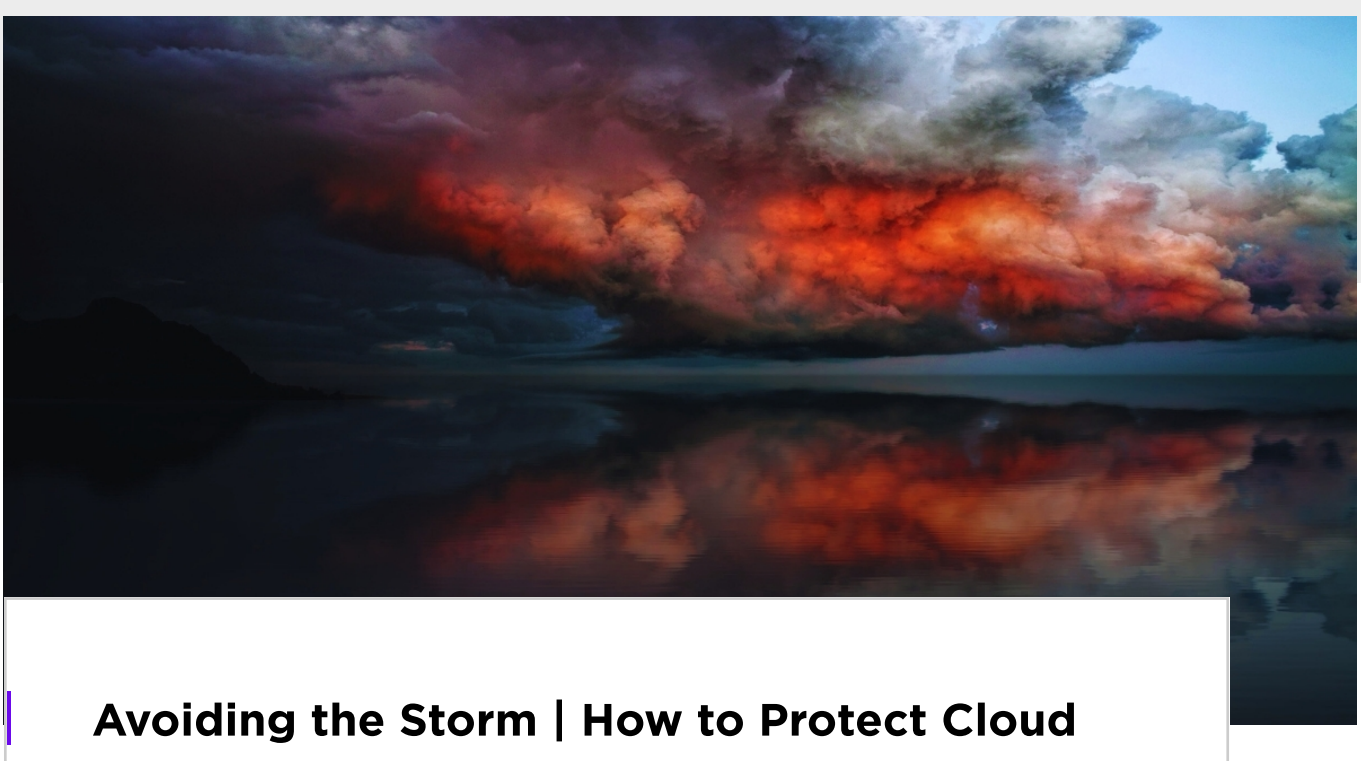

# Avoiding the Storm | How to Protect Cloud Infrastructure from Insider Threats

April 20, 2023
by Chris Boehm

One of the most significant security threats to cloud infrastructure is insider threats. As more businesses move to cloud and hybrid environments, employees sending sensitive data to unsecured or misconfigured clouds risk exposing their organization to advanced cyber threats and opportunistic attackers.

The importance of cloud infrastructure to businesses of all sizes along with the privileged access that insiders often have mean that mitigating the risk of insider threats is now high on the list of priorities for mature security teams. In this post, we describe and explore best practices that security teams can implement to safeguard cloud infrastructures from insider threats.


## Why Are Insiders Considered a Main Risk to Cloud?

Whether out of negligence or presenting malicious intent, insider threats pose a serious risk to cloud security as they are harder to detect and respond to. Since they are already part of the organization, they are considered 'trusted'. Unlike an external intruder, insiders do not have to breach external security measures to access sensitive assets.

Insider risks can stem from a great many reasons. Malicious insiders, for example, may be motivated to do harm to a system in return for a bribe or in retaliation for a perceived slight. Their goals can range from intentional data theft, data destruction, espionage, or personal benefit.  Since malicious insiders have the benefit of time, they are able to study the system and craft a serious attack based on specific weak points in the infrastructure they are privy to.

In Ponemon's most recent research on Insider Threats, the findings reveal that both negligent and malicious insider risks as well as credential theft have grown 44% in the last two years alone. Incidents involving compromised users have since racked up costs amounting to over $15 million dollars globally.

In many of these incidents, cloud infrastructures have been the main target with Ponemon's report indicating that 52% of enterprises name cloud security as one of their greatest risks.

The following best practices can help security teams to mitigate these risks.

## 1. Implement Least Privilege Access Control

Defending against insider threats is a persistent challenge that requires continuous monitoring. One of the key ways to defend sensitive data and systems is to limit the number of users who have access to it as well as the permissions they have whilst exercising that access. To minimize the access of potential insider risk, enterprises can implement the principle of least privilege (PoLP).

The principle of least privilege is a security concept that states that every user, program, or system component should only have access to the resources they need to perform their function and no more. This works to minimize the potential damage that can happen as a result of a security breach or a misconfiguration.

The idea behind the principle of least privilege is that by limiting access to resources, the attack surface is reduced. By limiting the resources that a user or program can access, it makes it more difficult for attackers to gain access to sensitive information. For example, a user who only needs to read files in a specific directory should not have write access to that directory. Similarly, a program that only needs to access certain system files should not have access to other parts of the system.

## 2. Conduct Regular Security Awareness Training

An uncomfortable fact is that sometimes, insider behavior is carried out unknowingly by a negligent or untrained legitimate user. The Ponemon report cited 56% of incidents related to negligence in comparison to the 26% related to criminal insiders. This makes negligence a root cause in most cybersecurity incidents and varies anywhere from unsecured devices, unprotected passwords, not following their organization's security policies, or forgetting to patch or upgrade their software.

Unintentional insider threats can arise from the smallest of actions, such as clicking on malicious links or sharing sensitive information with unauthorized individuals. Enterprise leaders can combat this type of insider threat by implementing regular and accessible security awareness training and fostering a culture of good cyber hygiene. Employees who are trained on how to recognize the signs and consequences of insider risks can help prevent them from occurring in the first place. Security awareness training programs often cover a wide range of topics including phishing, password hygiene, social engineering recognition, and how to correctly report anomalous behavior they see.

## 3. Use Behavioral Analytics

Behavioral analytics can be a powerful tool for security teams working to mitigate insider risks in their cloud environments. By measuring real-time behaviors against a predetermined state of normalcy, analytics can help raise a red flag on any anomalies that may indicate potential malicious activity.

For instance, behavioral analytics can monitor user activities such as login times, locations, and access patterns to detect any suspicious changes or deviations from their normal behavior. It can also detect attempts to access unauthorized resources, perform unauthorized actions, or exfiltrate data.

Behavioral analytics is instrumental to how security teams streamline their hunt for potential insider threats. The more time is saved during that crucial hunting stage, the more effective the response can be in stopping incidents from becoming full-blown security crises. Even in post-event processes, behavioral analytics provides valuable insights into the motivations and patterns of insider threats, helping teams to develop or improve their existing security policies and procedures. Learning from the analytic is often a strong foundation upon which training programs can be created.

## 4. Implement DSPM (Data Security Posture Management)

Planning the security of business-critical data requires a comprehensive approach to data security and privacy. Implementing data security posture management (DSPM) can help enterprises manage their data access and prevent data leakage by implementing policies and controls to protect sensitive data from unauthorized access, sharing, and exfiltration.

In cloud infrastructures, DSPM is designed to help prevent insider threats by detecting and blocking attempts to transmit sensitive data outside the infrastructure. It works by:

- Controlling Access – DSPM can help enforce access control policies, ensuring that only authorized users have access to sensitive data. This can include implementing role-based access controls, multi-factor authentication, and other access management controls.
- Classifying Data – DSPM can help classify data based on its sensitivity level and apply appropriate security controls to protect it. This can include encryption, data masking, and data loss prevention (DLP) technologies.
- Monitoring & Logging – DSPM solutions can monitor and log all data access and usage, enabling security teams to detect any suspicious activity in real-time. This can include monitoring access patterns, data transfers, and other user activities.
- Supporting Incident Response – DSPM can help organizations respond to security incidents quickly and effectively. This can include automated incident response workflows, as well as real-time alerts and notifications to security teams.

## 5. Conduct Regular Audits

Prolong the effectiveness of access control policies through regular audits. Security teams can effectively nip suspicion behavior in the bud when they are able to identify potential insider threats in their earliest stages. Audits should be conducted on a regular basis and cover all areas of the cloud infrastructure, including access controls, user activity, and data transmission.

Scheduling regular audits allow teams to detect subtle anomalies in user behavior and cloud infrastructure activity such as usual file sharing, copying, or deletions. Uncovering security gaps and vulnerabilities that a malicious insider could exploit is often the first step in improving security policies and processes and building a cycle of continuous improvement.

## Conclusion

As cloud computing is adopted across all major industry verticals, security leaders are looking at the bigger picture of cloud-centric cyber risks across all possible attack surfaces – endpoint, identity, and network – to protect against both external and internal threats.

Since protecting a cloud infrastructure from insider threats requires a multi-faceted approach, leaders will rely on cloud-focused security solutions that can combine autonomous threat hunting, endpoint detection and response capability, and AI or machine-powered analytics to support all areas of cloud security.

SentinelOne is here to help enterprise leaders bolster their cloud defense strategies with least privilege access control, behavioral analytics, data loss prevention, and cloud workload protection. Contact us or request a demo to see how SentinelOne's Singularity™ for Cloud leverages machine learning to provide detection, response, and threat hunting across user endpoints, containers, cloud workloads, and IoT devices.

---

**Like this article? Follow us on LinkedIn, Twitter, YouTube or Facebook to see the content we post.**

### Read more about Cyber Security

- Detecting a Rogue Domain Controller – DCShadow Attack
- A Myth or Reality? Debunking (Mis)Conceptions Surrounding Cloud Ransomware
- 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