blackpoint

EBOOK

Top Five Cloud Security Threats

A Closer Look at the SOC's Common Cloud Responses

Table of Contents

Introduction

When we released the first true MDR for the cloud in 2022, we were immediately able to level up our visibility into cloud security threats. With over a year under our belt, the Security Operations Center (SOC) team found themselves having to address five cyberattack types in particular, time and time again.

The five cloud threats are:

- The lack of MFA and/or MFA bypass
- The malicious use of RSS and External Forwarding Rules
- Logins from proxy or VPN to bypass Conditional Access Geoblocking
- The exploitation of legacy authentication
- Logins from Suspicious User Agents

In this eBook, we will examine each tactic, discussing what it is as well as how to defend against it. Use the checklists throughout as a guide to prepare your business and clients for the ever-evolving threat landscape.

Cloud security threats aren't going anywhere, and while threat actors are increasingly innovative, they also will not stop using old, reliable techniques, so long as the capability remains.

Six Universal Mitigation Steps

In addition to the threat-specific action items, let's first examine five universal steps you can take to immediately up your security game. Regardless of the specific threat at hand, these mitigation steps are universally critical to safeguard your business and clients from the majority of cloud cyberattacks.

1. Implementing **multifactor authentication** (MFA) introduces an extra security layer, ensuring dual verification before granting account access. It's also paramount to enhance monitoring and logging, observing user behaviors and system interactions to detect anomalies.

2. **Educating users** about potential threats and best practices significantly reduces the risk of breaches. blackpoint

3. **Conditional Access Policies** allow or limit access based on conditions set by your company.

4. Every business should have a clear **Incident Response Plan**, ensuring swift and effective reactions to security breaches.

5. With **User Behavior Analytics (UBA)**, companies can establish baseline behavior for each user and entity, enabling the detection of unusual activities or threats.

6. **Rate Limiting**, especially on MFA code entries, can deter potential brute force or Denial-of-Service (DoS) attacks by restricting the number of requests in a given time frame.

blackpoint

WHAT DOES THIS ICON MEAN?

This icon signifies services that Blackpoint provides!

THREAT #1

The Lack of MFA and MFA Bypass

WHAT IT IS:

Multifactor Authentication (MFA) is a security measure that requires users to provide multiple types of identification before they can access an account or system. This extra layer of security goes beyond traditional username/password systems, requiring users to prove something they know, have, are, or where they're located.

WHAT IS THE THREAT:

If MFA is not present, you may be susceptible to:

- **Brute force attacks:** A trial-and-error method used by adversaries where they try every possible combination of login values until the correct one is found.
- **Phishing attacks:** Fraudulent emails or messages that appear legitimate, often mimicking trusted organizations or individuals, aimed at tricking recipients into disclosing sensitive information.
- **Credential stuffing:** The use of automated tools to try many username and password combinations, often obtained from previous data breaches.

While the presence of a reputable, robust, and up-to-date multifactor authentication solution is an integral part of your foundational security measures, it should not be solely relied upon. Threat actors continually innovate and have found ways to bypass MFA. They do so via:

- **Stolen credentials:** MFA codes may be stolen through a phishing attack, the utilization of malware, and more.
- **Token theft:** MFA "tokens," such as the code sent via SMS, the app-generated token, or the physical token, can be intercepted or acquired.
- **Alert fatigue:** Sending constant push notifications from your MFA solution until permission is granted.
- **Social engineering tactics:** For example, a threat actor may use someone's stolen personal details to convince customer support that they need to reset "their" MFA.

HOW TO DEFEND AGAINST IT:

- Avoid MFA push notifications or SMS-based MFA when possible.
  - If push notifications are utilized, ensure it requires code verification or number matching.
- Use one of the following methods whenever possible:
  - App-based MFA solutions
  - Multi-digit vault codes
  - Biometric authentication
  - Adaptive authentication
  - Hardware keys
    - FIDO keys specifically — hardware keys that adhere to standards set by the FIDA Alliance — send codes directly and stop the capabilities for Man in the Middle (MitM) theft, phishing, keylogging, and social engineering attacks. Yubikey, for example, pairs with an app which requires a pin, passcode, or biometrics.
- Regularly review and audit your systems to check that MFA is up to date, enabled wherever possible, and functioning correctly.
- Set up systems to alert on unusual behavior such as multiple failed MFA attempts or logins from unexpected locations. blackpoint
- Use HTTPS and other secure communication methods to ensure MFA tokens or codes aren't intercepted during transmission.
- If several failed attempts have occurred, lock the account or introduce an increasing delay to deter automated attacks.
- Only allow approved applications to run on systems, preventing malicious software from intercepting MFA tokens or credentials.

THREAT #2

RSS and External Forwarding Rules

WHAT IT IS:

Really Simple Syndication (RSS) feeds are a way to distribute regularly updated content from websites, such as news articles, blog posts, podcasts, and videos. RSS feeds use eXtensible Markup Language (XML) to structure the content, allowing it to be read by RSS feed readers or aggregators. External forwarding rules refer to the configurations that automatically forward email messages from one email account to an email address outside the originating organization's domain.

WHAT IS THE THREAT:

Attackers use malicious Really Simply Syndication (RSS) feeds to distribute malware or phishing links and to exfiltrate data without directly interacting with the environment. If unauthorized individuals gain access to a user's account and set up malicious external forwarding rules, sensitive information can be redirected outside the organization without the victim's knowledge. Such cyberattacks are done with the goal of exfiltrating sensitive data or conducting malicious actions without detection.

HOW TO DEFEND AGAINST IT:

- Regularly review and clean up RSS subscriptions.
- Disable RSS if it's not being used.
- Monitor for unexpected data or sensitive information in RSS feeds.
- Disable auto-forwarding to external domains at a global policy level unless there's a business need.
- Regularly audit mailbox rules in email platforms for any unexpected or unauthorized forwarding rules. blackpoint
- Set up alerts for new or modified email forwarding rules, especially those that forward to external or unexpected domains. blackpoint
- Implement mail transport rules that block or alert on email messages attempting to leave the organization with sensitive information.
- Ensure that access to settings, especially forwarding and RSS functionalities, is restricted to those who need it.
- Limit the number of administrative accounts and ensure their privileges are limited to what's necessary.
- Limit the exposure of sensitive parts of the network. Even if an attacker gains a foothold, network segmentation can limit their movement and actions.

THREAT #3

Logins from Proxy or VPN to Bypass Conditional Access Geoblocking

WHAT IT IS:

Conditional Access Geoblocking is a security feature that allows organizations to restrict access to cloud resources based on the geographical location of the user. It helps protect sensitive data and resources by ensuring that only authorized users from specific locations can access them.

WHAT IS THE THREAT:

Attackers may attempt to bypass these geoblocking (a.k.a. geofencing) restrictions by using proxies or VPNs. The use of these technologies can mask the true location of an attacker, making it appear as if they're logging in from an approved location.

HOW TO DEFEND AGAINST IT:

- Monitor for anomalous activity and block suspicious IP addresses. blackpoint
- Regularly update a blocklist of known IP addresses associated with these services.
- Implement stricter conditional access policies that go beyond just location-based rules, such as device health and user risk profile.
- Implement impossible travel monitoring to detect when a user logs in from two locations that are not possible, whether it be different time zones or countries. blackpoint
- Regularly review and adjust conditional access policies as your organization evolves.
- Use device compliance policies to ensure that only approved and compliant devices can access cloud resources.
- Have a Geo-IP filtering strategy and regularly refine the list of approved and disapproved countries based on business needs. blackpoint

THREAT #4

Legacy Authentication

WHAT IT IS:

Older, less secure methods of user authentication, such as SMTP, IMAP, and POP3, that don't support MFA or Conditional Access. They often solely rely on a username and password.

WHAT IS THE THREAT:

These less secure methods lead to increased vulnerability when it comes to credential attacks. It often also lacks the ability to assess the context behind a user's login attempt, such as location, device, or behavior.

HOW TO DEFEND AGAINST IT:

- Disable legacy authentication protocols and implement MFA wherever possible.
- Upgrade systems and applications that require legacy authentication to newer versions that support modern authentication methods.
- If an update is unavailable, place the application behind a VPN, which requires MFA for initial access prior to application access.
- Restrict legacy protocol access to specific IP ranges or devices.
- Review logs to check for unexpected or unauthorized access attempts. blackpoint
- Enforce strong password policies.
- Implement network-level protections to monitor and block malicious traffic targeting legacy authentication services.
- Use the principle of least privilege.
- Set up policies that lock accounts after a specific number of failed login attempts.
- Periodically audit who and what is using legacy authentication.
- Set up alerts for suspicious login attempts or patterns, such as multiple login failures in a short period. blackpoint

THREAT #5

Logins from Suspicious User Agents

WHAT IT IS:

User agents are pieces of information that web browsers or applications send to identify themselves when connecting to a server. A suspicious user agent typically refers to an unusual or unknown one that isn't commonly associated with legitimate users or known devices.

WHAT IS THE THREAT:

Logging in from suspicious or unrecognized user agents can be a red flag for malicious activity, especially if the user agent represents outdated or uncommon software, or scripts pretending to be legitimate browsers.

HOW TO DEFEND AGAINST IT:

- Block or challenge requests coming from known malicious or suspicious user agents. blackpoint
- Use a combination of whitelisting (allowing known good user agents) and blacklisting (blocking known bad user agents). blackpoint
- Set up alerts for unusual user agents or abrupt changes in user agents for a given user or IP address. blackpoint
- Periodically re-verify sessions, especially long-lived ones. If the user agent changes abruptly during an active session, it might be a sign of session hijacking.
- Ensure that all devices accessing the cloud environment have up-to-date security software and patches. This can reduce the chances of them using insecure user agents.

In Conclusion

The digital transformation journey of businesses has paved the way for a dynamic cloud environment. With this shift, the threat landscape has evolved, presenting unique challenges and vulnerabilities that businesses must address. Our experience over the past year, as highlighted in this eBook, underscores the importance of safeguarding against the five primary cloud security threats:

1. **the lack of MFA and MFA bypass,**
2. **malicious RSS and external forwarding rules,**
3. **bypassing Conditional Access Geoblocking via proxies or VPNs,**
4. **exploitation of legacy authentication, and**
5. **logins from suspicious user agents.**

While cyber adversaries persist in their endeavors, leveraging both innovative techniques and tried-and-true methods, businesses have at their disposal a range of measures to fortify their defenses. Utilizing multifactor authentication, implementing 24/7 monitoring, fostering user education, applying Conditional Access Policies, and having a decisive Incident Response Plan are universal and paramount measures. Furthermore, leveraging User Behavior Analytics and Rate Limiting bolsters the defense framework.

It's imperative that organizations stay agile, continuously updating and refining their cybersecurity strategies. By doing so, they ensure they are not only prepared for current threats but are also preemptively mitigating future vulnerabilities. As we look to the future, let's carry forward the insights from this eBook, adopting and integrating the recommended best practices to foster a resilient and secure cloud environment for our businesses and clients.

About Cloud Response

Active Response For Your Cloud

Extend the power of MDR and bring 24/7 expert security monitoring and unified response capabilities to your cloud workflows. Trust leading edge cybersecurity to actively defend your cloud platforms, hybrid environments, and everything in between.

Cloud Response is available independently or through our cost-effective bundle, Blackpoint Response.

About Blackpoint Response

Elevate your security stack with the best in active response through one cost-effective package.

Blackpoint Response includes everything to protect modern hybrid workflows with comprehensive, next-generation endpoint protection and application control, supported by our industry-leading MDR, and the best in Microsoft 365 and Google Workspace protection and response.

By upgrading your security stack with Blackpoint Response, you can get proper protection against these common cloud insecurities. We threat hunt for, alert on, and respond to anomalous, unexpected, abrupt, and unauthorized behavior and alterations on your behalf. Through our proprietary MDR, Cloud Response, and Managed Application Control, our 24/7 SOC ensures known malicious or suspicious users in your cloud environments are challenged or blocked every time.

Why Blackpoint Cyber?

Founded in 2014 by former National Security Agency (NSA) cyber operations experts, the Blackpoint team continues to bring nation-state-grade technology and tactics to our partners around the world. By fusing real security with real response, our elite SOC team is empowered by the proprietary technology we built from the ground up.

Together, we detect breaches faster than any other solution on the market. With insight into network visualization, tradecraft detection, endpoint security, suspicious events, and remote privileged activity, Blackpoint detects lateral movement in its earliest stages and stops the spread.

By the time you hear from us, the threat has been triaged and removed, often before the malicious actor even saw us coming. Lastly, we optimize our architecture and data to its fullest extent, ensuring robust services and valuable intel for our partners. That way, critical facets of security—on-prem & cloud response, endpoint protection, application control, logging, and cyber insurance—can work in tandem to support an integrated cyber strategy. Sleep easy knowing we detect and detain threats on your behalf around the clock.

Our mission? To provide unified, 24/7 detection and response services to organizations of all sizes around the world.

SIGN UP FOR A DEMO TODAY!

CONTACT US

info@blackpointcyber.com

blackpointcyber.com