IDC

SPOTLIGHT

Sponsored by: Box

Hybrid working has complicated data protection. Valuable data now resides everywhere and is a key target for attackers. A data-centric security strategy is essential for balancing business needs with information protection and compliance.

Hybrid Work Drives Need for Native Data Security

July 2022

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

New Ways of Working Create New Challenges

The COVID-19 pandemic has loosened its grip on our daily lives. While not completely out of the woods, organizations are reopening offices. At the same time, many companies and their employees have eased into a comfortable routine after the haphazard methods of remote working forced upon them by the virus in March 2020. This new normal has shifted the mindset for many employers and employees about the shape of the new work environment.

AT A GLANCE

KEY STATS

According to IDC's December 2021 *Future Enterprise Resiliency and Spending Survey:*

- More than 50% of organizations globally reported suffering a ransomware attack that blocked access to systems or data.
- More than 20% of respondents stated that valuable, sensitive, or secret data was exfiltrated – and that number is growing.

Hybrid work – a combination of remote and in-office – seems to be the prevailing approach for most organizations. While this model strikes a nice balance between employee and employer needs, it also presents new challenges when it comes to protecting the integrity of business data. Today's workforce is logging in from home, from the office, and points in between, with the same expectation of productivity, connectivity, and security. For many users, working productively includes downloading files locally, sharing files in collaboration platforms or over email, or storing files in shared project tools. These activities generate a significant amount of unstructured data that can be hard to track and control. The result is a high volume of data is being used, processed, and sent from devices or networks that are outside of the organization's control. Valuable information about customers, employees, trade secrets, and business dealings is now extremely vulnerable to compromise.

Attackers are using this vulnerability to their advantage. With data being used and processed from non-corporate devices and/or home networks, ransomware remains a pervasive issue for businesses. According to IDC's December 2021 *Future Enterprise Resiliency and Spending Survey,* more than half of organizations globally reported suffering a ransomware attack that blocked access to systems or data. Ransomware is a type of malware that disrupts business operations by making important information unavailable. It may also obfuscate other, more nefarious activities such as exfiltrating valuable or sensitive data.

Protecting Data Requires Security on All Fronts

To ensure the integrity of business data and protect valuable information from being accessed or removed by malicious or errant users, security must be multifaceted. Data discovery and classification are the building blocks for cybersecurity motions that improve visibility and control of unstructured data across all fronts, including:

- **Inbound:** Hybrid work creates an expanded attack surface, making it more difficult to quickly identify and stop threats coming into the organization. There is simply too much data and too many areas of compromise to cover it all effectively. Knowing where data lives and who has access to it is essential for detecting and managing the threats that can cause the most damage.
- **Internally:** Ransomware and other inbound attacks on business operations are simply one form of cyberthreat, but security teams also need to address the risks from internal sources. These can include everything from inadvertent vulnerabilities created by configuration errors to malicious attackers using stolen credentials to move laterally into systems containing sensitive data. A zero trust approach – such as that identified in the Biden administration's Executive Order on May 12, 2021 – provides continuous authentication and least privileged access that limits propagation of threats internally and keeps valuable business information protected.
- **Outbound:** In IDC's December 2021 *Future Enterprise Resilience and Spending Survey,* nearly three-quarters of respondents indicated that some data was exfiltrated during a ransomware attack. More than 20% stated that valuable, sensitive, or secret data was exfiltrated – and that number is growing. It's important for cybersecurity teams to have clear policies on how data can be used and removed from the organization. This not only prevents malicious actors from stealing data but also reduces the risk of disgruntled or errant users from using data inappropriately.

Using Security Principles and Controls to Simplify Compliance

Cybersecurity and protecting data are central to building and maintaining trust in business. Privacy and regulatory compliance are a way to operationalize trust by documenting and demonstrating control over data. Personally identifiable information (PII) and its related privacy-oriented information are regulated by different entities around the world. Regulations such as GDPR and CCPA require organizations to gain an understanding of the location, ownership, and security of data collected on European Union and California citizens, respectively. Similar regulations exist elsewhere, and more are being created. Regulated data includes medical and health insurance information, credit card data, and other PII.

With cybersecurity teams already putting tools and policies in place to provide visibility, categorization, and protection of data, it's become common for governance and compliance to be added to their responsibilities. This makes sense since they are already using the tools and processes that give them the ability to enforce privacy and regulatory compliance rules. Further, they also manage the reporting tools to demonstrate adherence to documented policies. The challenge, however, is that cybersecurity teams are already stretched thin addressing protection and security requirements. Compliance is also a nuanced practice that is not always clearly aligned with the needs of security teams.

Data discovery and classification tools provide a foundation for not only securing data but also demonstrating governance and compliance with privacy or industry regulations, including:

- **Life-cycle management:** Part of protecting data includes managing the storage, retention, and disposal of sensitive or confidential elements. Security leaders can use their data discovery and classification tools to understand how much sensitive data is being created and how it is being spread through the organization. They can also take it a step further and create policies that not only document the life cycle of data but control where it can be stored, for how long, and if/when it can be destroyed based on industry regulations.
- **Keeping pace with changing regulations:** In today's decentralized and fluid workplace, democratizing data helps improve efficiency and productivity by informing multiple applications, systems, and functions. As demands on data expand, so will the privacy and industry compliance regulations that govern its use. Knowing where data lives, how it's used and categorized, and who can access it and when is not only critical to a zero trust security strategy, but also essential for easily addressing new and changing industry regulations.

IDC believes that following data security activities create a solid foundation for a data-driven security strategy that can also simplify compliance with privacy and industry regulations:

- **Data discovery:** These tools help organizations understand what data they have and where it resides. Organizations should assemble a team of data owners, line-of-business managers, and IT and data security leaders to inventory key business assets. Digital loss technologies can assist in this activity by uncovering hidden data repositories and unauthorized SaaS installations. This provides the basis for data classification.
- **Data classification:** Once data has been uncovered, it must be categorized based on its value and mapped to understand what users and applications have access to it. Data classification establishes where an organization's most sensitive assets exist and if there are enough security controls to keep them protected. This is time consuming, but essential for the next step: data governance.
- **Data governance:** With a clear map of valuable data, it's easier to establish policies to govern the use of that information. Security teams should build in appropriate controls to enforce these policies throughout the life cycle of the data.
- **Data monitoring:** The addition of new users and applications – as well as general working activities – mean that data is constantly being generated or used in new ways. This requires security teams to constantly monitor key ingress/egress points to assess when and where data is being used and if that use is acceptable or not.
- **Zero trust:** Data discovery, classification, governance, and monitoring are the basis for a zero trust security strategy. With zero trust, all devices and users must be authorized to access business assets depending on multiple factors, including valid credentials, role, timing, and need.

Benefits

The Advantages of Data-Centric Security

For businesses to succeed in a hybrid working environment, data must be available to the right users and devices at the right time. Data security issues can be inadvertent or malicious. Regardless of whether data is leaked through misuse, lost

through blatant theft, or simply unavailable, business operations are at risk. Critical projects may be delayed. Customer trust in the reliability and integrity of the organization may be questioned. The organization can also face numerous fines. A data-centric security strategy helps organizations solve two of their biggest challenges: protecting data from threats and exfiltration and securely managing data throughout its life cycle. By employing such a strategy, data security professionals can demonstrate value to the business in several ways, including:

- **Productivity:** With hybrid working, users are creating, changing, and moving more data into more places. When ransomware takes hold, it can be incapacitating. Protecting data by detecting and blocking the malware that makes up a ransomware attack is an effective way to keep the workforce operational and data workflows moving.
- **Brand equity:** Trust is rapidly becoming an influential brand characteristic. Fewer things violate trust between a business and its customers and partners than services that are unavailable or valuable data that's been exposed or worse. While data privacy and industry compliance regulations are a good base for operationalizing trust, data security technologies go a step further to protect valuable information from being lost or leaked due to attack or misuse.
- **Efficiency:** Security controls are only effective if they are used appropriately. For many organizations, that requires a frictionless security strategy integrated into the daily routine of users and operational processes. A good frictionless data-centric security strategy gives organizations the visibility and control to put policies in place that are virtually undetectable by the user but still provide clear protection of critical assets.

Considering Box

Founded in 2005, Box is a cloud content management platform designed to accelerate business processes, power workplace collaboration, and protect valuable information while using a best-of-breed enterprise IT stack. Box has simplified work for leading organizations such as AstraZeneca, General Electric, JLL, and Morgan Stanley.

With the Content Cloud, Box is aiming to help teams to secure their content and power collaboration. Security includes built-in controls for accessing content, encryption of data at rest and in motion, and the option of customer-managed encryption keys through Box KeySafe.

Box Governance gives organizations the ability to manage data easily and securely throughout its life cycle. It includes data retention schedules, preservation for defensible discovery, and disposition management.

Box Shield provides organizations with cloud-native data leakage protection and threat detection covering both data theft and malware. Its Smart Access controls are designed to help organizations protect information through custom security classifications and classification-based access policies. These policies are intended to prevent data leaks in real time through restrictions on sharing, external collaboration, downloads, and more. Box Shield's Threat Detection feature aims to provide machine learning-powered detection and alerts about potentially malicious activity and content. Native automated classification capabilities enable organizations to automatically scan files and classify them based on the content and admin-defined policies.

Further, user-driven and machine-driven classification can be combined helping customers protect their sensitive data at scale. This native classification capability augments the existing option for Box customers to classify files via API, through Box's ecosystem of security partners including IBM, Palo Alto Networks, Broadcom, McAfee, Netskope, and Microsoft.

In October 2021, Box strengthened the Box Shield portfolio with the addition of deep learning capabilities that will help identify more sophisticated malware. These new capabilities will aid customers in improving their security posture and productivity with higher malware detection rates and fewer false positives. Box Shield also helps customers reduce the risk of a data breach by automatically applying classification labels to millions (and growing) of files containing sensitive content like PII. During the first half of 2022, Box also added an access policy monitoring mode to Box Shield. This feature is designed to let customers monitor security policies before enforcing them, minimizing friction and allowing Box administrators to fully understand the impact of security controls before enforcing them. Box also provides for automatic watermarking to classified documents, helping to reduce unauthorized sharing.

Challenges

Data protection is the crux of all cybersecurity activity even if the methods to do so vary. For this reason, cybersecurity tools may include overlapping technologies, which makes data-centric security a very crowded market. Many vendors are adding light versions of traditional data security technologies to existing security products and offering them as differentiating features. This can dilute the value of standalone data security tools and make it harder for organizations to justify the purchase of these solutions.

Conclusion

Hybrid work is a reality in our post-pandemic world. At the same time, everyone from consumers to the board of directors is highly attuned to the risks of cybersecurity and data protection due to news coverage of ransomware and data breaches. This environment creates challenges for organizations as they try to stay competitive while responding to employee demands for flexible workplace arrangements.

Protecting data must be a priority for the post-pandemic, hybrid work environment.

A data-centric security strategy offers a solid foundation for balancing the needs of the business. Data discovery and classification are essential steps in data protection activities including loss prevention, threat detection, compliance, and zero trust. For Box, integrating these capabilities with other security tools will help to position the company for success.

About the Analyst

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

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

Box enables you to safeguard your most important data with enterprise-grade security, privacy, and compliance, while keeping teams connected — all from on one simple platform.

With security and compliance built right in, the Box is designed on a cloud-native, global infrastructure that scales with your business. From highly regulated PII, to employee information and everything in between, Box improves your quality of output and ensures your content stays both secure and accessible.

Take a zero trust approach and prevent data leaks with strong user authentication (including SSO and MFA support), device security, granular permissions, and vector-based watermarking. With Box Shield, you get classification-based security controls that automatically prevent data loss, plus AI-powered, context-aware alerts that detect potential data theft and malicious content. Streamline information governance with flexible retention schedules, preservation for defensible discovery, and disposition management in Box Governance.

More than 100,000 organizations trust Box to secure their most sensitive data, all while reducing risk. Visit box.com/security-compliance 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