SOLUTION BRIEF

The Top Challenges of Cloud Network Security

Cloud security is a broad topic, encompassing network security, application security, data security, identity and access management, workload protection, and much more. In this document, we will focus on network security fundamentals. However, it is important to note that network security tools should not be considered in isolation. Security solutions should be designed to work together to form a security fabric that can extend from data centers to branch locations then to the cloud or multiple clouds.

$4.45 M

According to a recent report, the average cost of a data breach was $4.45 million in 2022.[1]

What is cloud network security?

Cloud network security refers to the technology, policies, controls, and processes used to protect data and workloads in public and private clouds. It focuses on protecting cloud networks from unauthorized access, modification, misuse, or exposure.

Cloud network security forms one of the foundational layers of cloud security. It enables companies to embed security monitoring, threat prevention, and network security controls into their cloud infrastructure to help manage the risks of the dissolving network perimeter.

Cloud network security challenges

Cloud computing can be just as secure as traditional, on-premises computing. However, cloud deployments do present some challenges unique to cloud environments, such as:

1. **Lack of skilled cloud security experts**
   According to the Fortinet 2023 Cloud Security Report,[2] 43% of companies reported that the shortage of qualified staff is their biggest "day-to-day headache" in protecting cloud workloads. Cloud security requires high technical skills and knowledge to implement and maintain it effectively. However, many organizations face a shortage of qualified and experienced cloud security professionals who can handle the complexity and diversity of cloud security challenges. The cloud security skills gap can result in inadequate or ineffective cloud security practices, policies, and solutions and increased vulnerability and risk for organizations using cloud computing.

Figure 1: Reported biggest operational, day-to-day headaches trying to protect cloud workloads

2. Legal and regulatory compliance

Compliance requires ensuring that cloud-based applications and data meet different industries' and regions' standards and regulations. However, cloud environments are often complex, dynamic, and heterogeneous, which makes it difficult to monitor and enforce compliance policies consistently.

Cloud providers and the organizations that rely on them must comply with various laws and regulations that govern data protection, privacy, and security in different regions and industries. These include the General Data Protection Regulation (GDPR), the Health Insurance Portability and Accountability Act (HIPAA), the Payment Card Industry Data Security Standard (PCI DSS), and others. Compliance requires in-depth visibility into an organization's systems and data across clouds and data centers.

3. Lack of visibility

Modern IT environments are highly distributed, with applications deployed across private data centers, multiple public clouds, and edge locations. This means that most enterprises have potentially hundreds of applications spreading across a combination of SaaS-based, IaaS-based, private DC-based, or edge locations. Adding even more complexity is that shadow IT groups can spin up applications without full knowledge of the IT team.

As organizations build out their hybrid IT infrastructure, they must have end-to-end visibility of the IT environment and eliminate any blind spots, as it is impossible to manage something that you cannot "see." Visibility must be **broad** to identify and scan resources, activities, and potential vulnerabilities across the entire compute surface. Visibility must also be **deep** to pierce the veil of encryption to identify malicious or inappropriate traffic. And it must be application aware to quickly identify known and unknown applications and apply appropriate security and routing policies, including zero trust policies.

4. Consistent security policies

The Fortinet 2023 Cloud Security Report also found that 69% of organizations surveyed were using two or more cloud providers,[3] with each provider promoting its own network security tools and services. Unsurprisingly, companies that have relied on their cloud vendors for security are finding it a challenge to offer and enforce consistent security policies across clouds and data centers.

With multiple cloud providers in use, it can be difficult to keep track of everything and ensure that each component is configured correctly. Every cloud service provider has a different approach to security, models, responsibilities and compliance obligations, best-practice recommendations, and names for the same services. Worse, these security products may have different features and different detection rates. Given the above, it comes as little surprise that many organizations struggle to offer consistent security policies when relying on varied security tools.

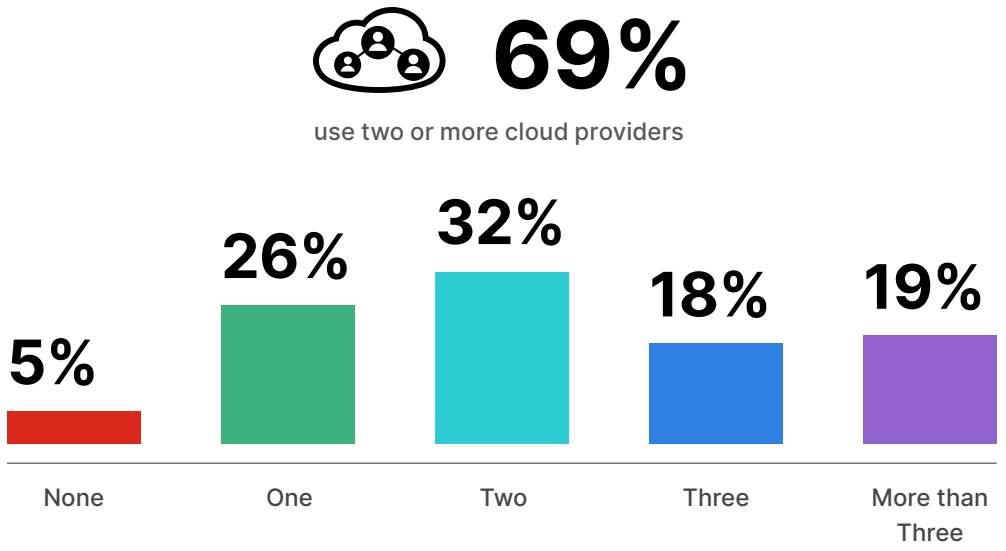

Figure 2: Most organizations struggle to apply consistent security policies across clouds.

5. Expanded attack surface

The attack surface is the sum of all possible entry points, or attack vectors, where an unauthorized user can access a system with nefarious intent. These include applications, code, APIs, ports, servers, websites, and even orchestration and automation systems. The attack surface also includes shadow IT, in which users bypass IT to use unauthorized applications or devices.

By definition, cloud services are accessed over the internet, making them more exposed to potential attackers. In this way, cloud computing is similar to DMZs in traditional networks, making them more vulnerable to attacks. Further, cloud-specific technologies and interfaces introduce new attack vectors that might not exist in traditional IT environments. These include attacks targeting cloud APIs, orchestration platforms, containerization systems, and serverless architectures.

6. Complexity

Complexity is the enemy of security. In fact, Gartner famously stated that by 2025, human failure, largely due to complexity, will be responsible for over half of significant cybersecurity incidents.[4] Complexity is not new; it's been creeping up on us for years. Multi-cloud and other complicated, heterogenous platform deployments have recently accelerated overly complex deployments. At the same time, security budgets, approaches, and tools have remained static. As complexity rises, the risk of breach accelerates at approximately the same rate.

7. Human error

Human error, the inevitable result of the six factors above, is ultimately at the root of most data breaches. Cloud computing, especially when multiple clouds are in play, increases the likelihood of mistakes and misconfigurations that can lead the best defenses to fail. For example, 59% of cybersecurity professionals surveyed said that misconfiguration remains the biggest cloud security risk.[5] These mistakes are all the more likely when organizations rely on cloud-specific security tools. One of the priorities of any digital transformation effort should be to reduce human errors by reducing complexity, reducing the number of tools staff need to learn and manage, reducing the attack surface, and increasing visibility into cloud systems, traffic, and users.

October 11, 2023 9:39 PM

2343766-0-0-EN