Microsoft

Office 365 Advanced Threat Protection

FUTURE IT TECHNOLOGIES

The Challenge

As hackers around the globe launch increasingly sophisticated attacks, organizations are seeking tools that provide additional protection. Microsoft is pleased to offer customers security capabilities in Microsoft Office 365 with Advanced Threat Protection (ATP), an email filtering service that provides stronger protection against specific types of advanced threats.

The Microsoft Approach

Office 365 ATP offers three core features to better secure your email:

1. Safe Attachments, which protects against unknown malware and viruses
2. Safe Links, which provides real-time, time-of-click protection against malicious URLs
3. Rich reporting and trace capabilities

Safe Attachments

Safe Attachments is designed to detect malicious attachments before anti-virus signatures are available, and to provide better zero-day protection to safeguard your messaging system. All messages and attachments without a known virus/malware signature are routed to a special hypervisor environment, where a behavioral analysis is performed using a variety of machine-learning and analysis techniques to detect malicious intent. Safe Attachments then detonates attachments that are common carriers of malicious content, such as Office documents, PDFs, executable (EXE) files, and Flash files. If no suspicious activity is detected, the attachment is released for delivery to the mailbox.

Safe Links

Safe Links is a feature that helps prevent users from going to malicious websites when they click them in email. Attackers sometimes try to hide malicious URLs within seemingly safe links, redirecting users to unsafe sites through a forwarding service after the message has been received. The ATP Safe Links feature proactively protects your users if they click such a link. That protection remains every time they click the link, so malicious links are dynamically blocked while good links remain accessible.

Dynamic delivery of Safe Attachments

Dynamic Delivery eliminates email delays by sending the body of the email with a placeholder attachment, while the actual, suspicious attachment undergoes the Safe Attachments scan. Recipients can then read and respond to the message, having been notified that the original attachment is being analyzed. If the attachment is cleared, it replaces the placeholder; if not, the admin can filter out the unwanted and potentially malicious attachment.

URL Detonation

URL Detonation provides deeper protection against malicious URLs. Not only does ATP check a list of malicious URLs when a user clicks on a link, but Office 365 ATP will also perform real-time behavioral malware analysis in a sandbox environment against malicious attachments at destination URLs. For example, if an email includes a link to a Word document on a web server, the document is downloaded into our sandbox environment and detonated as if it were an attachment.

Rich reporting

Safe Attachments has two traffic reports which show aggregated data for a tenant by disposition (blocked, replaced etc.) and the file types. The report also shows detailed data (i.e. date, sender, recipient, ID, subject). Safe Links has advanced reporting features that make it easy to determine who has clicked through a malicious link to support faster remediation. The rich reporting URL trace capabilities provide critical insights into who is getting targeted in the organization and the category of attacks being faced. Reporting and message tracing enable investigation of messages that have been blocked due to unknown viruses or malware, while the URL trace capability enables tracking of individual malicious links in the messages that have been clicked. Addtionally, ATP reporting will expand to provide analysis on why ATP flagged an email as a threat, identifiying threats caught by ATP which would have been missed without ATP (identifiying advanced threats specificially), and granular details on scan times for emails with attachments. ATP reporting, will ultimately enable proactive email protection.

To learn more, visit
https://products.office.com/en-us/exchange/online-email-threat-protection

To add advanced threat protection to your subscription or learn more, contact Future IT at 087 077 0808

FUTURE IT TECHNOLOGIES

Microsoft