proofpoint

PROOFPOINT THREAT PROTECTION FOR MICROSOFT OFFICE 365

KEY BENEFITS

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

If your organisation 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 continue to reach victims through email to compromise your network, steal credentials and gain access to your assets.
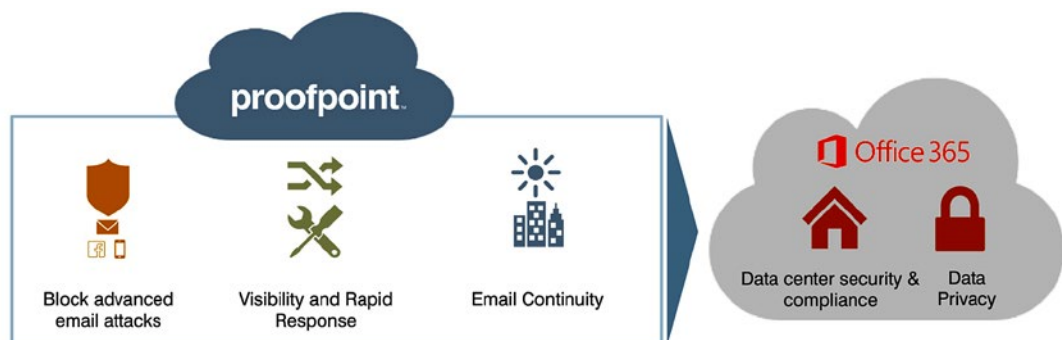
Proofpoint Threat Protection for Office 365 safeguards against advanced threats and targeted attacks against your Office 365 users, enables you with threat insights to identify these attacks, and helps your security teams orchestrate rapid response and containment. Further, you gain industry-leading hygiene efficacy, and assurances of email service availability, putting control back into IT hands. And 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. Our next generation approach not only delivers industry-leading email hygiene and bulk mail efficacy, it is designed to detect known and new, never-before-seen attacks in an Office 365 environment. These attacks may use non-malware based attacks using social engineering to target users with credential phish, impostor emails (i.e. business email compromise), or even use malicious attachment and URLs to drop malware on a device.

To detect threats as early as possible in the attack chain, legacy techniques reliant on host, URL and attachment

Proofpoint Threat Protection for Office 365

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

reputation is no longer sufficient. 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—beyond just standard Microsoft Office and Adobe PDF files— before users have an opportunity to click.

GAIN VISIBILITY AND INSIGHTS

Visibility is paramount to tracking down threats, improving cybersecurity posture, and supporting 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, and the context of an attack (i.e. was it part of a broad attack campaign, a vertical-specific campaign, or targeted specifically at your organization) to help you prioritize alerts and take action.

Critical forensic insights such as real-time visibility on which users clicked on which link from what device, DNS look ups, registry key changes, and more, helps security organizations respond quickly to advanced threats and prevent widespread compromise. This approach enables you to shift your focus to how to respond, rather than determining what happened.

RESPOND TO THREATS FASTER

Auto-Purge saves cleanup costs
How much time is spent extracting malicious emails from your user inboxes? With auto-purge, you can save hours per incident. It takes in real-time threat convictions and automatically, or on-demand, moves the identified messages containing the malicious content into a quarantine inaccessible by end users. Each action can also create a task history showing the protective action that was taken. You define the rules - such as whether you want to retain the email for review, retain for a short period then auto-delete, and more. Gain a powerful layer of protection against emerging threats and for users with audit-only or short delay requirements.

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. With Proofpoint Threat Protection for Office 365, you can integrate email events real-time with existing security investments such as a SIEM to correlate email data with other data points across your network. As threats are detected in email, you can drastically cut your time to protection with automation to URL enforcement points, network enforcement points, and user access enforcement points to prevent the machines from talking to Command & Control networks, or moving the users to a deprecated permission group, for example. This integrated ecosystem helps make all your other security investments work smarter, gain better ROI, increasing your speed to protection.

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, and rapid response 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.

proofpoint™   proofpoint.com