Proofpoint Cloud Account Defense

Proofpoint Cloud Account Defense (PCAD) protects Microsoft Office 365 users from account compromise. With PCAD, you can detect, investigate and defend against cyber criminals accessing your sensitive data and trusted accounts. Our powerful forensics and policy-based controls help you monitor and remediate based on the risk factors that matter to you.

Users account credentials are the keys to your organization’s kingdom. When cybercriminals compromise these credentials from your Office 365 accounts, they can launch attacks inside and outside of your organization. They can convince users to wire money or part with sensitive data. And they can access your critical data, such as intellectual property or customer data. This hurts your reputation and finances. And once attackers gain a foothold in your organization, they often install backdoors to maintain access for future attacks. While account compromise often occurs via phishing, it can also occur through:

- Brute-force attacks that automate credential guessing
- Credential recycling, or stuffing, which uses already stolen username and password pairs
- Malware, such as key loggers and credential stealers

You can defend against Office 365 account compromise with our integrated, people-centered approach that correlates cloud and email threat activity. We combine analytics that are based on cloud access and user behavior with our email threat intelligence. This allows you to identify at risk and to detect compromised accounts.

Detect Compromised Accounts

PCAD uses contextual data like user location, device, network and login time to detect compromised accounts. We use analytics to establish safe baseline behaviors. And we monitor for anomalies using captured footprints, thresholds and advanced machine learning. We look for suspicious activities like excessive and unusual login attempts, such as brute-force behavior and too-fast-to-travel.

PCAD also combines our rich threat intelligence with user-specific risk indicators. This allows you to detect logins from suspicious sources. Using our global threat intelligence, we conduct IP reputation checks. We also correlate threat activity across email and cloud. And our email-based threat intelligence helps to connect the dots between credential phishing email attacks and suspicious logins. Attackers may use a compromised account to launch a phishing attack and compromise other users in your organization. To identify other compromised accounts, we study the attacker’s footprint, looking for unusual user agent and activities, such as email forwarding.

KEY BENEFITS

- Identify top users at risk and monitor for incidents via drilldown dashboards
- Customize and prioritize alerts based on the risk factors that matter to you
- Correlate threats across email and cloud to accurately detect compromised accounts
- Investigate security incidents through detailed forensics and customizable reports
- Automate security response with flexible policy controls
- Deploy quickly in the cloud
- Rely on award-winning customer support

Proofpoint Cloud Account Defense
PROOFPOINT CLOUD ACCOUNT DEFENSE | DATA SHEET

DATA SHEET   | Proofpoint Cloud Account defense

Investigate Incidents with Granular Forensics
When an incident occurs, you can investigate past activity and alerts through our intuitive dashboard. There you can review granular forensics data on transactions, such as user, date, time, IP, device, browser, user agent, location, threat, threat score and more. You can also view and analyze this data via drill-down graphs and log reports. And you can sort or filter activity and alert logs customize your investigative reports. And you can subscribe to your reports on a daily, weekly, or monthly basis. For further analysis, forensics data can be exported manually or via SIEM integration, supported through REST APIs.

Defend Office 365 Accounts with Flexible Policies
With insights you gain from our detailed forensics, you can build flexible policies based on multiple parameters. These include user, location, network, device, suspicious activity and more. For example, you can generate login alerts for blacklisted countries or for devices that don’t meet your corporate guidelines. Also, when monitoring a high-usage service like Office 365, you need to prioritize alerts to prevent alert fatigue. With PCAD, you can generate alert notifications based on their severity. You can customize each notification or use the default template. And you can monitor at-risk users more closely or suspend them if a suspicious login is successful.

Deploy Quickly in the Cloud
Cloud-based platforms need cloud-based protection. Our cloud architecture and protection through Office 365 APIs enable you to deploy quickly and derive value immediately. You can protect hundreds of thousands of users in days—not weeks or months. As an industry leader in threat protection, we use the cloud to update our software daily to help you stay ahead of attackers. Our cloud-based deployment also provides you with the flexibility to protect users on any network or device.

For More Information

LEARN MORE
For more information, visit proofpoint.com.

ABOUT PROOFPOINT
Proofpoint, Inc. (NASDAQ: PFPT) is a leading cybersecurity company that protects organizations’ 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 organizations 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 trademark of Proofpoint, Inc. in the United States and other countries. All other trademarks contained herein are property of their respective owners. Proofpoint.com