7 Practical Solutions for Modern Businesses Combating Cloud-Based Attacks

May 2, 2023
by SentinelOne

With cloud services, modern businesses have been able to scale up their operations, meeting changing market conditions, customer demand and improving both flexibility and productivity. As more businesses move their operations to the cloud, robust security for cloud environments has proved more critical than ever. Cloud security is now a non-negotiable; a top priority for many Chief Information Security Officers (CISOs) who take proactive measures to safeguard their organization's data and assets from potential threats.

Cloud security is a significant concern for organizations of all sizes, and there are many challenges that businesses need to address to ensure that their cloud environment remains secure. This post explores the main cloud security challenges facing modern businesses and provides practical solutions to help mitigate these risks and secure their cloud infrastructure.

1. Defend Against Data Breaches and Cyber Attacks

Attackers are constantly on the lookout for vulnerabilities in cloud-based systems, and they can gain access to sensitive information through various means, such as phishing attacks and ransomware. In fact, IBM's Cost of a Data Breach 2022 latest insights on breaches found that 45% started with a cloud-based cyber attack.

Cloud-based cyberattacks have become a leading cause for data breaches due to several reasons. As more businesses move their data and applications to the cloud, cybercriminals have shifted their focus to target these platforms. Since cloud providers store vast amounts of data from multiple clients on the same infrastructure, they are – to cyber criminals – a springboard to many lucrative assets in one source.

Cloud-based cyber attacks are often highly sophisticated, and cybercriminals are continually developing new tactics and techniques to infiltrate cloud environments. They can exploit vulnerabilities in cloud applications, manipulate system settings, and steal login credentials to gain unauthorized access to sensitive data.

Attacks on clouds can be difficult to detect, and businesses may not realize they have been breached until significant damage has been done. Threat actors can remain undetected for weeks or even months, quietly siphoning off data and stealing valuable information before causing devastating consequences for the victims including downtime, lost productivity, and reputational damage.

How to Mitigate the Risk

To mitigate the risk of cloud-based cyberattacks, businesses can adopt a comprehensive security strategy centered around continuous monitoring, threat detection, and a strong incident response plan. Implementing strong access controls, encrypting sensitive data, segmenting their networks, and regularly backing up critical information are all proactive approaches CISOs can take to fortify their cloud security, better protect their data, avoid costly data breaches, and maintain their customers' trust.

2. Tackle the Risk of Insider Threats

Insider threats pose a significant risk to cloud environments, making them vulnerable to attacks. Unlike external threats, insider threats come from individuals who have authorized access to the cloud infrastructure – trusted employees, contractors, or even third-party vendors are all considered insider risks when it comes to cloud security.

Whether through malicious intent, or causing security breaches due to lack of training or accident, those with trusted access to sensitive data may expose it by leaving their login credentials in plain sight. Insiders with administrative access to cloud systems can make unauthorized changes to configurations, misconfigure security settings, or bypass security controls, creating pathways for attackers to exploit.

A significant challenge for CISOs facing inside threats is how hard they are to detect. Once users have legitimate access to the cloud environment, they can easily bypass basic security measures.

How to Mitigate the Risk

To address the risk of insider threats, businesses should implement strict access controls, regularly monitor cloud environments for suspicious activities, and provide regular security training to employees. Regular employee training and education programs can help raise awareness of the risks of insider threats and help employees understand their shared role in maintaining the organization's security.

3. Meet Compliance and Regulatory Requirements

The regulatory landscape is often a tricky one for CISOs to navigate on their own as it is constantly changing, meaning businesses must keep up with the latest laws and regulations to ensure compliance. Varying across different industries, geographies, and even the type of data being stored or processed in the cloud, these requirements can be a complex and time-consuming process, requiring significant resources and expertise. Different data protection regulation means businesses need to ensure that their cloud infrastructure meets all relevant compliance standards.

Furthermore, compliance is not a one-time event but an ongoing process that requires regular audits, assessments, and reporting. Businesses must ensure that they have proper documentation and evidence to demonstrate their compliance. Failure to comply with regulatory requirements can result in significant penalties, fines, and legal consequences, including reputational damage.

How to Mitigate the Risk

To address this challenge, businesses should thoroughly assess their compliance and regulatory requirements and work with their cloud service provider (CSP) to ensure that their infrastructure meets these standards. Regular compliance audits, risk assessments, and compliance monitoring can also help ensure ongoing compliance with relevant laws and regulations.

4. Mitigate the Risks of Integration and Interoperability

Interoperability, or the ability of different systems and technologies to work together seamlessly, can have a significant impact on cloud security. Cloud environments often consist of multiple cloud providers, platforms, and applications, each with its own security protocols and configurations. These disparate systems can make it difficult to manage security effectively, leading to vulnerabilities and gaps that can leave businesses vulnerable to attack.

Say one cloud application has weak security controls or is misconfigured. This could spell a potential pathway for attackers to access other connected systems or data. Additionally, if cloud platforms and applications cannot communicate with each other, security teams may not be able to detect and respond to security incidents in real-time.

How to Mitigate the Risk

Mitigating the risk of interoperability on cloud security starts with business leaders implementing a robust security framework that includes a unified approach to security across different platforms and applications. This can involve establishing standardized security protocols, implementing encryption and access controls, and conducting regular vulnerability assessments and penetration testing.

When working with cloud providers, CISOs will be looking for built-in security measures that can seamlessly integrate with other systems and applications. By adopting an interoperable approach to cloud security, businesses can better protect their data, mitigate risks, and ensure compliance with regulatory requirements.

5. Shine a Light on Shadow IT

Shadow IT refers to the use of unsanctioned cloud services by employees who need the knowledge or approval of the IT department. This can pose a significant security risk as these services may not meet the organization's security standards and can expose sensitive data to potential threats.

Shadow IT increases cloud security risks as it creates unmanaged and unmonitored access points into the cloud environment, while also being inherently exposed to risk as its applications can be misconfigured, outdated, or lack the necessary security controls to defend against attack.

How to Mitigate the Risk

To address the risk of shadow IT, businesses should implement clear, company-wide policies and procedures that govern employees' use of cloud services and applications. This can include educating employees on the risks of using unsanctioned services, providing secure alternatives for approved services, and monitoring network activity to identify any unauthorized use of cloud services.

In tandem with establishing security policies and employee awareness programs, businesses should monitor their cloud environments for unauthorized access and take immediate action to remediate any identified risks or vulnerabilities.

6. Dig in Against DDoS Attacks

Distributed denial-of-service (DDoS) attacks are another common threat to cloud infrastructure. When a victim organization comes under an active DDoS attack, their cloud service is purposefully flooded with arbitrary traffic and requests, sent by the attackers to overwhelm the system and cause system crashes for legitimate users. They can cause significant disruption to businesses by overwhelming their network and rendering their applications and services unavailable.

Based on recent research, DDoS attacks have been on the increase since 2020, and increased 109% in the last year, with more cases of hyper-volumetric DDOS appearing in recent months alone.

Cloudflare reported in February the case of a massive attack where attackers sent 50-70 million requests per second making it one of the latest HTTP DDoS attacks on record – 54% higher than the previously reported attack of 46 million requests per second back in June of last year.

How to Mitigate the Risk

Faced with increasingly powerful attacks and the rising ease of availability of DDoS-for-hire services on dark forums, businesses should ensure they have implemented robust network security protocols, such as firewalls, intrusion detection and prevention systems, and content filtering. Additionally, companies should work with their cloud service provider to implement DDoS mitigation strategies, such as traffic filtering and load balancing.

7. Stop Cryptominers in Their Tracks

Cryptocurrency mining uses cloud computing resources to validate transactions to generate new units of cryptocurrency such as Monero and Bitcoin. Attackers have leveraged this technology in recent years to steal computing resources and, in the case of cloud, perform unauthorized activity in cloud environments.

One of the main risks of cryptomining to cloud security is its potential impact on performance and availability. Since cryptomining uses significant amounts of computing resources, this means a slow down in cloud-based applications and services, affecting user experience and increasing costs for cloud providers and customers. Security experts have also noted that attackers can use cryptomining to cover up other malicious activities including network infiltration, data theft, malware installs, or the launch of botnet operations.

How to Mitigate the Risk

To mitigate the risks of cryptomining in cloud environments, security teams often focus on implementing monitoring tools, access controls, network segmentation, and the use of intrusion detection and prevention systems. The cloud environment itself can also be hardened against the risks of cryptomining. Security teams can implement usage controls and rate limiting, as well as work with their CSP to monitor the environment proactively for suspicious activity.

Conclusion

Modern cloud problems require modern cloud security solutions. With cloud operations now critical for businesses across various industries, the cloud surface is an attractive target for opportunistic and targeted attackers. Since threat actors count on cloud networks to be large, complex, and requiring in-depth management and regular maintenance, it is key for CISOs to choose the right cloud security platform to support their cloud security strategy.

CISOs focused on bolstering their cloud security understand that their strategy should be adaptive and agile, encompassing risks from across all surfaces including identity, email, endpoint, and network. Getting ahead of cloud-based attacks means having deep visibility across all vulnerable surfaces associated with the cloud and evaluating risks across the board.

SentinelOne's Singularity™ Cloud ensures organizations get the right security in place to continue operating in their cloud infrastructures safely. Contact us today or book a demo to see how we can help improve your cloud defenses and fuse autonomous threat hunting, EDR capability, and security together to fit your business.

Read more about Cyber Security

- Detecting a Rogue Domain Controller – DCShadow Attack
- Customer Value, Innovation, and Platform Approach: Why SentinelOne is a Gartner Magic Quadrant Leader
- Surviving the Storm | Defending Against Cloud Misconfigurations, Vulnerabilities, and Insider Threats
- Threat Landscape | The Most Dangerous Cloud Attack Methods In The Wild Today
- Accelerating Your Cloud Security with Workload Protection
- Defending Cloud-Based Workloads: A Guide to Kubernetes Security