DATA SHEET

proofpoint.

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 cybercriminals 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.

KEY BENEFITS

- Identify top users at risk and monitor for incidents via drill-down 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

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 impacts 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 users at risk and to detect compromised accounts.

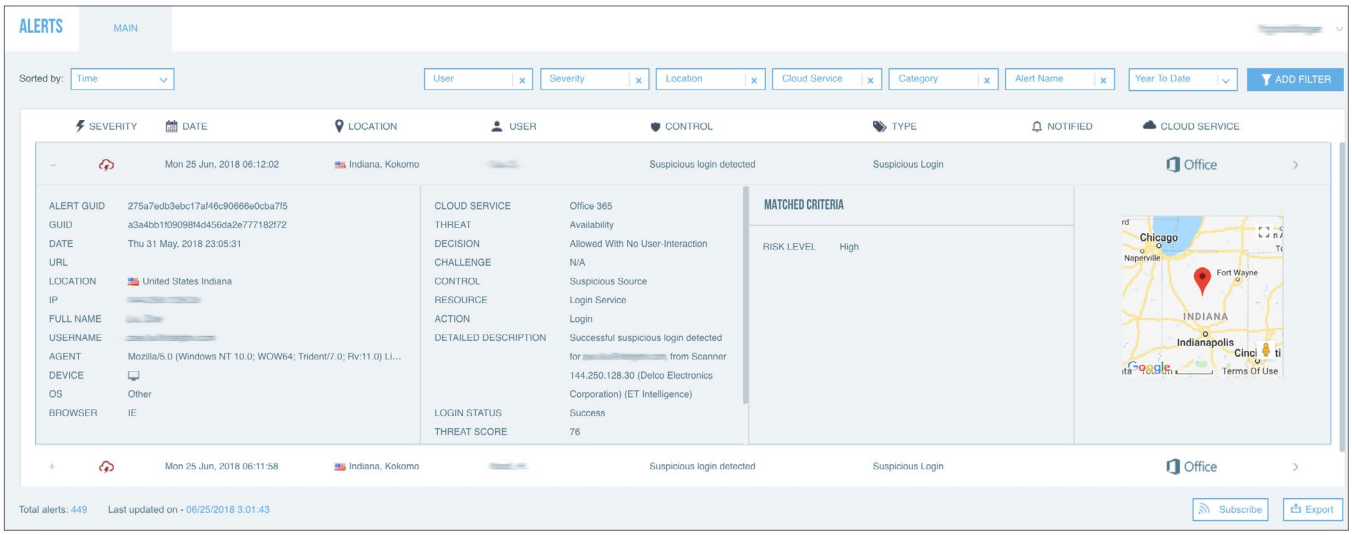
DETECT COMPROMISED ACCOUNTS

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.

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.

LEARN MORE

Proofpoint Cloud Account Defense helps you deploy and use Office 365 with confidence. Sign up for a free assessment at proofpoint.com/us/products/cloud-account-defense.

ABOUT PROOFPOINT

Proofpoint, Inc. (NASDAQ:PFPT), a next-generation cybersecurity company, enables organizations to protect the way their people work today from advanced threats and compliance risks. Proofpoint helps cybersecurity professionals protect their users from the advanced attacks that target them (via email, mobile apps, and social media), protect the critical information people create, and equip their teams with the right intelligence and tools to respond quickly when things go wrong. Leading organizations of all sizes, including over 50 percent of the Fortune 100, rely on Proofpoint solutions, which are built for today's mobile and social-enabled IT environments and leverage both the power of the cloud and a big-data-driven analytics platform to combat modern advanced threats.