Check Point
SOFTWARE TECHNOLOGIES LTD

WELCOME TO THE FUTURE OF CYBER SECURITY

IS YOUR DATA EXPOSED?

TOP 5 CLOUD SECURITY CHALLENGES

> (Public cloud IaaS) is projected to grow 36.8 percent in 2017 to reach $34.6 billion.
>
> — Gartner, Inc.

INSIGHTS

Businesses of all sizes are rapidly migrating workloads and data to public cloud environments to improve efficiencies, drive innovation and increase responsiveness to market conditions. So much so that analyst firm Gartner predicts adoption of public IaaS services will grow "38.6 percent in 2017 to reach $34.6 billion" and is forecast to exceed $71 billion by 2020. While the cloud provides numerous benefits there are also some rather unique security challenges organizations face when they move resources to the cloud.

The first step in minimizing your exposure is to identify your security challenges and threats. The top five security challenges in the public cloud are:

1 Data Breaches

A server connected to the internet on premise or in the cloud is vulnerable to the same threats. We spend a great deal of time, resources and money building a security posture to defend our premise-based networks against attacks but these same security solutions don't reach the cloud. Cloud providers focus their efforts on protecting their infrastructure, cloud fabric, hypervisors, services and tenant environments, but you are responsible for protecting any assets or data you place in the cloud.

Additionally, the lateral movement of modern threats means that once a cloud asset is infected, malware then looks to see what else it can infect and it starts to spread uninhibited. And with the cloud now connected to premise-based networks, that same malware now has unfettered access to potentially all your corporate assets.

It's imperative not to be lulled into a false sense of security when moving to the cloud; it is your responsibility to protect any assets and data you place in the cloud. To keep your cloud environment protected, it is highly recommended to deploy an advanced threat prevention solution to inspect all traffic entering and leaving your cloud to prevent attackers from targeting your assets.

2 Compromised or Hijacked Accounts

Scripting tools, keylogging, spear phishing, brute force attacks and weak passwords mean attackers have a variety of ways to gain access to your cloud assets and data. Worse still, stolen or hijacked user credentials can be used to falsify or manipulate data, alter configurations and other networking parameters and give attackers carte blanch over your cloud environment.

Even developers can contribute to this problem unknowingly, embedding credentials and cryptographic keys into source code then exposing that code to repositories such as GitHub. Keys should be appropriately protected and like passwords, rotated periodically to make it harder for the bad guys to use any keys they obtain.

Make it hard for attackers who target user accounts. Implement the use of multifactor authentication as well as good key management practices when utilizing public cloud environments.

3 Insider Threats

This doesn't just pertain to users behaving maliciously, but also includes users doing dumb things like connecting cloud assets directly to the internet, using default settings or weak passwords, or misconfiguring the infrastructure. And if current headlines are any indication, this is going to be a challenge organizations will have to deal with for quite some time.

The issue gets compounded due to the fact that cloud architects and DevOps disciplines don't have a strong security pedigree. These teams are woefully unaware of the security implications that defining new infrastructure or making new connections in the cloud have on the overall posture of a cloud-based application or asset.

Traditional security teams – on the other hand – also have limited knowledge of cloud or DevOps processes and tools. These teams are often unaware of changes to the infrastructure until something goes wrong. Add it all up and you have a perfect storm of unintentional exposure of data and assets in the cloud.

Proper training and alignment of all disciplines that now define and implement infrastructure is more critical than ever when migrating infrastructure to the public cloud.

4 Insecure APIs

Application programming interfaces (APIs) allow organizations to customize cloud services to suite their unique needs, giving programmers the ability to integrate their applications with other cloud-centric processes such as provisioning, orchestration and management. However, APIs can also be used to manipulate a cloud environment due to the fact that they are designed to authenticate, provide access controls and effect encryption – providing a handy exploit route for savvy hackers.

Risk increases exponentially when other organizations are introduced to the mix, as customers use APIs to now expose services, applications and credentials to a variety of third-party partners and other service providers. Worse still, these interfaces are increasingly accessible over the Internet.

Apart from rigorous code reviews and penetration testing, it is imperative that adequate controls around APIs be implemented to prevent misuse and mitigate risks.

5 Encryption (or Lack Thereof)

Encryption has long been one of the most basic methods for securing data; still many enterprises fail to adequately encrypt sensitive data – especially in the cloud. While some cloud providers are more advanced than others regarding security, information stored in the cloud is often beyond a customer's control. Meaning the integrity of your data may rely entirely on the security practices of your cloud provider.

Also, the rising trend of the bring-your-own-device (BYOD) phenomenon transforming the workplace, employees also feel empowered to use their own cloud-based apps or collaboration tools to store and share corporate data. This inadvertently ushers in the rise of shadow IT services, which could expose your data to unknown third-party applications.

And this trend hasn't gone unnoticed by the bad guys. In fact, Gartner predicts that one-third of security breaches will result from shadow IT services by 2020. As a general rule of when using public cloud services; trust no one and encrypt everything. This is true of any data stored in the cloud but should also be true of any data transmissions to and from the cloud.

THE BOTTOM LINE

With benefits like increased agility, improved efficiencies and lower overall fixed costs, it's not a surprise that nearly 95 percent of businesses are now using the cloud. Still, the cloud has its share of unique security issues. In a recent Cyber Security Survey, 81 percent of those polled expressed concern over public cloud usage, with 49 percent being 'extremely' or 'very concerned.'

From the constant threat from malware to malicious users and misconfigurations, there are number of specific challenges organizations face when moving data, assets and workloads to the cloud. It is important to not only understand these risks but also to identify the proper technology and techniques to properly secure your public cloud environment.

CONTACT US **Worldwide Headquarters** | 5 Ha'Solelim Street, Tel Aviv 67897, Israel | Tel: 972-3-753-4555 | Fax: 972-3-624-1100 | Email: info@checkpoint.co
U.S. Headquarters | 959 Skyway Road, Suite 300, San Carlos, CA 94070 | Tel: 800-429-4391; 650-628-2000 | Fax: 650-654-4233 | www.checkpoint.com