proofpoint. DATA SHEET

Proofpoint Cloud Account Defense

Proofpoint Cloud Account Defense (CAD) protects Microsoft 365 and Google Workspace users from cloud account compromise. With CAD, 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 threats based on the risk factors that matter to you.

KEY BENEFITS

- Identify top users at risk and monitor for incidents via drilldown dashboards
- Customise and prioritise 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 customisable reports
- Prevent unauthorised access to cloud apps and services with adaptive access controls
- Automate security response with flexible policy controls
- Deploy quickly in the cloud
- Rely on award-winning customer support

User account credentials are the keys to your organisation's kingdom. When cybercriminals compromise the credentials for your Microsoft 365 or Google Workspace accounts, they can launch attacks inside and outside of your organisation. 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 organisation, 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 cloud account compromise with our integrated, people-centric approach that correlates cloud and email threat activity. We combine analytics that are based on cloud access and user behaviour with our email threat intelligence. This allows you to identify users at risk and to detect compromised accounts.

We also prevent unauthorised access with our adaptive access controls for IT-approved cloud apps and services. Our people-centric policies alert you to issues in real-time and apply risk-based controls, such as VPN enforcement or multi-factor authentication when needed.

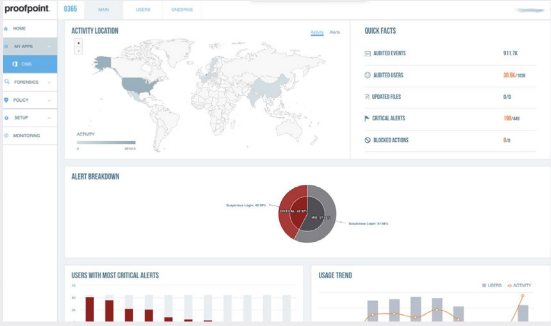
Detect compromised accounts

CAD provides people-centric visibility into email and cloud threats. We help you:

- Identify your Very Attacked People (VAPs) and protect their cloud accounts
- Detect compromised attacks by using contextual data like user location, device, network and login time
- Establish safe baseline behaviours by applying analytics
- Monitor for anomalies using captured footprints, thresholds and advanced machine learning and look for suspicious activities like excessive and unusual login attempts, such as brute-force behaviour and too-fast-to-travel

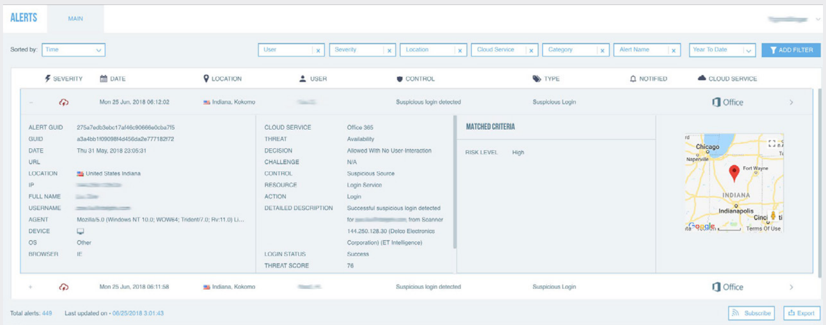
CAD also combines our rich cross-vector threat intelligence from Proofpoint Nexus Threat Graph with user-specific risk indicators. This allows you to detect logins from suspicious sources.

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 organisation. To identify other compromised accounts, we study the attacker's footprint, looking for unusual user agent and activities, such as email forwarding.



QUICK FACTS

AUDITED EVENTS	911.7K
AUDITED USERS	30.5K/103K
UPDATED FILES	0/0
CRITICAL ALERTS	190/449
BLOCKED ACTIONS	0/0



SEVERITY	DATE	LOCATION	USER	CONTROL	TYPE	NOTIFIED	CLOUD SERVICE
	Mon 25 Jun, 2018 06:12:02	Indiana, Kokomo	[redacted]	Suspicious login detected	Suspicious Login		Office
	Mon 25 Jun, 2018 06:11:58	Indiana, Kokomo	[redacted]	Suspicious login detected	Suspicious Login		Office

ALERT GUID 275a7edb3ebc17af46c90666e0cba7f5
GUID a3a4bb1f09098f4d456da2e777182f72
DATE Thu 31 May, 2018 23:05:31
URL
LOCATION United States Indiana
IP [redacted]
FULL NAME [redacted]
USERNAME [redacted]
AGENT Mozilla/5.0 (Windows NT 10.0; WOW64; Trident/7.0; Rv:11.0) Li...
DEVICE
OS Other
BROWSER IE

CLOUD SERVICE Office 365
THREAT Availability
DECISION Allowed With No User-Interaction
CHALLENGE N/A
CONTROL Suspicious Source
RESOURCE Login Service
ACTION Login
DETAILED DESCRIPTION Successful suspicious login detected for [redacted] from Scanner 144.250.128.30 (Delco Electronics Corporation) (ET Intelligence)
LOGIN STATUS Success
THREAT SCORE 76

MATCHED CRITERIA
RISK LEVEL High

Total alerts: 449 Last updated on - 06/25/2018 3:01:43

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 analyse this data via drill-down graphs and log reports. And you can sort or filter activity and alert logs customise 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 Microsoft 365 and Google Workspace Accounts with flexible policies

With the insights you gain from our detailed forensics, you can build flexible remediation 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 Microsoft 365 or Google Workspace, you need to prioritise alerts to prevent alert fatigue. With CAD, you can generate alert notifications based on their severity. You can customise 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.

CAD's adaptive access controls enable people-centric real-time security measures based on risk, context and role. You can automatically block access from risky locations and networks and by known threat actors. And you can apply risk-based controls to VAPs and high-privilege users, including step-up authentication and VPN enforcement.

Deploy quickly in the cloud

Cloud-based platforms need cloud-based protection. Our cloud architecture and protection through Microsoft 365 or Google Workspace APIs enable you to deploy quickly and derive value immediately.

When implementing adaptive access controls, you can redirect your cloud app logins to our security assertion markup language (SAML) gateway. This gateway brokers the federated authentication between each service provider and the identity provider. CAD supports any IT-approved cloud service that is SAML 2.0 federated. And for strong authentication, you can integrate your multi-factor authentication solution or use our mobile authenticator app, Proofpoint Mobile Access included with CAD. 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

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

ABOUT PROOFPOINT

Proofpoint, Inc. (NASDAQ: PFPT) is a leading cybersecurity 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**.