IDC

ANALYST BRIEF

Sponsored by: NetApp

Expanding data volumes fueled by digital transformation are driving an increasing need to understand, organize, and secure data wherever it resides. Organizations that succeed will not only achieve security but numerous other business benefits.

Generating Ideal Business Outcomes with a Strong Security Foundation

July 2023

Written by: Jennifer Glenn, Research Director, Information and Data Security Products

Introduction

Digital transformation is fueled by data. It underpins the products and services being delivered. It informs and improves the customer experience. It creates opportunities for operational efficiency.

With all of these uses, data volume is growing rapidly and is now located across an expansive hybrid, multicloud environment. According to IDC's December 2022 *Data Privacy Survey,* 68% of organizations expect their data volume to increase over the next three years. Of those, nearly 40% expect volume to increase by 25% or more. In addition, privacy and compliance regulations require security teams to answer critical questions about this massive amount of data including:

» Where is it?

» Is it sensitive or confidential?

» Who or what application has access?

» How can it be used?

Failure to answer these questions can lead to inappropriate use or access to customer information or a data breach, either of which can result in privacy violations, fines, costly fixes, and lost revenue.

While avoiding security and compliance risks is a goal in and of itself, organizations that can take control of this data – see it, secure it, and govern its use – will be better positioned to build and empower their teams, engage with and support customers, and create innovative products or services that beget brand loyalty.

AT A GLANCE

KEY STAT

68% of organizations expect their data volume to increase over the next three years. Of those, nearly 40% expect volume to increase by 25% or more (source: IDC's *Data Privacy Survey,* December 2022).

KEY TAKEAWAYS

- Digital transformation efforts have increased data volume and spread it to more infrastructures and devices, making it harder to protect.
- Experienced security organizations are finding ways to address these challenges and benefit the business by:
  - Limiting the risk profile of the organization
  - Finding efficiency with automation
  - Building confidence with regulators

Three levers that organizations can use to incorporate security to achieve these outcomes are detailed in the sections that follow.

Shrink Attack Surface Area

The ample use of data to build customer-facing applications and strategic operations has provided a larger landscape for malicious actors to gain a foothold into the business. Not only has the amount of data grown; it is located in more places as the organization's infrastructure expands. This has created more surface area for security teams to cover – increasing the chance that attacks are successful. One of the key strategies for minimizing this risk, and the disruption that follows, is to limit exposure wherever possible. Continuous scanning at each layer of the organization – users, networks, applications and data – provides critical visibility and monitoring of where business information lives and how it is used. This also provides insight into the vulnerabilities and risks present.

In addition to visibility, organizations need to set up a well-protected environment that enforces key policies to keep business data safe. Web application firewalls and anomaly detection help to identify and address suspicious behavior. Centralized logging through an XDR or SIEM can offer additional insights on the risks posed to the business and its data. Taking this a step further, individual business units that deal with highly sensitive or confidential information can be segmented from the rest of the organization with virtual private clouds each leveraging the same protections.

Simplify Through Automation and Standardization

Securing a digital business is a challenge even for adequately staffed teams. The reality is the most security teams are struggling to find and hire skilled practitioners. This may explain why configuration errors are a leading cause of inadvertent data exposure – to attackers or even trusted insiders. Great security teams are finding ways to work smarter and extend their skills in a tight hiring environment. From a process perspective, standardizing key control monitoring is a good step. By identifying top controls – such as prohibiting public access to cloud storage – teams can create and enforce polices that keep data better protected.

Another way to simplify configuration of multiple cloud environments is building and implementing templates. By implementing templates, organizations have a much more consistent approach to configuring cloud environments. It also provides a clear benchmark for what is "ideal" where organizations easily and quickly see any changes that might put the business at risk. Finally, standardizing templates, offers a foundation for automation. This offers two benefits – it reduces workload by eliminating the need to configure multiple environments and it limits the possibility of human error.

Build Trust and Confidence with Regulators and Customers

Cybersecurity and data security are critical control mechanisms for privacy and compliance regulations. They are also one of the key levers mature organizations can (and should) use to build trust with both regulators and customers.

First, organizations can leverage the ready-made compliance codes from their hyperscalers. This supports automation for compliance initiatives.

Next, one of the simplest things security teams can do to demonstrate their commitment to compliance is to be transparent about the products and process – and how these meet privacy and compliance regulations. From there, security organizations that are serious about growing trust can build public-facing portals that allow customers, partners, and/or regulators to pull information on their security controls.

Benefits

Security teams provide a critical service to the organization. They sit at the control point for not only securing information but also demonstrating compliance and privacy. Despite this – or perhaps because of it – these teams are often understaffed and burning out at a rapid rate. Mature organizations recognize that using the above levers gives these teams the tools and process to be more productive, improve efficiency, and perhaps be more content in their job.

Subsequently, by strengthening the security team, businesses can reap several benefits to the organization overall, including:

- **Adaptability for future growth:** Adhering to compliance regulations and implementing security fixes can be a time-consuming process for any team. This can put a strain on resource-strapped security teams and may also delay other (revenue-generating) projects. Reducing the risk profile of the business and implementing automation can help improve efficiency of the security and compliance process. This gives security teams the resources they need to support the business in whatever capacity is needed for future initiatives.
- **Cultivating customer trust:** Building trust with customers relies on security in several ways. For example, keeping critical services and customer tools available and running optimally demonstrates reliability. Another example would be building security into the product development at the design stage. This not only speeds up the time it takes to get innovative services or features into customers' hands by reducing last-minute development changes to add security features; it also eliminates the need for bolted-on security features that may impact desired functionality. In both cases, customers get a better-quality product, helping to build trust and loyalty. Finally, perhaps the clearest example of leveraging security to build trust is simply keeping customer information private and protected. In all of the examples, improving security using the previously mentioned levers helps organizations offer customers reliable services, innovative and engaging experiences, and confidence that their information is safe. This continued cultivation of trust is a foundation for establishing brand loyalty and preference.

Conclusion

Data for the digital business is portable, consumable, and lives in more hybrid and multicloud environments for use in customer products, business operations, and collaboration. Protecting that data is essential for complying with privacy and compliance regulations – as well as demonstrating trust to partners, employees, and customers. Security teams are in the crosshairs trying to implement the controls that keep data secure, while still maintaining the flexibility and collaboration that are the spirit of digital transformation. Security teams that improve processes with a lens toward achieving business outcomes can go beyond risk reduction to be a valuable contributor to team empowerment, customer satisfaction, and brand preference.

About the Analyst

***Jennifer Glenn,** Research Director, Information and Data Security Products*

Jennifer Glenn is Research Director for the IDC Security and Trust Group and is responsible for the information and data security practice. Ms. Glenn's core coverage includes a broad range of technologies including messaging security, sensitive data management, encryption, tokenization, rights management, key management, and certificates.

MESSAGE FROM THE SPONSOR

Learn what experienced teams do to secure an expanded hybrid multicloud IT landscape and how to improve your processes to achieve business outcomes that go beyond risk management to include team empowerment, customer satisfaction and brand preference.

Click here to learn more

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
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.