THE STATE OF CLOUD NATIVE SECURITY 2020

paloalto NETWORKS | PRISMA CLOUD BY PALO ALTO NETWORKS

Executive Summary

SECTION ONE

The State of the Cloud and Cloud Native Adoption

Cloud will become the dominant computing model over the next 24 months

- Enterprises using the cloud are close to the halfway point in their journey to the cloud. They now run 46% of their workloads in the cloud and expect to get to 64% in the next 24 months.

We are in a multicloud, multi-compute world

- 94% of organizations use more than 1 cloud platform
- 60% use between 2 and 5 platforms
- AWS is the most popular public cloud service provider

Diversity in application architectures is likely to continue, leading to growth in all forms of compute (IaaS, CaaS and PaaS) that power cloud applications

- No one compute dominates: Companies are spreading their workloads across all four computes (VMs 30%, containers 24%, CaaS 21%, PaaS 22%)
- 86% of companies expect their usage of all four computes to increase or stay the same over the next two years

Customers expect cloud to continue to evolve

- 80% of respondents say their company's cloud infrastructure is constantly evolving

SECTION TWO

The State of Securing the Cloud and Cloud Native Workloads

The top three challenges for moving workloads to the cloud

- Technical complexity (42%)
- Maintaining comprehensive security (39%)
- Ensuring compliance (32%)

Security cannot be addressed by solving for a single issue

- Asked to select the top three threats facing their company's cloud services, respondents chose the following:
  - Data security and malware
  - Application vulnerabilities
  - Weak and broken authentication
  - Insider threats
  - Credential leakage
  - Insecure APIs
  - Over-permissioned access
  - Misconfigurations

Challenges to providing comprehensive cloud security are often internal to a company's culture and organization

- The top four challenges identified by survey takers:
  - Lack of visibility of security vulnerabilities (15%)
  - Employee training on security tools (14%)
  - Employee training on safe practices (11%)
  - Evaluating the current state of security (11%)

Cloud security team structures are in transition. Most companies have a hybrid model comprising a center of cloud security excellence that works closely with security points of contact in decentralized development teams

- 77% of companies have more than 20 people on their cloud security teams
- 47% have both a centralized cloud security team and security experts embedded with delivery teams (cross-functional)
- 31% have a fully centralized cloud security structure
- 22% use a fully cross-functional cloud security structure

Organizations don't understand that cloud security responsibilities are shared

- 73% of companies struggle to clearly delineate between their cloud security provider's (CSP's) security responsibilities and their own

More security tools doesn't necessarily mean better security

- Companies investing more than $100 million in cloud are trimming the number of tools they use
    - 53% of this high-spending group use just 5 or fewer cloud security tools
- Acquiring more tools and vendors can create inefficiencies and make employee tool training more difficult
- Companies start to see overlaps between tools and vendor offerings, so they consolidate and rationalize tools and tool providers
- 71% of companies use third-party vendor tools, 65% use CSP-provided security tools and 62% use open source tools

Security spend is growing disproportionately with cloud spend

- Cloud security spend is highest for companies with an annual cloud budget of $100 million or more
- 34% of these high spenders allocate 16% or more of their cloud budget to security

SECTION THREE

Measuring Security Preparedness

Keeping your cloud secure depends on a set of cloud security actions

- To determine how secure a company's cloud estate is, we developed a metric called *cloud security preparedness*
- This measure was derived from answers to questions about 19 specific security practices across cloud workloads
    - Two of the practices span the entire cloud infrastructure
    - The other 17 practices refer specifically to three types of cloud compute:
      VMs, containers and PaaS
- We identified three levels of security preparedness among surveyed organizations: low, medium and high
    - Only 18% of companies are highly prepared to keep their cloud estates secure
    - 29% of companies fall into the lowest-prepared category

Companies at the highest level of cloud security preparedness are embedding security into their DevOps process and integrating security into the software development lifecycle

- 45% of highly prepared companies have embedded security into DevOps processes, and 41% integrate security in at least four stages of the development lifecycle
- By contrast, 21% of the lowest-prepared companies have embedded security in DevOps, and just 12% involve security in at least four stages of the development lifecycle

As companies improve security preparedness and expand security practices, they recognize that using many security tools can actually hinder cloud security

- 52% of employees at highly prepared companies with 11 or more security tools said a high number of tools made it more difficult to prioritize risks and prevent threats
- By contrast, just 16% at low-preparedness companies with 11 or more tools saw multiple tools as a problem

As companies improve their security preparedness, they agree that using a single, comprehensive security solution would improve their security

- For highly prepared companies using 11 or more security tools:
    - 50% say they're actively reducing the number of tools
    - 51% agreed that using a single, end-to-end cloud security solution would improve their cloud security posture

paloalto NETWORKS

3000 Tannery Way
Santa Clara, CA 95054

Main: +1.408.753.4000
Sales: +1.866.320.4788
Support: +1.866.898.9087

www.paloaltonetworks.com