Market Pulse

The Habits of Highly Data-Secure Companies

New IDG survey reveals three technologies that are helping enterprises build immunity to data breaches, in and out of the cloud

Today's businesses grapple with securing digital assets scattered across a variety of IT environments. These hybrid infrastructures might comprise a mix of traditional data centers, public cloud services, and on- and off-premises private clouds.

In a study conducted by IDG in May 2020, companies expressed high levels of confidence in their IT teams' ability to secure applications and data across these infrastructures. At the same time, however, the survey results indicate that keeping pace with data security when traditional network perimeters have all but disappeared still presents formidable challenges. Among those challenges:

- **Data breaches remain common.** Among the surveyed companies, 42% reported having experienced at least one data breach within the past 12 months. Given that breaches often go undetected, the percentage of companies actually compromised may be higher.
- **Security is considered a daunting task by many.** More than half of the companies that did not experience a breach described securing their data as "very" or "extremely" challenging. The percentage was approximately the same whether companies were referring to securing data on-premises (54%) or in a public cloud (51%). However, in companies that had been compromised, the numbers were far higher: 78% found cloud security very or extremely challenging, and 76% found on-premises security to be so.
- **Dissimilar on- and off-premises security models are a sticking point.** Traditional three-tier data centers evolved with security best practices and tools built for that environment. But the cloud uses different technology principles and new types of access control tools that IT security traditionalists must learn.

Businesses are clearly looking for harmonization across these environments: Securing data moving between on-premises and the cloud was the No. 2 data protection challenge (35%), after guarding against malicious damage/hacking (36%). Much as with other results, companies that had experienced a breach also reported higher levels of difficulty with moving assets between cloud environments.

Distinguishing Characteristics of Data-Secure Enterprises

Why is securing newer hybrid IT environments such a struggle?

"You're trying to secure a moving target," says Ravi Srinivasan, vice president, solutions and platform marketing, at Forcepoint. "It's challenging and complex, because businesses often try to solve security by using a subset of data, such as deploying a data loss prevention [DLP] solution for emails or a cloud access security broker [CASB] to protect their cloud assets. Today you need a more programmatic approach that looks at all your data sources and channels and combines them into a [holistic] security strategy."

Srinivasan recommends implementing enterprise security systems fueled by powerful data analytics engines that take a user-centric view of data. "We call this dynamic data protection," he explains. "Based on where you fall on the risk continuum, policies applied

Forcepoint CSO FROM IDG

to each user will be individualized and dynamically change as that user's behavior changes and the associated risk varies."

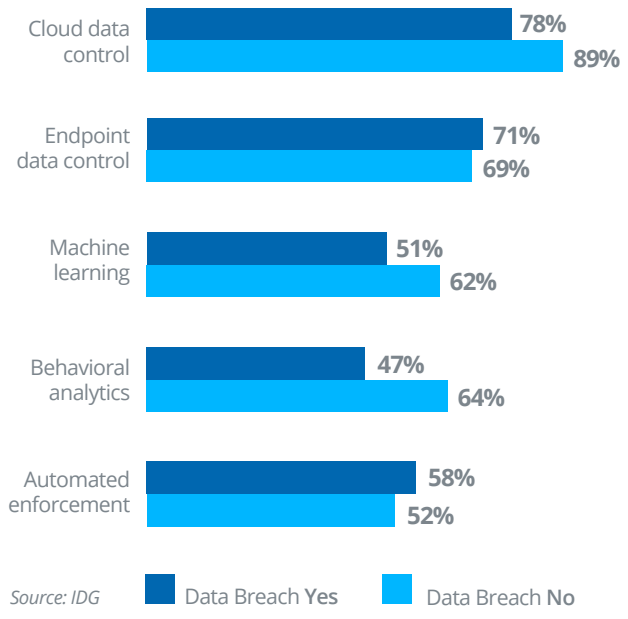
The company size or the number of cloud applications in use did not make a difference in the companies that had not experienced a breach. Rather, companies that had deployed behavior analytics tools and machine learning (ML) capabilities, along with those that had mastered the cloud data access controls offered by their cloud service providers, were less likely to have been infiltrated (see Figure 1).

Behavioral analytics involves using software tools that detect patterns of high-risk or unusual user behavior. Those tools then alert an IT team member or take automated action to counter the threat before damage can occur. Nearly two-thirds of the surveyed companies (64%) that had not experienced a breach are using this capability.

(Figure 1) Uncompromised Companies: What's in Their Security Arsenals?

Enterprises deploying behavioral analytics, machine learning, and cloud-based access controls were least likely to have been breached in the past 12 months.

Types of challenges remote workers pose to security:



Machine learning is becoming fundamental to cybersecurity, in part because of the sheer volume of data needing protection. ML-powered cybersecurity systems can rapidly analyze large numbers of patterns and translate those learnings to help prevent future attacks. Automation is essential when there simply isn't time for humans to track down and verify alerts and then remediate issues. Among the IDG survey respondents, 62% that had not experienced a breach are using ML.

The use of behavioral analytics and ML in the more secure enterprises implies an IT awareness of the changing nature of data in those companies. Protecting the moving target of expanding data repositories component by component is less effective than a user-centric, "follow-the-data" approach to security, says Ankur Chadda, senior product marketing manager at Forcepoint. "Traditional security methods built to protect monolithic infrastructures with definable network perimeters don't work as well when workloads are prone to moving dynamically across data centers and clouds," he explains.

The security policies associated with those moving workloads need to become dynamic, too, and they should account for changing risk variables, he says. "For example, you can automate security to deny or grant access—or different levels of access—based on factors such as the user's identity and job role; the access device in use, such as corporate- or user-owned equipment; and the network in use, such as a virtual private network [VPN] or unsecured public Wi-Fi. That means controlling what data a user can access, view, edit, download, share, and email, based on dynamic circumstances," Chadda says.

Automated policy enforcement that centers on users, their credentials, and their dynamic behavior serves enterprise security purposes better than building a static fortress around a physical population of servers, he notes, in large part because "you can't count on data that needs protecting to stay in one place."

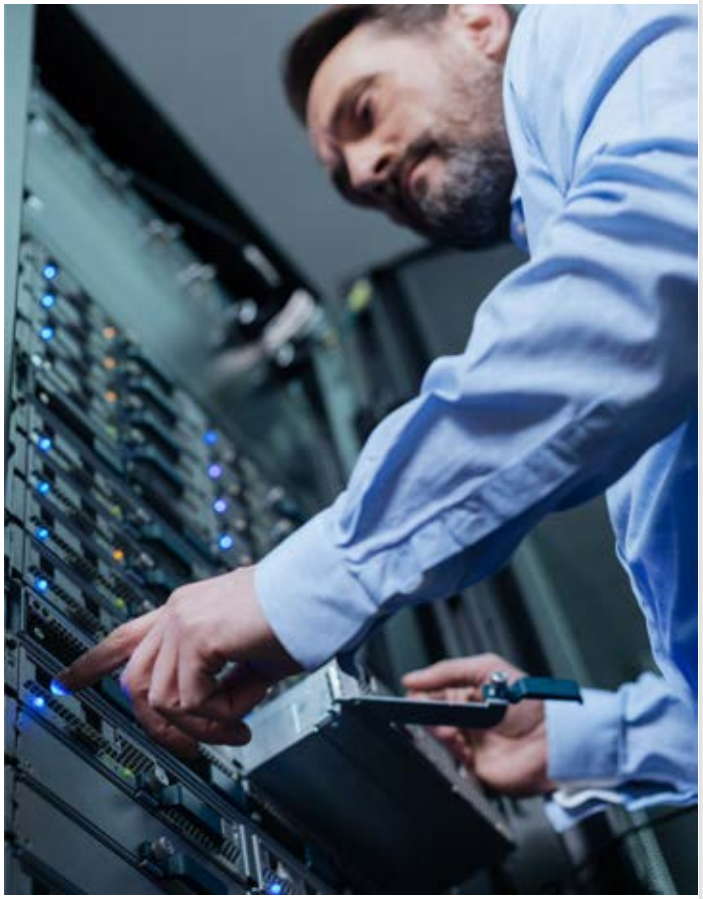
Upgrade Plans and Priorities

Companies that suffered a data breach in the past year, unsurprisingly, are most likely to upgrade their DLP infrastructures this year: Nearly all (96%) said they had plans for security upgrades. In addition, 88% of the companies that didn't report a breach also said they were planning upgrades.

However, most respondents of all types indicated that the greatest area of focus for those upgrades is on a variety of data backup solutions. These plans reflect a greater concern with business continuity and avoiding data loss than with protecting data privacy and avoiding theft of company and customer data.

Chadda theorizes that, given the high profile that ransomware has earned in the past few years, it follows that enterprises would want to bolster their data backup infrastructures. "If you have a backup, you keep working. If you don't, you're held hostage," he says. But although protecting the enterprise from the crippling downtime and financial devastation of a ransomware attack is essential, it's just one piece of the overall security picture, he points out.

Chadda and Srinivasan indicate that in addition to guarding against ransomware, it's just as important to secure data in ways that comply with privacy laws and critical data such as keeping intellectual property or trade secrets from falling into the wrong hands—protecting the personally identifiable information (PII) of consumers and patients, for instance. Noncompliance also can threaten devastation in the form of a damaged reputation, regulatory fines, and lawsuits—and data theft can destroy a company's value proposition(s) and competitiveness.



Upgrade Plans and Priorities

Although respondents indicated a high degree of confidence in their security strategies and abilities, they also acknowledged very real challenges, both on- and off-premises, of keeping pace with threats and bridging the on-premises/cloud security divide. Forcepoint's Srinivasan and Chadda offer some recommendations for addressing these challenges:

- **Deploy DLP systems integrated with machine learning, data analytics, and automation.** Smart systems that see the entire IT environment holistically can help enterprises keep pace with security issues cropping up in the massive volumes of data that might dynamically be stored across multiple IT infrastructures. Automated DLP systems rapidly identify usage patterns and learn from them to automatically grant or deny access based on the variables important to the company. Companies that have added these types of automation to their security arsenals reported fewer breach incidents in the IDG survey than companies not using these technologies.

- **Create user-centric policies.** "In today's IT model, users might interact with data using a variety of channels, such as a PC, a smartphone, a USB stick, an email application, the cloud, or a network," notes Srinivasan. "Trying to keep up by protecting each channel, one by one, using different, siloed products that don't intercommunicate, is less effective than controlling data based on user variables," he says. These include the device, network, and application being used for access, "and they're independent of any given data source or channel," he adds.

- **Be wary of protecting only part of your data environment.** To enhance user accessibility and productivity, it's not uncommon for an organization to run its DLP systems in audit-only mode, says Chadda. "That option is strong on usability but only allows a breach to be investigated after the fact, not prevent it," he says. Companies that use this approach might be compliant with the basics of some regulatory mandates, but it still leaves organizations open to downtime, damaged reputation, fines, lawsuits, and data loss, he adds.

  Similarly, some companies take a black-and-white tack of blocking or allowing all data access. "While it's true that completely locking down resources keeps them secure, the usability and productivity side of the equation—employees' need to access resources to adequately perform their jobs—goes unfulfilled," Chadda says. And, again, leaving all data and applications open so as not to hinder worker productivity leaves organizations vulnerable.

- **Avoid a hodge-podge of unintegrated, point security products.** A collection of tools may be optimized for a single application or device, but lack of integration means that the tools are not holistic in nature. As such, they offer no context about what's going on elsewhere in your environment, Chadda and Srinivasan advise.

- **Evaluate emerging unified cloud management and security platforms.** Unified platforms deliver visibility across hybrid private and public cloud infrastructure, with the ability to automate security policies to follow workloads among environments as conditions change.

The Bottom Line

Companies that have added automation in the form of cloud data control, behavioral analytics, and machine learning report fewer breach incidents than companies not using these technologies. The implication is that deploying them has helped enterprises build stronger defenses.

Chadda underscores the role that user risk should play in enterprise security strategies. "User risk ebbs and flows, depending on where and how a user is working. Static policies are challenged to address the security landscape on this level," he notes. Dynamic data protection, by contrast, adapts to the changing risk levels as circumstances dictate. Systems with this kind of protection combine DLP systems with powerful data analytics and cloud access control technology, working in concert, to keep pace with security needs across on-premises, public cloud, and private cloud environments.

About the Survey

Between May 4, 2020 and May 12, 2020, IDG conducted a research study to understand the business and technical benefits and challenges associated with securing data in the cloud. To qualify for the survey respondents were required to work for a company with 500+ employees and have a title of IT Manager or higher.

There were 106 respondents, of which 33% were C-level IT; 10% Executive VP, Senior VP, or VP; 21% Director; and 36% Manager. Fifty-six percent had an IT role in infrastructure and operations, including cloud; 33% in network management; and 11% in security management. Of the respondents, 63% categorized themselves as the final decision maker, while 36% are on a team that makes the final decision. The remaining 9% did not label themselves final decision makers.

Represented industries include technology (45%), hardware/software/network (12%), banking and financial services (8%), information/media/entertainment (7%), and high tech and electronics (5%). The remaining 19% split across other verticals including business/professional services, manufacturing/industrial, healthcare, and food and beverage.

For more information on DLP analytics, automation, and unified IT security, visit www.forcepoint.com

Forcepoint

CSO FROM IDG