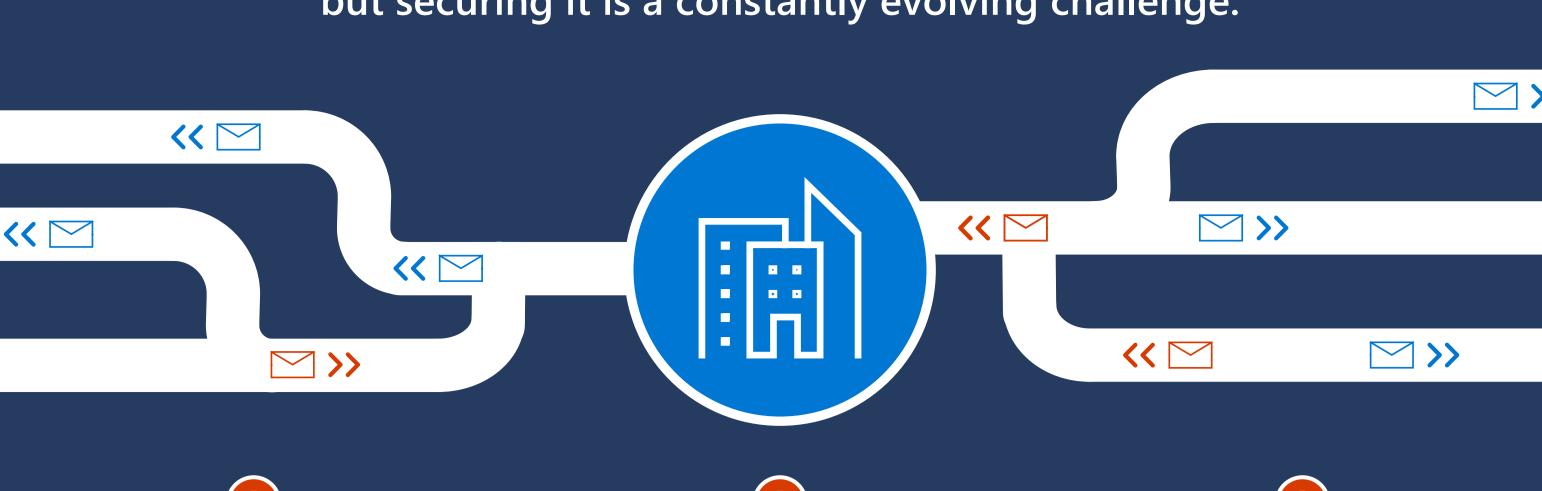
## How to secure email and collaboration with Microsoft Defender for Office 365

Email remains the primary method of communication for most organizations... but securing it is a constantly evolving challenge.



Email is the top entry

point for ransomware. Over 90% of cyber attacks start with

email. Defending email is critical to stopping threats throughout your entire organization.



continues to evolve Advanced attacks like business email

compromise are difficult to spot, requiring an intelligent solution that stays one step ahead.



in popularity Hybrid work has given rise to new methods of communication, all of which

represent new threat vectors to defend.



posture management, threat protection, response, and education.

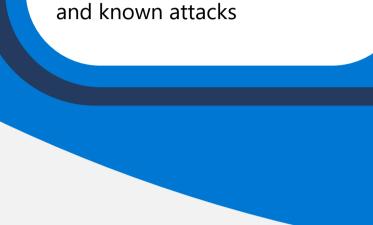
Microsoft Defender for Office 365 provides a comprehensive solution that offers



called Exchange Online Protection (EOP). But with Microsoft Defender for Office 365, you can extend that protection with advanced detection, investigation, and response.

**Every Office 365 subscription comes** 

with basic email security built-in,



**Exchange Online Protection** 

Prevents broad volume-based

Protects email and collaboration

from targeted malware, phish, and

business email compromise attacks.

and XDR integration.

**Defender for Office 365 Plan 2** 

Post breach investigation, huntinga

and response. Inlcudes automation,

attack simulation training,



### All the benefits of a leading security Unparalleled cloud scale, AI based on Protection across all your vendor deeply integrated Microsoft's trillions of security signals, Office 365 workloads, from and automation built into every phase

Industry-leading AI & automation

### with Office 365, so you can boost productivity, simplify administration,

Deeply integrated protection

and lower cost of ownership.

## of the security lifecycle.



### advanced threat protection to posture to response

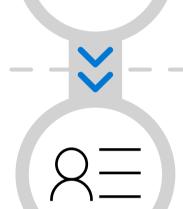
Comprehensive security

and remediation.

Blocks known threats at the edge, like DDoS attacks,

known-bad IP addresses and senders, and other

immediate signs of bad actors.



Layer 2 Sender

Intelligence

**Edge Protection** 

Layer 1

Analyzes the sender of the email, using AI & ML to profile typical user behavior and detect suspicious anomalies.

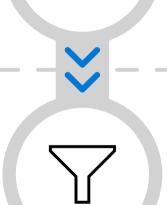
113 million threats eliminated

monthly

1.5 billion

threats eliminated

monthly



Layer 3 Content Filtering

attachments, is analyzed. Microsoft Defender for Office 365 uses the power of the full Microsoft Defender family to scan and analyze email content.

In this phase, the content of the email, including links and

216 million threats eliminated

monthly



**Post-Delivery Protection** 

Layer 4

auto purge (ZAP) can remove emails that are weaponized after they have been delivered, and Safe Links and Safe Attachments continue to protect users across the Office 365 suite.

Protection doesn't end after email hits the inbox. Zero-hour

29 million

threats eliminated

monthly

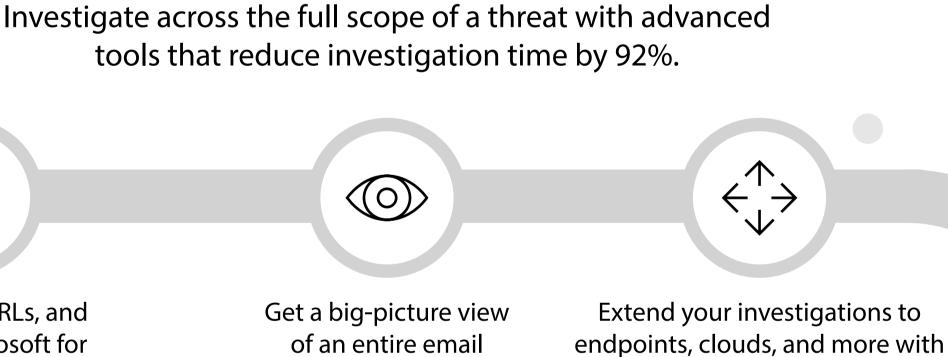


Nearly 2 billion threats are filtered before they reach the inbox each month.

**⟨⟨** ∑



**Investigate & Hunt for threats** 



××

playbooks integrated across

Microsoft 365 Defender.

Submit files, URLs, and

emails to Microsoft for

deeper investigation.

**Respond & Remediate** Remediate threats with built-in automation, cutting down mean time to respond.

emails marked as malicious

post-delivery with

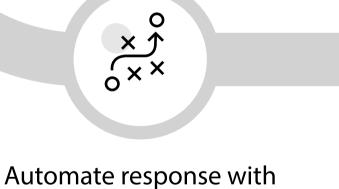
Zero-Hour Auto Purge (ZAP).

campaign at once.



Microsoft 365 Defender and

Microsoft Sentinel.



**⟨⟨** ∑

Automatically neutralize Centralize your response to





**†** | |

Easily tune and configure

security policies with

a threat in a single queue,

allowing you to easily keep

track of the investigation

and remediation process.

**<<** [ ]

Conduct advanced

phishing simulations

with direct injection.

Educate users and continue to enforce security posture with built-in tools.

A H

Assign and manage

user training based on simulation results.

**→ >>** 

built-in analysis.

A safer organization and empowered SecOps team

Improved threat investigation. Microsoft Defender for Office 365 improved averages time to investigate from 12 hours to 1 hour.<sup>1</sup>

92%

no time cost.1

95%

Improved malicious link

blocking, reducing time

needed from 2.5 hours to

# Ready to learn more?

Get more information

29%

Reduced risk of an email or

collaboration tool breach

when moving from a

competitive tool.1

Learn more about

Visit the website

Defender for Office 365.

today

Contact sales

© Microsoft Corporation. All rights reserved. This material is provided for informational purposes only. MICROSOFT MAKES NO WARRANTIES, EXPRESSED OR IMPLIED.

Get started

Find out how you can get started with Defender for Office 365 in your environment now.

**>>** 

Go deeper with integrated SIEM + XDR

cloud workloads.

Learn about SIEM + XDR >>

Get integrated threat protection across

devices, identities, apps, email, data and

<sup>1</sup> Results are for a composite organization based on interviewed customers.

**>>** 

Forrester Total Economic Impact™ of Microsoft Defender for Office 365, a commissioned study from Forrester Consulting, 2021.