Adapting to the New Reality of Evolving Cloud Threats

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.

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.

Limited visibility (76% reported difficulty identifying clouds and cloud services) has been one of the biggest challenges, putting a strain on security operations. Moreover, IT has never been busier. 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.

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

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.

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

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

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

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% OF CLOUD WORKLOADS HAVE BEEN MIGRATED TO THE CLOUD.

Increased lateral movements and cross-cloud attacks are becoming more prevalent as organizations are now more connected. As of 2020, 64% of organizations experienced a security event caused by an employee.

64% REPORT THAT THE FACTOR RESIDENT IN AN ORGANIZATION IS MOST LIKELY TO AFFECT SECURITY OUTCOMES.

Data for sale

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

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.

Increased Complexity

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.

Unexpected Threats

Funder Threats

There are only three things a cybercriminal wants. They want to know who you are, what you do and where you are. In 2020, 68% of organizations have been targeted at least once by a hacker.

68% OF ORGANIZATIONS HAVE BEEN TARGETED AT LEAST ONCE BY A HACKER.

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

66% REPORT THAT THE FACTOR RESIDENT IN AN ORGANIZATION IS MOST LIKELY TO AFFECT SECURITY OUTCOMES.

Poor password hygiene

Poor password hygiene is symptomatic of overall lax security behavior.

53% OF USERS CHOOSE A PASSWORD BASED ON A PICTURE OR PET’S NAME, ACCORDING TO SYMANTEC DATA.

Cultural and behavioral awareness is the key to successful security.

85% OF ORGANIZATIONS REPORT INADEQUATE CULTURAL AND BEHAVIORAL AWARENESS AS A SECURITY RISK.

Preventance of Risk

Downward Trend

Building an Effective Cloud Security Strategy

Develop a governance model 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

To download the full report here...