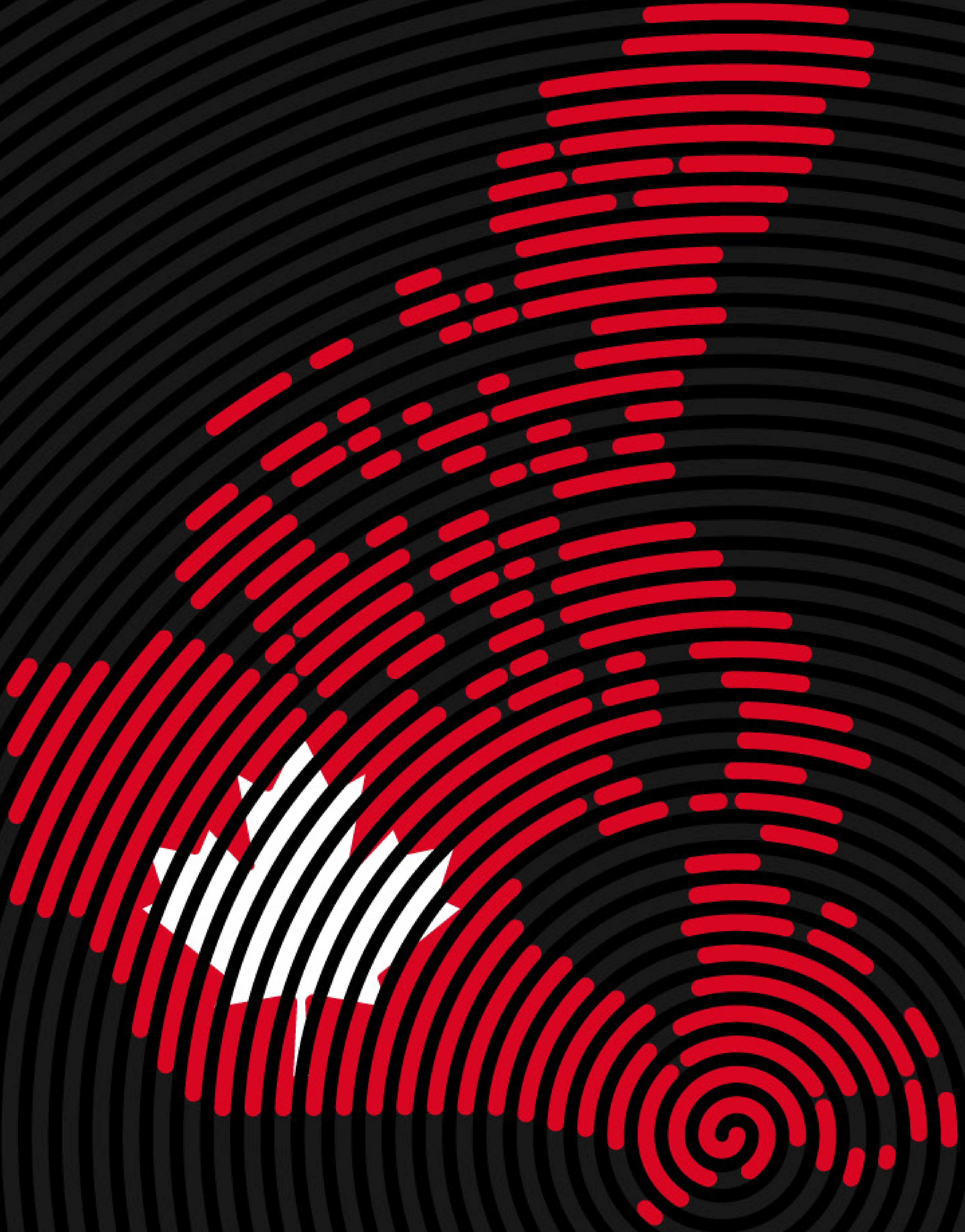
Building Smarter: Strengthening Cybersecurity Defences Across Canada’s Education Sector

How educational institutions are exploring actionable guidance and key trends shaping cybersecurity in Canada.



Education Edition A companion to 2025 CDW Cybersecurity Study

Introduction

Canadian educational institutions are navigating a critical inflection point. While the frequency of cyberattacks in the education sector is around 229 incidents annually, close to the national average of 241, the consequences for learning environments can be far more disruptive. Constrained budgets, competing system priorities and limited executive oversight are impeding the sector's ability to safeguard digital infrastructure. This comes at a time when digital systems now support every aspect of modern learning, including curriculum delivery, attendance tracking, individualized support and the protection of sensitive student records.

The CDW 2025 Canadian Cybersecurity Study highlights that, amid accelerated digital adoption and hybrid learning models, foundational weaknesses in cyber resilience now threaten not only data integrity, but also learning continuity, student safety/privacy, equity and the operational stability required to deliver effective education.

Security budgets are under pressure: 36.7 percent of education sector respondents described their budgets as inadequate to even cover essential operations, compared to just 16.6 percent respondents across industries. Leadership involvement also lags, with education reporting the lowest levels of executive engagement in building cybersecurity culture.

These challenges are reflected in outcomes: 96.3 percent of educational organizations reported suffering negative impacts due to cyberattacks, one of the highest rates across industries. Meanwhile, key performance indicators such as mean time to detect (MTTD), mean time to respond (MTTR) and mean time to recover (MTTRc) have worsened over the past year.

Despite these headwinds, the education sector is still investing in GenAI experimentation and MDR services, recognizing that stronger technology adoption and operational rigour are critical to resilience. The following key findings explore key trends shaping cybersecurity in education and provide actionable guidance for closing the gap.

Key Finding 1

GenAI Adoption Gains Traction, but Full Integration Remains Elusive

The education sector is showing interest in GenAI, conducting an average of 16 PoCs involving significant GenAI use cases. However, only 28.6 percent of these PoCs have made it into full production, highlighting persistent operational challenges.

Top barriers preventing broader GenAI deployment include:

- Concerns around data privacy and regulatory compliance.
- Lack of skilled resources to operationalize GenAI goals.
- Difficulty integrating GenAI models with existing AI/ML systems.

When asked about the impact of GenAI on business risk:

- 52.3 percent believe GenAI has reduced risk by improving decision-making and automation.
- 26.6 percent believe it has increased risk due to security, bias or compliance concerns.
- 6.4 percent believe it has had no significant impact.

Despite these challenges, several high-value use cases are emerging in security operations, including real-time threat detection, AI-assisted incident response, cyber risk identification, compliance automation and precision threat hunting.

Key Finding 2

MDR Adoption Rises to Strengthen Detection and Response

Managed detection and response (MDR) services are rapidly gaining traction in education. 45.9 percent of education sector respondents reported MDR adoption, with another 37.6 percent planning to adopt within the next 12 months.

Primary drivers for MDR adoption include:

- Improving the ability to prevent or mitigate security breaches.
- Reducing incident response time.
- Enhancing visibility into security threats.

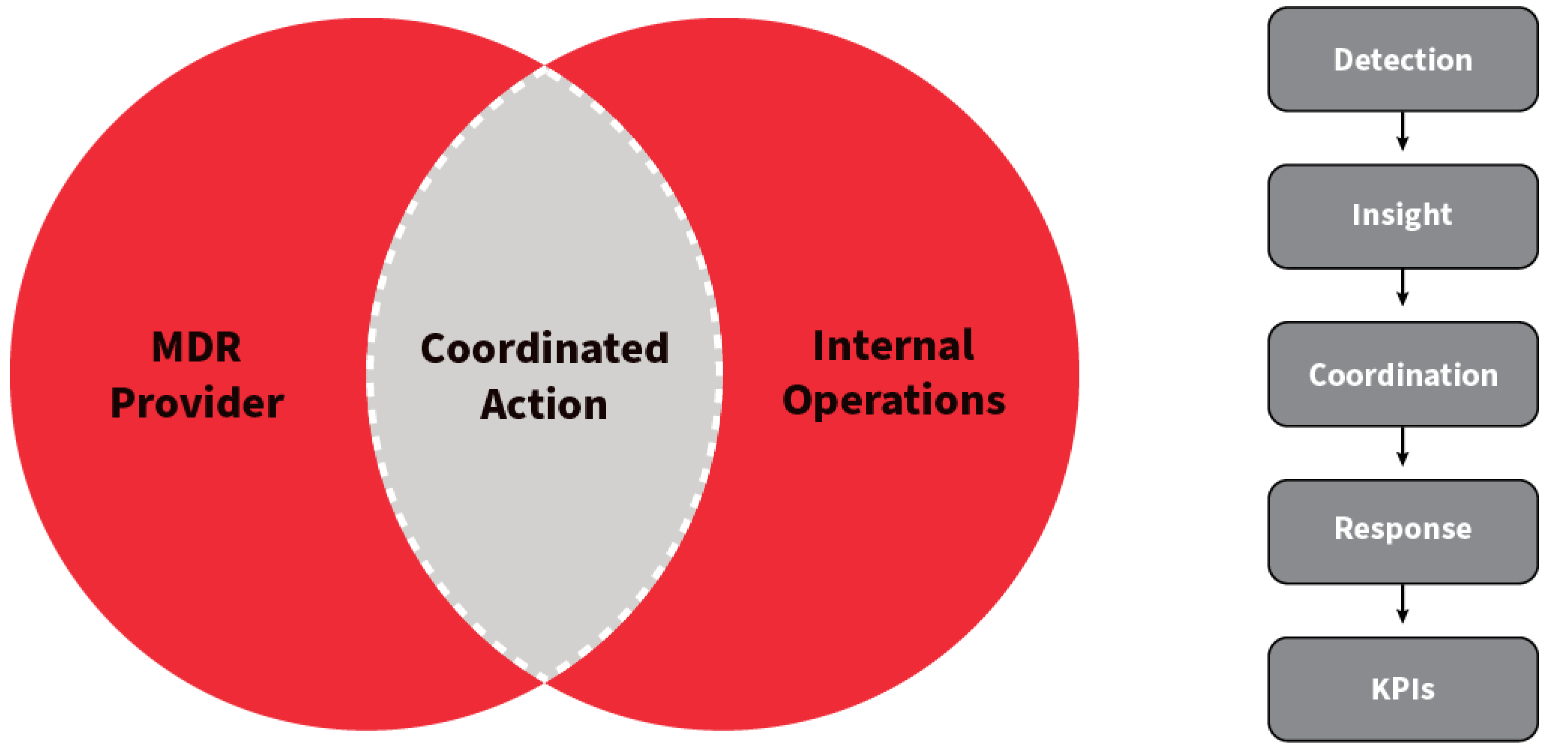
Despite higher MDR adoption, worsening security KPIs reveal challenges in execution:

- MTTD increased from 5.25 days to 6.33 days.
- MTTR increased from 11.48 days to 12.22 days.
- MTTRc improved slightly, from 26.27 days to 25.64 days.

This divergence suggests that while MDR is being deployed, integration into broader IT and security operations is lacking. To drive tangible improvements, MDR providers must be aligned not only with internal response protocols but also with day-to-day operational workflows, ensuring that detection insights lead to timely, coordinated action. Clear KPI-driven management is essential to realizing the full value of MDR investments.

Bridging the MDR Integration Gap

MDR alone is not enough – integration and accountability are key to success.



What MDR Brings to the Table:

- 24/7 Monitoring
- Threat Detection & Alerting
- Investigation & Triage
- Threat Intelligence
- Incident Escalation
- Response Recommendations
- Detection Engineering
- Reporting & Compliance Support

What Still Needs to be Handled In-House or with an MSP:

- Identity Management
- Patch Management
- Network Configuration
- Endpoint Remediation
- Business Impact Analysis
- Communication & Legal
- KPI Governance

Key Finding 3

Security Testing is Infrequent, Leaving Critical Gaps

Security testing practices in education lag behind those in other industries. 35.8 percent of education respondents admitted they either perform security testing annually or only on an ad hoc basis – the poorest cadence among industries surveyed.

Compounding the issue, many education organizations are not tailoring their testing approaches for cloud environments. Only 48.6 percent report using cloud-specific security testing tools and methodologies. A further 20.2 percent rely solely on their cloud provider’s built-in tools and 26.6 percent continue to apply the same testing methods used for on-premises systems, approaches that often fail to detect cloud-native vulnerabilities. This misalignment increases the risk of undetected gaps in hybrid and multicloud deployments.

This lack of frequent testing, combined with failure to adapt testing methodologies for cloud environments, leaves vulnerabilities undiscovered for longer periods. However, when testing is conducted:

- 100 percent of education respondents reported that penetration testing helped uncover vulnerabilities that could have prevented incidents.
- 71.9 percent believe that past incidents could have been avoided if vulnerabilities had been identified earlier.

The data highlights a missed opportunity: while penetration testing is clearly effective, infrequent testing schedules undermine its full value. Improving testing frequency could serve as a simple, high-impact step toward strengthening the education sector’s resilience against targeted threats.

Key Finding 4

Translating Zero Trust Strategy into Action Remains a Major Hurdle

Zero trust remains an aspirational goal for the education sector but translating it into practice is a significant challenge. 34.9 percent of education respondents – by far the highest across all industries – reported an inability to convert zero-trust strategy into actionable technical requirements.

Key architectural challenges cited include:

- Lack of centralized IAM infrastructure.
- Incompatibility between legacy systems and modern zero-trust architectures.
- Difficulties integrating zero-trust principles across multicloud environments.

Further compounding the issue:

- 54.4 percent of education respondents indicated operational handovers after maturity assessments were ineffective (vs. 37.2 percent across industries).
- Customization needs were also higher, with IAM, data security and network segmentation identified as the top areas requiring tailored strategies.

The gap between strategy and execution exposes education institutions to risks, particularly as reliance on cloud services and digital learning platforms continues to rise.

Essential Guidance for Education Security Teams

To meet the urgent challenges facing the sector, educational organizations should prioritize the following focused actions:

Reinforce Security Testing Cadence: Increase the frequency of vulnerability assessments and penetration testing to at least a quarterly cycle. Regular testing will help surface and address key risks proactively before attackers exploit them.

Strengthen MDR Integration with KPIs: Define success metrics such as MTTD, MTTR and incidents remediated when adopting MDR services. Regularly review MDR performance to ensure that service delivery translates into measurable operational improvements (inside and outside the security purview).

Operationalize GenAI with Governance in Mind: Ensure that GenAI deployments are supported by strong data governance, privacy controls and integration frameworks. Focus initial efforts on security use cases like threat detection and incident response to demonstrate value while controlling risks.

Tackle Zero-Trust Execution Gaps: Develop clear technical roadmaps that move beyond strategy documents. Assign ownership for IAM modernization, multicloud integration and network segmentation to accelerate tangible progress on zero-trust initiatives.

Elevate Cybersecurity to Executive Priority: Encourage district leadership and school boards to formally recognize cybersecurity as critical to institutional resilience and educational continuity. Link security investments to student data protection, operational risk reduction and compliance with provincial guidelines to ensure cybersecurity becomes a shared responsibility, not just an IT concern.

Conclusion

The Canadian education sector faces an increasingly complex cyberthreat environment, compounded by budget pressures, skill shortages and operational challenges. However, opportunities for improvement are within reach. By embedding frequent security testing, operationalizing MDR effectively, translating GenAI potential into production use cases and closing the gap on zero-trust execution, educational organizations can significantly enhance their resilience.

Improving resilience will require intentional collaboration across IT, cybersecurity and education leadership, with each playing a defined role in securing the systems that support teaching and learning. The return on this investment is not only institutional credibility, but the sustained delivery of safe, equitable and uninterrupted education for all students.

Download the 2025 CDW Canadian Cybersecurity Study

For the full findings and detailed recommendations download the full 2025 CDW Cybersecurity Study: **CDW.ca/cybersecuritytrends**

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