Adapting to the New Reality of Evolving Cloud Threats

Visibility is Cloudy

According to a 2019 survey of 1,250 security decision makers conducted by Symantec, the average organization believes its employees are using 452 cloud apps. However, according to Symantec’s own data, the actual number of Shadow IT apps in use per organization is nearly four times higher, at 1,807.

Increased Complexity

Cloud is the business

53% of IT leaders believe that cloud has changed the nature of their business environment.

Security can’t keep up

54% of IT leaders say their security solution is not as effective as it should be.

Limited visibility

93% of IT leaders say they have a problem with visibility and lack of complete cloud app inventories.

Insider threats

93% of IT leaders have a problem with over-sharing of cloud files containing sensitive data.

Limited data protection

68% of IT leaders say they have seen or likely have evidence that their data has been for sale.

Security can’t keep up

64% of IT leaders say security can’t keep up with the rapid expansion of new cloud apps.

Data for sale

There is significant evidence of data for sale on the Dark Web.

Increase in lateral movements and cross-cloud attacks

Enterprises often underestimate the scale and complexity of cloud threats. Perceptions are that data breaches, DDoS attacks and cloud malware injections are the most common incidents.

Surprises

#3 Science for lateral movement and cross-cloud attacks:

A 2020 report by Symantec found that about 75% of organizations were not aware of the extent of their Shadow IT and about 50% of their Shadow IT apps were unknown.

#1 Shocking statistic:

A 2020 report by Splunk found that 96% of organizations said they had experienced a security breach, with 48% of those organizations experiencing multiple breaches.

#2 Security awareness:

A 2019 survey by the Ponemon Institute found that 71% of security professionals said that they had experienced a security breach, with 48% of those organizations experiencing multiple breaches.

Immature Security

Multi-factor authentication

65% of IT leaders say they have not yet implemented multi-factor authentication (MFA) for cloud apps.

Poor password hygiene

85% of IT leaders say they have a problem with poor password hygiene.

Few employees know:

68% of IT leaders say that their employees are not aware of the potential risks associated with cloud apps.

Culture and behavior

85% of IT leaders say that cultural and behavioral issues are some of the greatest risks.

Unexpected Threats

Multi-factor authentication

85% of IT leaders say that they have a problem with multi-factor authentication.

Insecure remote work

68% of IT leaders say that their employees are not aware of the potential risks associated with remote work.

Loss of control

Cloud makes it easy to lose control of the data.

Data for sale

There is significant evidence of data for sale on the Dark Web.

Increase in lateral movements and cross-cloud attacks

Enterprises often underestimate the scale and complexity of cloud threats. Perceptions are that data breaches, DDoS attacks and cloud malware injections are the most common incidents.

Insider threats

Those who are closest to the organization (trusted insiders with access to protected data) represent some of the greatest risks.

Building an Effective Cloud Security Strategy

Develop a governance strategy supported by a Cloud Center of Excellence (CCoE)

Embrace a Zero-Trust model

Promote shared responsibility

Use automation and artificial intelligence wherever possible

Learn more about the shifting cloud security landscape

Download the Cloud Security Threat Report

For more information, visit Symantec.com/CloudSecurity

Visibility is Cloudy

According to a 2019 survey of 1,250 security decision makers conducted by Symantec, the average organization believes its employees are using 452 cloud apps. However, according to Symantec’s own data, the actual number of Shadow IT apps in use per organization is nearly four times higher, at 1,807.