proofpoint

PROOFPOINT THREAT PROTECTION FOR MICROSOFT OFFICE 365

KEY BENEFITS

- Superior blocking of malware and malware-free threats
- Actionable visibility and insights
- Respond to threats faster
- Threat Operations Center security expertise
- Ensure email uptime

If your organization is looking to migrate to Microsoft Office 365, you might be wondering whether additional security is needed.

As Microsoft continues to invest in securing its infrastructure, today's threat actors are exploiting people as their favorite way to beat cybersecurity.

Email is the most reliable way to reach nearly every person in every organization around the world. That is why more than 90 percent of targeted attacks use email to compromise your network, steal credentials and assets.

Proofpoint Threat Protection for Office 365 safeguards users advanced threats and targeted attacks. It enables you with threat insights to identify these attacks, and helps your security teams orchestrate rapid response and containment. Email continuity provides assurance of email uptime. Our award- winning customer support reflects our commitment to your success.

SUPERIOR SECURITY

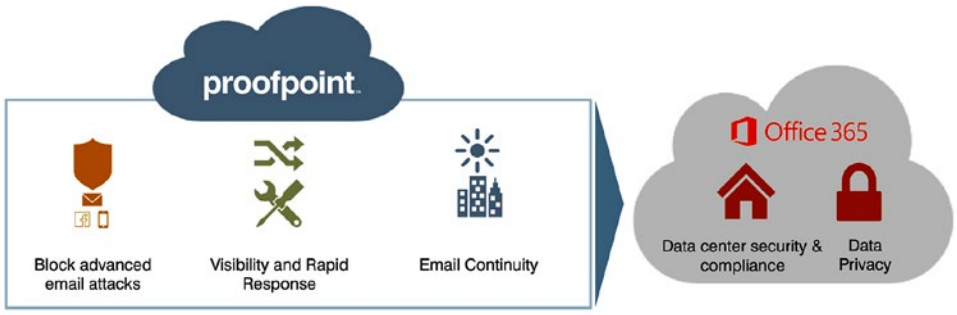
Proofpoint's threat intelligence spans email, network, mobile apps and social media. This next generation approach results in industry-leading email hygiene and bulk mail efficacy. It also detects new, never-beforeseen and attacks in an Office 365 email environment.

Legacy techniques reliant on host, URL and attachment reputation are no longer sufficient. That's why more is needed to combat credential phishing, business email compromise, ransomware, and more.

Proofpoint analyzes threats in several stages using multiple approaches to examine behavior, source code and protocol. Predictive analysis identifies and sandboxes suspicious URLs and attachments before users have an opportunity to click - an important step to avoid patient zero.

GAIN ACTIONABLE VISIBILITY AND INSIGHTS

Visibility is paramount to track down threats, improve cybersecurity posture, and support business objectives. As security becomes a board-level conversation, it is even more critical to provide the "who, what, when, where, how" of an incident. With visibility that spans malware and non-malware based attacks, knowing whether an attack was part of a broad attack campaign, targeted at your vertical or specifically at your organization, helps you prioritize actions.



Proofpoint Threat Protection for Office 365

Real-time visibility of critical forensic insights - which users clicked on which link from what device, DNS look ups, registry key changes, analyst curated IoCs and more - helps security organizations respond quickly to advanced threats. Shift your focus to how to respond, rather than determining what happened.

RESPOND TO THREATS FASTER

Auto-Purge saves cleanup costs
Save hours extracting email threats from Office 365 and Exchange mailboxes. This powerful layer of protection against emerging threats takes in real-time threat alerts for malicious URLs and attachments, and moves identified emails into a quarantine inaccessible by end users. Each action creates a task history showing the protective action that was taken. You define the rules – whether emails are extracted automatically or on-demand, if you want to retain the email for review or retain for a short period then auto-delete, and more.

Quickly assess and confirm compromise
While a target machine received a malicious email, how do you know whether that machine has been compromised? Automated endpoint forensic collection and compromise verification rapidly gives you the visibility to prioritize response efforts. Organizations can remediate only the fraction of machines that require it, gaining a scalable way to reduce risk and protect your brand.

Make your security investments smarter
An integrated approach is critical to building a sustainable security program. enables your security investments to work smarter, faster, and result in a stronger ROI. With Proofpoint, email events detected in Office 365 email can integrate real-time with your existing security SIEM to correlate email data with other data points across your network. Automated or orchestrated response actions via existing URL, network, or user access enforcement points can quickly cease outbound communications with command & control networks, move compromised users to deprecated permission groups, and more.

INTEGRATIONS:

Threat Insight Enrichment
- Palo Alto Networks
- Splunk

URL Enforcement
- Blue Coat
- Open DNS

Network Enforcement
- Cisco
- Check Point
- Fortinet
- Juniper
- Palo Alto Networks

User Access Enforcement
- Active Directory
- Cyberark
- Imperva

Threat experts committed to your success
Your success is paramount, and dedicated security expertise can be hard to come by. In addition to our award-winning global product support organization, the Threat Operations Center is a unique benefit to customers. This team is comprised of top threat research talent, staffed around-the clock. As an extension of your security team, they leverage sophisticated threat intelligence to provide context and insights to help you understand actor/campaign activities within your environment, and can help you prioritize which threats are important.

ENSURE EMAIL AVAILABILITY

In the event of any sort of outage, be it on Microsoft's side or an authentication issue on yours – email can be readily accessed natively in Outlook via a web portal. It enables IT to regain control with always-on secondary email service with a 30-day rolling inbox to eliminate single vendor dependency on uptime.

TIME TO LEARN MORE

Gain the security, visibility, rapid response and continuity capabilities to increase the success of your Office 365 initiative. Backed by our award-winning global support organization, Proofpoint has helped many customers be successful with a unified security experience before, during, and after the transition to Office 365. Learn more at, including how you can sign up for a threat assessment, at www.proofpoint.com/office365.