CDW

Canada's Prescription for Cybersecurity

How Healthcare Organizations Are Tackling Threats with AI, Security Testing, Zero Trust and MDR

Healthcare Edition A companion to 2025 CDW Cybersecurity Study

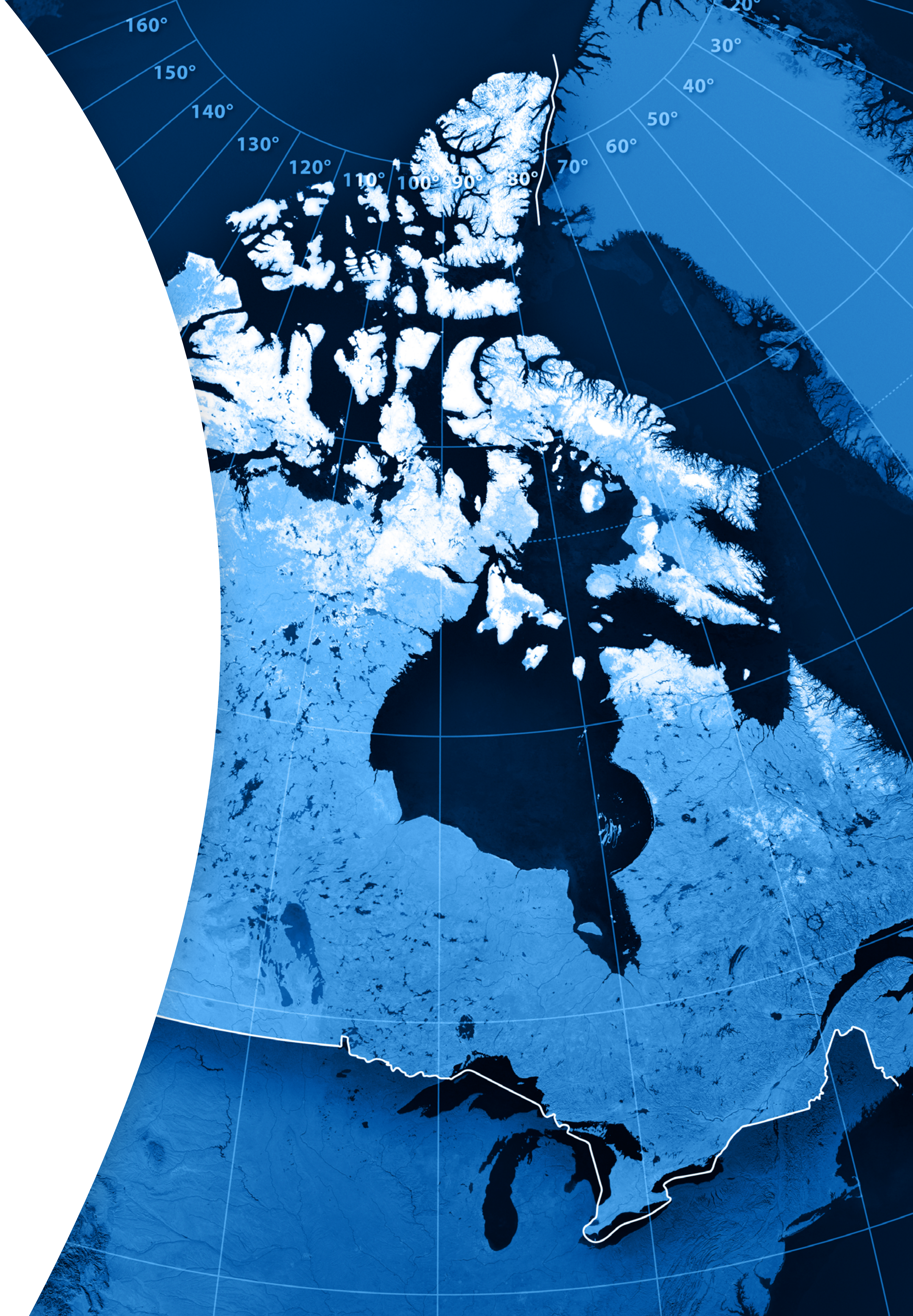
Introduction

Canadian Healthcare Cybersecurity

Healthcare leaders are under mounting pressure to modernize IT infrastructure, navigate complex compliance demands and protect increasingly vulnerable patient data – all while preserving the bedrock of clinical care: patient safety and quality. But these efforts carry real risk; when systems fail or data is compromised, the consequences extend far beyond IT – threatening trust, disrupting operations and putting patient outcomes in jeopardy. The stakes are high, as even a single breach can have devastating consequences on patient trust, operations and public safety.

The 2025 CDW Canadian Cybersecurity Study reveals that the healthcare sector has made significant strides in cybersecurity, particularly in areas such as zero trust execution and GenAI adoption – but gaps remain. Notably, the sector reported more cyberattacks than any other, with healthcare organizations experiencing an average of 297 attacks per organization – well above the national average of 241. Furthermore, 80.2 percent of healthcare respondents reported negative impacts as a result of cyberattacks.

However, this high-risk environment has also triggered substantial budgetary increases, with cybersecurity spending in the healthcare sector more than doubling since 2024, including a sharp increase in cloud security investment. With 79.2 percent of healthcare organizations reporting abundant budgets that allow for experimentation and modernization, many are accelerating their adoption of security technologies and frameworks. The following key findings dive into technology adoption, strategic enablement and executional maturity across the healthcare sector.



Key Finding 1

GenAI Takes Hold, but Risk Perception and Integration Challenges Persist

Healthcare organizations have emerged as early adopters in GenAI experimentation – averaging nearly 19 proof-of-concept initiatives per organization, a figure that outpaces most other industries. More notably, many of these pilots are gaining traction beyond the testing phase, signaling a growing maturity in how the sector is approaching AI integration. Impressively, 32.13 percent of these PoCs have progressed to production – one of the highest conversion rates across all industries.

Still, risk and integration barriers persist. The top blockers preventing wider adoption of GenAI include concerns around data privacy and regulatory compliance, lack of skilled resources to operationalize AI models and difficulty integrating GenAI into existing systems. Notably, 45.5 percent of respondents believe GenAI has helped reduce business risk, citing improvements in automation and decision-making. However, 31.7 percent believe it has increased risk due to data security concerns, bias and compliance gaps.

When asked about top technical challenges in implementing GenAI, respondents cited:

- Lack of high-quality labeled data.
- Integration of GenAI models with existing AI/ML workflows.
- The need for model explainability and transparency.

While technical hurdles like data quality, workflow integration and model explainability remain barriers, healthcare organizations are already identifying high-value areas where AI can meaningfully enhance security operations. In environments where speed, precision and resilience are critical, the following use cases are emerging as the most promising applications of AI within healthcare security teams:

- Threat detection and real-time anomaly detection.
- AI-assisted or fully automated incident response.
- Cyber risk identification and prioritization.
- Compliance reporting automation.
- Precision threat hunting with AI-driven insights.

Key Finding 2

MDR Drives Faster Detection and Response Across Healthcare

Faced with the highest average number of attacks per organization (297 compared to a national average of 241), healthcare providers are increasingly leaning on managed detection and response (MDR) services to manage and mitigate security threats. According to the 2025 survey, 42.6 percent of healthcare organizations have already adopted MDR services, while another 35.6 percent are planning to do so within the next 12 months.

The top drivers for MDR adoption in healthcare include:

- Improving the ability to prevent or mitigate security breaches.
- Reducing incident response time.
- Enhancing threat visibility and reporting capabilities.

These objectives are reflected in measurable improvements across security KPIs:

- Mean time to detect (MTTD) decreased from 4.9 to 3.07 days.
- Mean time to respond (MTTR) improved from 12.11 to 8.12 days.
- Mean time to recover (MTTRc) declined from 25.84 to 16.51 days.

These efficiency gains validate the growing confidence in MDR providers to deliver tangible outcomes. Importantly, healthcare organizations prioritize performance and outcomes over the underlying technology stack, using KPIs like MTTD, MTTR and incident remediation count as the main benchmarks for MDR provider effectiveness. As threat complexity grows and internal security teams remain stretched, MDR services are playing a vital role in improving cyber recovery and resilience across healthcare environments.

Key Finding 3

Frequent Security Testing Sets Healthcare Apart – but Missed Opportunities Remain

Healthcare organizations are setting the bar high when it comes to proactive security testing. Compared to other industries, a greater proportion of healthcare respondents report a consistent and frequent approach – 48.5 percent conduct security testing either quarterly or on an ongoing basis. This places the healthcare sector among the top performers in terms of regular security validation.

Beyond frequency, the perceived value of testing is remarkably high:

- All healthcare respondents confirmed that penetration testing revealed vulnerabilities that could have prevented past incidents or will help avert future ones.
- 57.7% believe some past incidents could have been avoided entirely had those vulnerabilities been discovered earlier.

Despite this progress, challenges still persist. For example:

- Some organizations still struggle to evolve testing for cloud environments, even as cloud security spending continues to increase.
- Downtime per incident remains a concern, with healthcare seeing a 38% increase in downtime per incident for cloud-related breaches – the highest across all industries.

This contrast underscores that while testing is frequent, its breadth and cloud-specific depth must improve to match evolving infrastructure realities. With healthcare organizations facing an average of 297 cyberattacks per year, staying ahead of attackers requires not only consistency in testing but expansion into cloud-native and hybrid testing capabilities.

Frequent, meaningful and targeted testing is not just a compliance measure – it's a frontline defence. The opportunity now lies in closing the gap between regular testing and full-spectrum coverage, particularly for fast-growing areas like cloud and identity-based threats.

Key Finding 4

Progress with Zero Trust, but Technology Gaps and Vendor Complexity Still Pose Risks

The healthcare sector leads in translating zero-trust strategy into actionable technical implementation. An impressive 91.1 percent of healthcare respondents indicated they could do so successfully, compared to 74.4 percent across all industries. This speaks to the sector's maturity and strong alignment between strategic and operational teams.

However, architectural and operational gaps persist:

- The top architectural challenges include a lack of centralized IAM infrastructure, poor compatibility between legacy systems and zero-trust components, and difficulty scaling continuous authentication and monitoring across environments.
- 31% of respondents flagged operational handover post-assessment as ineffective, suggesting a gap between zero-trust evaluations and execution.
- Top areas needing customization for zero trust include identity and access management (IAM), network segmentation and endpoint detection and response (EDR).

Additionally, organizations face difficulty in adopting new technologies for zero trust due to high costs, the complexity of managing multiple vendors and a lack of clarity around vendor capabilities specific to zero-trust needs.

Essential Guidance for Healthcare Security Teams

In an environment where healthcare organizations face rising cyberthreats that directly impact patient care and operational continuity, the following actions can help leaders build resilience and respond decisively to risks unique to the sector:

- **Prioritize Cloud-Ready Security Testing:** As cloud adoption increases, evolve security testing methods to address cloud-native systems. Adopt tools and practices designed for hybrid environments and ensure cloud-specific vulnerabilities are part of regular assessments.
- **Refine Zero Trust Through Customization:** Despite strong zero-trust implementation confidence, areas like IAM, network segmentation and EDR need tailored approaches. Focus customization on protecting clinical data, workflows and third-party integrations without disrupting operations.
- **Strengthen Incident Response with MDR:** With over 40% MDR adoption in healthcare, ensure these services align with internal processes. Define key KPIs (MTTD, MTTR, incidents remediated), and regularly test joint response plans to improve coordination and response time.
- **Expand the Scope of Security Testing:** While testing frequency is high, organizations should ensure full system coverage. Prioritize critical platforms like EHRs, IoT devices and cloud assets. Use test findings to guide remediation and support security planning.
- **Prepare for GenAI Scale with Foundational Readiness:** GenAI PoCs are common, but production rates remain low. Address privacy, skill and integration gaps by improving data governance, offering AI-focused training and assessing infrastructure readiness for GenAI deployment.

Conclusion

Cyberthreats continue to challenge the healthcare sector at scale – but the industry is also charting a path forward through leadership in zero-trust adoption, GenAI experimentation and proactive security testing. This growing duality – heightened risk alongside accelerating readiness – demands not just vigilance, but strategic clarity. What's needed now is deeper investment in AI readiness, more intentional use of MDR services and a disciplined, system-wide approach to operationalizing zero-trust architecture – so cybersecurity not only protects care delivery, but enables it.

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