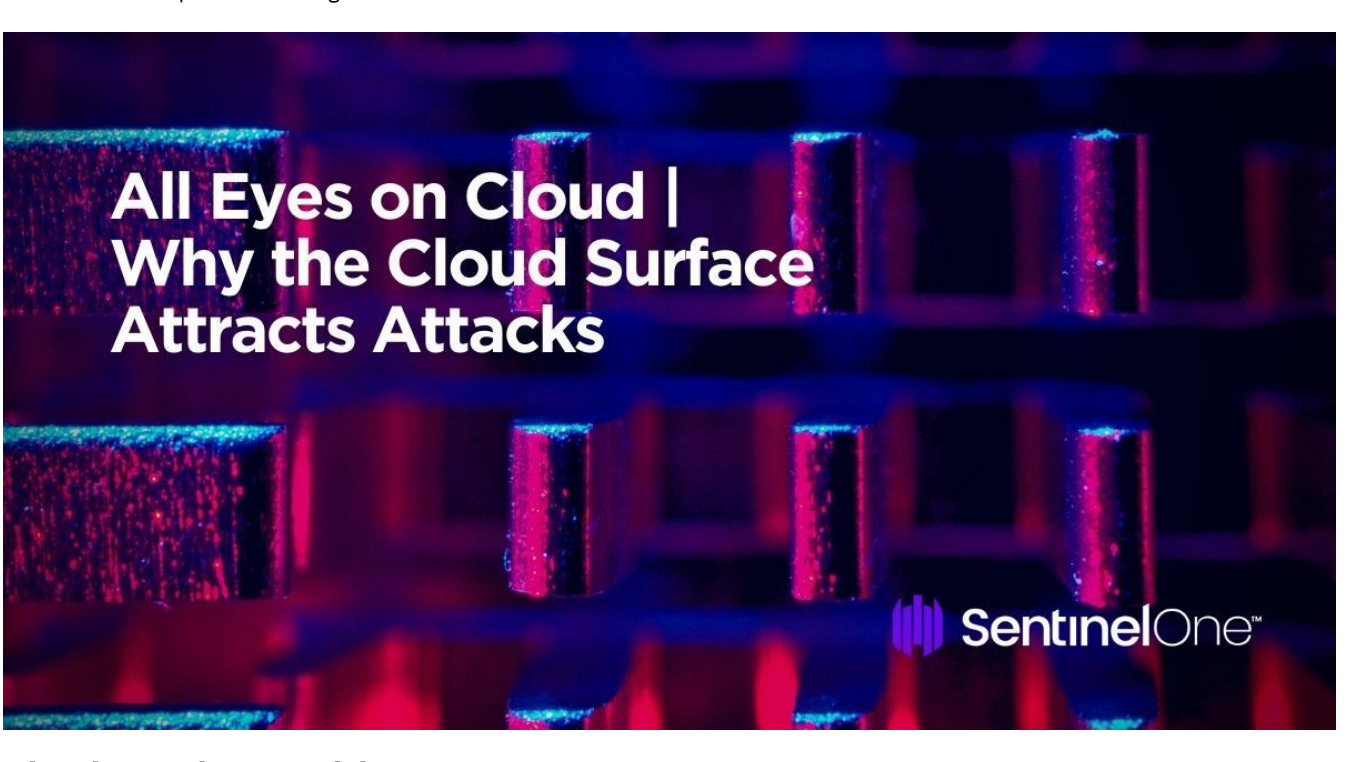
All Eyes on Cloud | Why the Cloud Surface Attracts Attacks

October 17, 2022
by SentinelOne

Cloud environments have seen a meteoric rise in the past decade. What began as means of data storage has now become a full-scale computing platform, enabling a global shift in how businesses share, store, optimize, and manage information. However, threat actors have witnessed these changes and taken to targeting the cloud, knowing that more and more businesses continue to make the transition to hybrid workspaces and cloud technologies.

The same features that make cloud services beneficial to organizations are the same that make them attractive to threat actors. In recent years, attacks on cloud environments have surged as threat actors took advantage of the high volumes of sensitive data flowing between organizations and their cloud service providers. Opportunistic by nature, threat actors thrive off of weak credentials, misconfiguration, and human errors when it comes to planning their attacks on the cloud surface.

While the related security challenges haven't slowed cloud adoption, organizations should be aware of their scope, significance, and how to secure against them. This blog post outlines why cloud has emerged as one of the most attacked surfaces and what security measures businesses can implement to safeguard their cloud environment and data.



Cloud Attacks Are Rising

The number of reported attacks on clouds has increased dramatically in the last few years, in part spurred on by the COVID-19 pandemic when businesses of all sizes needed to adapt quickly to alternative means of operation.

According to Gartner, the pandemic along with a surge in digital services have made cloud the "centerpiece of new digital experiences", and global cloud revenue will total $474 billion this year – a $66 billion dollar increase from 2021. The research firm also predicts that more than 95% of new digital workloads will be deployed on cloud-native platforms resulting in a 30% increase from the year before.

Businesses need to plan beyond traditional security strategies to manage a widening enterprise attack surface as well as the risks associated with cloud services. The following statistics show the rise in cloud adoption and just how much clouds have come under attack in the last few years:

- 69% of organizations have accelerated their cloud migration in the last 12 months. The percentage of organizations with most or all of their IT infrastructure in the cloud is expected to increase from 41% to 63% in the next 18 months (Foundry, 2022).
- 49% of IT professionals reported that cloud-based attacks led to unplanned expenses.
- 80% of CISOs surveyed by PurpleSec were unable to identify instances of excessive access to data in their cloud environments.
- 79% of organizations have suffered at least one cloud-based data breach in the last 18 months. Further, 43% have reported 10 or more breaches within that same time frame (Emertic, 2021).
- 83% of cloud breaches are derived from access-related vulnerabilities (CyberTalk.org, 2021).

Understanding Cloud Risks

Using cloud services inherently exposes organizations to new security challenges, often related to unauthorized access, insider threats, and supply chain risks. To a threat actor, cloud vulnerabilities are means of gaining access to exfiltrate data from the targeted organization's network whether by service disruptions, ransomware, or unauthorized data transfer. More sophisticated threat actors may employ lateral movement and detection evasion techniques, or account takeovers to establish and maintain a long-term foothold within the targeted network before leveraging existing services and tools found within it.

Common cloud security risks include the following:

- User Account Takeovers – Whether credentials are stolen through phishing, brute force, or malware, weak password policies often lead to compromised user accounts.
- Misconfiguration – Cloud service providers offer different tiers depending on the needs of the organization. This allows the cloud to work to scale with the organization. However, many organizations lack the security posture needed to ensure the safety of these services, resulting in security risks in the deployment stage of implementation. Misconfigured servers are a leading cause of compromise when it comes to cloud-based attacks.
- Vulnerable Public APIs – Public APIs allow trusted users to interact and operate within the cloud. If exploited, these APIs become a straightforward method for threat actors to gain access to the platform and exfiltrate sensitive data in the cloud database. Further, if the original configuration of the API harbors any vulnerabilities, this leaves threat actors with a backdoor for future exploits.
- Insider Threats – Even organizations with a healthy cyber ecosystem can fall victim to a legitimate, malicious user with a mind to leak data. Malicious users often already have access to sensitive or critical data, and may also have the permissions to remove certain security protocols. The threat of malicious insiders is greatly minimized through zero-trust policies and identity and access management solutions.
- Denial-of-Service (DoS) Attacks – Designed to overload a system and bar users from accessing services, DoS attacks are especially devastating to cloud environments. When the workload increases in a cloud environment, it will provide extra computational power to address the extra load. Eventually, the cloud slows down and legitimate users lose their access to any files in the cloud.
- Third-Party Vendors – It is important for organizations to assess third-party risks when using vendor services. Clouds are susceptible to supply chain attacks when threat actors infiltrate a network through unsecured third-parties that work with the organization. Cyber risk is inherited when organizations choose to work with vendors who have more lax cybersecurity posture than their own.

Defending the Cloud – Cyber Hygiene Matters

Securing the cloud begins with the basics. Cloud environments require short and long-term security planning, implementation, and strategy, and practicing cyber hygiene is the first step of that strategy.

Organizations that have processes in place for strong password requirements, multi-factor authentication, patch management, software updates, and device security can impede threat actors from grabbing those low-hanging fruits and lessen the attack surface under target.

Cover the Bases with Zero Trust & Segmentation

There is no such thing as immunity from cyber attack, but implementing zero trust policies goes a long way when building a holistic defense against threat actors who are eyeing a vulnerable cloud. Threat actors cause the most damage when they are able to move laterally through a victim's network and escalate privileges along the way.

Adopting zero trust makes life more difficult for threat actors. The zero trust principle works by eliminating the concept of 'trust by default'. Implementation of zero trust requires each user and machine to authenticate before receiving only the specific access pre-determined for their role.

Network segmentation plays an important part in successful zero trust implementation as well. By segmenting networks into smaller subnets that each act like their own, independent network, administrators can better control and secure the flow of traffic between each one via granular rules. This approach breaks up the architecture of a network and allows administrators to pinpoint technical issues more easily and be able to improve monitoring efforts.

Develop a Cloud Operational Strategy

Clouds are, at their core, designed to help businesses scale and store data, not to provide security. For many organizations, clouds are managed by DevOps and CloudOps teams rather than the in-house security team. In siloed organizations, security measures may not be uniform across different teams and could cause discrepancies in how the cloud is protected.

Defending cloud infrastructure requires a joined-up strategy that looks at the organization's cloud footprint with a holistic approach. Data needs to be collected and analyzed from all available sources in a way that security teams can ingest and understand.

Simplify the Challenges of Multi-Cloud Environments

Many organizations have multiple clouds deployed to optimize support for a larger data infrastructure. However, this scales up the complexity of the cloud infrastructure. Protecting multi-cloud environments means trying to find a common way to cover clouds that may each have a unique deployment, set of regulatory requirements, and policies.

A lack of uniformity here can be a big challenge for organizations, particularly if the organization does not have access to cloud security experts. Multi-cloud environments become even more complex if they are provided by different vendors. Integration between each of the cloud solutions may be difficult and result in a loss of visibility.

Dealing with these challenges involves considering the future as well as the present. Will technology investments made yesterday and today integrate with those of tomorrow? Many organizations have understood the need to move to an XDR platform, but only an open XDR platform that integrates existing solutions and can integrate with them, analyzing data, receiving alerts and automatically sending responses, can effectively address the challenges of a multi-cloud environment.

Conclusion

The widespread adoption of cloud technologies continues to re-shape the modern day workforce. A significant part of the digital transformation happening globally, cloud implementation has allowed businesses to lessen costs, increase organizational agility, and improve long-term scalability. Though the migration to cloud has benefited many businesses, it has come with a variety of new attack vectors for threat actors.

To get ahead of threat actors, organizations using cloud services must fully understand how the services are being implemented and maintained. Visibility within the cloud is critical to seeing how file sharing is being done, the type of data being stored and its security, and what applications are connected.

SentinelOne can help organizations improve their cloud security strategy through a combination of endpoint detection and response (EDR) capability, autonomous threat hunting, and runtime solutions that can defeat cloud-based threats without compromising agility or availability. Learn more about Singularity™ Cloud or contact us today for a demo.

Read more about Cyber Security

- Building Blocks for Your XDR Journey, Part 2 | Why EDR Is the Cornerstone for Great XDR
- Our Take: SentinelOne's 2022 MITRE ATT&CK Evaluation Results
- Cloud Computing Is Not New | Why Secure It Now?
- Cloud Credentials Phishing | Malicious Google Ads Target AWS Logins
- ITDR For the Win | Moving Beyond IAM and PAM to Protect Digital Identities
- 22 Cybersecurity Twitter Accounts You Should Follow in 2022