

Proofpoint Account Takeover

Detect, investigate and respond to multistage account takeover

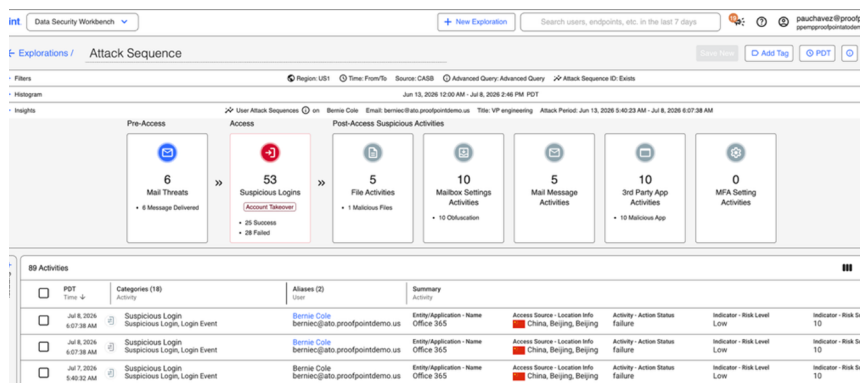
Key Highlights

- Detect multistage account compromise with high precision
- Accelerate investigations with unified visibility across the attack lifecycle
- Reduce attacker dwell time through automated response and remediation
- Minimise fraud, data loss and business disruption from compromised accounts
- Strengthen defence-in-depth with Proofpoint Collaboration Security Prime

Proofpoint Account Takeover Protection helps organisations detect, investigate and contain compromised user accounts across the entire account takeover (ATO) lifecycle—from pre-access indicators and successful compromise to post-access attacker activity.

Powered by Proofpoint Nexus® AI and threat intelligence, Proofpoint Account Takeover Protection delivers high-confidence detection of confirmed account compromise while providing complete visibility into attacker behaviour. Security teams can quickly understand the scope of an incident, speed up investigations and contain threats before they escalate into business email compromise (BEC), data theft, lateral movement or other business-impacting attacks.

As part of Proofpoint Collaboration Security Prime, Proofpoint Account Takeover Protection integrates with Threat Protection Workbench and Threat Interaction Map to extend investigations beyond a single compromised account. By correlating identity compromise with email threats, user interactions and attacker activity, it helps security teams gain a broader understanding of the attack campaign. This enables faster investigations, more informed response decisions and stronger remediation.



1. Figure 1. Gain comprehensive visibility across the ATO attack lifecycle from pre-access to post-access activities.

High-Confidence ATO Detection

Powered by Proofpoint Nexus AI, Proofpoint Account Takeover Protection delivers high-confidence detection of confirmed account compromise across Microsoft 365, Google Workspace and Okta.

By continuously analysing user activity across the account takeover lifecycle—from pre-access indicators to post-access attacker behaviour—Proofpoint Account Takeover Protection identifies confirmed compromise with high confidence, and it prioritises detections based on risk severity (Critical, High and Medium). Each detection includes the behavioural indicators and evidence that contributed to the finding, helping analysts quickly understand why an account was identified as compromised, prioritise response efforts and take action with confidence.

Complete Attack Visibility

Once account compromise has been confirmed, Proofpoint Account Takeover Protection provides complete visibility into the attack sequence, enabling security teams to understand how the attack unfolded and what the attacker did after gaining access.

Comprehensive forensic insights reveal post-access activities—including mailbox manipulation, malicious inbox rules, OAuth abuse, privilege changes, internal phishing, suspicious email activity and persistence techniques. This helps analysts quickly determine the scope, sophistication and reach of the attack. By reconstructing the attack sequence and highlighting affected users and assets, Proofpoint Account Takeover Protection helps accelerate investigations, supports more informed response decisions and improves remediation.

Automated Threat Response

Account Takeover Protection helps organisations rapidly contain active threats through automated remediation actions that disrupt attacker access and accelerate recovery. Response actions include forcing password changes, resetting user passwords, revoking active user sessions, removing malicious mailbox rules, revoking unauthorised third-party OAuth applications and other remediation measures designed to eliminate attacker persistence and restore account integrity.

By automating critical containment actions, security teams can reduce attacker dwell time, limit lateral movement, minimise business disruption and accelerate recovery from account compromise.

Defence-in-Depth with Proofpoint Collaboration Security Prime

As part of Proofpoint Collaboration Security Prime, Proofpoint Account Takeover Protection extends beyond account compromise to deliver coordinated protection across the entire human attack lifecycle. While Proofpoint Account Takeover Protection detects, investigates and contains compromised accounts, Proofpoint Prime enhances protection by preventing threats before compromise, correlating attacks across email and collaboration channels, improving user behaviour through adaptive education and providing unified investigation and response through Threat Protection Workbench and Threat Interaction Map.

Together, these capabilities support a defence-in-depth strategy that helps organisations prevent attacks, mitigate active threats, strengthen user resilience and continuously improve their security posture from a single integrated platform.

Learn more at proofpoint.com/uk

About Proofpoint, Inc. Proofpoint, Inc. is a global leader in human- and agent-centric cybersecurity, securing how people, data and AI agents connect across email, cloud and collaboration tools. Proofpoint is a trusted partner to over 80 of the Fortune 100, over 10,000 large enterprises and millions of smaller organisations in stopping threats, preventing data loss and building resilience across people and AI workflows. Proofpoint's collaboration and data security platform helps organisations of all sizes protect and empower their people while embracing AI securely and confidently. Learn more at www.proofpoint.com/uk.

Connect with Proofpoint: [LinkedIn](#)

Proofpoint is a registered trademark or trade name of Proofpoint, Inc. in the United States and/or other countries. All other trademarks contained herein are