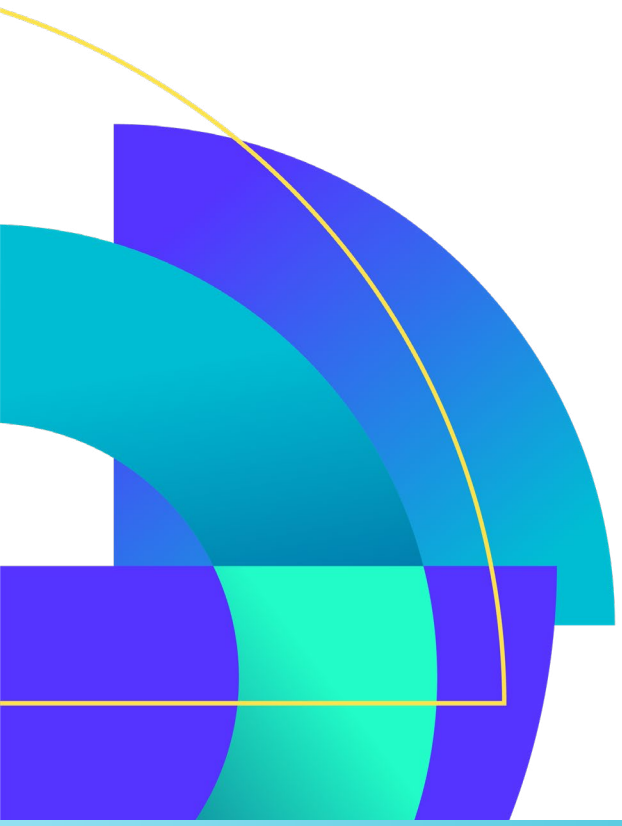
sysdig

Top Business Impacts of Cloud Breaches and How to Mitigate Them

Although you are increasingly seeing cloud breaches in the news, that is still only a fraction of what is actually happening, as cybercrime is vastly underreported. Cyber attacks have become pervasive, so it is not a question of 'if' your organization will experience a cloud breach. It will happen, but you can take steps to block attacks and reduce the frequency and business impact of cyber incidents.



Our team analyzed publicized breaches to understand the tactics threat actors used to gain access and successfully progress the attack to cause serious harm, some with broad and long lasting implications. We identified security posture aspects that facilitated the breach, which you can use to assess your risk exposure. Our suggestions to mitigate risk provide steps your teams can take to prevent or minimize the impact of cyber attacks.

1

Escalating Costs from PII and PHI Data Leak

A breach revealed in October 2022 hit the Australian health insurance company Medibank hard, but their customers were hit even harder. The Personal Identifiable Information (PII) and Protected Health Information (PHI) data of 3.9 million customers was stolen. It is concerning to see the snowball effect unfolding as impact aspects are factored in. From the initial investigative work to the hacker's distressing disclosure of the complete 200GB of data containing patients' procedures and health conditions, including "naughty" and "abortion" lists, Medibank's bill is now estimated to reach $45 million in the first year after the breach. But the impact of the breach is far from over. Lawsuits were announced and individuals will continue to suffer the consequences of such exposure.

Let's take a look at the attack to identify risk and risk mitigation strategies.

1 Entered the environment using stolen credentials:

Risk => Access without MFA (weakness) + compromised credentials (threat).

Mitigation strategy:

Prevent => Enforce MFA for privileged access to mitigate risk of compromised credentials.

Protect => Detect logins without MFA in real time to avoid windows for exploitation using compromised credentials.

2 Discovered additional privileged credentials:

Risk => Credentials access (weakness) + excessive permissions (weakness) + lateral movement (threat).

Mitigation strategy:

Prevent => Enforce secrets security through the full lifecycle to mitigate the risk of leaked credentials. Implement least privilege principle by identifying and removing unnecessary permissions to reduce the risk of lateral movement and privilege escalation in case of compromised credentials.

Protect => Implement holistic threat detection with real-time visibility into the workload, cloud, and user activity to stop malicious actions and detect masqueraders.

3 Ran a malicious tool to collect and exfiltrate data:

Risk => Data not encrypted (weakness) + exfiltration software (threat).

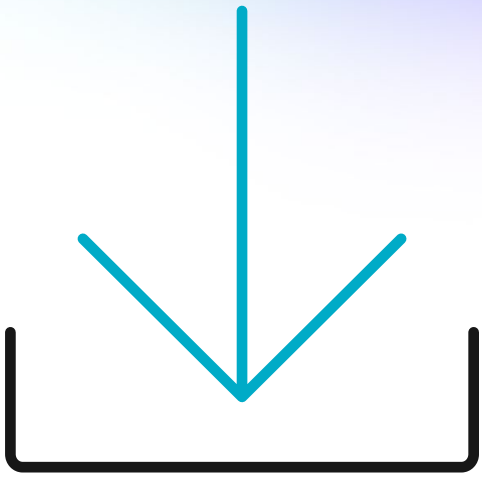
Mitigation strategy:

Prevent => Encrypt confidential and sensitive data. Implement microsegmentation to isolate sensitive data and zero trust principle on network communications to avoid anomalous connections to untrusted IPs/addresses.

Protect => Enforce the immutability principle by stopping workload drift in real time to block unexpected software from running and stop attacks. Block connections to known malicious IPs/addresses to avoid data leak.

2

Cascading Impacts Include Revenue Loss, Lawsuit & Credit-worthiness Drop



In February 2023, MKS Instruments, a key supplier in the semiconductor industry, reported a massive cyberattack that resulted in production disruption and exfiltration of sensitive data.

Although the full scope of the incident is still unknown, some costs and cascading impacts have been felt not only by the company, but also by its investors, supply chain customers, and individuals exposed by the data leak. MKS says the attack will cost $200 million in lost revenue (27% hit), and Applied Materials announced a $250 million reduction in sales as a consequence of the attack on its supplier. MKS is also facing class-action litigation and a negative credit assessment from Moody's Analytics. The incident serves as a reminder of the importance of supply chain security and business risk in the event of compromise of any component (physical or digital), partner, or supplier in a given chain.

Ransom campaigns are on the rise with attackers trying to maximize gain. So, let's see some security measures that could have prevented the massive blast.

1 Unknown initial access but attacker dwelled in the environment long enough to discover accessible systems and data assets.

Risk => Vulnerable data assets (weakness) + unprotected networks (weakness) + intruder (threat).

Mitigation strategy:

Prevent => Encrypt sensitive and confidential data to reduce the impact of leaks. Implement network microsegmentation to avoid lateral movement.

Protect => Implement real-time behavior-based detection of malicious user, file, and network activity to look for suspicious pre-compromise activity to preempt attacker steps, as well as stop harmful actions in progress.

2 Disrupted production systems:

Risk => Vulnerable systems (weakness) + attack/ malware campaigns activity (threat).

Mitigation strategy:

Prevent => Remediate vulnerabilities on critical systems immediately by prioritizing exposure at runtime to reduce risk of exploitations. Implement IaC practices and maintain reliable backups for fast redeployment and restoration of the pre-compromised state.

Protect => Implement multi-layered defense with up-to-date threat intelligence to detect malicious behavior of adversarial campaigns in activity and stop attacks.

3

FTC Taking Action over Lapses on Cloud Security

The Federal Trade Commission (FTC) took action against Drizly and its CEO based on the company's continued security failures that led to a data breach exposing the personal information of about 2.5 million consumers. The final order carries the force of law concerning future actions with a penalty for each violation, forcing a shift of the executives' attention to security. In the case of Drizly, cloud security has been an Achilles heel – they have been previously breached in a cryptojacking attack. Federal agencies in the U.S. are beginning to enforce cybersecurity best practices as part of the U.S. National Cybersecurity Strategy, particularly for private sector entities but also in cases of significant impact to citizens from public sector misfires. This action by the FTC against Drizly is one example of how these events will likely play out in the years ahead.

Drizly uses AWS cloud services to store data and host its e-commerce platform, and uses GitHub for development. Hackers used compromised GitHub accounts to harvest AWS and database credentials found in repositories. With valid AWS credentials, the attacker was able to lower security controls, access databases, and collect and exfiltrate data, all undetected. Drizly learned about the compromise from the news that its customers' accounts were for sale on the Dark Web.

Let's take a look at the attack to identify risk and mitigation strategies.

1 Entered environment using valid credentials found on GitHub:

Risk => Access without MFA (weakness) + compromised supply chain/ GitHub (threat).

Mitigation strategy:

Prevention => Enforce MFA for privileged access to version control systems to mitigate risk of compromised credentials or source code .

Protection => Scan code before uploading to GitHub to avoid the presence of persisted secrets in source code.

2 Lowered security controls:

Risk => Unsecure settings (weakness) + masquerader (threat).

Mitigation strategy:

Prevention => Enforce security controls on cloud resources and workloads to avoid weak posture.

Protection => Monitor security controls drift in production and detect violations in real time to stop intentional and unintentional lowering of protection.

3 Accessed the database, collected, and exfiltrated PII data:

Risk => Excessive permissions (weakness) + masquerader (threat).

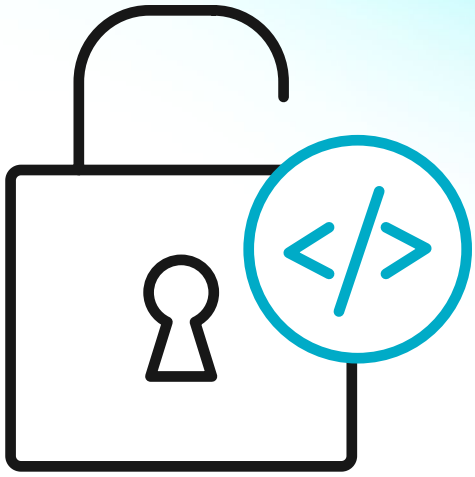
Mitigation strategy:

Prevention => Identify and remove excessive permissions of user accounts and service identities to reduce the blast radius of potential attacks. Encrypt sensitive data to reduce the impact of compromises.

Protection => Protect against the access of sensitive data through least privilege and access controls. Detect suspicious access to sensitive file/data in real time to avoid data leaks. Implement holistic threat detection with real-time visibility into the workload, cloud, and user activity to stop malicious actions, detect masqueraders, and alert on exfiltration to external addresses.

4

Rising “Gold Rush” of Source Code Leaks



Recently, Twitter joined a fast-growing list of organizations with leaked source code – a trending sought-after asset by hackers. Twitter’s code was uploaded to GitHub by a user named "FreeSpeechEnthusiast," who executives believe to be former employee(s). Toyota also suffered a similar incident with unintentional exposure of source code in a public GitHub repo for nearly five years until Toyota discovered the issue in late 2022. Source code repositories are common ground for leaks by malicious insiders and adversaries, or by unintentional actions and misconfigurations. Concerns include competitiveness loss, intellectual property theft, credentials or secrets harvesting, and increased exposure of vulnerabilities in code.

Details of Twitter’s attack, and how the actors got access to the source code to post on GitHub, have not been disclosed. For Toyota, everything started with a subcontractor uploading a portion of source code to a public GitHub repository. Let’s see some risk reduction measures against intentional and unintentional source code leaks.

1 Unknown actor collected and exfiltrated source code:

Risk => excessive privilege (weakness) + disgruntled employee or masquerader (threat).

Mitigation strategy:

Prevention => Implement least privilege and need-to-know principles. Apply fine-grained controls and identify and remove excessive permissions to reduce insider threat risk.

Protection => Implement behavior-based detection to detect suspicious access to sensitive file/data in real time and avoid data leaks.

2 GitHub repository public exposed unintentionally:

Risk => Repo configured public (weakness) + unauthorized access (threat).

Mitigation strategy:

Prevention => Require that code commits are done to private code repositories. Enforce security settings on GitHub repositories to avoid unintentional misconfigurations that expose code publicly.

Protection => Scan for secrets before pushing to repositories. Detect violations in real time to avoid providing exploitation windows.

3 Third-party trusted relationship risk:

Risk => This-party trusted relationships (weakness) + infiltrators (threat).

Mitigation strategy:

Prevention => Enforce least-privilege principle using fine-grained access and security controls over third-party relationships.

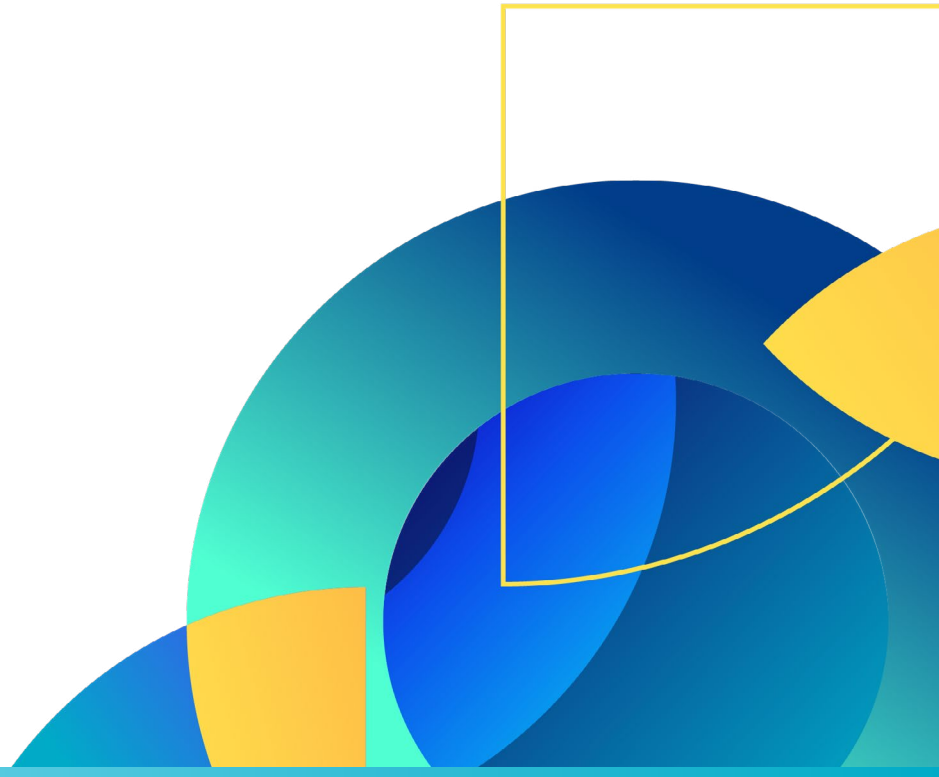
Protection => Get unified visibility into your environment and supply chain. Monitor version control system activity to detect suspicious user, workload, and third-party/ecosystem behavior early and stop attacks quickly.

Stopping Breaches Requires Security Designed for the Cloud

Organizations relying on security processes and tools that were not designed for the cloud will experience more frequent and harmful cyber incidents. These analyzed breaches and their impact point to the need for prevention that is architected specifically for the cloud's complex and dynamic attack surface. Cloud attack methods are evolving and require real time detection techniques that stop malicious activities before they cause damage.

Sysdig helps companies secure and accelerate innovation in the cloud. Powered by Runtime Insights, our cloud security platform stops threats in real time and reduces vulnerabilities by up to 95%. Rooted in runtime, we created Falco, the open standard for cloud threat detection. By knowing what is running in production, developers, IT operations, and security teams can focus on the risks that matter most. From shift left to shield right, the most innovative companies around the world rely on Sysdig to prevent, detect, and respond at cloud speed.

REQUEST A DEMO



sysdig

CL-028 Rev. A 05/23.