Symantec Research Finds More Than Half of Enterprises Believe Security Can't Keep Up With Cloud Adoption
Monday, June 24, 2019 04:00:00 PM (GMT)

Symantec's Cloud Security Threat Report (CSTR) finds cloud security exacerbated by immature security practices, overtaxed IT staff and risky end-user behavior

- 73% of respondents experienced a security incident due to immature security practices
- 93% report issues with keeping tabs on all cloud workloads
- 83% feel they do not have processes in place to be effective in acting on cloud security incidents and 25% of cloud security alerts go unaddressed
- 93% say oversharing is a problem, estimating that more than a third of files in the cloud should not be there

Symantec Corp. (NASDAQ: SYMC), the world's leading cyber security company, today announced new research revealing enterprises are struggling to keep up with the rapid expansion of cloud within their businesses. Surveying 1,250 security decision makers across the globe, Symantec's Cloud Security Threat Report (CSTR) uncovered insights on the shifting cloud security landscape, finding enterprises have reached a tipping point: more than half (53%) of all enterprise compute workload has been migrated to the cloud. However, security practices are struggling to keep up – over half (54%) of enterprises indicate their organization's cloud security maturity is not able to keep up with the rapid expansion of cloud apps.

"The adoption of new technology has almost always led to gaps in security, but we've found the gap created by cloud computing poses a greater risk than we realize, given the troves of sensitive and business-critical data stored in the cloud. In fact, our research shows that 69% of organizations believe their data is already on the Dark Web for sale and fear an increased risk of data breaches due to their move to cloud," said Nico Popp, senior vice president, Cloud & Information Protection, Symantec. "Data breaches can have a clear impact on enterprises' bottom line, and security teams are desperate to prevent them. However, our 2019 CSTR shows it's not the underlying cloud technology that has exacerbated the data breach problem – it's the immature security practices, overtaxed IT staff and risky end-user behavior surrounding cloud adoption."

Security modernization isn't keeping pace with the cloud

Companies are struggling to modernize their security practices at the same pace that they adopt cloud – 73% experienced a security incident due to immature practices. Lack of visibility into cloud workloads is the leading cause – an overwhelming majority of survey respondents (93%) report issues with keeping tabs on all cloud workloads. For example, Symantec's research found that while companies estimate they use 452 cloud apps on average, the actual number is nearly four times higher, at 1,807. As a result of these immature practices, including poor configuration or failing to use encryption or multi-factor authentication (MFA), enterprises are facing an increased risk of insider threats – ranked by respondents as the third biggest threat to cloud infrastructure. CSTR data shows that 65% of organizations fail to implement MFA in IaaS configurations and 80% don't use encryption.

Complexity is taking a toll

With cloud adoption introducing increased complexity in how IT is deployed – now across public cloud, private cloud, hybrid, on-prem – and where data needs to be secured, IT teams are becoming overtaxed. Given this, it's not surprising that the CSTR revealed 25% of cloud security alerts go unaddressed. A majority (64%) of the security incidents occur at the cloud level, and more than half of respondents admit they can't keep up with security incidents. What's more, the future looks foggy – 83% feel they do not have processes in place to be effective in acting on cloud security incidents.

Risky behaviors run rampant

One of the biggest challenges for security teams attempting to get a handle on the cloud is rampant risky user behavior. According to CSTR respondents, nearly one in three employees exhibit risky behavior in the cloud, and Symantec's own data shows 85% are not using best security practices. As a result of these risky behaviors, sensitive data is frequently stored improperly in the cloud, making enterprises more susceptible

to breach; 93% of CSTR respondents say oversharing is a problem, estimating that more than a third of files in the cloud should not be there. Additionally, the cloud is not immune to the risky behavior that plagued past technologies – respondents report users with weak passwords (37%) using poor password hygiene (34%), using unauthorized cloud apps (36%), and connecting with personal devices (35%) as common risky behavior.

The way forward

While the cloud has introduced new efficiencies and capabilities to the enterprise, the CSTR reveals that too many companies are not confronting the security risks that cloud adoption has introduced, including an increased risk of data breaches. Investment in cloud cyber security platforms that leverage automation and AI to supplement visibility and overtaxed human resources is a clear way to automate defenses and enforce data governance principles. However, as the consequences of cyber security become increasingly impactful to business success, it is also time to recalibrate culture and adopt security best practices at a human level.

To learn more, register to attend the webinar, read the blog and download the full report.

Methodology

The Symantec 2019 Cloud Security Threat Report compares and contrasts the perceptions versus realities of cloud security using a combination of an external market study of 1250 IT decision-makers in 11 countries worldwide against various security telemetry that Symantec tracks across Cloud, email, Web security services, threat intelligence and other internally managed data sources.

About Symantec

Symantec Corporation (NASDAQ: SYMC), the world's leading cyber security company, helps organizations, governments and people secure their most important data wherever it lives. Organizations across the world look to Symantec for strategic, integrated solutions to defend against sophisticated attacks across endpoints, cloud and infrastructure. Likewise, a global community of more than 50 million people and families rely on Symantec's Norton and LifeLock product suites to help protect their digital lives at home and across their devices. Symantec operates one of the world's largest civilian cyber intelligence networks, allowing it to see and protect against the most advanced threats. For additional information, please visit www.symantec.com or connect with us on Facebook, Twitter, and LinkedIn.

View source version on businesswire.com: https://www.businesswire.com/news/home/20190624005128/en/

--30-- AR/SF

Contact:

Nicole Murphy
Symantec
650-527-8000
Nicole_murphy@symantec.com

Industries: Data Management, Security, Technology, Software, Networks
Languages: English
Primary Identifiers: NLOK-US
Related Identifiers: NLOK-US, US871503108
Source: Symantec Corporation

Subjects: Survey