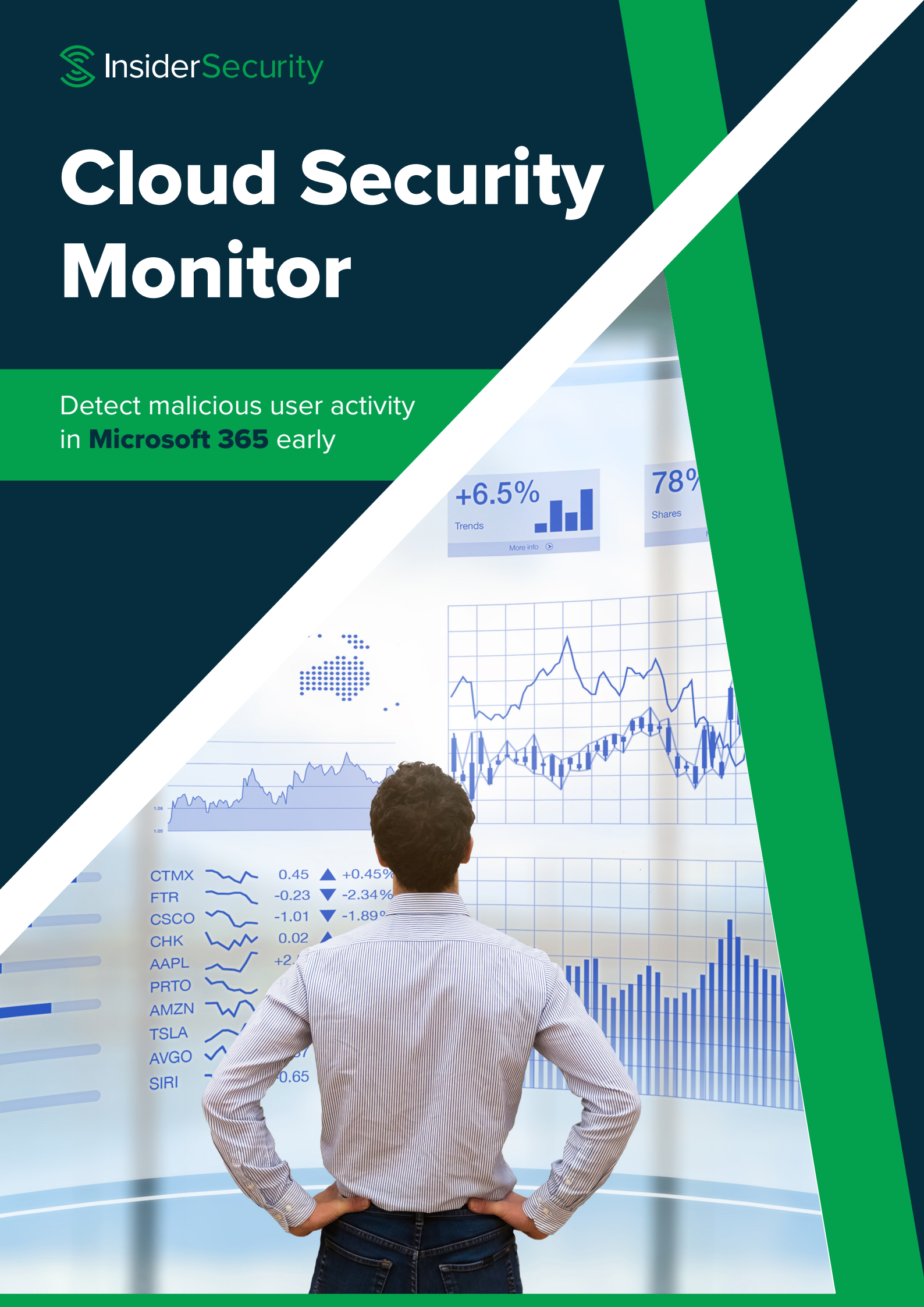
InsiderSecurity

Cloud Security Monitor

Detect malicious user activity in **Microsoft 365** early



How does **Cloud Security Monitor** help you?

With the shift to remote working and adoption of Microsoft 365 cloud services, there is a need to monitor for data security in employees' use of Microsoft 365 cloud services.

Microsoft 365 can provide a large amount of logs, however, it is difficult to make sense of them to discover account abuse or hacker activity. This is what InsiderSecurity solves.

Are you concerned if your company's accounts are compromised, and a hacker may be accessing your company data and emails?

Cloud Security Monitor detects if your online accounts have been hijacked by hackers.

How can you discover if there is a disgruntled employee or insider threat stealing your valuable company data?

Our award-winning solution detects suspicious user activity due to insider threats and hackers automatically.

Can you identify if a user has accidentally exposed confidential documents on OneDrive to the public?

Smart behavior analytics discover if files are accidentally left exposed.

What does **Cloud Security Monitor** cover?

- Rogue administrators
- Insider threats
- Compromised accounts
- Data thefts

How is **Cloud Security Monitor** different?

Conventional Solutions	VS	Cloud Security Monitor
RAW LOGS		**SMART REPORTS**
■ Report the numerous log events by Microsoft 365 accounts		■ Deploys sophisticated user behavior analytics to detect suspicious user activities
■ Need to manually make sense of large amount of log events or alerts, which is not practical		■ Automatically makes sense of log events to report high-risk Microsoft 365 accounts
■ Difficult to spot suspicious activities		■ No need to comb through large amount of log events or alerts

Cloud Security Monitor

Use Cases

Azure Active Directory

1 Suspicious Login Activity

An attacker is trying to take over a user account. Cloud Security Monitor detects such suspicious login activity using indicators such as frequency, time and location.

2 Privilege Escalation

An unwanted user managed to obtain administrator rights, allowing them to perform privileged actions like removing accounts and modifying system settings. Cloud Security Monitor keeps track of admin roles and access rights, and alerts when there is a high risk of privileged escalation.

OneDrive / SharePoint Online

3 Suspicious Data Access

A user account has been compromised and the attacker has accessed OneDrive for Business or SharePoint Online to download sensitive files. Cloud Security Monitor is able to detect suspicious file downloads. Cloud Security Monitor also analyses other data operations such as delete, edit, create and restore.

4 File Permission Change

A malicious user has made changes to file sharing permissions in OneDrive for Business or SharePoint Online. This may lead to a potential data breach. Cloud Security Monitor can detect changes to file sharing permissions.

5 Unauthorized Sharing

An external user has gained access to sensitive or private information on OneDrive for Business or SharePoint Online app via a shared link. Unauthorized shared links are constantly tracked by Cloud Security Monitor to detect suspicious access to sensitive information.

Cloud Security Monitor Use Cases

Exchange Online

6 Non-owner Mailbox Access

A user account has been compromised and the hacker has accessed Microsoft Exchange Online and has been reading sensitive emails from another user's mailbox. Cloud Security Monitor detects non-owner mailbox permissions.

7 Unauthorized Policy Change

There has been a change in Microsoft Exchange Online policies to enable user to receive spam mail that contains phishing or malicious content, or to forward a copy of all user emails to an attacker. Cloud Security Monitor keeps track of Microsoft's policies to detect suspicious changes.

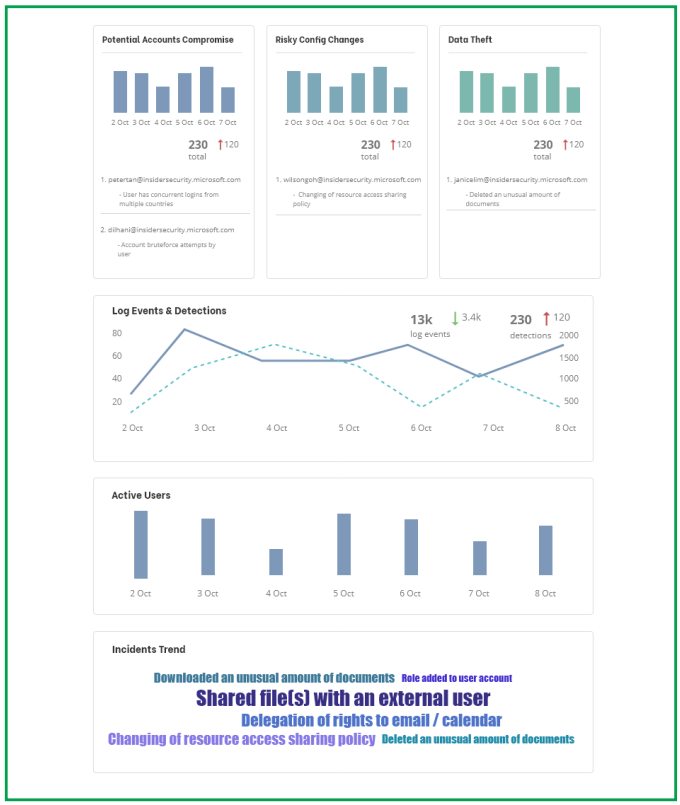


Figure 1: Receive alerts and regular reports on high risk accounts

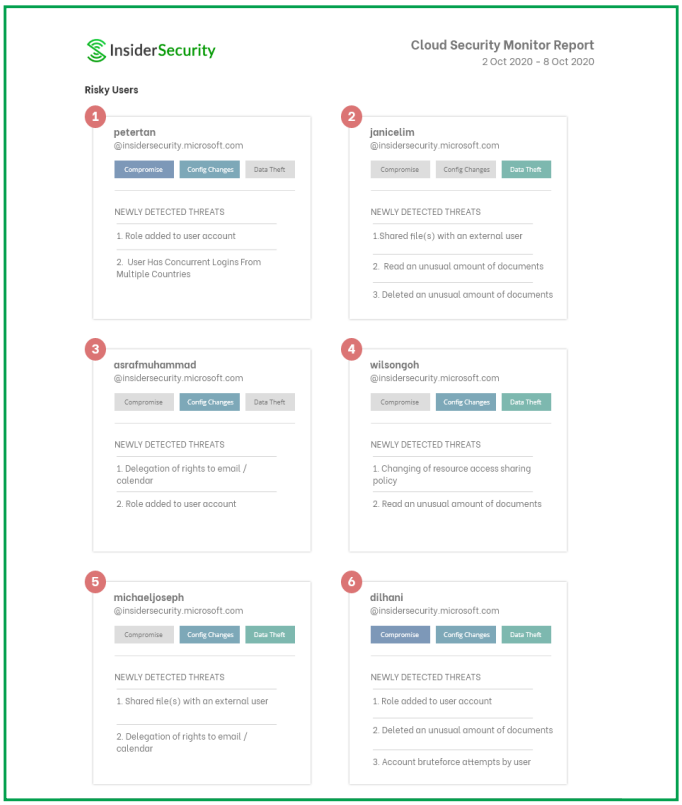


Figure 2: Provides visibility of user activity

InsiderSecurity

+65 6270 4029

hello@insidersecurity.co

https://insidersecurity.co

81 Ayer Rajah Crescent, #03-48,
Singapore 139967