Microsoft Security

Investigation & Hunting
in Microsoft Defender for Office 365

Get better visibility into the threat landscape. Microsoft Defender for Office 365 offers powerful experiences built to help identify, prioritize, and investigate threats, with advanced hunting capabilities to track attacks across Office 365. Defender for Office 365 is also a key component of Microsoft's XDR solution, Microsoft 365 Defender. With Microsoft 365 Defender, your security teams can detect threats and automate response across domains, like email, endpoint, identity, and cloud apps.

Detailed reporting

Our real-time reports in Microsoft Defender for Office 365 allow you to investigate email and collaboration threats within your organization and understand how they were handled by Office 365. In addition, Defender for Office 365 will proactively surface insights and recommendations on what additional policies and protections you need to consider within your environment. In the Microsoft 365 Defender portal, you can investigate threats, review quarantined messages, view detonations, and get details on the nature of threats and why they were detected. This includes messages flagged by users as potential threats.

User submissions

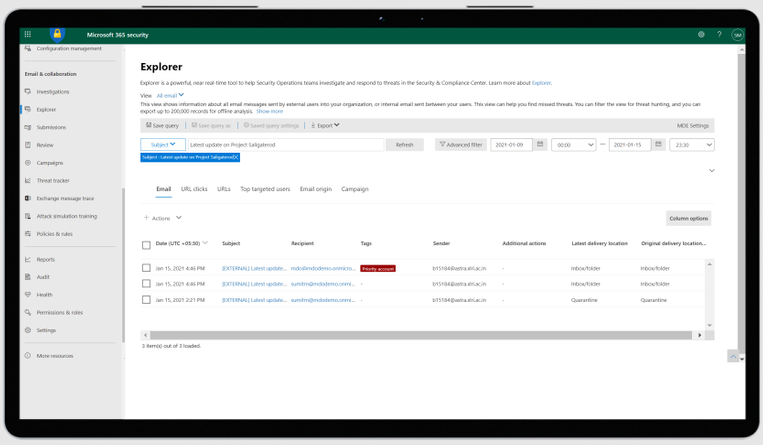
Of course, while protections are automated in the background, we also encourage email recipients to be vigilant in identifying messages that appear suspicious. By enabling the report message add-in capability, users can self-report suspect emails to receive validation by Microsoft and your security teams. Administrators can create admin submissions, which triggers an investigation by a human grader at Microsoft.

Quarantine

If messages were misclassified as spam, bulk, or a phish email, users can view, release, and delete messages from the quarantine folder. The dedicated quarantine policy gives admins control over how users interact with quarantined messages.

Threat Explorer

Threat Explorer helps you dive deep into the threat landscape. Malicious emails can be quickly identified with options to filter on sender or recipient, or more advanced metadata like detection technology, system overrides, or inbound connector. Filtering on system overrides helps you to see all the emails that were marked as malicious by Office 365 but delivered to users because of an override such as an allowed domain policy or safe senders list. You can then investigate these emails further and take actions such as purging a malicious email campaign entirely from all mailboxes in your organization at once. Investigation into an incident can also be separately delegated to your security investigation team, leaving it to your security admins to take the final action.



360-degree view

The email entity page in Defender for Office 365 provides a comprehensive view of critical details for investigation. It provides a 360-degree view of an email, helping security analysts investigate more efficiently.

Advanced hunting

With Microsoft 365 Defender, you can create custom queries to inspect events in your environment using Advanced Hunting. This powerful tool enables security teams to create custom detection rules that run automatically to detect and respond to threats. These queries can be saved and shared, simplifying the hunting experience across endpoint, identity, email, and collaboration.

Protecting priority accounts

Priority Account Protection in Defender for Office 365 helps security teams prioritize focus on critical individuals within the organization, offer them differentiated protection and thwart costly breaches in the process. Highly visible individuals aren't always the target of attacks. Often times, the most targeted users are those with access to critical tools and information. By focusing attention on these priority accounts, security teams can find early warning signals and protect the organization better. Priority Account Protection helps by tracking priority accounts throughout the lifecycle of an attack, drawing attention to those who matter most.

Protect all of Office 365 against advanced threats like business email compromise and credential phishing. Automatically investigate and remediate attacks.

For more information, visit:

aka.ms/DefenderO365 >>