ANALYST BRIEF
Sponsored by: Bell

Security in the cloud requires a strategic approach that aligns cloud adoption with key security processes along with the required layers of technology.

The State of Cloud Security in Canada: Top Actions for Strong Outcomes

October 2022

Written by: Yogesh Shivhare, Research Manager, Security and Infrastructure, IDC

Introduction

Improving business operations with cloud services has clear advantages. However, the path to enjoying those advantages may be coming at the expense of maintaining security. With security technology and the threat landscape in constant evolution, there has been little information on the steps that Canadian organizations are taking to secure their cloud operations. While one might anticipate a correlation between security outcomes and increased implementation of security technologies, a survey conducted by IDC with participation from Bell suggests otherwise. The survey uncovered large gaps in approaches to cloud security at Canadian organizations: Security strategies are not always keeping pace with cloud adoption, yet organizations continue to fast-track public, hybrid, and multicloud initiatives, with an average of 43% of data now in public cloud. Moreover, security technology alone isn't enough — and often leads to a false sense of safety. Proper security processes are vital.

AT A GLANCE

KEY STATS

- 43% of organizations' data now resides in the cloud.
- Cloud adoption rates are on the rise, but only 52% of organizations have been able to protect themselves from a security breach.
- Only 34% of organizations have deployed cloud security posture management, leaving the remainder exposed to misconfigurations.

KEY TAKEAWAY

Organizations with high security budgets and large investments in security technology can still experience much lower security effectiveness when they don't have the right security processes in place.

Studying Cloud Security

To better understand the state of cloud security in Canada, Bell participated in an IDC Canada survey of more than 300 medium and large organizations across a range of industries and geographies. The survey questions focused on cloud adoption, security capabilities, and success at delivering strong security outcomes in the cloud. The results are surprising, and they provide a window into the best practices of organizations that are highly innovative in the cloud while still maintaining robust security.

The Cloud Security Effectiveness Matrix

Using the results of the survey, IDC and Bell categorized the responding organizations within a Cloud Security Effectiveness Matrix (CSEM). The CSEM provides organizations an opportunity to learn from the successes — and the mistakes — of their peers.

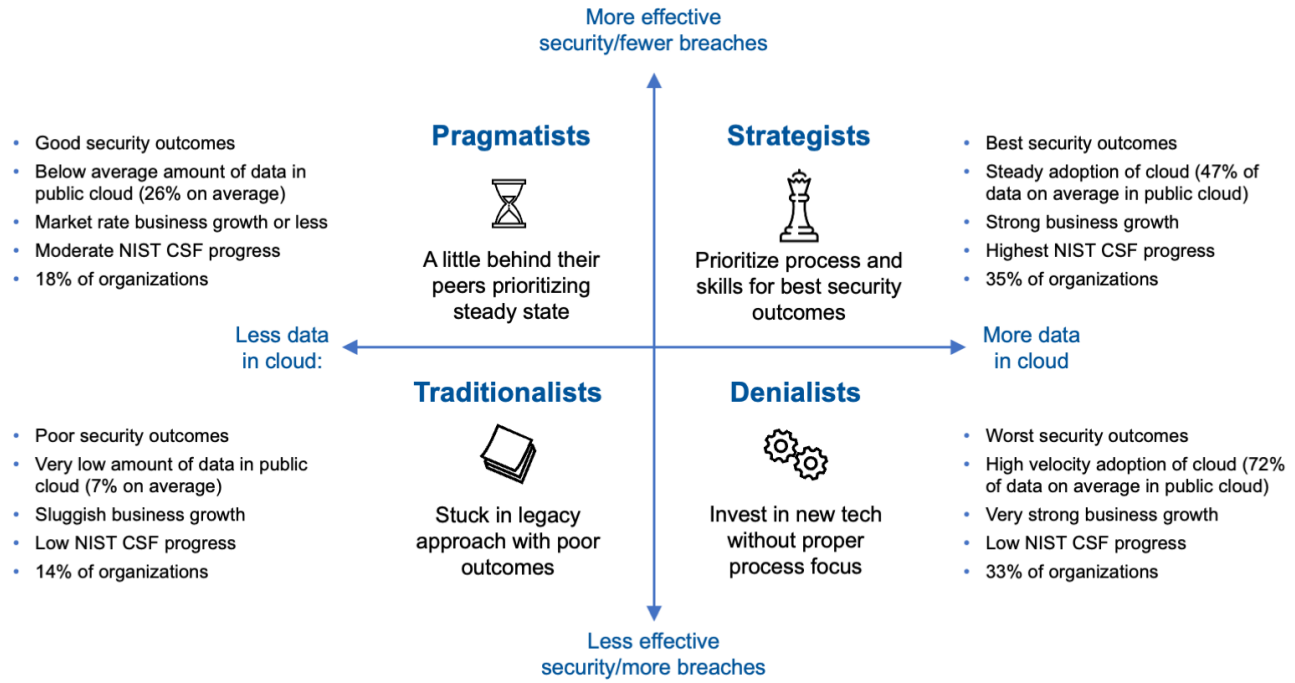
Through our analysis of the research, organizations were grouped into four distinct categories (see **Figure 1**) based on their cloud usage, security skills, capabilities, technologies, and progress in implementing key security processes.

Due to its simplicity and growing ubiquity, we use the NIST Cybersecurity Framework (CSF) as a tool to communicate the research findings at times in this report. If an organization does not use the NIST CSF, there are similar processes across other frameworks for easy comparison.

As developed in collaboration with Bell, the research helped identify common characteristics of how four groups of organizations are approaching cybersecurity:

- **Traditionalists** typically see the benefit of moving to the cloud, but they are stuck in legacy skills, processes, and technology. They show slower business growth and limited cloud adoption and have poor security. Technical debt dramatically affects their security success.
- **Denialists** demonstrate rapid cloud migration and high business growth but they primarily rely on security technologies for data protection. They suffer the worst security outcomes of the four groups because the right security processes are not in place. This group seems to be in denial that it needs to go beyond security technology (of which they purchase a lot) and focus on processes and people.
- **Pragmatists** show slower-than-average cloud adoption, but they are starting to take the right security actions. However, they are missing some of the benefits they could gain by ramping up cloud adoption. Because they are starting to do the right things from a process perspective, they typically fare well from a security outcomes perspective.
- **Strategists** take a measured approach to cloud, with slightly higher-than-average adoption. They have strong business growth and have the best security outcomes. As described below, this is the group that organizations should strive to emulate.

Figure 1. Canadian Cloud Usage and Security Effectiveness Matrix



Source: IDC and Bell, 2022

Lessons Learned from Strategists, the Security Leaders

The group in the upper right quadrant of the CSEM is the Strategists. The organizations in this group find the proper balance between speed of cloud adoption and taking time to implement security processes. In addition, they focus on increasing the security skills of developers and IT and security staff. They do not rely as heavily on technology solutions as the less-secure Denialists do. They acknowledge that improving security maturity involves a continuous investment of resources and ongoing management; it is a strategy, not a project. They recognize that maintaining security takes time and if planned properly, without significant hardship.

Strategists adopt the following guidelines to advance their cloud security effectiveness:

- **Use frameworks.** Strategists tend to adopt frameworks because they help to ensure the breadth and depth of cloud and cloud security requirements are covered. These include cloud frameworks for migration (e.g., from AWS, Azure, GCP), operations (e.g., cloud security alliance cloud controls matrix), and, most importantly, security (e.g., NIST, ISO, CIS). Using a framework establishes the needed breadth of security capabilities and sets the groundwork for success.
- **Focus on key security processes.** There are countless controls and related processes within security frameworks that help ensure cloud security. The research highlights that taking an ongoing inventory of cloud services, continuous assessment of cloud configurations, managing entitlements, and threat detection (including logging and monitoring across cloud services) are critical. These processes largely

fall within the "Identify" and "Detect" functions of the NIST CSF. Processes within the other three NIST CSF functions ("Protect," "Respond," and "Recover") are clearly important, but Identify and Detect are aligned even more to cloud security effectiveness.

- **Shift left and shield right.** Organizations that are far down the path of DevSecOps (security integrated early in the development pipeline, also known as "shift left") are not necessarily more secure than their peers. The research suggests that this counterintuitive result is due to the poor execution of processes within the Identify and Detect functions. Unlike Denialists, Strategists perform security well both left and right of application deployment. They "shield right" by executing on strong security of their live applications.
- **Assure security skills.** Skilled staff — including cloud architects, cloud-native developers, and operations and security professionals — are scarce in Canada. CIOs and CISOs often find it challenging to ensure the availability of necessary skills. The good news is that cloud enables the automation of some security tasks (e.g., attack surface management, logging, monitoring, aspects of response and recovery), which in turn allows lower-skilled resources to accomplish more. Strategists are ahead of their peers on security automation and integration across tools and cloud environments, which enhances their security effectiveness.
- **Prioritize cloud-native protection.** Cloud-native workloads need cloud-native security. The misconfiguration of cloud services creates large security issues. Strategists monitor for changes in cloud configurations, both on initial setup and as changes occur. Cloud security posture management (CSPM) tools and processes are essential to detecting misconfigurations and drifts from a known good state. Because the cloud has so many features with a variety of settings and configurations, business users, IT, developers, and others can unintentionally introduce bad changes. Moreover, as the number of cloud services and application programming interfaces (APIs) increase, the likelihood of security exposure builds up. In addition to CSPM, a cloud workload protection platform (CWPP) helps secure cloud-native workloads whether optimized within one provider, in a hybrid environment, or across multiple clouds. It provides visibility into vulnerabilities, anomalous behaviour, and other security protections that go beyond misconfigurations.
- **Ensure cloud control.** Beyond CSPM, there are solutions such as cloud access security brokers (CASBs) and zero-trust network access (ZTNA), which are important for discovery/inventory, access control, visibility, and controlling data through data loss prevention. These help control the bidirectional security of data between user and cloud. Without them, public cloud environments are susceptible to cloud abuse, by shadow IT and external threats alike.

Considerations

For a majority of Canadian organizations, cloud adoption is still evolving, so effective security can feel like a moving target. Here are additional gaps to those outlined above, where organizations can fail to deliver on effective security in the cloud:

- **Lack of visibility and control:** Poor visibility across user accounts, services, and change control is a leading issue that can result in more severe security breaches.
- **Lack of robust cloud governance:** Misconfigurations, human errors, poor access controls, and exploitation of known vulnerabilities often stem from inadequate security governance and the lack of follow-up required to continuously and automatically measure risk and exposure. Moreover, good governance will guide good planning in areas such as incident response and recovery.
- **Lack of shared responsibility:** In a multicloud environment with varying deployment models (IaaS, PaaS, SaaS),cloud service providers' responsibilities for layers of the security stack vary significantly. It is vital to review the shared responsibility model and to clearly define roles and responsibilities for securing data, APIs, services, and user credentials in the cloud.
- **Overreliance on traditional security:** Cloud deployments don't benefit from some of the ways in-depth, on-premises defenses have been structured in the past. Threat detection, investigation, and response are different in cloud environments, for example. Logging and monitoring across cloud services is even more critical, as some of the traditional on-premises controls do not apply as well. It is important to identify and set up sources of log data across multiple clouds, which facilitates ingestion and a single point of analysis. Organizations also should automate wherever possible (e.g., to inspect and triage alerts, etc.).
- **Insufficient adversarial testing:** Failure to extend risk assessments and security penetration testing to cloud environments increases risk. Proper testing helps prioritize security investments in addition to minimizing immediate exposure.

Strategists focus on people and processes; they acknowledge that reaching security maturity is a continuous investment of resources and ongoing management.

Conclusion

Cloud is foundational to business success. The security choices made now will have a far-reaching impact. Organizations need to become like the Strategists within the Cloud Security Effectiveness Matrix and find a balance between the pace of technology adoption and a systematic approach to security processes and skills improvement. This will help avoid the trap of the Denialist approach: an overreliance on secure technologies that has resulted in the worst security effectiveness. Further, it is critical to follow basic frameworks such as the NIST Cybersecurity Framework and Cloud Security Alliance Cloud Capability Model (CSA CCM). With this underlying investment in security processes and skills, organizations can achieve strong business and security outcomes.

Methodology

In July, with participation from Bell, IDC conducted a survey of more than 300 medium and large Canadian organizations across Canadian regions and many industries to measure cloud adoption, security capabilities, and how successful Canadian organizations are at delivering strong security outcomes in the cloud.

All survey participants were involved in IT strategy, budgeting, technical requirement specifications, or vendor evaluation and final purchase authorization.

To organize these findings, and help organizations accelerate cloud and digital efforts while reducing the likelihood of a breach, Bell and IDC developed a Cloud Security Effectiveness Matrix. The matrix categorizes the respondent organizations into four distinct groups based on their cloud usage, security capabilities, and security processes in line with popular frameworks like the NIST CSF. The distribution of organizations among the groups was:

- Traditionalists = 14%
- Denialists = 33%
- Pragmatists = 18%
- Strategists = 35%

About the Analyst

Yogesh Shivhare [Yogesh Shivhare (idc.com)], Research Manager, Security and Infrastructure, IDC

Yogesh Shivhare is a research manager at IDC Canada within the Infrastructure Solutions and Security research team. He manages the cybersecurity research and provides insight and analysis into industry and technology trends as they shape the Canadian security market.

MESSAGE FROM THE SPONSOR

To learn more about Bell cybersecurity solutions, visit www.bell.ca/cybersecurity

IDC Custom Solutions

IDC Canada
33 Yonge St. Suite 902
Toronto, ON M5E 1G4
Canada
Twitter @IDC
idc-insights-community.com
www.idc.com

This publication was produced by IDC Custom Solutions. The opinion, analysis, and research results presented herein are drawn from more detailed research and analysis independently conducted and published by IDC, unless specific vendor sponsorship is noted. IDC Custom Solutions makes IDC content available in a wide range of formats for distribution by various companies. A license to distribute IDC content does not imply endorsement of or opinion about the licensee.

External Publication of IDC Information and Data — Any IDC information that is to be used in advertising, press releases, or promotional materials requires prior written approval from the appropriate IDC Vice President or Country Manager. A draft of the proposed document should accompany any such request. IDC reserves the right to deny approval of external usage for any reason.

Copyright 2022 IDC. Reproduction without written permission is completely forbidden.