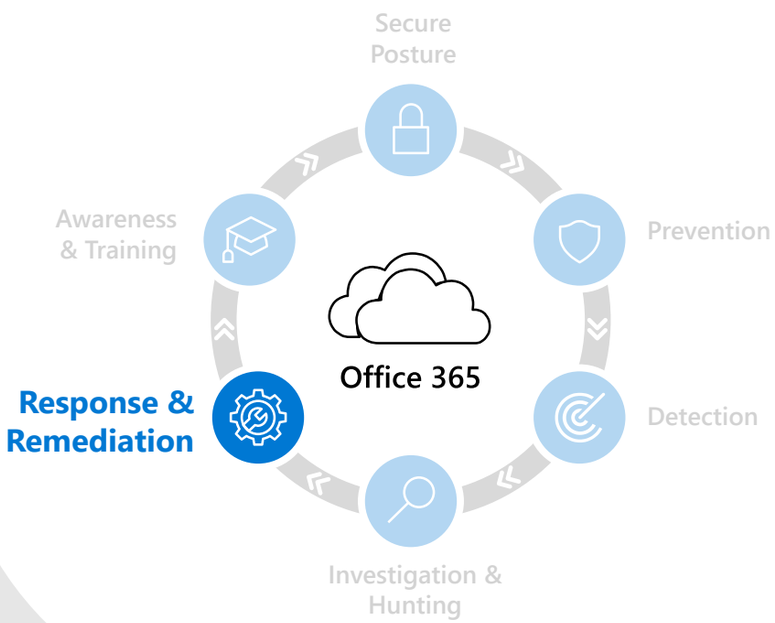
Microsoft Security

Response & Remediation
in Microsoft Defender for Office 365



When threats are detected, time is of the essence. Get extensive incident response and automation capabilities that amplify your security team's effectiveness and efficiency. Integration with Microsoft 365 Defender helps you stop attacks with automated, cross domain security.

Guided hunting with inline actions

When Defender for Office 365 identifies a threat in your organization, we make it easy for you to take a variety of actions on the message, like moving or deleting the message, or automatically triggering an investigation.

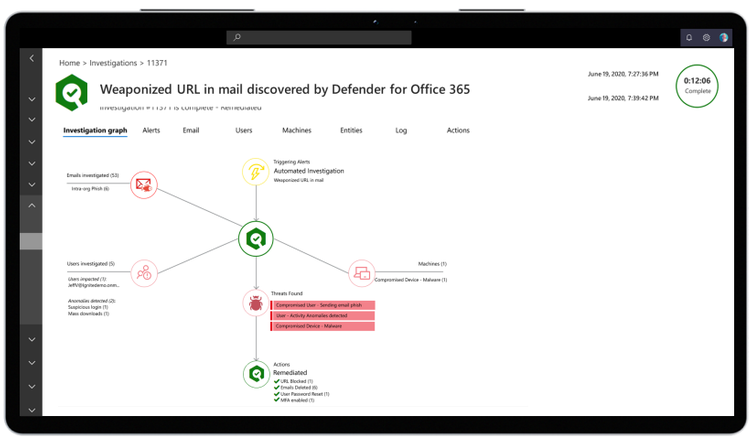
Integrate threat data for rapid response

Defender for Office 365 is 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.

Save time with automation

Automated investigation & response (AIR) in Microsoft Defender for Office 365 provides playbooks to automatically investigate threats. Here, the breadth of data backing Microsoft Security is a powerful benefit. We've created predefined playbooks to automatically investigate many common scenarios, like compromised user detection, malware detected post-delivery, and user-reported phish.

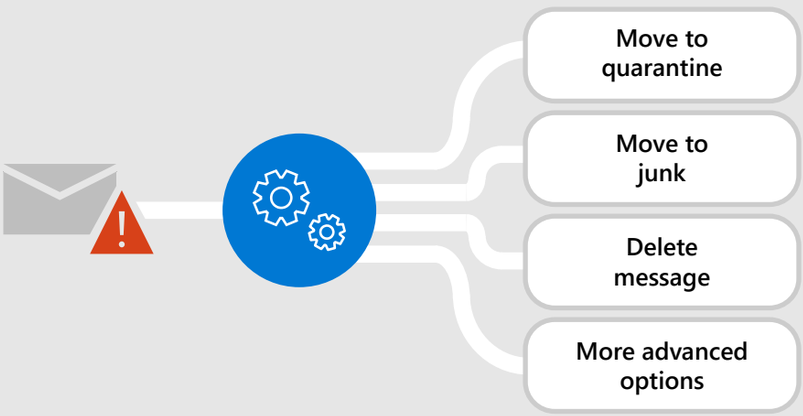
The investigation graph is a powerful visual representation of the security playbook that maps out the results of our automated analysis. You can see the event that triggered the investigation, and all the emails, users, and endpoints involved in this attack; and under each entity, you'll see what was discovered. Towards the bottom of the investigation graph is an overall summary of the threats found and the remediation actions taken to address each threat. The investigation graph is a great tool that gives admins a quick, detailed overview of any investigation in the environment.



Zero-Hour Auto-Purge

Zero-Hour Auto-Purge or ZAP retroactively detects and neutralizes malicious phishing, spam, or malware messages that have already been delivered. ZAP can take a variety of actions on a message, like moving it to quarantine or junk, deleting the message, or more advanced actions like adding an X-header or modifying the subject line.

When configuring policies in Defender for Office 365, you can specify the action taken on different types of messages when they are identified as malicious post-delivery.



ZAP is built-in to Office 365 and applies to both external and internal emails. ZAP can quickly act on all instances of an email without relying on clumsy methods like journal rules or anything risky like delegating full access to an external party.

See the bigger picture

Incidents correlate alerts and investigations to reduce SecOps cases. By looking at data across the entire service, we've seen an 80%[1] decrease in the number of cases customers manage when leveraging incidents compared to managing investigations themselves in Defender for Office 365. Security teams can assign incidents to individual analysts, helping teams manage the lifecycle of an incident. This unified investigation view delivers consistent experience for email, endpoint, and identity investigations.

Centralized action queue

The centralized action queue in Microsoft 365 Defender helps you view actions and history across your Defender workloads. The pending queue helps prioritize actions that require approval, and lets you approve them in bulk. The history tab allows you to review actions that have been taken and reverse them if the action taken wasn't quite right.

Built with extensibility in mind

Microsoft 365 Defender and Microsoft Defender for Office 365 offer a variety of APIs that provide programmatic access to data from your environment and help you integrate our industry-leading tools with your existing solutions.

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 >>

[1] Source: Microsoft