Proofpoint TAP Account Takeover

Detect and remediate compromised accounts in your email and cloud environments

Key Benefits

- Employ threat intelligence and behavioural analytics to detect compromised email accounts
- Protect against multifactor authentication bypass
- Accelerate and unify email threat investigations of account takeover attacks and post-compromise cloud activities
- Remediate accounts, malicious mailbox rule changes, manipulations of third-party apps and data exfiltration across email and cloud environments

Proofpoint TAP Account Takeover extends the power of Proofpoint Targeted Attack Protection (TAP) by detecting compromised accounts and protecting your email and cloud environments. It defends against phishing, brute force attacks, business email compromise (BEC), malware, data exfiltration and attackers' persistent access.

TAP Account Takeover uses artificial intelligence (AI) as well as correlated threat intelligence and behavioural analytics to detect suspicious activity across the entire email account attack chain. It lets you see the kind of mail threats that target accounts. If an attacker accesses an account, you can take action to protect it. It also automatically remediates malicious mailbox rule changes, abused third party apps and the oversharing of sensitive files. TAP Account Takeover gives you a detailed report of suspicious logins, account takeovers, impacted users and the actions taken to remediate the threats. These insights help you quickly investigate malicious activities, respond to threats and limit risk

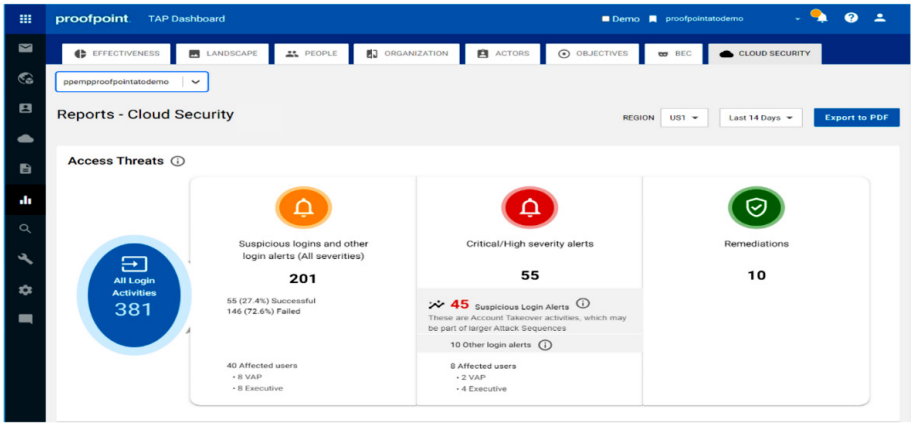

Figure 1: Proofpoint monitors all login activity. And the Access Threats report helps you visualise suspicious logins and automated remediations.

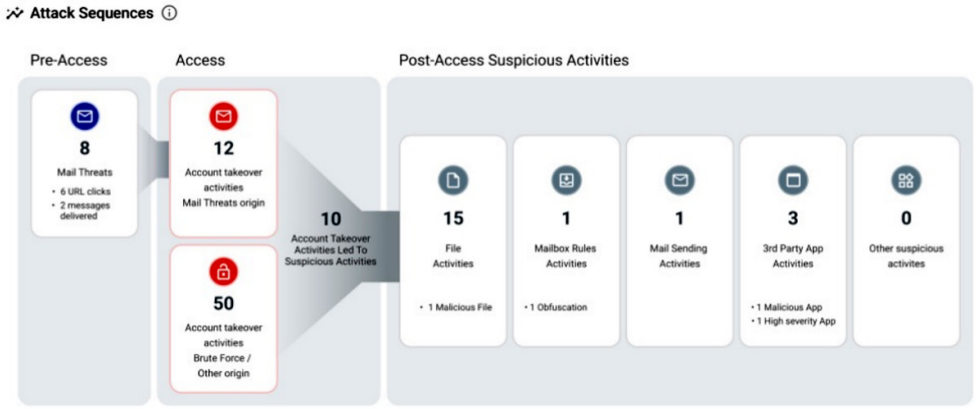

Figure 2: The Attack Sequence report displays access threats across the attack chain.

Visibility

TAP Account Takeover surfaces compromised accounts and suspicious post-access activity in your email and cloud environments. It correlates threat intelligence with AI/ML and behavioural analytics to detect malicious events. This approach provides you with complete visibility. You can see whose account is compromised and how. It also reduces false positive alerts. This way you can have more confidence in account takeover verdicts.

TAP Account Takeover issues automated alerts in the TAP dashboard when an account is compromised. An attack sequence timeline displays an overview of account takeover risk. It also shows impacted accounts and malicious activities pre-access to post-access. It can tell you how attackers accessed the account as well as what they did after logging in. It can tell you about their file activities, for example. And it can spot changed mailbox rules that help hide their presence in your system, their mail-sending activities and when they manipulate third-party apps.

Accelerate Investigations

With TAP Account Takeover, your security analysts can quickly understand what happened and how to limit risk.

Information about account takeover is integrated with the TAP investigation system and process. You get the same correlated people-centric insights and threat intelligence provided in the TAP dashboard. A timeline view of activity provides insights about accounts that have been taken over. All data is clickable. This allows analysts to drill down and investigate each incident post account compromise. You can see if the user is a Very Attacked Person™ (VAP). You can also see how the account was compromised as well as the location of the attacker. And you can learn about other users who have been hit by similar threats.

Automated Response

TAP Account Takeover automatically detects and remediates when attackers make changes to mailbox rules. Attackers often change these rules to hide their identity before they stage a BEC attack. TAP Account Takeover also detects and revokes abused third-party apps that can help attackers control an account without being detected. These actions help reduce attackers' dwell time in accounts. They can limit damage to your organisation and reduce your team's workload. If an investigation reveals other malicious activity, you can take action to remediate accounts that have been taken over. You can limit data loss. And you can delete malicious files that attackers have inserted into your environment.

LEARN MORE

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