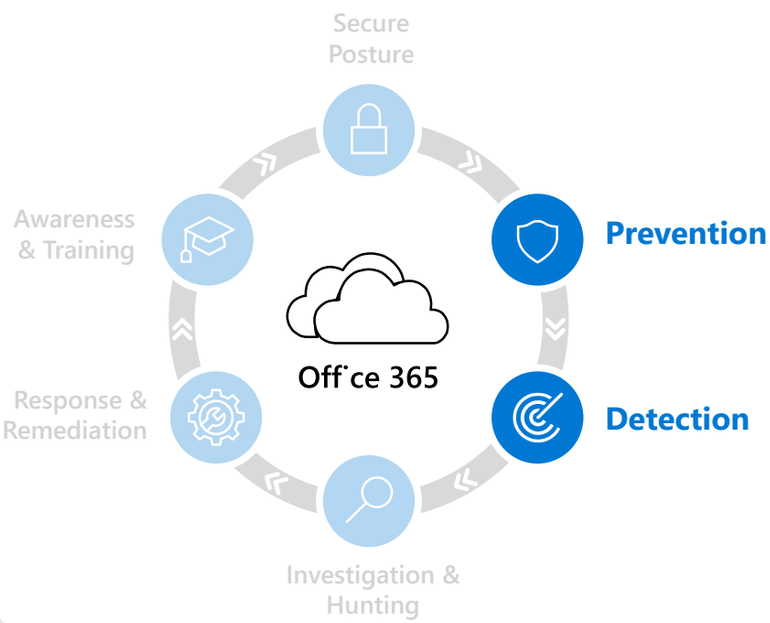
Microsoft Security

Prevention & Detection

in Microsoft Defender for Office 365



Stopping attacks before they happen is the easiest way to stay secure. Microsoft Defender for Office 365 uses industry-leading AI to detect malicious and suspicious content and correlate attack patterns to identify campaigns specifically designed to evade protection. Our robust filtering stack prevents a wide variety of volume-based and targeted attacks including business email compromise, credential phishing, ransomware, and advanced malware.

Multi-layered protection stack

Edge protection

- Network throttling
- IP reputation/ throttling
- Domain reputation
- Directory-based edge filtering
- Backscatter detection
- Enhanced filtering for on-prem routing

Sender intelligence

- Account compromise detection
- DMARC DKIM, SPF, ARC
- Intra-org spoof intelligence
- Cross-domain spoof intelligence
- Bulk filtering
- Mailbox intelligence
- Mailbox intelligence impersonation
- User impersonation
- Domain impersonation

Content filtering

- Transport custom rules
- AV engines
- Type blocking
- Attachment reputation blocking
- Heuristic clustering
- ML models
- Tenant allow/ block lists
- URL reputation blocking
- Content heuristics
- Safe attachments
- Linked content detonation
- URL detonation

Post-delivery protection

- Safe links
- Phish zero-hour auto-purge
- Malware zero-hour auto-purge
- Spam zero-hour auto-purge
- Campaigns
- End-user reporting
- Office clients
- OneDrive/ SharePoint
- URL detonation

Layered defense-in-depth approach

Defender for Office 365 catches threats before they disrupt your organization by applying a multi-layered defense in-depth approach that analyzes and protects against threats from the point at which an email is received by Office 365 to when it is delivered.

This starts by identifying:

1

Where the email is coming from by understanding the source

- Before an email is delivered to an inbox, around 25% of all malicious messages received are blocked immediately at the edge
- At the same time, machine learning models running on the edge determine email traffic patterns for your domain and, when necessary, block anomalous email traffic

2

Who the sender is and if the person, brand, and domain are authentic

- We check that the sender really is who they appear to be by authenticating the source to prevent against spoofing or Business Email Compromise attacks
- Internal emails are subjected to the same protection stack as external emails
- Emails sent between domains owned by your organization are checked by our anti-spoof technology to validate the message truly originated in your organization
- For external domains, our spoof intelligence checks to see if the domain has been set up according to SPF, DKIM and DMAC standards. If not, it will observe and learn message sending patterns from the domain to identify when a message has been spoofed.
- To protect against impersonation of your high-profile users, mailbox intelligence applies a machine learning model to form a contact graph of whom they are normally in contact with, deciphering anomalous and good behavior to detect impersonation attempts of trusted individuals in your organization

3

What's inside the email that could be compromising

- We utilize several standard anti-virus and anti-malware engines, combined with our Safe Attachment and Safe Links capabilities, to detect malicious content
- Attachments or links in the email are opened inside a sandbox environment where the content is analyzed by our machine learning models that check for malicious signals and apply deep link inspection, allowing for zero-day malicious attachments and links to be detected

4

What post-delivery protections need to be put in place once the email is delivered to the recipient

- Sophisticated attackers will plan to ensure links pass through the first round of security filters by making the links benign, only to weaponize them after the message is delivered, altering the destination of the links to a malicious site
- With Safe Links, we can protect users at the time of click by checking the link for reputation and triggering detonation if necessary. Safe Links protection extends to messages sent internally as well.
- The service continues to scan email content for multiple days, leveraging new intelligence to move newly discovered malware or phish, by design, to quarantine through a capability called zero-hour auto purge (ZAP)

Personalized protection

Mailbox Intelligence in Defender for Office 365 applies machine learning models to form a contact graph for each user that tracks who they are normally in contact with, deciphering anomalous and good behavior to detect impersonation attempts of individuals in your organization.

Unique insights informed by trillions of signals

470 billion
emails analyzed per month

2 million
distinct URL-based payloads blocked monthly

40 million
impersonation/ spoofing emails blocked monthly

100 million
phishing emails containing malicious URLs blocked monthly

Thousands
of compromised account activities blocked monthly

Source: Microsoft

Protect all of Office 365

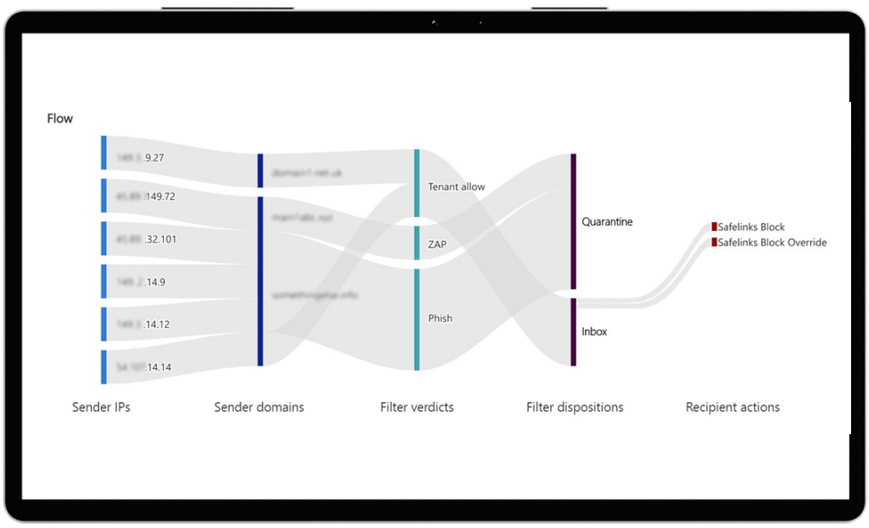
While email remains the primary attack vector, it is no longer the only way individuals collaborate at work. Beyond email, it's important to ensure protections extend to malware infected content and suspicious links across the digital estate. Defender for Office 365 uniquely extends protections beyond email to SharePoint, OneDrive, Office applications and Microsoft Teams. If malicious files or links are uploaded or shared, our protection layers will detect it, block it, and contain the threat by preventing the file from being opened or shared in the future.

Detect compromised user accounts

Attackers look to compromise user accounts and gain access to the organization, establish persistence, and eventually execute an attack. Compromised accounts typically exhibit atypical behavior, and spotting this behavior early is key to stopping attackers before they can cause real damage. Defender for Office 365 can detect anomalies in email patterns and collaboration activity within Office 365, alert your security teams, and automatically limit the activities of these accounts.

See the bigger picture

We use our signal strength and our industry-leading AI to correlate data across Office 365 and detect attacks as they happen in real time.



Today, attackers can easily morph their attacks to avoid conventional security products. What may appear to your security team as hundreds of separate malicious messages are likely coordinated campaigns carefully designed to evade detection. Defender for Office 365 creates Campaign Views that use AI to stitch together these attacks, showing you where the attacks originated, how they were handled by our service, and whether your users interacted with them.

Detailed alerts

Defender for Office 365 lets you build alert policies to notify your security teams when actions are performed by users or suspicious activities are spotted. A variety of default alert policies help you get started, by notifying you of events like detection of a potentially malicious URL click, malware campaigns detected after delivery, and suspicious email forwarding activity.

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 >>