Microsoft Defender for Office 365 Delivers Powerful, Integrated Email Security

The modern workplace continues to depend on email for essential business communication. However, this versatile tool also exposes organizations to dangerous cyber threats. Microsoft Defender for Office 365 includes the tools necessary to prevent, detect, and respond to attacks on email and collaboration tools.

Utilizing AI and machine learning, Defender for Office 365 analyzes billions of signals and detects even highly sophisticated cyber threats. It also integrates with other Microsoft security solutions, including Microsoft Defender XDR and Microsoft Sentinel. This unified security operations platform provides protection across the organization's digital landscape.

Prevent and Detect Attacks

More than 90 percent of cyber attacks begin with an email. Thus, stopping attacks before they reach user inboxes or the network delivers the easiest and most effective security. Using multiple layers of filtering, Defender for Office 365 prevents a wide range of attacks.

Defender first looks at the source of the email to determine the authenticity of the individual, brand, and domain sending the message. This guards against spoofing and BEC attacks. Machine learning models build an understanding of message patterns, allowing the system to identify anomalies and impersonation attempts.

Defender also analyzes the content of the email. Using Safe Attachments and Safe Links, it tests attachments and links in a secure cloud environment, blocking content deemed unsafe. These capabilities even detect zero-day malicious attachments.

Sophisticated attackers set malicious links to weaponize only after they have passed initial security filters. Consequently, Defender continues to scan emails for several days after delivery. And it extends protection against malware across Office applications, Microsoft Teams, SharePoint, and OneDrive.

Investigate Threats and Track Attacks

In addition to preventing and detecting attacks, Defender for Office 365 assists security teams with prioritizing and investigating possible threats. Detailed, real-time reports aid in threat investigation. Defender also provides proactive recommendations on additional protections that will help strengthen security.

The Microsoft 365 Defender portal provides a centralized view of threats flagged by the system and by users. It also delivers insights into actions taken, including quarantined messages and detonation of malicious links. The Campaign Views feature uses AI to build a picture of where attacks originated, what actions were taken, and what users were affected.

Full-featured Response and Remediation

Microsoft Defender for Office 365 includes automated investigation and response (AIR). Using predefined playbooks, the system will automatically address common scenarios such as malware and phishing attempts.

For instance, Zero-hour Auto-Purge (ZAP) works retroactively to identify and neutralize malicious messages even after delivery. Depending on policy configuration, it will move dangerous messages to quarantine or junk, delete them, or perform more advanced actions.

Automated analysis shows the triggering event, as well as all users, emails, and endpoints affected. It also provides a summary of both the threats detected and the remediation actions taken.

Arm Users with Attack Simulation Training

Companies with Microsoft Defender for Office 365 Plan 2 gain access to attack simulation training. By integrating these simulations within the day-to-day workload, Defender empowers users with the understanding they need. Users learn to identify possible attacks and take appropriate action.

This powerful security awareness training uses real phishing attempts taken from the customer's system. Administrators can target specific users and groups. And a diverse catalog of additional training options allows them to present training for a variety of languages and learning styles.

Accessing and Implementing Microsoft Defender for Office 365

Microsoft customers with Microsoft 365 Business Premium have access to Microsoft Defender for Office 365 Plan 1. This provides protection against phishing, malware, spam, and BEC attacks. It also includes additional security features such as device management, identity protection, and cloud app security.

Customers with Microsoft 365 E5 or E5 Security plans gain access to Microsoft Defender for Office 365 Plan 2. In addition to all the features provided with Plan 1, Plan 2 includes Safe Attachments, Safe Links, anti-phishing policies, attack simulator, threat investigation and response tools, and more.

Organizations with Defender for Office 365 need to configure it to their needs and preferences. This includes specifying polices for alerts, as well as for the actions to take in response to threats. To optimize their use of Defender, many customers find it beneficial to work with a Microsoft partner such as Messaging Architects.