X-Force Cloud Threat Landscape Report 2024

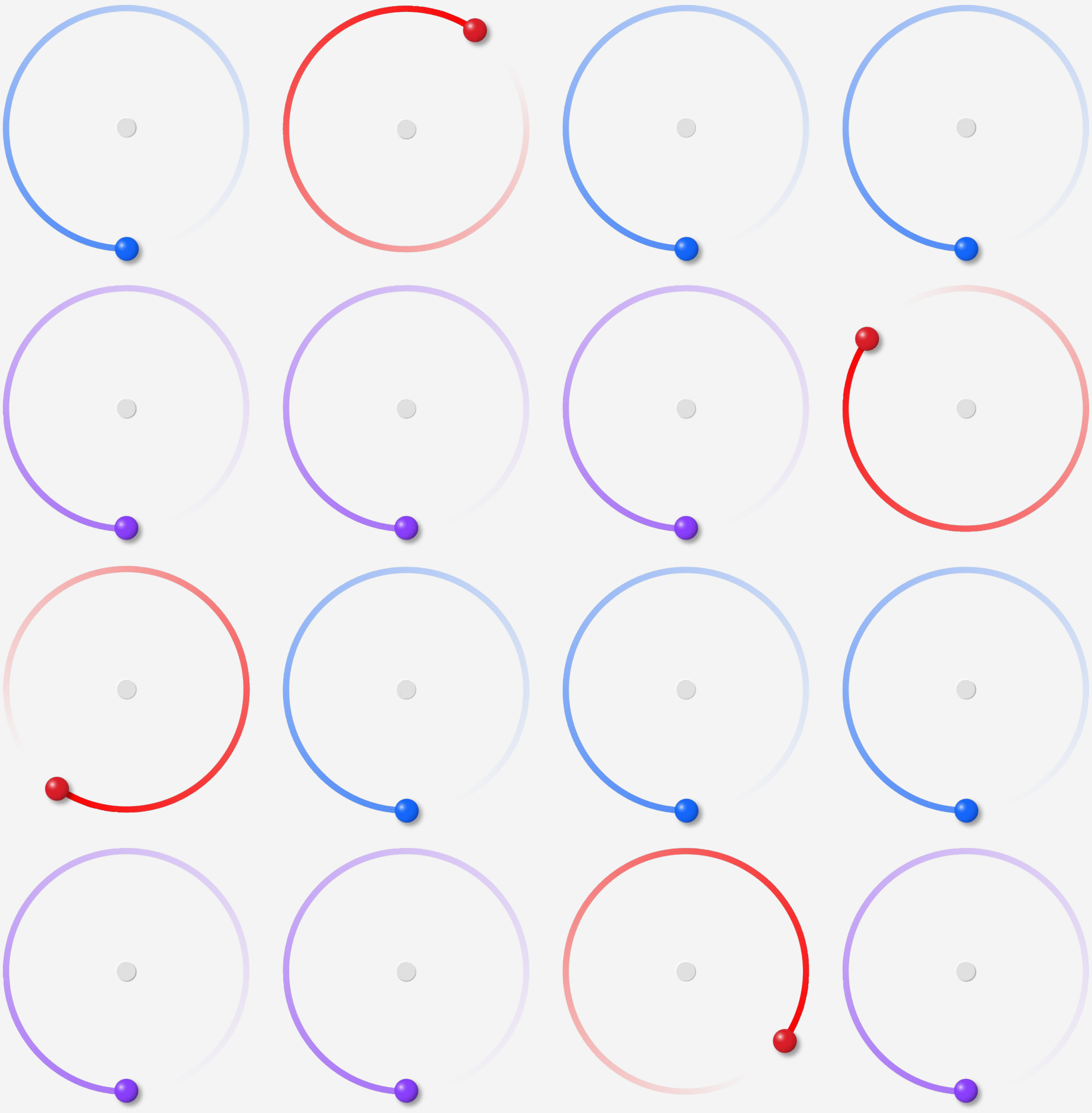


Table of contents

02 **Introduction**

03 **Key takeaways**

05 **Cloud vulnerabilities**

06 **Cloud and the dark web**

09 **Targeting cloud-based platforms and software as a service (SaaS)**

11 **Initial access vectors**

13 **Actions on objective**

15 **Security rule failures in cloud-based environments**

20 **Cloud and AI**

21 **Recommendations**

23 **About us**

Introduction

With the cloud computing market expected to reach approximately USD 600 billion in 2024, the adoption of cloud infrastructure continues to rise. Organizations are increasingly moving business-critical data from on premises to cloud infrastructure and services, driving the need for proper defensive measures and securing data in the cloud. Businesses are also seeking to maximize the value of their cloud investments and leverage the potential of AI and, therefore, must do so with an intentional approach.

For organizations undergoing a cloud migration, transformation is a multistep process that takes time, energy and resources. The 2024 Cost of a Data Breach Report found approximately 40% of all breaches involved data distributed across multiple environments, such as public clouds, private clouds and on premises. Therefore, as part of the migration process, it's vital that organizations develop and implement proper security strategies and best practices to protect key organizational assets.

Understanding the cloud threat landscape and its potential impacts on the business is essential for both IT and the C-suite. This insight enables proactive measures to limit exposure and safeguard business-critical information and resources, ensuring a secure and smooth cloud transformation journey and successful future implementations.

The IBM® X-Force® team is well-positioned within the security domain to provide organizations with industry best practices and strategies to aid in their cloud journey. Now in its fifth year of publication, the X-Force Cloud Threat Landscape Report provides a global cross-industry perspective on how threat actors are compromising cloud environments, the malicious activities they're conducting once inside compromised networks and the impact it's having on organizations.

To produce this report, X-Force gathered and analyzed data compiled from June 2022 through June 2024 from the following sources:[1]

- IBM X-Force Threat Intelligence
- IBM X-Force Red penetration tests, as well as adversary simulation and vulnerability management services engagements
- IBM X-Force incident response (IR) engagements
- Red Hat® Insights
- Dark web analysis by X-Force with data provided by report contributor Cybersixgill

Key takeways

In their data gathering and analysis, X-Force uncovered the most prevalent security risks organizations could encounter from threat actors in their cloud journey. Here are the key takeaways.

Cross-site scripting (XSS) leads as most impactful common vulnerabilities and exposures (CVE)

- XSS vulnerabilities composed 27% of newly discovered CVE during the reporting period, which could allow threat actors to steal session tokens or redirect users to malicious web pages.

Continued demand for cloud credentials on the dark web despite market saturation

- While the overall mentions of SaaS platforms on dark web marketplaces decreased by approximately 20% compared to 2023, gaining access using compromised cloud credentials is the second most common initial attack vector.
- There's been a steady decrease in the average price per compromised cloud access credentials, from USD 11.74 in 2022 to USD 10.23 in 2024, equating to an overall decrease of 12.8% over a 3-year period.

Increased use of trusted cloud-based file hosting services for malicious activities

- Threat actors are increasingly leveraging trusted cloud-based services, such as Dropbox, OneDrive and Google Drive, for command-and-control communications and malware distribution.
- North Korean state-sponsored groups, including APT43 and APT37, carried out multistage attacks against cloud-based services to distribute remote access trojans (RATs).

Phishing is the leading initial access vector

- Phishing accounted for 33% of all cloud-related incidents X-Force responded to over the past 2 years, with attackers often using phishing to harvest credentials through adversary-in-the-middle (AITM) attacks.

Frequent exploitation of valid credentials

- 28% of cloud-related incidents involved the use of legitimate credentials to get into victim environments. Often these accounts are overprivileged, with users having more privileges than needed to carry out their tasks, posing a significant security challenge for organizations.

Business email compromise (BEC) going after credentials

- BEC attacks, where attackers spoof email accounts posing as someone within the victim organization or another trusted organization, accounted for 39% of incidents over the past 2 years. Threat actors commonly leverage harvested credentials from phishing attacks to take over email accounts to conduct further malicious activities.

Compliance failures harm security of client cloud environments

- The #1 failed security rule in 100% cloud-only environments involved improper configuration of essential security and management settings in Linux® systems.

- The #1 failed security rule in environments where 50% or more of the systems are in the cloud involved the failure to ensure consistent and secure authentication and cryptography practices.

Cloud vulnerabilities

Following last year's analysis, X-Force categorized new CVE according to their potential impact if they were to be successfully exploited. What X-Force observed is obtaining information, gaining access and gaining privileges were the top 3 impacts of the CVE discovered during the previous reporting period. This year, XSS, gaining access and obtaining information were the top 3 impacts of the CVE discovered. This year-over-year comparison highlights a shift in the types of vulnerabilities being disclosed, with XSS emerging as a potentially significant threat. See Figure 1.

The exploitation of vulnerabilities is a top initial access vector for attackers. For example, XSS can be used to steal session tokens or redirect users to malicious web pages, while gaining access can lead to further exploitation of cloud resources. Ultimately, this exploitation can result in the deployment of cryptominers, infostealers, ransomware and other types of malware to achieve malicious objectives.

CVE impact

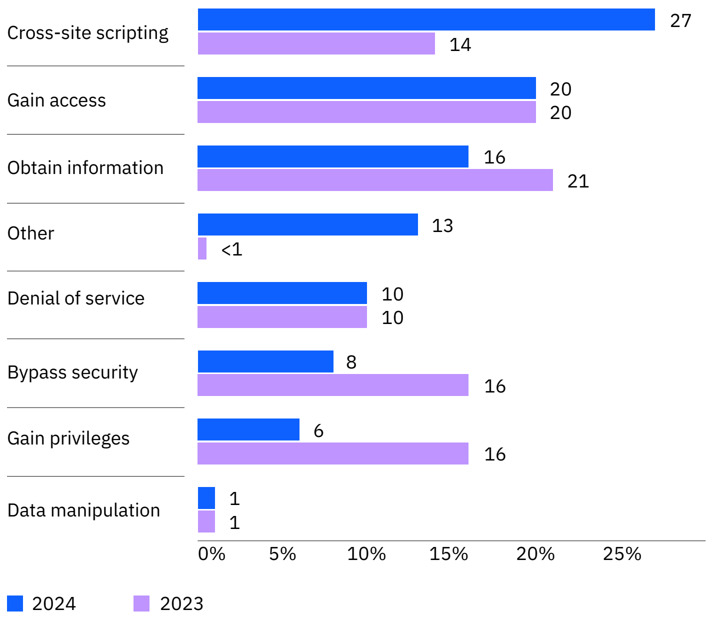


Figure 1. XSS is the #1 CVE impact. Source: X-Force

Cloud and the dark web

For this year's report, X-Force researchers once again partnered with Cybersixgill to gain insights into how cybercriminals exploit cloud environments and infrastructure on the dark web. In doing so, X-Force analyzed Cybersixgill data, pulled from various dark web forums and marketplaces between June 2023 and June 2024, to help inform the following analysis.

X-Force observed a steady decrease in the average price per cloud access credentials on the dark web from USD 11.74 in 2022 to USD 10.68 in 2023 and USD 10.23 in 2024, equating to an overall decrease of 12.8% since 2022. See Figure 2.

This trend could indicate the market for compromised cloud credentials is becoming oversaturated, leading to a devaluation in credentials. Increasingly, organizations are shifting to the cloud, meaning more credentials are likely being stolen or compromised, raising the overall volume of for sale cloud access credentials. Additionally, each year defensive security measures for cloud infrastructure improves, such as the speed of detection and response capabilities, rendering these credentials less effective and, therefore, less valuable.

Average price of cloud access credentials

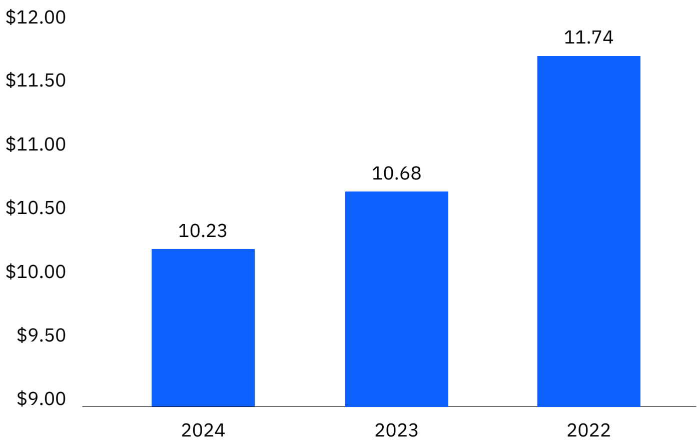


Figure 2. There's been an overall decrease of 12.8% in the price of cloud access credentials since 2022. Measured in USD. Source: Cybersixgill

While access to compromised cloud credentials continues to be a popular for sale asset on dark web marketplaces, especially regarding cloud-based SaaS solutions, overall mentions of SaaS platforms on dark web marketplaces decreased by an average of 20.4% compared to 2023. See Figure 3.

The reduction in mentions of these SaaS solutions on the dark web suggests a positive trend from a defensive security point of view. Reasons for this drop likely stem from law enforcement action and disruption of dark web marketplaces, which can severely impact the availability of stolen credentials and other listings. High-profile takedowns, such as Nemesis marketplace, highlight this outcome. Furthermore, as security around SaaS solutions improves, attackers may start to seek weaker alternatives to drive profit and conduct malicious activity. Organizations should continue to prioritize security, invest in advanced technologies, and foster a culture of security awareness and preparedness to maintain this shift.

- Research by X-Force indicates Microsoft Outlook was the most frequently mentioned SaaS solution discussed in dark web marketplaces by a wide margin at 68%, followed by Zoom at 7%.
- The overall number of mentions for each SaaS platform in dark web marketplaces decreased significantly compared to 2023, except for Microsoft TeamViewer, which increased by 9%. Despite the slight increase, it only represented 1.8% of total discussions regarding SaaS solutions.
- Notably, the most significant decrease in marketplace discussions was regarding WordPress-Admin at 98%, followed by Microsoft Active Directory at 44% and ServiceNow at 38%.

The significant drop in mentions of the previously named SaaS platforms on the dark web can be attributed to a few factors. Shifts in threat actor tactics, techniques, and procedures (TTP), potential lack of return on investment (ROI), and enhanced security measures from enterprises, such as the implementation of advanced encryption, multifactor authentication (MFA) and robust patch management, have significantly reduced vulnerabilities and the exploitability of these solutions.

Top-mentioned SaaS solutions on the dark web

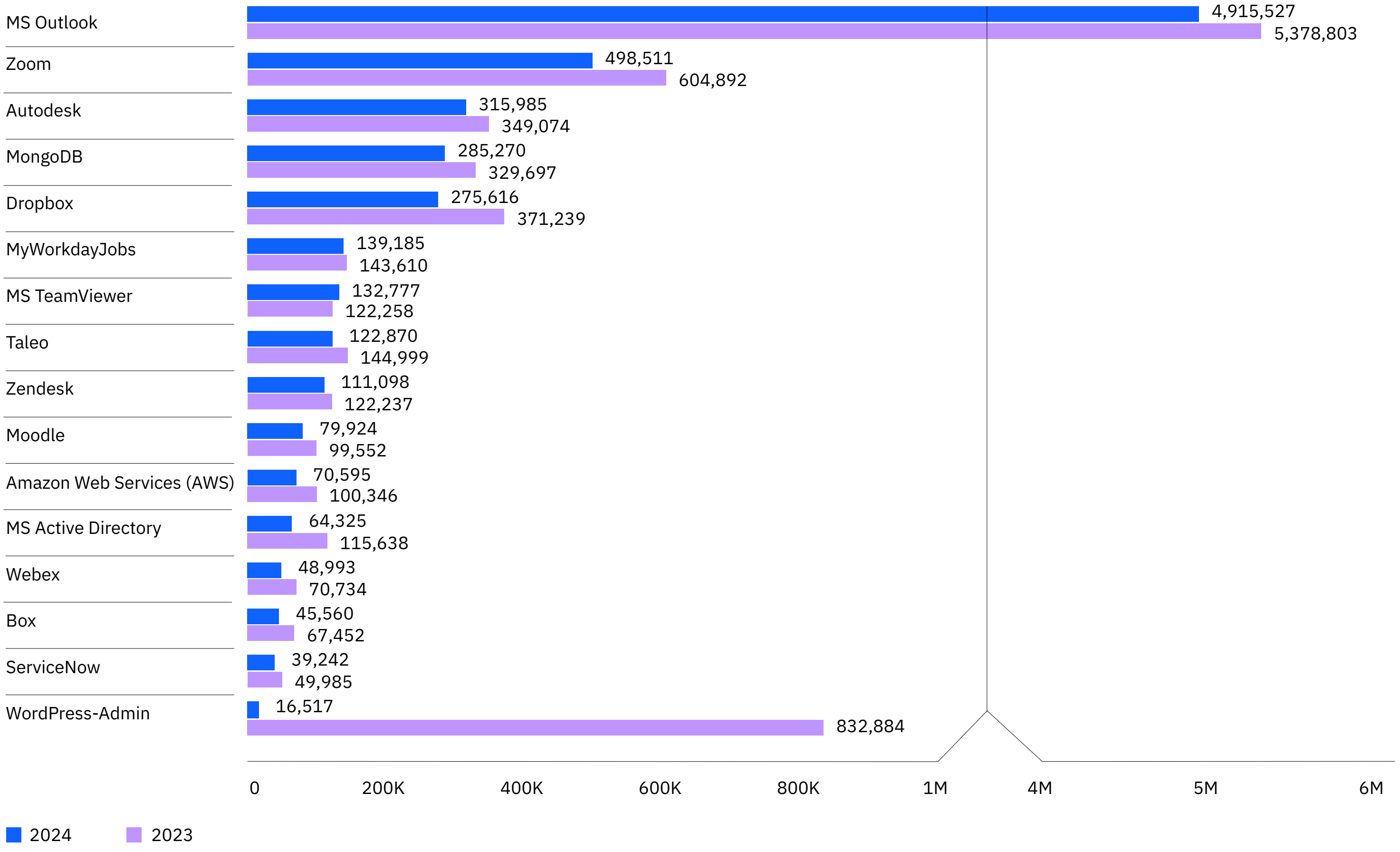


Figure 3. Top-mentioned SaaS solutions are based on dark web marketplace discussions. Source: Cybersixgill

Top-mentioned infostealers on the dark web

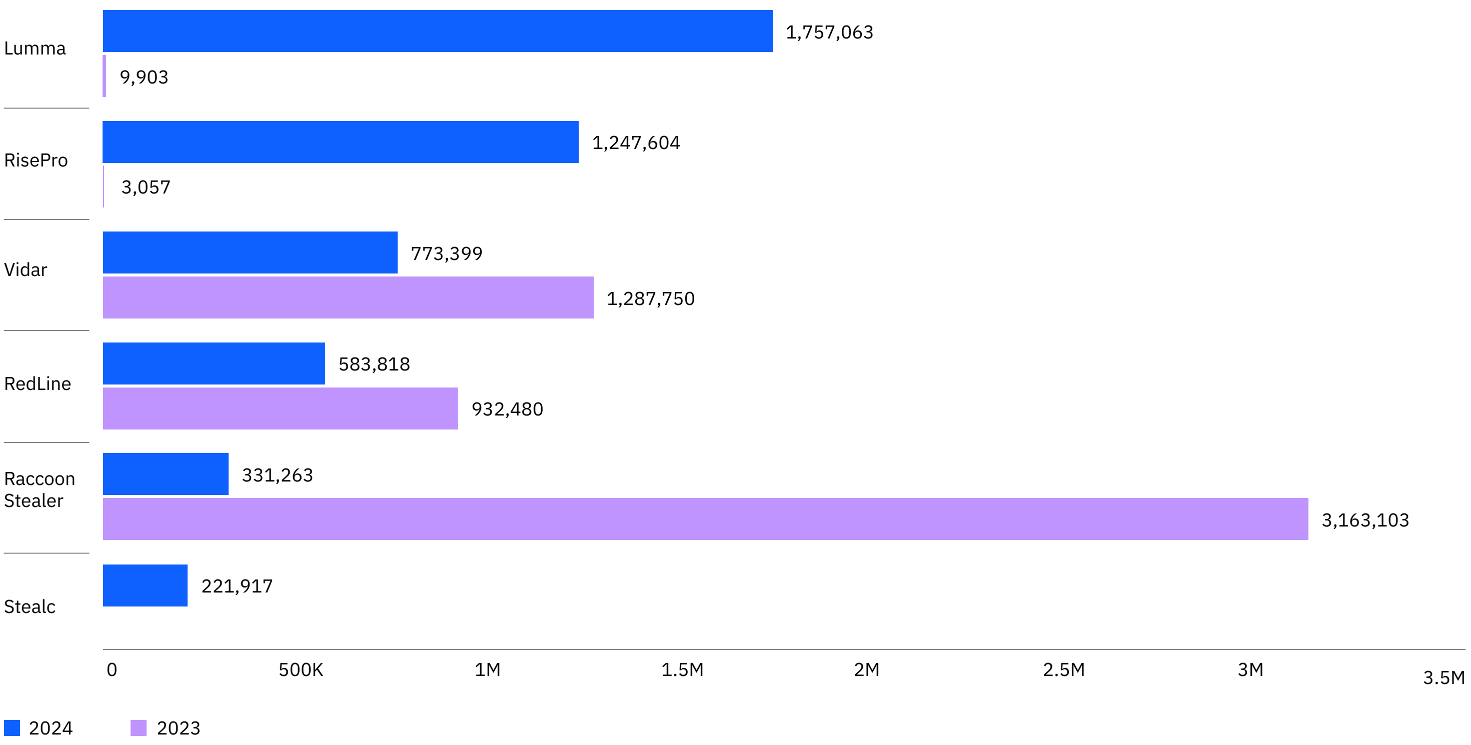


Figure 4. Top-mentioned infostealers are based on dark web marketplace discussions. Source: Cybersixgill

X-Force observed that Lumma, RisePro and Vidar were the most popular infostealers sold on the dark web in 2024. In comparison, the top infostealers in 2023 were Raccoon Stealer, Vidar and RedLine. Notably, Lumma and RisePro had little to no dark web activity in 2023, while Vidar was the second most popular stealer that year. Additionally, Raccoon Stealer was by far the most popular stealer at over 3 million mentions in 2023, but that number drastically dropped in 2024 to only 300,000. See Figure 4.

Over the past year, international law enforcement collaboration led to the dismantling of major cybercriminal networks distributing Raccoon Stealer. Additionally, the emergence of new infostealers like Lumma and RisePro shifted the focus of threat actors, reducing the popularity of Raccoon Stealer.

> Notably, while Lumma and RisePro had little to no dark web activity in 2023, they were the 2 most popular infostealers sold on the dark web in 2024.

Targeting cloud-based file hosting services, platforms and SaaS

Analysis from several X-Force Red adversary simulation engagements revealed an increasing use of cloud-based services for command-and-control communications, since these services are trusted by organizations and blend seamlessly with regular enterprise traffic. Adversaries are reconfiguring cloud-based resources to facilitate their objectives and grant themselves elevated privileges.

Additionally, X-Force observed cloud-based services targeted in the following 2 ways:

Cloud-based file hosting services: Malware distribution

X-Force has continued to observe threat actors widely using cloud-based file hosting services, such as Dropbox, OneDrive and Google Drive, to distribute malicious software that appears to be legitimate. 3 notable malware campaigns include 2 from North Korean state-sponsored groups:

- APT43, which has been leveraging Dropbox to facilitate a multistage attack campaign involving malware known as TutorialRAT
- APT37, which has been conducting a widespread phishing campaign using OneDrive to distribute RokRAT malware

The third notable campaign is an email spam campaign using OneDrive to host and distribute Bumblebee malware. These campaigns successfully exploited the trusted nature of public cloud services by bypassing traditional security measures and effectively delivering malware to unsuspecting users.

Cloud platforms and services: Infostealers, cryptominers and ransomware

In 2024 there's been a continuous trend of credential theft from infostealers specifically designed to exfiltrate credentials from cloud services. Many popular infostealers, such as RedLine, Raccoon Stealer, Vidar, Lumma, MetaStealer and Stealc, as well as different hacking toolkits, such as FBot, AlienFox and Legion, have been targeting cloud platforms. These platforms include AWS, Microsoft Azure, Google Cloud and other SaaS solutions, such as Office 365, Google Workspace (formerly G Suite) and Salesforce.

These infostealers and hacking toolkits have been used to steal platform and service-specific credentials, including:

- **Cloud infrastructure credentials**, such as AWS Identity and Access Management (IAM), Microsoft Azure Active Directory, Google Cloud IAM and Snowflake, control access to cloud resources, such as virtual machines, storage and databases.
- **Cloud storage credentials**, such as Dropbox, Box and Microsoft OneDrive, allow attackers to exfiltrate sensitive files and documents.
- **Cloud-based email services**, such as Office 365 and Gmail, contain valuable communication data and may be used for password reset procedures for other cloud services.
- **Cloud-based collaboration tool credentials** on platforms, such as Microsoft Teams, Slack or Google Workspace, where sensitive information is often shared among team members, are often targeted.
- **Cloud-based development platforms**, such as WordPress, GitHub, GitLab and Bitbucket, are used to steal credentials for accessing source code repositories, potentially obtaining proprietary code or sensitive development information.
- **Cloud-based customer relationship management (CRM) systems**, such as Salesforce, contain a wealth of customer data. Stolen credentials can provide unauthorized access to valuable customer information.

> There's been a continuous trend of credential theft from infostealers specifically designed to exfiltrate credentials from cloud services.

X-Force researchers have also observed cryptominers being deployed in cloud environments, highlighting the critical need for robust cloud security measures. Kinsing, a notorious malware family, has increasingly targeted and launched cryptominers inside cloud environments. For instance, Kinsing hides as a system file, specifically manual file or *man page*, to avoid detection while exploiting vulnerabilities inside cloud containers to deploy cryptomining operations on cloud servers.

In addition, ransomware has become a prevalent threat in recent years, frequently making headlines with attacks on various organizations worldwide. However, the impact on cloud environments often goes unnoticed. An incident involving CloudNordic, a Danish cloud-hosting company, starkly illustrates this growing issue. The reported ransomware attack led to the complete loss of all customer data. The attack exploited a vulnerability during a data center migration, encrypting all servers and backup systems. Despite existing security measures, the company couldn't recover data and chose not to pay the ransom. This incident demonstrates ransomware's severe impact on cloud environments, emphasizing the necessity for security best practices, mitigation strategies and effective disaster recovery plans.

Initial access vectors

The following outlines the techniques threat actors employed to gain initial access, listed in order of most-used vectors.

Conducting phishing campaigns

Despite the multitude of tactics and techniques used by threat actors to gain initial access into victim networks, phishing was the #1 tactic of choice, used in 33% of all cloud-related incidents that X-Force responded to over the past 2 years. Specifically, attackers use phishing as a starting point for AITM attacks in which they harvest credentials from the recipient of a phishing email after tricking them into entering login information on an attacker-controlled login page.

The use of valid credentials

The use of valid credentials was the #2 initial infection vector in attacks where cloud infrastructure was a potential target in the attack surface. Over the past 2 years, 28% of incidents involved the use of legitimate credentials as an initial access vector. Organizations continue to face challenges balancing their user access levels and security risk. These challenges are demonstrated most clearly in situations where attackers gain access to overprivileged user or service accounts and can do more damage in the environment.

Phishing was the #1 tactic, used in 33% of all cloud-related incidents.

Exploiting public-facing applications

The third most common vector is exploiting vulnerabilities in public-facing applications. It remains a reliable method for threat actors to gain access to both cloud and on-premises environments. This exploitation accounted for 22% of cloud-related incidents. See Figure 5.

Managing cloud applications—and access to them—poses a significant challenge for organizations, particularly as the number of applications and services continues to grow in modern cloud or hybrid cloud environments. If not implemented correctly, there's a risk of overlooking unpatched applications running in the cloud or, even worse, being unaware they exist and are running in the first place.

There are many vulnerabilities highlighting the critical need for robust security measures and proper patching processes in cloud environments. The following are 2 notable examples disclosed this year:

First, in May 2024, a critical Microsoft Outlook remote code execution vulnerability (CVE-2024-21413) emerged as a significant threat to cloud environments. Malicious actors can exploit this vulnerability through phishing emails and, if successful, can seize and manipulate communications, compromising cloud-based email services and other sensitive cloud resources.

Second, in July 2024, a critical vulnerability was disclosed in OpenSSH servers containing sshd on glibc-based Linux systems. This vulnerability, known as *regreSSHion* and tracked as CVE-2024-6387, can allow an unauthenticated attacker to execute remote code on a vulnerable system with root privileges. OpenSSH is a widely deployed connectivity tool in cloud environments for remote login with the Secure Shell (SSH) protocol.

Top initial access vectors

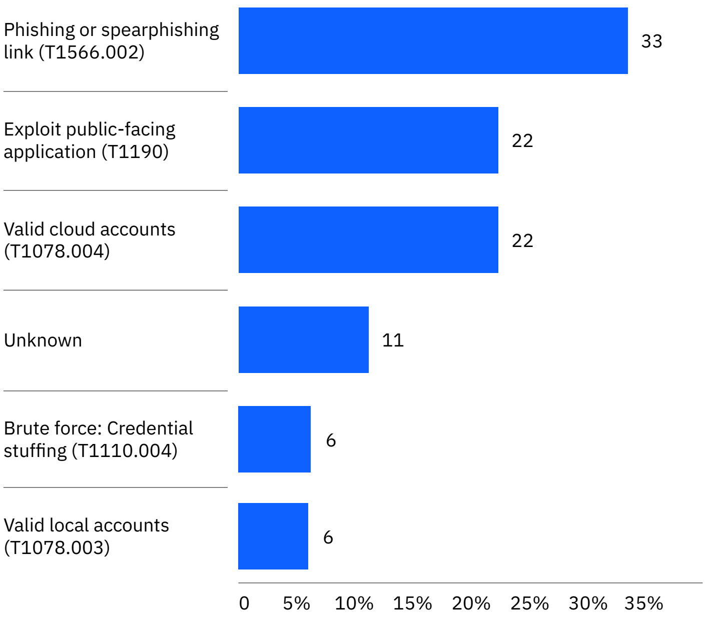


Figure 5. Top initial access vectors X-Force observed in cloud environments. Sources: X-Force and MITRE ATT&CK Matrix for Enterprise framework.[2]

> Exploiting vulnerabilities in public-facing applications remains a reliable method for threat actors to gain access to both cloud and on-premises environments.

Actions on objective

Threat actors used several avenues to gain access to accomplish their goals. X-Force found the following to be their most popular actions on objective.

Business email compromise

X-Force has repeatedly observed threat actors abusing cloud-hosted Active Directory servers to conduct business email compromise attacks within victim environments. This activity accounted for 39% of incident response engagements over the last 2 years, which made it the #1 action on objective. More specifically, threat actors are frequently leveraging AITM phishing tactics to bypass user MFA.

In this scenario, attackers use a proxy server to intercept the authentication process between the target and a legitimate service. This strategy allows the attacker to collect the target's credentials *and* token that's generated upon successful MFA input from the target, enabling an authenticated session to be maintained for the attacker to use. See Figure 6.

If the attack is successful, the threat actor has authenticated using the victim's credentials and is able to perform any action inside the application. In most cases, the attacker can send phishing emails from the compromised account, add mail forwarding rules or even log into additional cloud resources that share the same enterprise login credentials.

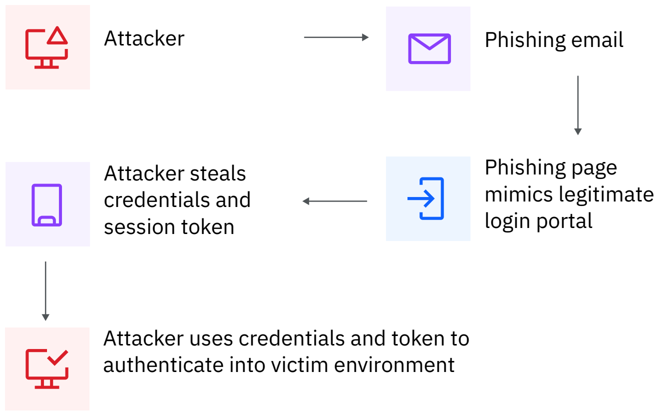
Cryptomining

Making up 22% of incidents over the past 2 years, cryptomining was the second most common action on objective, remaining popular among threat actors, especially in cloud environments. Because it's extremely resource-intensive, powerful cloud infrastructure is a perfect location to deploy cryptomining malware. Additionally, users are less likely to notice the effect of this malware when it isn't running locally on their endpoint. See Figure 7.

Credential harvesting

Credential harvesting is one of many techniques threat actors employ to steal user authentication credentials to conduct further malicious activities, typically using phishing, keylogging, and watering hole and brute force attacks. Credential harvesting attacks was the third most common action on objective, accounting for 11% of incidents. It's commonplace that stolen credentials are listed and sold on dark web marketplaces or used to compromise other accounts. See Figure 7.

BEC attack steps



Attacker

Phishing email

Phishing page mimics legitimate login portal

Attacker steals credentials and session token

Attacker uses credentials and token to authenticate into victim environment

Figure 6. An attacker-controlled web page steals the victim's credentials during an AITM attack, which was the most common threat scenario X-Force observed in cloud environments.

Actions on objective

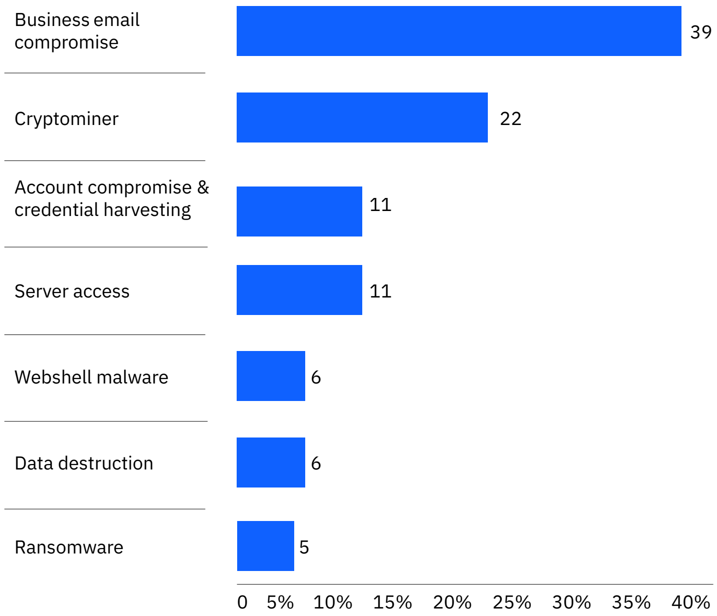


Figure 7. Top actions on objective observed by X-Force in cloud environments. Incidents can have more than 1 top action on the objective observed.

Security rule failures in cloud-based environments

As part of IBM’s partnership with Red Hat Insights, X-Force analyzed 2 sets of data from approximately 100 Red Hat Insights compliance service clients globally. The first set of data was from clients operating in 100% cloud-only environments, whereas the second set of data included clients with 50% or more of their systems in the cloud. X-Force assessed the security rules for their respective environments. These security rule or compliance failures provide key insights on how organizations can mitigate potential risks to their cloud environments.

Organizations operating in fully or partially integrated cloud environments frequently encountered significant challenges in maintaining a robust security posture, as evidenced by the repeated failures of key security rules in Red Hat Insights client environments. These failures often stemmed from the complexity of configuring and enforcing security policies consistently across dynamic and expansive cloud infrastructures. The context around setting up firewall zones, isolating file systems and applying secure mount options require specialized knowledge and diligent monitoring, which can be challenging for IT and security teams. Furthermore, the reliance on outdated practices, manual configurations and insufficient automation tools can exacerbate these issues, leading to more security misconfigurations and an increase in vulnerabilities.

In the broader context, these technical issues in cloud infrastructure should signal substantial risks to organizations, including the increased likelihood of cyberattacks, noncompliance with regulatory standards and operational deficiencies. As cloud environments continue to grow and evolve, it becomes vital for organizations to adopt comprehensive security measures, strategies and best practices. These measures enable them to fully leverage the benefits of cloud technologies while protecting critical assets and maintaining operational success and regulatory compliance.

> Rule failures in cloud infrastructure signal substantial risks to organizations.

Top 5 failed rules for 100% cloud environments

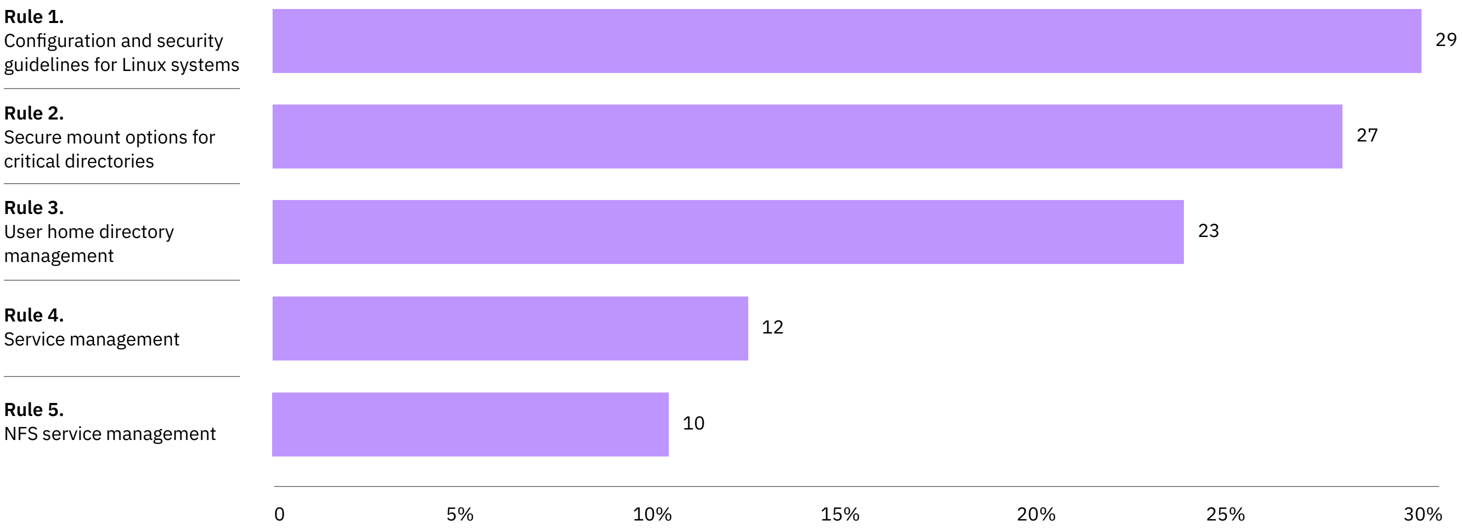


Figure 8. Number of top 5 failed rules for 100% cloud environments by order of importance. Source: Red Hat Insights

Top 5 failed rules for 100% cloud environments

From the Red Hat Insights data X-Force analyzed, the following highlights the top 5 security rules that frequently failed within 100% cloud environments, and the recommended guidance to resolve them. See Figure 8.

Rule 1. Configuration and security guidelines for Linux systems (29%)
This rule set focuses on configuring essential security and management settings in Linux systems, including setting the default zone for firewalld and isolating the /tmp directory on a separate partition to enhance security and manage disk space effectively. To mitigate:

- Configure the default zone for the firewalld service to ensure proper network security configurations in Red Hat-based systems.
- Isolate the /tmp directory on a separate partition to enhance security and manage disk space effectively, preventing denial of service attacks and improving system performance.

Rule 2. Secure mount options for critical directories (27%)
This rule set emphasizes configuring secure mount options for critical directories by preventing the execution of binaries, the creation of device files, and the execution of setUID and setGID programs, thereby enhancing security and enforcing proper directory use. To mitigate, prevent the:

- Execution of binaries in the /var/log directory
- Creation of device files in the /var/log directory
- Execution of setUID and setGID programs in the /var/log/audit directory
- Creation of device files in the /home directory
- Creation of device files in the /var directory
- Execution of setUID and setGID programs in the /var/log directory
- Creation of device files in the /var/log/audit directory
- Execution of setUID and setGID programs in the /var directory
- Execution of binaries in the /var/log/audit directory
- Execution of setUID and setGID programs in the /home directory

Rule 3. User home directory management (23%)
This rule set ensures proper ownership and permissions of user home directories, enhancing security by preventing unauthorized access and maintaining a consistent and organized file system structure. To mitigate:

- Ensure all interactive user home directories are group-owned by the primary user to maintain proper ownership, access controls and organizational consistency.

Rule 4. Service management (12%)
This rule set involves disabling unnecessary services, such as rpcbind and Network File System (NFS), to reduce the attack surface, enhance security and free up system resources.
To mitigate:

- Disable the rpcbind service.
- Disable the NFS service.

Rule 5. NFS service management (10%)
This rule set is exclusively dedicated to the management of the NFS service, emphasizing its specific role in network file sharing and the security implications of having this service enabled unnecessarily. To mitigate:

- Disable the NFS service to reduce the attack surface, enhance security and free up system resources. NFS allows file sharing between systems over a network but, if not required, disabling it can improve security and performance.

Top 5 failed rules for 50% cloud environments

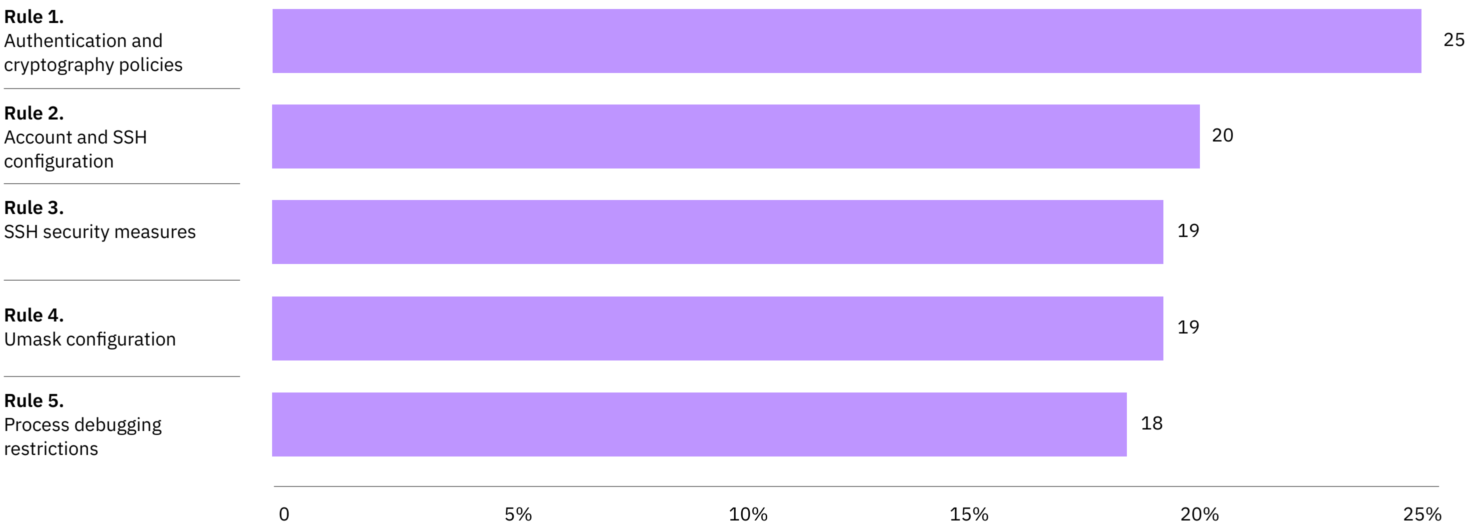


Figure 9. Number of top 5 failed rules for 50% cloud environments by order of importance. Source: Red Hat Insights

Top 5 failed rules for 50% or more cloud environments

From the Red Hat Insights data X-Force analyzed, the following highlights the top 5 security rules that frequently failed within 50% or more cloud environments and the recommended guidance to resolve them. See Figure 9.

Rule 1. Authentication and cryptography policies (25%)
This rule set focuses on standardizing and securing authentication mechanisms and cryptographic policies to ensure consistent and strong security practices across the system.
To mitigate:

- Use authselect to standardize and simplify the management of authentication settings, ensuring consistency and enhancing security.
- Set system-wide cryptographic policies to ensure the use of strong, secure cryptographic algorithms and protocols, enhancing security and compliance.

Rule 2. Account and SSH configuration (20%)
This rule set involves managing user account inactivity, SSH session limits, file ownership and password expiration to enhance security, reduce risks and comply with regulatory requirements. To mitigate:

- Disable user accounts automatically after a specified period of inactivity to reduce security risks associated with dormant accounts.
- Set SSH ClientAliveCountMax to ensure idle or unresponsive connections are terminated, enhancing security and freeing up resources.
- Ensure all files are owned by a valid user, investigating and correcting any unowned files to maintain proper file ownership and security.
- Set a maximum age for passwords to ensure regular password changes, enhancing security and compliance.

Rule 3. SSH security measures (19%)
This rule set enhances SSH security by disabling access and encourages best security practices. To mitigate:

- Disable SSH access via empty passwords to prevent unauthorized access and mitigate brute force attacks.
- Disable SSH root login to prevent direct root access, reducing the risk of unauthorized administrative access.

Rule 4. Umask configuration (19%)
This rule set involves configuring the default umask values to ensure new files and directories have secure permissions, enhancing security and maintaining consistency. To mitigate:

- Set appropriate umask values in /etc/profile to ensure new files and directories have secure default permissions.
- Set appropriate umask values in /etc/bashrc to ensure new files and directories have secure default permissions.

Rule 5. Process debugging restrictions (18%)
This rule set restricts process debugging and inspection to descendant processes only, enhancing security by preventing unauthorized access and manipulation of processes. To mitigate:

- Restrict the use of ptrace to descendant processes to enhance security by limiting process debugging and inspection capabilities, reducing the risk of malicious use.

Cloud and AI

Although cybercriminal and state-sponsored threat actors have been conducting global phishing and spam campaigns to spread various malware through cloud services, the near-term threat from AI-generated attacks targeting cloud environments remains moderately low. Still, there's a possibility threat actors are already leveraging AI to carry out malicious activities against cloud environments. X-Force research has shown AI can be used to develop sophisticated social engineering prompts and phishing campaigns in a fraction of the time it would take a human to craft a convincing phishing email.

Furthermore, X-Force has observed Hive0137, an extremely active malware distributor since at least October 2023, likely leveraging large language models (LLMs) to assist in script development, as well as creating authentic and unique phishing emails. While AI tools can allow attackers to potentially improve the authenticity of their lure materials, making it easier for threat actors to evade detection, the use of AI technology for malicious activities is early in its maturity curve.

In terms of attacking AI platforms, whether deployed in the cloud or on premises, there's a complexity hurdle to overcome and, in its current state, the immediate return on investment isn't worthwhile. However, as the AI market matures and becomes more integrated into business operations across industries, the attack surface can widen, and threat actors can be more incentivized to conduct attacks. X-Force analysis projects that when a single generative AI technology approaches 50% market share or when the market consolidates to 3 or less technologies, it could trigger at-scale attacks against these platforms. Organizations are encouraged to refer to the recommendations in this report, which can help mitigate the risk of cyberthreats whether they emanate using AI or not.

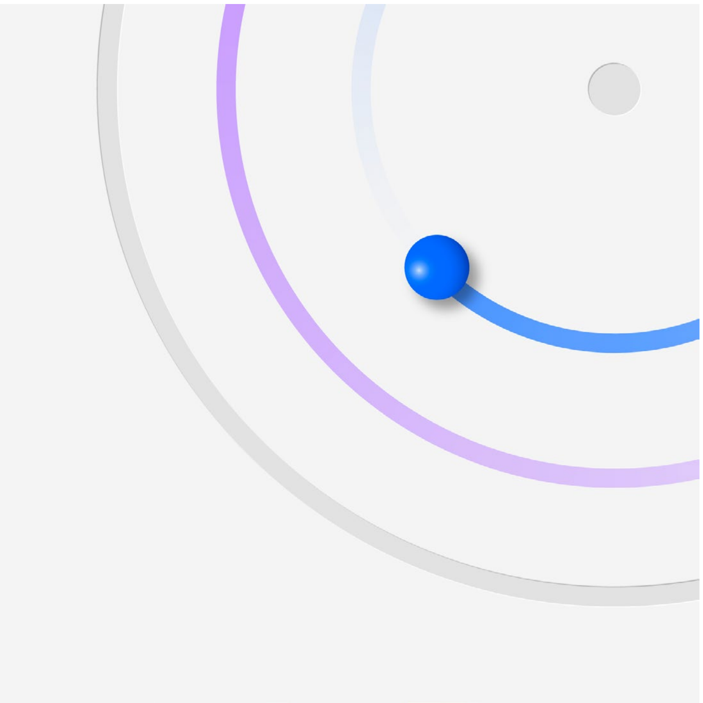
> Threat actors may already be leveraging AI to carry out malicious activities against cloud environments.

Recommendations

Considering the evolving cloud threat landscape, organizations must continuously monitor, adapt and enhance their security strategies to safeguard cloud and SaaS environments.

X-Force has observed organizations improving cloud security by enhancing email protections and requiring MFA for cloud access, making phishing attacks more difficult. However, protecting identity and data in cloud and SaaS environments requires ongoing adjustments to address evolving threats.

Here are some recommendations to help build a robust framework for improving cloud security.



Conduct comprehensive preparation and testing

A proactive, holistic security approach is paramount in the cloud landscape. Integrate security throughout development through secure DevOps, threat modeling and rigorous testing to build resilience. Automation minimizes human error and helps ensure continuous compliance, enabling organizations to navigate evolving threats with confidence.

Strengthen incident response capabilities

In today's dynamic threat landscape, a swift and effective incident response can make all the difference. Leverage security threat intelligence to understand attacker motivations and respond more rapidly. During investigations, preserving forensic evidence by redeploying affected machines, rather than reimaging them, helps ensure critical data is retained. Regular testing of disaster recovery and backup procedures is also essential for business continuity and resilience.

Protect data with robust security measures

Data protection remains a cornerstone of a comprehensive cloud security strategy. Encrypt data in storage, use and transit, and manage keys securely to help ensure sensitive information is safeguarded. Organizations should minimize data exposure by reducing the amount of sensitive data stored and limiting access strictly to necessary personnel. Automating security group privileges and decommissioning dormant accounts further enhances security by adhering to the principle of least privilege and preventing potential account compromises.

Build a stronger identity security posture

A streamlined identity management strategy is no longer a luxury, but a necessity. Simplify identity policies to strike a balance between robust security and user-friendly experiences. Embrace modern authentication methods, such as MFA, and explore passwordless options, such as a QR code or FIDO2 authentication, to fortify defenses against unauthorized access.

Design secure AI strategies to stay ahead of cloud threats

Harnessing the power of AI is crucial for staying ahead of evolving cloud threats. AI offers transformative potential to revolutionize authentication and identification, enhancing both the efficiency and security of these critical processes. As generative AI continues to advance, safeguard the integrity of data and models with robust encryption and access controls.

Organizations must proactively manage risks associated with shadow AI and unsanctioned use of AI tools in the workplace, helping ensure transparency and control over AI initiatives. Additionally, organizations should prepare for the potential impact quantum-enabled threats could have on the long-term security of AI projects.

About us

IBM X-Force
IBM X-Force is a threat-centric team of hackers, responders, researchers and analysts. The X-Force portfolio includes offensive and defensive products and services, fueled by a 360-degree view of threats.

With a deep understanding of how threat actors think, strategize and strike, X-Force can help you prevent, detect, respond to and recover from incidents and focus on business priorities.

If your organization would like support strengthening your security posture, schedule a one-on-one briefing with an IBM X-Force expert.

IBM
IBM is a leading global hybrid cloud, AI and business services provider, helping clients in more than 175 countries capitalize on insights from their data, streamline business processes, reduce costs and gain a competitive edge in their industries. All of it is backed by IBM's legendary commitment to trust, transparency, responsibility, inclusivity and service. For more information, visit www.ibm.com.

Schedule a briefing →

Contributors
Austin Zeizel
Christopher Caridi
David McMillen
Michelle Alvarez
Agnes Ramos-Beauchamp
Christopher Bedell
Johnny Shaieb
Scott Lohr
Scott Moore
Sophie Cunningham
Cybersixgill
Red Hat Insights

1. All data gathered and analyzed in the report, except for the incident response engagement data, was from June 2023 through June 2024. X-Force expanded the timeline for the incident response engagement data to June 2022 through June 2024 to provide the 2-year overall initial access vector and actions on objectives trends.
2. MITRE ATT&CK Matrix, The MITRE Corporation, 19 July 2019.

This document is current as of the initial date of publication and may be changed by IBM at any time. Not all offerings are available in every country in which IBM operates.

THE INFORMATION IN THIS DOCUMENT IS PROVIDED “AS IS” WITHOUT ANY WARRANTY, EXPRESS OR IMPLIED, INCLUDING WITHOUT ANY WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND ANY WARRANTY OR CONDITION OF NON-INFRINGEMENT. IBM products are warranted according to the terms and conditions of the agreements under which they are provided.

No IT system or product should be considered completely secure, and no single product, service or security measure can be completely effective in preventing improper use or access. IBM does not warrant that any systems, products or services are immune from, or will make your enterprise immune from, the malicious or illegal conduct of any party.

The client is responsible for ensuring compliance with all applicable laws and regulations. IBM does not provide legal advice nor represent or warrant that its services or products will ensure that the client is in compliance with any law or regulation.