ANALYST BRIEF
Sponsored by: ThinkOn

Data protection as a service enables organizations to enhance resilience, optimize data management, and align protection strategies with business outcomes.

Data Protection as a Service: Empowering Business Continuity and Resilience

November 2024

Written by: Yogesh Shivhare, Research Manager, Security and Trust

Introduction

In an era where Canadian CEOs expect 49% of their organizations' revenue to come from digital products, services, and experiences by 2028, safeguarding data is crucial. With the increasing threats of ransomware, the rising complexity of cloud-based infrastructure, and the ever-growing importance of compliance, organizations are turning to data protection as a service (DPaaS) to secure their most valuable asset — data. DPaaS solutions provide organizations with end-to-end services that include backup, disaster recovery, cyber-recovery, and data replication. These services enable businesses to ensure data availability, business continuity, and regulatory compliance.

Benefits of DPaaS

For organizations that adopt DPaaS effectively, the benefits are numerous and include the following:

- **Defense against cyberthreats:** With ransomware attacks and other cyberthreats on the rise, organizations need robust cyber-recovery capabilities. Ransomware attacks have surged globally, with the infection rate for Canadian organizations rising from 52% in 2021 to 60% in 2023. DPaaS provides solutions that offer fast recovery and isolation from cyberthreats, allowing businesses to bounce back quickly without compromising sensitive data or losing critical time in recovery.

AT A GLANCE

KEY STATS

- The ransomware infection rate for Canadian organizations was 52% in 2021, rising to 60% in 2023.
- 74% of North American organizations that suffered ransomware attacks in 2023 and paid ransom despite having backups that were unaffected by adversaries did so because their backups were incomplete. For 26%, paying ransom to recover was faster than recovering from their own backups.

KEY TAKEAWAY

"Backups matter, but recovery makes them meaningful." The key takeaway for decision-makers is to prioritize outcomes — focus on restoration capabilities, conduct regular disaster recovery testing, and choose flexible solutions that meet the needs of their organization.

- **Business continuity and rapid recovery:** DPaaS ensures that organizations can recover quickly and efficiently in the event of data loss, system failure, or a cyberattack. Despite having backups, 74% of North American organizations that paid a ransom in 2023 did so because their backups were incomplete or insufficient. The ability to restore data in real-world scenarios is crucial, as companies must not only back up data but also ensure that they can recover it within their defined recovery time objectives (RTOs) and recovery point objectives (RPOs).
- **Enhanced recovery testing:** In 2023, 61.6% of North American organizations that experienced ransomware attacks reported adversaries attempting to delete or destroy their backups. Regular disaster recovery testing — a critical component of DPaaS — ensures that businesses not only have backups but also know that those backups are uncompromised, comprehensive, and capable of supporting a full recovery in real-world scenarios.
- **Simplified management, scalability, and flexibility:** DPaaS solutions simplify the complexities of managing data protection across multiple environments — whether on premises, in the cloud, or in hybrid setups. In addition, the flexibility of DPaaS allows businesses to adopt protection services incrementally, scaling as their data grows and ensuring that they can respond dynamically to evolving business needs.
- **Regulatory compliance:** Organizations today face increasing pressure to meet data privacy and protection regulations such as the Payment Card Industry Data Security Standard (PCI DSS), the Personal Information Protection and Electronic Documents Act (PIPEDA), System and Organization Controls 2 (SOC 2), and ISO 27001. DPaaS helps organizations comply with these regulations by providing auditable processes, ensuring that data protection measures meet regulatory standards and support data sovereignty where required.

Key Considerations for Adopting DPaaS

While DPaaS offers many advantages, organizations need to carefully consider potential challenges and risks before adoption. In detail:

- **Incomplete backup systems:** Even with robust backup systems in place, some organizations may still be vulnerable. For instance, in 2023, 26% of organizations found that paying ransom was faster than recovering from their own backups. This situation highlights the importance of ensuring that DPaaS includes not only backup capabilities but also clear, tested recovery processes.
- **Cost considerations:** DPaaS can involve up-front investments that may seem high for smaller businesses. Organizations must weigh these costs against the long-term benefits of having reliable recovery options and reduced downtime during an incident. The cost of a ransomware attack can far exceed the initial investment in comprehensive data protection.
- **Fear, uncertainty, and doubt (FUD):** Shifting data protection to a service model may evoke concerns around data control, security risks, or vendor lock-in. Organizations must work closely with their DPaaS providers to establish clear SLAs and security protocols to mitigate these concerns.
- **Technology limitations and compatibility:** Not all DPaaS solutions may support every emerging technology. As businesses increasingly adopt containerized workloads and AI-driven applications, DPaaS must evolve to provide the enhanced security and recovery measures that these environments require.

- **Implementation pitfalls:** Successful adoption of DPaaS depends on aligning the solution with desired business outcomes. Organizations should prioritize restoration over mere backup as incomplete or outdated recovery plans can leave businesses vulnerable during a crisis. Regular testing (ideally every six months) is critical for ensuring that recovery times and objectives are met in practice.

Industry Trends Shaping Data Protection as a Service

Several major trends are shaping the DPaaS market, influencing both service providers and organizations seeking data protection solutions. In detail:

- **Growing cyberthreats (particularly ransomware):** The increasing sophistication of ransomware attacks is driving demand for robust cyber-recovery services. Companies are seeking DPaaS solutions that offer fast, secure recovery capabilities, isolating infected environments and ensuring clean recovery processes.
- **Cloud and hybrid adoption:** As businesses continue to embrace cloud-based and hybrid infrastructures, DPaaS must support a wide range of environments. Organizations are looking for services that can seamlessly integrate with their cloud workloads, SaaS applications, and hybrid deployments, ensuring that data protection strategies can evolve alongside their IT environments.
- **Platformization and simplification:** The complexity of managing multiple disparate data protection tools has led to a demand for platform-based solutions that consolidate backup, disaster recovery, and replication into one service. Businesses are seeking DPaaS offerings that simplify procurement, management, and scalability while providing comprehensive data protection across all environments.
- **Compliance and data sovereignty:** With tightening regulations around data privacy and cross-border data flows, businesses are increasingly concerned about the physical location of their data backups. DPaaS providers that offer solutions ensuring compliance with data sovereignty regulations are likely to see growing demand, particularly from organizations that must adhere to region-specific laws.
- **Support for AI and advanced workloads:** As organizations adopt AI and other data-intensive workloads, the need for more advanced data protection becomes apparent. DPaaS solutions must evolve to protect and recover these highly valuable data sets, ensuring that organizations can maintain business continuity even in AI-driven environments.

Conclusion

Data protection as a service is an essential component for organizations seeking to safeguard their operations, maintain business continuity, and comply with stringent regulatory requirements. By adopting DPaaS, IT and business leaders can ensure that their data is protected, recoverable, and aligned with strategic business goals.

For IT and business leaders — CEOs, CTOs, CIOs, and CISOs — the key takeaway is to focus on outcomes. Organizations should prioritize restoration over backups, conduct regular disaster recovery testing, and choose DPaaS solutions that align with their organization's growth and technology road map. As cyberthreats evolve and businesses become more reliant on digital services, DPaaS will play a critical role in enabling resilience, protecting revenue streams, and supporting long-term success.

About the Analyst

Yogesh Shivhare, *Research Manager, Security and Trust*

Yogesh Shivhare is a research manager at IDC Canada within the Infrastructure Solutions and Security research team. He manages cybersecurity research and provides insight and analysis into industry and technology trends as they shape the Canadian security market. He is also responsible for market sizing and forecasting the security appliance hardware market. His research focus enables him to support Canadian technology providers by identifying key market trends in the cybersecurity space where end-user demand and preferences are changing rapidly.

MESSAGE FROM THE SPONSOR

ThinkOn DELL Technologies

Think On, Inc. is a global, channel-only cloud-managed service provider helping organizations achieve business outcomes through secure, data-centric managed infrastructure services. We empower partners to deliver exceptional customer results with our scalable portfolio of critical compute, protection, and archiving solutions. Supported by trusted partners like Dell Technologies, we ensure high-performance, secure, and reliable cloud services. Dell's industry-leading infrastructure enhances our ability to meet diverse partner and customer needs efficiently. Our data protection services provide tangible value by delivering peace of mind through a multi-layered approach that transforms data protection into a strategic advantage. Flexible outcomes scale seamlessly with your business to ensure resilience. From SMBs needing essential protection to enterprises requiring advanced capabilities, our tiered Essential, Enhanced, and Elite services cater to diverse needs. Discover more about our channel-only services and resources by visiting our Partner page: https://thinkon.com/partners/.

IDC Custom Solutions

The content in this paper was adapted from existing IDC research published on www.idc.com.

IDC Research, Inc.
140 Kendrick Street
Building B
Needham, MA 02494, USA
T 508.872.8200
F 508.935.4015
Twitter @IDC
blogs.idc.com
www.idc.com