Microsoft Security

Microsoft Defender for Office 365

Securing an organization has never been simple. Over the past few years we've seen significant changes in the threat landscape that have had a major impact on organizations of every size in every sector. The frequency and sophistication of cyber events have increased dramatically, and with more organizations pivoting to embrace hybrid work, we're living through unprecedented growth of digital interactions.

Email is essential

Email is still a key part of any organization. Over the past 50 years, email has transformed the way we communicate and become a critical workload for businesses. As email has proliferated across the globe, so has its appeal to cybercriminals.

Over ninety percent of cyberattacks start with email.[1]

When breaches occur, it takes an average of 280 days to identify and contain them.[2]

The financial impact of email-related attacks is also substantial. Since 2016, the cost of business email compromise (BEC) attacks has been more than $26B USD.[3]

The cost of BEC attacks in 2020 alone was $1.8B USD. And each year, time wasted responding to erroneous alerts costs organizations an average of $1.37M USD.[4]

[1] Verizon 2019 Data Breach Investigations Report
[2] IBM Cost of a Data Breach Report 2020
[3] US Federal Bureau of Investigation, April 2019
[4] "The Cost of Insecure Endpoints" Ponemon Institute© Research Report

Collaboration tools are becoming fundamental

Over the last decade businesses have adapted to collaborate more using a variety of cloud-based tools. The shift to hybrid work has only accelerated that journey for many organizations, leading to increased adoption of platforms that facilitate online meetings, document co-authoring, and persistent chat. These new collaboration tools lead to increased productivity, but also introduce new ways for attackers to take advantage of users and their data. Today's organizations need security capabilities that go beyond email to protect users in the tools they use every day.

On the following pages you'll learn how Microsoft Defender for Office 365 natively protects all of Office 365 against advanced attacks. The service leverages industry-leading intelligence fueled by trillions of signals to continuously evolve to prevent emerging threats, like phishing and impersonation attacks. Effective threat protection requires a comprehensive approach, and Defender for Office 365 supports organizations throughout the lifecycle of an attack. By combining prevention and detection capabilities with rich reporting and playbooks for automated investigation and response, Defender for Office 365 helps protect against attacks across the kill chain. Beyond protection, our attack simulation and training for end users, and secure posture guidance for administrators round out our holistic approach which helps simplify administration, leverages automation to increase efficiency, and improves secure posture through insights and awareness.

Prevention & Detection

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.

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.

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.

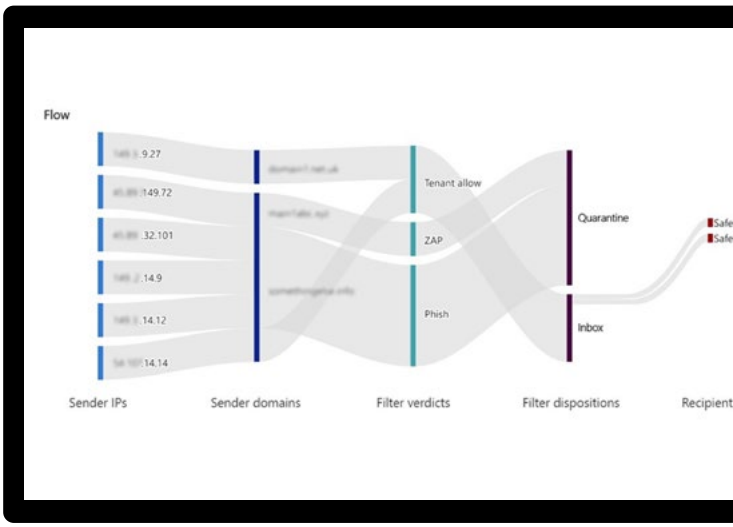
See the bigger picture

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.



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

Investigation & Hunting

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

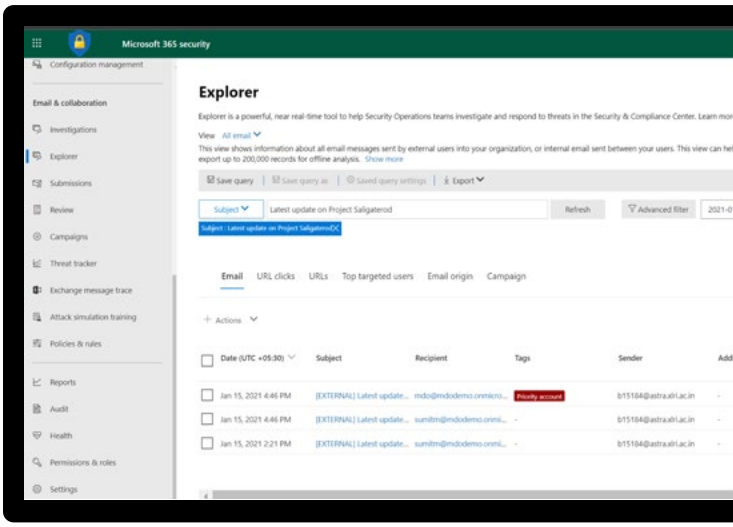
Our real-time reports in Microsoft Defender for Office 365 allow you to investigate email and collaboration threats within your organization and understand how they were handled by Office 365. In addition, Defender for Office 365 will proactively surface insights and recommendations on what additional 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 action 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

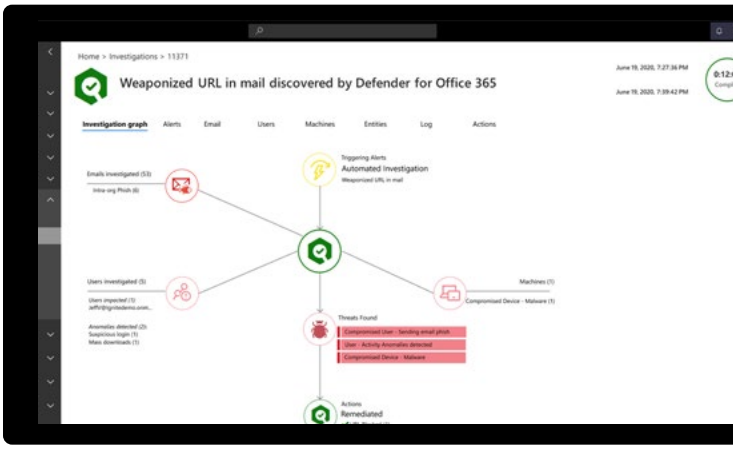
The email entity page in Defender for Office 365 provides a comprehensive view of critical details for investigation. It provides a 360-degree view of an email, helping security analysts investigate more efficiently.

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.

Response & Remediation

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.

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 email, 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.

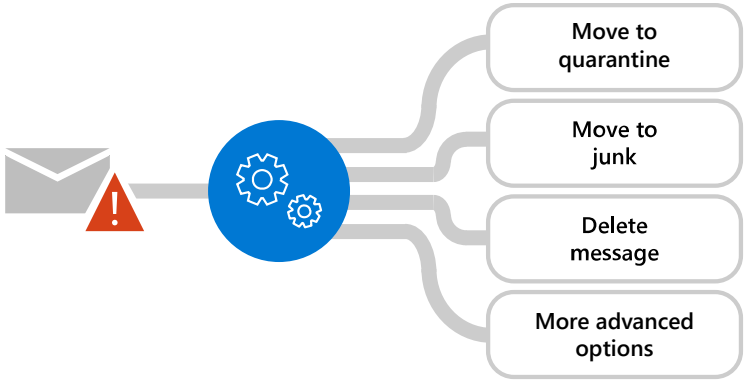
Integrate threat data for rapid response
Defender for Office 365 is a key component of Microsoft's XDR solution, Microsoft 365 Defender. With Microsoft 365 Defender, your security teams can detect threats and automate response across domains, like email, endpoint, identity, and cloud apps.

Zero-Hour Auto-Purge 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.

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.



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%[6] 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.

[6] Microsoft

Built with extensibility in mind

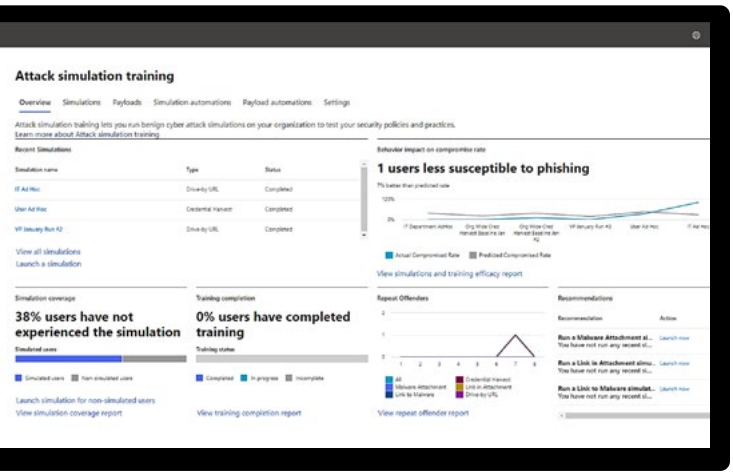
Microsoft 365 Defender and Microsoft Defender for Office 365 offer a variety of APIs that provide programmatic access to data from your environment and help you integrate our industry-leading tools with your existing solutions.

Awareness & Training

Your people are your perimeter. Attack Simulation Training provides rich simulation and training capabilities that help users spot threats, and Defender for Office 365 offers integrated experiences within client applications that build awareness to key indicators of suspicious activity.

Simulate real world attacks

While today's technology stops a majority of phish attacks before they reach your user's inbox, you also need to arm and empower your users to identify and take action against attacks at the first line of defense. In talking to our customers, we understand that designing and deploying an effective security training program at every level is challenging.



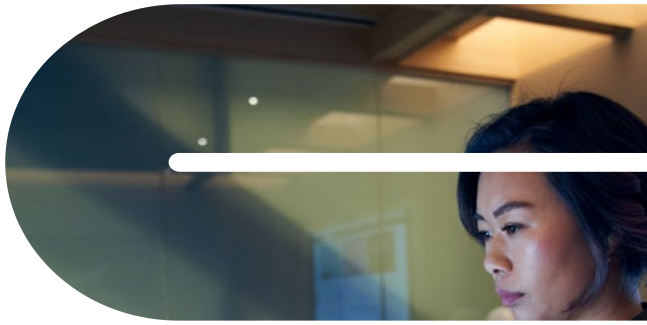
That's why we offer Attack Simulation Training in Microsoft Defender for Office 365, which focuses on addressing our customers concerns about tackling the complexity of designing a security awareness training program that is effective and easy to manage.

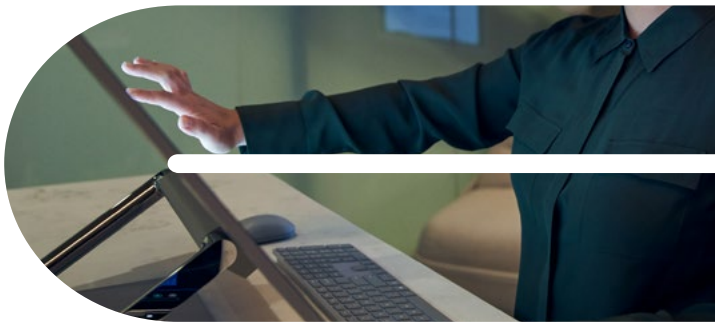
We automate the process of harvesting phish from your tenant based on conditions you set, which allows you to use these real phish attempts in a simulation to accurately test points of vulnerability within your organization. Simulation creation, scheduling, launch, and reporting are all automated, and the ability to target users and groups is integrated with Azure Active Directory.

Harden your human firewall with targeted trainings

We've included content by Terranova Security to deliver the right training to the right user at the right time. Terranova Security's training catalog caters to different learning styles, is available in a variety of languages, and meets our highest accessibility standards ensuring that every employee in your organization can benefit.

We've also made it easy to track your organization's progress against a predicted compromise rate per simulation. The predicted compromise rate reflects Microsoft's intelligence about that simulation at a global level as well as your organizations' previous simulation performance. Gain visibility over training completion and simulation coverage for your entire organization.

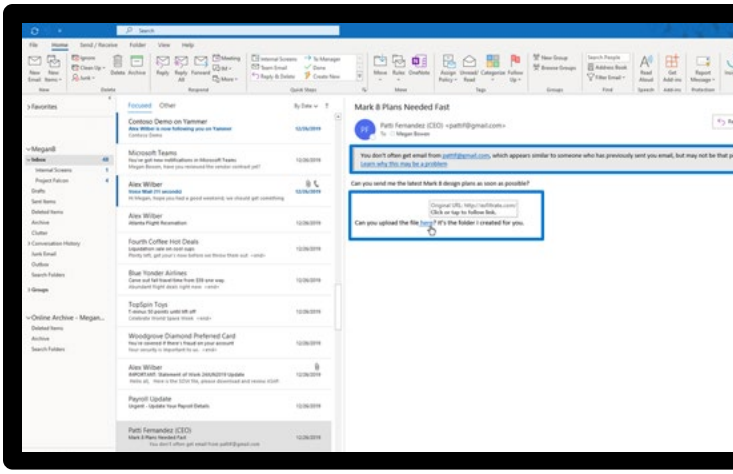




Defender for Office 365 is integrated with the apps your users use every day, which gives Microsoft the unique ability to customize security tools and workflows to seamlessly integrate with apps like Outlook, Word, OneDrive, and Microsoft Teams.

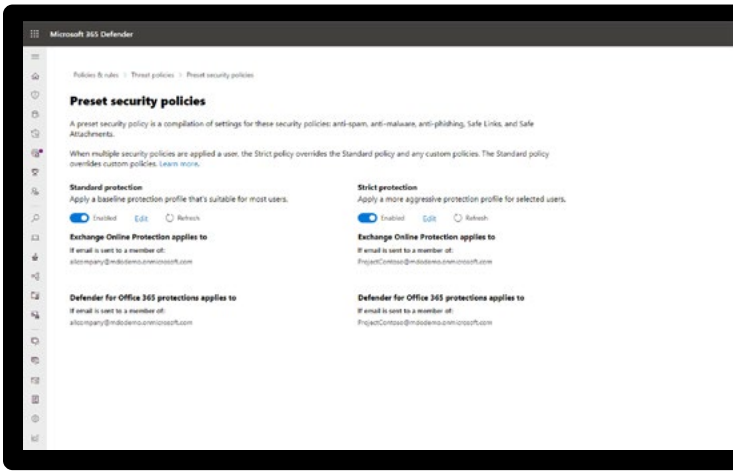
Simple, native experiences
Outside of simulation and training, Defender for Office 365 builds user awareness through in-product guidance. In email, for example, you'll notice that safety tips callout that this isn't the email address that Patti usually uses to send you messages. In the body of the email, we see that Patti is urgently looking for access to a confidential document—a key warning sign of suspicious activity.

Even though Safe Links wraps URLs to ensure they're not malicious at the time-of-click, users see the original URL, and can make a determination about the legitimacy of it without having to click.



Secure Posture

Staying secure should be easy. Take advantage of simplified configuration guidance and tools that help you identify coverage gaps to get and stay secure. Trust that Microsoft has your security in mind and is working to keep your users safe.

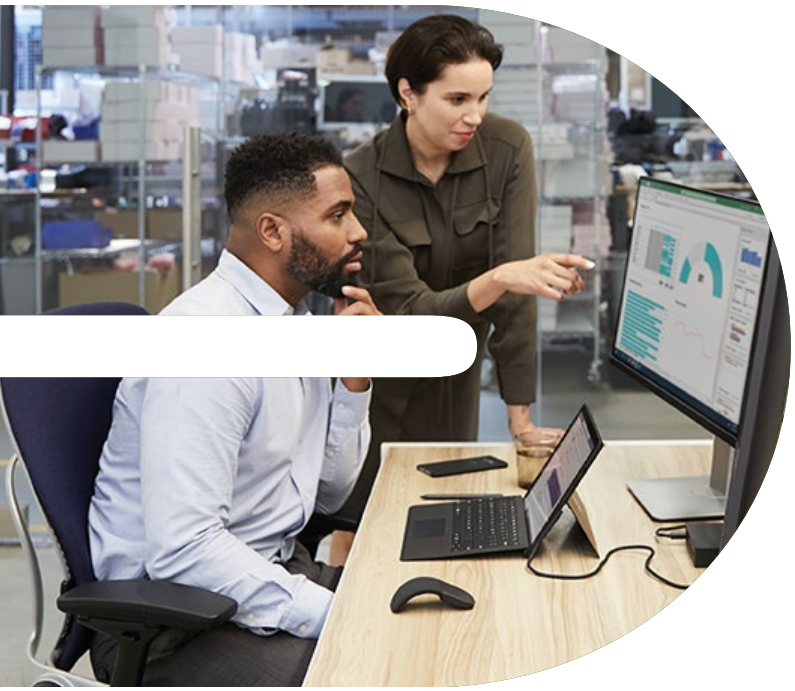


Simplified configuration
Get started on the right foot. Defender for Office 365 provides preset security policies, allowing you to choose to easily configure your environment with our recommended settings. We offer both a standard and a strict version of these recommendations and make it easy to deploy different presets to different groups.

Identifying policy drift
Just as technology has evolved, so have attackers. Over time, the needs of your organization will shift, and it's important that your configuration stays up to date to keep your users secure. Configuration analyzer lets you compare your configuration to our recommended settings, provides policy guidance whenever you need it, and surfaces legacy configurations you might have overlooked.

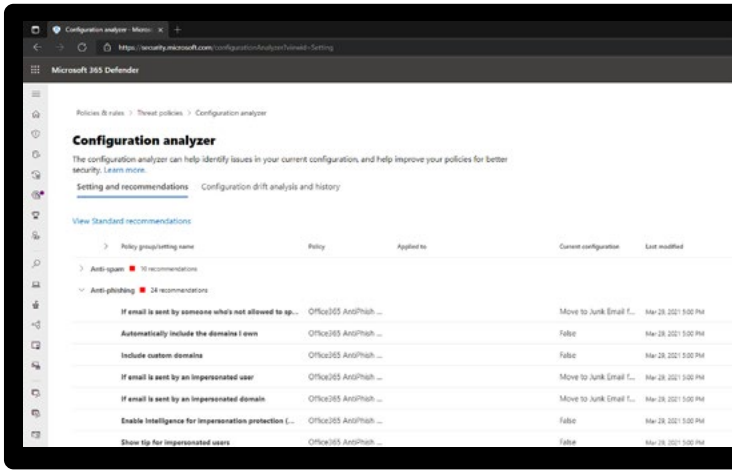
Override reports and alerts

Overrides are user level configurations that instruct Office 365 to deliver mail even when the system has determined that the message is suspicious or contains malicious content. While we want to enable organizations to customize their Office 365 environment to meet their needs, we also want to make sure that malicious content like malware or phish doesn't land in the inbox of users. You can find a report of message overrides in the threat protection status report, helping your security teams understand why threats may have been delivered to users despite your best efforts to eliminate them. You can also be automatically notified when an override causes a malicious email to be delivered to your users with a variety of default alert policies.



Secure by default

Transport rules are a double-edged sword. While they give admins the ability to ensure delivery of legitimate mail, they can also inadvertently allow delivery of malicious mail. Advanced Delivery in Microsoft Defender for Office 365 ensures that things you want delivered—like phishing simulations or security operations mailboxes—can be delivered, and things you don't—like high confidence phish—aren't delivered.



Protection behind the scenes

We're always looking for ways that we can help make our customers more secure across the entirety of Office 365. Our goal is to offer customers an easy way to be "secure by default", and we're constantly adjusting the way Defender for Office 365 protects your environment. This includes things like adding stricter verdicts for high confidence phish, and implementing automated control of email forwarding rules to limit data exfiltration.

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