Market Pulse

Protecting the Human Side of Cybersecurity

Behavioral analytics tops the list of cybersecurity best practices

The majority of enterprise companies have hundreds of apps deployed in the cloud, and that trend is expected to continue, according to a new survey by IDG. That said, 52% of companies find that securing those apps continues to be challenging.

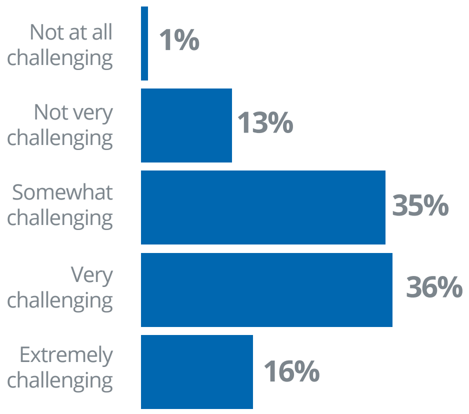
But that doesn't mean that the remaining 48% are fully confident in their cloud app security or are fully aware of all of the facets of cloud security they should be considering.

"Cloud security is a broad issue," says Jim Fulton, Director, Cloud & Edge Protection Solutions for Forcepoint. "From what I've seen, about 10% of companies really understand all of the facets. A more realistic answer is from the folks who express their lack of complete confidence in cloud security because as apps and data move to the cloud, there's often a corresponding lack of visibility. IT doesn't know where data is, and with 'shadow IT' projects, it can also be difficult to determine who's using what tools and applications, let alone reliably secure them all."

Half of the companies IDG surveyed said their infrastructure impedes protecting data when moving it to and from the cloud. Major reported threats to cloud security include lack of visibility (especially from shadow IT cloud apps); lack of monitoring; and malicious actors, both internal and external.

(Figure 1) Most Companies Find Securing Cloud Applications Challenging

Challenge of securing applications, data, and infrastructure in the cloud



Source: IDG

Cloud Security: Perceptions and Reality

The companies surveyed reported having an average of 18 vendors for security solutions. A majority of the companies believe they have the right tools to provide dependable cloud security (e.g., to prevent data loss in cloud apps; to manage data loss across the premises, cloud, and endpoints; to provide secure access and connectivity; etc.). Most of the survey respondents believe that their teams understand their security technology needs.

But perception is at odds with the reality that a majority of companies are experiencing or will encounter security threats they are unprepared to handle, leaving them open to exploitation. Among the surveyed companies, 31% said data loss at the edge—which can have major reporting and regulatory impacts—is a bigger concern than a direct attack (18%) or breach (21%).

Forcepoint CSO FROM IDG

The biggest data mobility issues with remote workers are securing multiple devices (50%), tracking and managing cloud assets (41%), and data backup and recovery (40%), which are generally the most common challenges of remote workers from an IT perspective (see Figure 2).

Shadow IT is a big issue, with 43% of the respondents listing it as their No. 1 security issue.

"With the increased necessity of working from home during the pandemic, the prevalence of shadow IT has definitely increased," says Fulton. "People are scrambling to find ways to get their jobs done while IT is often unavailable, fighting fires. Shadow IT presents more potential situations and vulnerabilities for attacks, breaches, and data loss."

Fulton also highlights other high-risk behavior outside of the office—such as using a personal computer for work, putting work files in Dropbox and Google Drive instead of an internal file server, and mixing personal web browsing with work-related browsing.

Behavioral Analytics to the Rescue

Among the cloud security technologies used by the respondents, behavioral analytics is currently in deployment at 28% of the surveyed companies. Another 32% of the respondents said they'll deploy behavioral analytics within the next year. This means that *by 2021, 59% of companies will be using the technology.* When used with intent, behavioral analytics can shine a light on the human element that plays a role in most any cybersecurity incident.

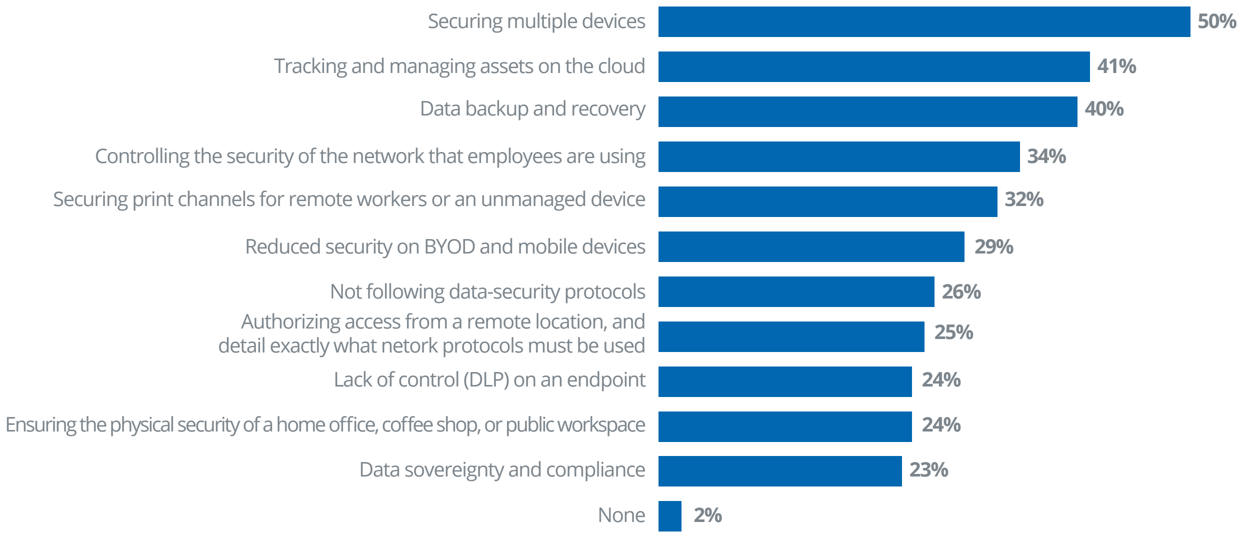
But behavioral analytics is still in its infancy. As a result, Fulton speculates that most companies and IT professionals lack a full understanding of the technology and may in fact misidentify it.

"There is a tendency to confuse looking at the data and correlations in security information and event management (SIEM) scripts from different log files and calling it behavioral analytics," he says. "With behavioral analytics, you're able to look at a much broader data set from email, browsing, usage patterns, time of day, location, etc., to identify abnormalities and then to get real-time, proactive mitigation instructions."

Among the companies reporting the most applications, a slight majority tend to favor behavioral analytics technology, with 65% either currently deploying it or planning to. These companies also tend to run more of their applications in the cloud and plan to move even more next year.

(Figure 2) Remote Workers Need IT to Secure Multiple Devices, Track and Manage Cloud Assets, and Back Up Data

Types of challenges remote workers pose to security



Source: IDG

This suggests that cloud transformation and behavioral analytics cybersecurity may go hand in hand.

Companies that currently deploy behavioral analytics say they find securing applications in the cloud less challenging than those that don't (47% versus 58%). Although behavioral analytics is considered among the most useful cloud security technologies by just 13% of companies overall, *46% of companies that use it find it to be the most useful cloud security technology* (see Figure 3).

Behavioral analytics users are much less likely to be concerned about data loss (18%) than are users in companies that have not adopted the technology (46%). Although nearly three-quarters of those who currently use or plan to use behavioral analytics said that it is very important or critical to the security stack, the finding begs the question: What about the other 25%?

"The use of behavioral analytics typically reflects a more advanced level of security expertise," says Fulton. "I don't think companies would go to the trouble without a clear understanding of how important it is to their cloud security." As previously noted, this finding may reflect a lack of awareness of what behavioral analytics is and the features and benefits it delivers, he notes.

Defining Behavioral Analytics

Behavioral analytics in cybersecurity is the use of software tools to detect patterns of high-risk human behavior or behavior that is out of the norm. BA tools detect these anomalies (e.g., malware that evades firewalls, intrusion-prevention systems, and antivirus software to silently take action from users' devices), compare them to a baseline of normal behavior, and alert IT managers.[1]

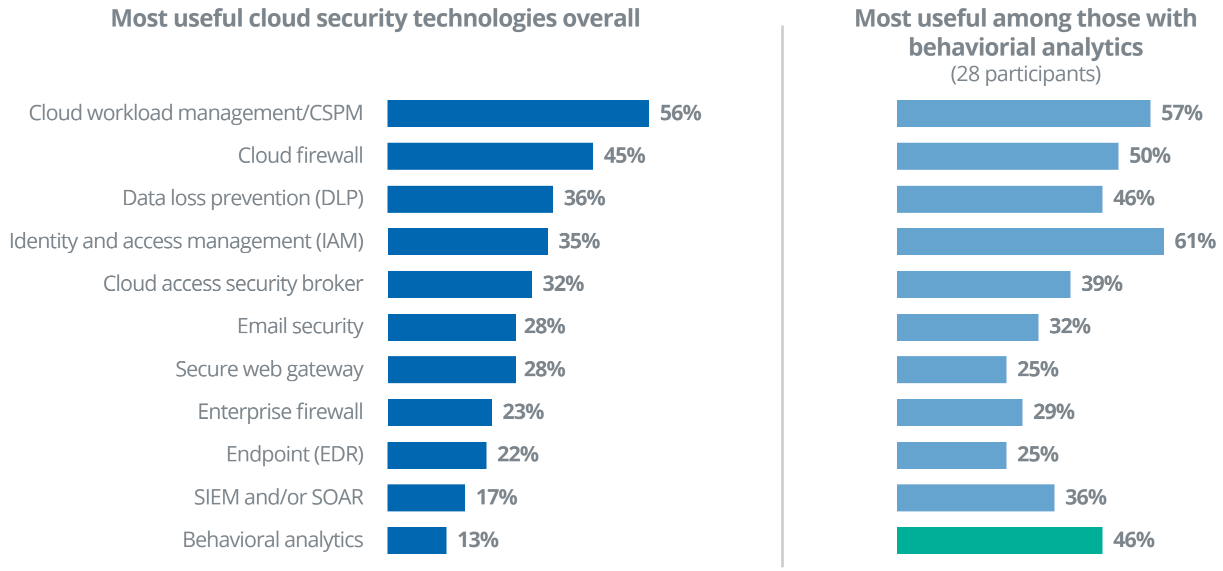
Best Practices for Filling Cybersecurity Gaps

Asked how they currently assess cybersecurity infrastructure to identify gaps in protection, survey respondents gave the following responses in three categories of activity.

1) Process review, passwords, and threat audits

- "Identify and understand business processes. Pinpoint the applications and data that underlie business processes. Find hidden data sources. Determine what systems underlie applications and data."
- "We constantly change passwords and are careful to look for human error."
- "We have frequent audits to ensure that there are no unidentified threats."

(Figure 3) Companies with Behavioral Analytics Find It Among the Most Useful Cloud Security Technologies



Most useful cloud security technologies overall

Most useful among those with behaviorial analytics (28 participants)

Source: IDG

Fulton adds several important considerations regarding the survey responses. “[Making] frequent password changes—password flailing—has been shown to cause more problems than it solves,” says Fulton. “Frequent audits, unless automated, can be cumbersome and disruptive. Some audits are ineffective, because they’re simple checklists that users gloss over. Unidentified threats often remain unidentified.”

2) Monitoring and tracking

- “We have our cloud security notifications on for anyone outside of our industry who is attempting to gain access to our cybersecurity infrastructure.”
- “We use intrusion detection systems (IDSs) to identify potential hostile cyberactivity, and we also make use of identity and access management (IAM) to limit and track employee access.”
- “We monitor our data from end to end continuously and are able to identify potential risks and data breaches.”
- “We do complete monitoring of the database information and use a strange-information alert.”

Fulton questions what constitutes the cybersecurity infrastructure of most companies today. “Does it include various software-as-a-service apps in the cloud along with proprietary apps running in the public cloud? Using IDS alone is very old-school. And monitoring and protecting end to end is difficult when a laptop is outside of the office.”

3) Technology solutions

- “We increasingly use different types of technology, including more endpoints and EdTech software.”
- “We are using cloud analytics to monitor access and alerts when activity is not expected or dangerous.”
- “We are employing security information and event management (SIEM) solutions to identify and stop network breaches before they occur, as they relate to policies for remote users and cloud-based traffic.”
- “We are currently undergoing SSAE-18 and SOC-2 assessments, with the hope that our weaknesses will be revealed and our strengths will be familiarized.”

As previously mentioned, looking at SIEM log files provides a limited view of user behavior. SIEM is also difficult to set up. “It tends to generate lots of noise and very little insight,” notes Fulton.

The Bottom Line

Enterprise companies have deployed hundreds of applications in the cloud, and the trend will continue. But securing those apps and stemming data loss continue to be challenging for more than half of the enterprises surveyed by IDG.

At the same time, according to IDG, 59% of companies will be using behavioral analytics solutions by 2021. Among those companies currently using it, there is less stated concern about data loss and less concern about user access management and data backup/recovery than among those not using it. These companies recognize that people and technology are working together to further the goal of cybersecurity.

The truth is, enterprise IT professionals may not yet fully understand the features and benefits of behavioral analytics cybersecurity in this early phase of its market introduction. Working with a trusted and knowledgeable partner, such as Forcepoint, is key for success.

About the Survey

Between April and June 2020, IDG conducted a research survey that looked at current and planned adopters of behavioral analytics cybersecurity. The survey focused on cybersecurity concerns with the continued movement of applications to the cloud and data moving between cloud, edge, and remote worker environments. It looked specifically at current and planned adoption of cybersecurity solutions that use behavioral analytics (BA), benefits derived by companies using BA, and best practices for assessing cybersecurity gaps as more apps move to the cloud.

To qualify for participation, respondents had to work for a company with 500+ employees in an IT or operations role and have a title of manager or above. Companies must have begun some form of cloud deployment.

There were 101 respondents, with 95% in IT and 5% in operations, mostly (67%) from organizations with more than 1,000 employees. The largest group (45%) was managers, and 22% were C-level or top IT executives. More than half (52%) work in technology or at a hardware, software, or network OEM.

[1] *https://www.computerworld.com/article/3147017/behavior-analytics-tools-for-cybersecurity-move-into-enterprises.html*