Proofpoint Account Takeover Protection

Detect and respond to cloud account takeovers

Key Benefits

- Detect compromised Microsoft 365, Google Workspace and Okta accounts
- Defend against account takeover attacks that bypass MFA
- Accelerate your investigations with a centralised view of post-account-takeover activities
- Reduce attacker dwell time by suspending accounts and forcing password resets
- Revert malicious changes to mailbox rules and MFA settings
- Remove suspicious third-party applications

Proofpoint Account Takeover Protection (ATO Protection) extends Proofpoint Targeted Attack Protection (TAP) to detect compromised cloud accounts and protect your cloud environments.

ATO Protection extends Targeted Attack Protection (TAP) to detect and secure compromised cloud accounts. ATO Protection uses artificial intelligence (AI), correlated threat intelligence and behavioural analytics to detect suspicious activity across the whole attack chain. It detects post-compromise changes made by attackers and removes their access. It reverts malicious updates to mailbox rules and multi-factor authentication (MFA) settings. It also removes suspicious third-party applications and quarantines and removes suspicious files.

ATO Protection provides detailed reports that show suspicious logins, attacked users and impacted systems and settings. Integration with Proofpoint Identity Threat Defense shows you the potential impact of an account takeover on other accounts and hosts with one click. These insights help you to stop attacks before they become serious breaches that harm your business.

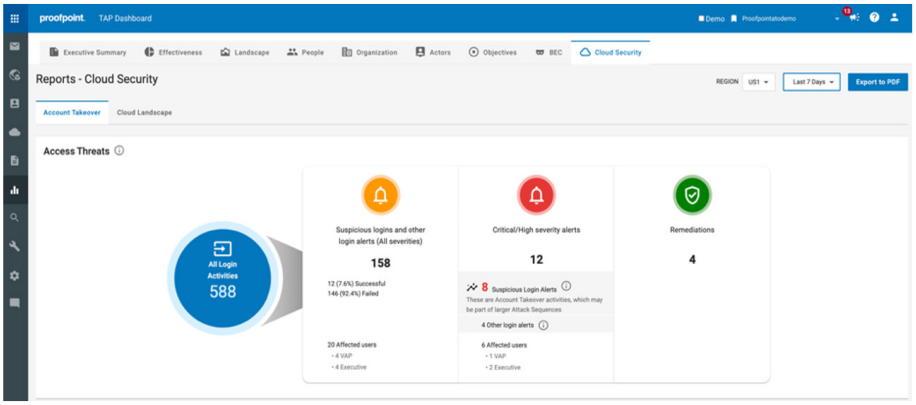
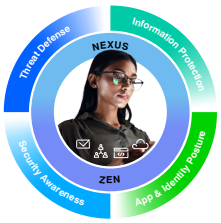


Figure 1: ATO Protection detects suspicious logins, gives you detailed insights that help you investigate threats and reverts malicious changes.

This solution set is part of Proofpoint's integrated Human-Centric Security platform, mitigating the four key areas of people-based risks.



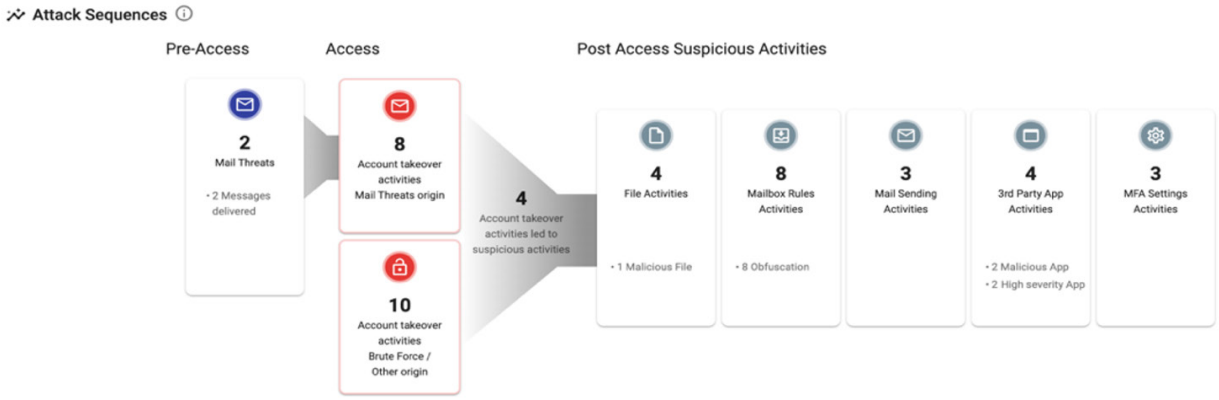


Figure 2: The Attack Sequence report shows you pre- and post-access threat activity for affected accounts.

Improved detection and visibility

ATO Protection detects compromised accounts and suspicious email and other activities in your cloud environments. It uses threat intelligence from over 40 million users monitored across thousands of organisations. It combines this information with AI and behavioural analytics to detect unusual activity in your environment. This combination of techniques reduces false positive alerts. You are assured of accurate detections and gain a clear view of all the activity in your attacked accounts.

When an account is taken over, ATO Protection adds alerts to the TAP dashboard. An attack timeline shows account takeover activities, file and email activity, changes to mailbox rules and MFA settings and the addition of third-party apps.

Accelerated investigations

ATO Protection shows your security analysts the cause of an account takeover and how to limit further risk.

This information is integrated with the TAP investigation system and process to give you insights that complement the ones TAP provides. An attack timeline shows accounts that have been taken over. You can click and investigate each event in the timeline.

You can see how an account was attacked and the location of the attacker. You can also learn about users who have been hit by similar threats. Advanced analytics provide detailed activity timelines for users, IP addresses, domains and other attributes. These rich insights help you assess further risks to your organisation.

Automated response

ATO Protection detects and reverts malicious changes to mailbox rules and MFA settings. Attackers often change mailbox rules to hide in your system and monitor it before they initiate internal phishing or take other attack steps. ATO Protection also removes malicious third-party apps. All of these actions limit damage to your organisation and reduce the time you need to investigate and respond to threats. If your investigation shows other malicious activities, you can fix the accounts that have been taken over. You can also remove files that attackers have added to a user's account

'Proofpoint Account Takeover Protection' was formerly 'Proofpoint TAP Account Takeover'.

LEARN MORE

For more information, visit **proofpoint.com**.