SOLUTION BRIEF

proofpoint.

PROOFPOINT FOR HIGHER EDUCATION

Proofpoint takes a people-centered approach to meet the security and compliance needs of higher education. We deliver the most effective tools available to protect your people. We help you:

- Stop advanced threats that target your people
- Protect the information they create and access
- Secure their personal activity and train them to spot and report attacks before they spread

Our solutions span the key technologies, applications and platforms your people use to interact, communicate and learn: email, social media and cloud apps.

HIGHER EDUCATION'S HEADACHE

Modern ways of learning pose unique cybersecurity and IT challenges for colleges and universities.

Open network environments access web, mobile and cloud applications—such as Microsoft Office 365 and Google G Suite. Faculty, researchers industry partners and students are generating, exchanging and accessing a wealth of sensitive information through email and cloud apps. Unprotected financial, research and personal data puts people in the user community at risk of being exploited.

These trends leave schools struggling to address the speed, volume and complexity of today's evolving cyber threats. At the same time, schools are under more pressure than ever to protect people's privacy under FERPA, HIPAA and other rules.

That's why we're focused on protecting you against advanced threats, improving your incident response, and ensuring operational continuity.

BRING TRUST BACK TO EMAIL

Unlike other security vendors, we solve the entire email threat problem. Our unified, advanced email security helps you prevent, detect and respond to today's most advanced attacks.

This starts with the email gateway and extends to web, network and other incident response tools. We equip your team to do more, respond faster and act with confidence.

Protection against bulk mail and common email threats

We stop email threats and other unwanted messages in just about any language for any platform. This includes Office 365 and G Suite. Using multilingual analysis, our email classifiers divide incoming email into separate quarantines by type. This gives you granular control over a wide range of message types, including spam, phishing, impostor email, malware, bulk and adult content.

We also detect threats that do not involve malware, such as credential phishing and email fraud. We assess the reputation of the sender by analyzing hundreds of thousands of email attributes. These include the sender/recipient relationship, headers and content.

You can also authorize all legitimate senders and block fraudulent emails before they reach your users. Only we offer an email authentication solution that helps you fully deploy DMARC (Domain-based Message Authentication, Reporting & Conformance) faster and with less risk.

Stopping advanced threats

We effectively detect and block advanced threats—including ransomware—that target people through email. We detect known threats and new, never-before-seen attacks that use malicious attachments and URLs through our dynamic and static analysis techniques.

No one is better at stopping attack techniques such as polymorphic malware, weaponized documents and sandbox evasion. And with our comprehensive dashboard, you can better prioritize your response to threats, compare your organization with the broader threat landscape, and delve into threat intelligence.

PROTECT CLOUD ACCOUNTS

Our researchers have seen a sharp increase in account compromises—especially for Office 365—among colleges and universities. These compromised accounts are then used in everything from email fraud to internal phishing attacks. Many of these attacks can occur via phishing. But they also frequently occur through credential reuse, brute force (or credential stuffing) attacks, and credential-stealing malware.

To stop them from spreading, we can scan internal emails with the same detection techniques that we use on external email.

But threat detection addresses only part of your cloud challenge. To help you solve the entire problem, our cloud app security features for Office 365 and more look for signs of trouble. These include suspicious email forwarding rules, deletion of login alerts, abnormal device usage and other indicators of account takeover.

CONTROL SENSITIVE AND PERSONAL DATA LOSS

We give you far-reaching visibility outside of the inbox with advanced data loss protection (DLP). Our flexible, cloud-based platform spans email, cloud apps and on-premises file repositories without the complexity and costs of legacy tools.

We can help you:

- Easily manage sensitive content sent through email
- Automatically classify information according to your security policies and industry standards
- Transparently encrypt and quarantine your data

REMOVE MALICIOUS EMAILS FROM THE INBOX

We take the manual labor and guesswork out of incident response. This helps you resolve threats faster and more efficiently.

We can automatically remove already-delivered email from inboxes and give you an actionable view of threats. Our platform enriches alerts and automatically collects and compares forensic data. What's more, you can quarantine and contain users, hosts and malicious attachments—automatically or at the push of a button.

MAINTAIN EMAIL COMMUNICATION DURING A SERVER OUTAGE

We can ensure that emails, calendars and contacts are always available to users, even when your regular email service is down. Your users can continue to send and receive email with no IT intervention needed.

Our service is always on, hands off and works automatically. This ensures that an email outage does not disrupt learning, research and operations.

INTEGRATE WITH YOUR SECURITY ECOSYSTEM

Staying ahead of cyber attacks means providing different lines of defense. That’s why we’ve built integrated solutions with other leading providers to advance a common mission: to help our customers be more secure.

- **Palo Alto Networks:** You can now combine Proofpoint TAP with Palo Alto Networks WildFire in a matter of minutes, with a simple API key-based activation. With the integration of these solutions, you increase visibility and synchronized protection across all control points: in your network, endpoint, cloud, email and social media platforms.
- **Splunk:** The Proofpoint Email Protection TA add-on allows users to search and report on Proofpoint Email Protection logs. By normalizing the data produced by Email Protection to the Splunk Common Information Model (CIM), email data can be correlated with other data sources to detect threats and data exfiltration.

LEARN MORE

For more information visit **proofpoint.com**

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.

©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.