Symantec.

Adapting to the New Reality of Evolving Cloud Threats

Today's cloud migration is challenging existing security paradigms, leaving organizations scrambling to keep up. To maintain visibility and control, companies need new and automated cloud-based security solutions as well as the skill sets and processes to effectively manage them.

You can download the full report here

Visibility is Cloudy

According to 1,250 security decision makers Symantec surveyed worldwide in Spring 2019, 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.

452
PERCEPTION

1807 CLOUD APPS
REALITY

Increased Complexity

Cloud IS the business now

This is where mission-critical workloads, data and business functions are now taking place. Security must follow.

53%
OF ALL COMPUTE WORKLOAD HAS NOW BEEN MIGRATED TO THE CLOUD ACCORDING TO THE EXTERNAL STUDY.

Security can't keep up

Cloud adoption is moving too fast and enterprises are struggling to manage increased the complexity and loss of control.

54%
AGREE THAT THEIR ORGANIZATION'S CLOUD SECURITY MATURITY IS NOT ABLE TO KEEP UP WITH THE RAPID EXPANSION OF NEW CLOUD APPS.

Limited visibility

The complexity in how IT is deployed (public cloud, private cloud, hybrid, on-premises) is creating visibility problems for IT.

93%
REPORT ISSUES KEEPING TABS ON ALL CLOUD WORKLOADS.

Loss of control

Cloud makes it easy to lose control of the data.

93%
HAVE A PROBLEM OVERSHARING CLOUD FILES CONTAINING SENSITIVE DATA.

Unexpected Threats

Increase in lateral movements and cross-cloud attacks

Enterprises often under-estimate the scale and complexity of cloud threats. Perceptions are that data breaches, DDOS attacks and cloud mal-ware injections are the most common incidents.

64%
OF CLOUD SECURITY INCIDENTS ARE DUE TO UNAUTHORIZED ACCESS (AN OPEN DOOR FOR LATERAL MOVEMENT), ACCORDING TO SYMANTEC DATA.

Insider threats

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

#3
ACCIDENTAL INSIDER THREAT RANKED THIRD ON LIST OF THREATS TO CLOUD INFRASTRUCTURE, ACCORDING TO SURVEY.

Data for sale

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

68%
HAVE EITHER SEEN DIRECT OR LIKELY EVIDENCE THAT THEIR DATA HAD BEEN FOR SALE. 31% DID NOT BELIEVE THEIR DATA WAS AT ANY RISK.

Immature Security

Multi-Factor Authentication

Immature security practices are driving higher incidents of insider threats.

65%
NEGLECT TO IMPLEMENT MULTI-FACTOR AUTHENTICATION (MFA) AS PART OF THE CONFIGURATION OF IAAS AND 80% DON'T USE ENCRYPTION, ACCORDING TO SYMANTEC DATA.

Culture and behavior

are struggling to keep pace with the shift to cloud.

85%
SYMANTEC INTERNAL DATA REPORTS THAT 85% OF SYMANTEC CUSTOMERS ARE NOT USING CENTER FOR INTERNET SECURITY (CIS) BEST PRACTICES.

Poor password hygiene

is symptomatic of overall lax security behavior.

#1
WEAK PASSWORDS (37%) AND POOR PASSWORD HYGIENE (34%) TOP THE LIST OF BAD BEHAVIORS.

BEST PRACTICES FOR

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

Symantec.