## 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.



Collaboration tools are growing 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,

and known attacks

**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 advanced threat protection to

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.



### posture to response and remediation.

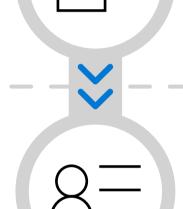
Comprehensive security

driven by AI and automation based on 43 trillion signals anlayzed daily.

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.

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

attachments, is analyzed. Microsoft Defender for Office 365

uses the power of the full Microsoft Defender family to scan

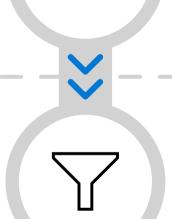
113 million threats eliminated

monthly

1.5 billion

threats eliminated

monthly



Content Filtering

Layer 3

Layer 4

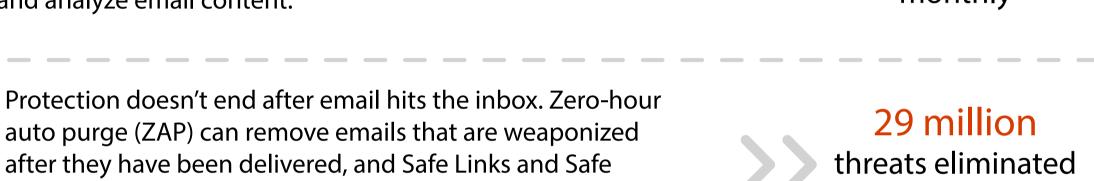
**Post-Delivery** 

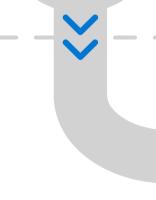
suite.

**Protection** 

and analyze email content.

216 million threats eliminated monthly





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

Attachments continue to protect users across the Office 365

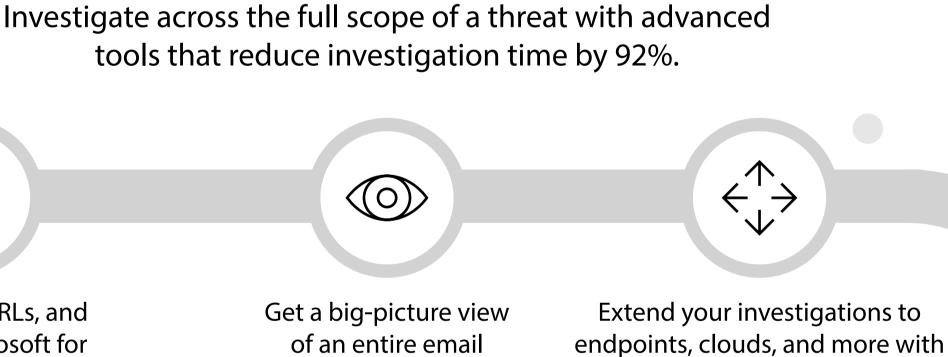
**⟨⟨** ∑

monthly



**Investigate & Hunt for threats** 

campaign at once.



××

Automate response with

playbooks integrated across

**⟨⟨** ∑

Submit files, URLs, and

emails to Microsoft for

deeper investigation.

**Respond & Remediate** 

Remediate threats with built-in automation,

cutting down mean time to respond.

Automatically neutralize

emails marked as malicious

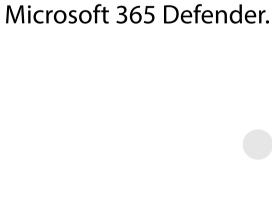
post-delivery with

Zero-Hour Auto Purge (ZAP).

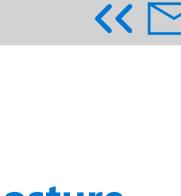
**⟨⟨** ∑

Microsoft 365 Defender and

Microsoft Sentinel.



Maintain ongoing awareness & security posture



**†** | |

Easily tune and configure

Centralize your response to

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.

**→ >>** 

security policies with built-in analysis.

A safer organization and empowered SecOps team

92%

Improved threat investigation.

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

Ready to learn more?

Contact sales

**>>** 

Learn more about Defender for Office 365.

Get more

information

Visit the website

29%

Reduced risk of an email or

collaboration tool breach

when moving from a

competitive tool.1

today

95%

Improved malicious link

blocking, reducing time

needed from 2.5 hours to

no time cost.1

Get started

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

cloud workloads.

Learn about SIEM + XDR >>

Go deeper with integrated

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

**>>**