proofpoint.

SOLUTION BRIEF

# How Proofpoint Defends Against Cloud Account Takeover

## Prevent and mitigate potentially devastating cloud account takeovers

### Products

- Proofpoint Cloud App Security Broker
- Proofpoint Zero Trust Nework Access
- Proofpoint Browser Isolation
- Proofpoint Email Isolation
- Proofpoint Threat Protection Platform
- Proofpoint Targeted Attack Protection

### Key Benefits

- Prevent initial account takeover by blocking phishing attacks designed to steal credentials or activate malware
- Detect and remediate all instances of a cloud attack takeover
- Erect a solid barrier around your valuable assets to defend them against threats
- Prevent your people from unwittingly introducing threats into your environment
- Garner invaluable intelligence to help you prepare for potential emerging threats

Cyber criminals are following businesses into the cloud. As more companies adopt hosted email and webmail, cloud productivity apps like Microsoft 365 and Google Workspace, and cloud development environments like AWS and Azure, cyber criminals have quickly learned that the basic corporate account credential is a potential source of money and power. They now target these credentials in growing numbers of threat campaigns. And their relentless efforts are just the opening salvos in their mission to execute wire fraud, industrial espionage, PII data theft and more.

A cloud account takeover starts with attackers compromising user credentials and gaining entry into user systems. These attacks often originate from email in messages that carry malware or trick users into providing their credentials. Once they take over an account, they can pose as legitimate or trusted persons within the user's organisation. The infiltrators can move laterally and wreak widespread damage. They can steal or encrypt important data. They can also upload malware to use the sync-and-share capabilities between your endpoints, Microsoft 365 and other cloud repositories. From there, they can quickly spread across your organisation or download sensitive files to use for extortion.

And with the growing use of single sign-on systems, it only takes one compromised credential to give an attacker access to many different systems in the company.

One of the most menacing and disruptive forms of a cloud account takeover is ransomware. This type of cyber attack puts victims out of business, forces hospitals to turn away patients and can bring entire governments to a standstill. Last year alone, the United States saw more than 65,000 ransomware attacks. And according to Unit 42 of Palo Alto Networks, three-quarters of these attacks originated from email.[1] It is a top concern for CISOs. And it has even become a national security issue.

## Proofpoint Solutions

Cyber criminals use multiple strategies and threat vectors to gain a foothold in your network. They often come at you with hybrid approaches to get the information they need. And their arsenal can include brute-force attacks, social engineering schemes and malware. You need a comprehensive, multilayered defence to protect against their schemes. Proofpoint offers a number of products and services that can help.

Used together, the Proofpoint solutions help you defend against the cloud account takeover threat by enabling you to:

- Prevent initial account takeover
- Detect and remediate cloud attack takeover
- Erect barriers around your valuable assets—both people and systems—to keep outside threats from attacking them
- Prevent your people from unwittingly introducing threats into your environment
- Garner invaluable intelligence to help you prepare for potential upcoming threats

### Prevention, detection and remediation

The Proofpoint Threat Protection Platform is an integrated, multilayered solution that reduces the risk of cloud account takeover. It features industry-leading threat-detection that prevents users from receiving malware, credential phishing and other types of email-based attacks. It also orchestrates security to remediate compromised accounts.

1 Unit 42, Palo Alto Networks *(https://unit42.paloaltonetworks.com/ransomware-families/)*. "Ransomware Families: 2021 Data to Supplement the Unit 42 Ransomware Threat Report" July 2021.

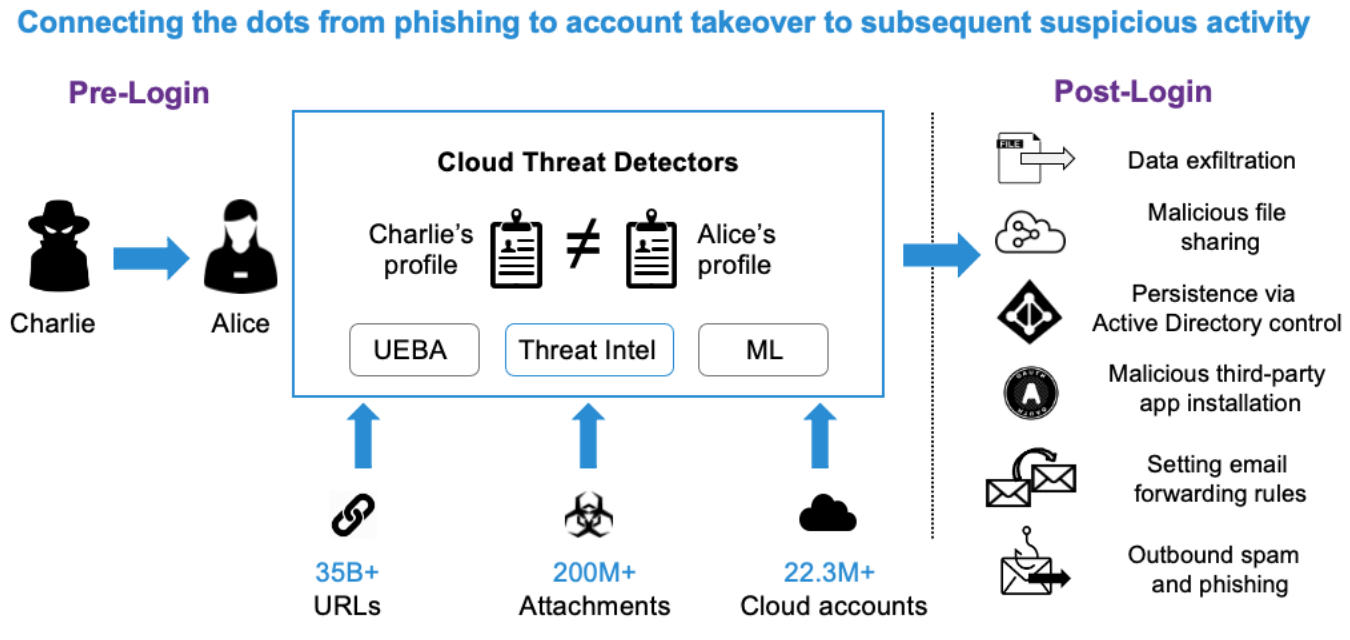


Figure 1: CASB compromised account detection.

This shortens incident response times and reduces IT overhead. Targeted users and those who engage with real credential threats can receive short, timely lessons through security awareness training. And through informative and customisable HTML banners, the platform can nudge users to be careful with messages that may be dangerous. It can authenticate inbound and outbound messages via DMARC. It can also identify compromised supplier accounts. This layered approach is why more than 60% of the Fortune 1000 trust Proofpoint for threat protection to reduce the risk of cloud account takeover.

Proofpoint Cloud App Security Broker (CASB) is the cornerstone of our defence against cloud account takeovers. It takes a people-centric approach to protect your users from cloud threats and safeguard your sensitive data. Its defence starts with visibility and access controls. This is because until you know what you don't know, you cannot really wage an effective defence against a cloud account takeover. CASB helps you deploy preventative security measures such as adaptive access controls, including step-up authentication. We detect all takeover attempts and let you know what threat actors do once they have gained access to an account. CASB suspends compromised accounts and remediates all post-takeover threats. This means that even if an attacker has gained access to one of your accounts, CASB can thwart attempts at using it for email forwarding and delegation, data exfiltration, and sending phishing and spam emails.

## Zero trust-alternative to VPN

The world's remote and mobile workforce is expanding. With it, the network perimeter is dissolving as more apps migrate to the cloud. Many companies are just beginning to grapple with the new security challenges that come with this new paradigm. They are thus only now finding that their legacy security systems, built around site-centric connectivity and security stacks, are not up to the task of protecting against increasingly innovative cloud-based threats.

Proofpoint Zero Trust Network Access (ZTNA) can help securely connect your users to apps both in the data centre and the cloud. This people-centric alternative to VPN microsegments permissions, drastically reducing a network's attack surface. It provides a software-defined perimeter (SDP) to achieve zero-trust network access.

## Browser and email isolation

IT and security teams must ensure a secure operating environment for their users. But they should also allow the users to research and collaborate with team members effectively. This can be tricky when two of the primary vectors for cloud account takeovers are the very same tools used for research and communication: web and email. Proofpoint offers two solutions that give your teams the best of both worlds. They provide seamless browsing and communications experiences, but they still protect the users from cloud-account compromise.

Proofpoint Browser Isolation defends against cloud account compromise by letting your users browse the web while protecting them from inadvertently clicking on phishing links and downloading malicious files to your corporate devices.

Proofpoint Email Isolation extends the capabilities of Targeted Attack Protection (TAP). It enables risk-based isolation for URL clicks within corporate emails. It can also highlight your most attacked people and determine the riskiest URLs that get into your users' inboxes.

## Up-to-date intelligence

In depth and broad knowledge of the threat landscape allows you to prepare for the next big threat. Proofpoint Nexus Threat Graph provides the comprehensive threat intelligence you need to keep you abreast of today's biggest cyber threats. It combines trillions of real-time data points across multiple threat vectors around the world, advanced AI and machine learning, and a global team of cyber security research experts.

## LEARN MORE

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

**ABOUT PROOFPOINT**

Proofpoint, Inc. is a leading cybersecurity and compliance company that protects organisations' greatest assets and biggest risks: their people. With an integrated suite of cloud-based solutions, Proofpoint helps companies around the world stop targeted threats, safeguard their data and make their users more resilient against cyber attacks. Leading organisations of all sizes, including more than half of the Fortune 1000, rely on Proofpoint for people-centric security and compliance solutions that mitigate their most critical risks across email, the cloud, social media and the web. More information is available at **www.proofpoint.com**.

©Proofpoint, Inc. Proofpoint is a trade mark of Proofpoint, Inc. in the United States and other countries. All other trade marks contained herein are property of their respective owners.