce security incidents and improve AI reliability.

Successfully transitioning from PoC to full-scale deployment of GenAI requires a focus on resolving broader organizational security and integration challenges. By prioritizing foundational security and operational excellence, organizations will not only unlock AI's transformative potential but also achieve lasting improvements in their overall cybersecurity and risk management capabilities.

The MDR Advantage: Faster Detection, Smarter Response, Better Security

Managed detection and response (MDR) services are becoming a critical security investment for Canadian organizations, offering enhanced threat detection, incident response and security automation. The adoption of MDR services is not technology-driven but outcome-driven – organizations prioritize reduced risk, faster threat mitigation and improved security KPIs over the specific security tools MDR providers use. Additionally, GenAI integration within MDR services has significantly improved efficiency, but human oversight remains essential to ensure accuracy and contextual decision-making in cybersecurity operations.

Essential Guidance

- Focus on KPIs: Select MDR providers based on their ability to demonstrate measurable improvements in mean time to detect (MTTD), mean time to respond (MTTR) and overall incident reduction rather than the specific technologies used.
- Leverage Advanced Technologies: Choose MDR providers that integrate GenAI, machine learning and automated threat analysis to speed up threat detection and response, while ensuring human oversight for complex decision-making.
- Prioritize Alignment with Compliance: Ensure MDR services include built-in regulatory compliance features, audit reporting capabilities and comprehensive security governance to meet industry and legal requirements.
- Incorporate Incident Response (IR): Select MDR providers that offer integrated incident response capabilities or partner closely with IR specialists. This ensures rapid, coordinated action during critical security incidents, reducing downtime and improving recovery effectiveness.
- Review and Optimize Regularly: Continuously assess MDR provider performance, conduct quarterly security effectiveness reviews and refine detection and response strategies based on real-time threat intelligence.

MDR services act as force multipliers for cybersecurity teams, filling skill gaps, automating threat response and enhancing security operations. By choosing MDR solutions based on security outcomes, regulatory alignment and AI-driven efficiencies, organizations can significantly improve their ability to detect and mitigate threats at scale.

Appendix A: Detailed Survey Results

Demographics: A sampling frame of 8,748 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 704 surveys, or a 8 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?

	%
Business/Professional Services (e.g. Legal, Accounting, Engineering, Architecture, etc.)	2.6
Personal/Consumer Services (e.g. Travel, Beauty, Personal Training, Dry Cleaning etc.)	1.8
Construction	3.1
Hospitality	2.8
IT industry	5.4
Not for profit	0.0
Manufacturing	5.8
Crown Corporation or other publicly funded organization	0.3
Education K-12	5.8
Education College/University	9.7
Financial Services	8.7

	%
Government	14.2
Healthcare	14.3
Primary (e.g. Agriculture, Mining, Forestry, etc.)	1.1
Oil & Gas or Field Services related	4.0
Retail	6.0
Communications (e.g. Cable and Telecommunications Services, etc.)	2.0
Media (e.g. Radio/TV Broadcasting)	2.0
Printing, Publishing, etc.	1.0
Transportation and Warehousing	3.1
Utilities	3.4
Wholesale and Distribution	2.8

Does your company have headquarters in Canada -- and if so, which of the following areas is it headquartered in?

	%
Not headquartered in Canada	4.0
Western and Central Canada (BC, AB, SK, MB)	15.9
Ontario	30.3
Quebec	25.1
Atlantic Canada (NB, NS, NFLD, PEI)	16.8
North (Yukon / Northwest Territories / Nunavut)	8.0

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

	%
C-level Executive Management excluding IT	9.8
Line of Business Management excluding IT	4.0
C-Level IT including CIO/CTO/CSO/CISO	7.2
Finance/Accounting	5.0
IT/IS/MIS/Data Centre/IT Security	63.1
Legal/Compliance/Risk	10.9

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

	%
Directing the IT function	38.2
Improving/Managing IT security	100.0
Setting IT priorities	43.5
Managing IT budgets	41.3

We make technology work so people can do great things.

CDW Canada Corp. is a leading provider of technology services and solutions for business, government, education and healthcare. Established in 2003, CDW Canada is the country's trusted advisor for cybersecurity, hybrid infrastructure and digital transformation. CDW Canada experts design, orchestrate and manage customized services and solutions, making technology work so people can do great things. Through its services-led approach, CDW Canada simplifies complex technology to empower customers to focus on their business and thrive in a rapidly evolving landscape. CDW Canada is a wholly owned subsidiary of CDW Corporation (Nasdaq: CDW), a Fortune 500 company.

For more information about CDW, please visit CDW.ca

International Data Corporation (IDC) is the premier global market intelligence, data and events provider for the information technology, telecommunications and consumer technology markets. With more than 1,300 analysts worldwide, IDC offers global, regional and local expertise on technology and industry opportunities and trends in over 110 countries. IDC's analysis and insight help IT professionals, business executives and the investment community make fact-based technology decisions and achieve their key business objectives.

IDC document reference #US53206325