Microsoft Security

Microsoft Defender for Office 365

Integrated threat protection for all of Office 365

Microsoft Defender for Office 365 offers a comprehensive solution to protect your organization and employees from advanced, targeted and zero-day phishing, malware and business email compromise attacks.

Secure Posture

Awareness & Training

Prevention

Office 365

Response & Remediation

Detection

Investigation & Hunting

Top 10 advantages of Defender for Office 365

» = Unique to Defender for Office 365

1. Industry leading protection
- » Built on Microsoft's 24 trillion daily security signals
- » Low latency file detonation—average <45s
- » URL detonation in mail-flow and at time-of-click
- • BEC protection using mailbox intelligence
- » Enhanced spoof protection beyond DMARC checks
- • Internal email protection within compliance boundary

2. Integrated protection across Office 365
- • Advanced protection for Teams, SharePoint, and OneDrive
- » Time-of-click protection within Office 365 apps (Word, Excel, PowerPoint) and Microsoft Teams
- » Native client experiences increase user awareness
- » Native hover experience to show original URLs for wrapped links

3. Easy to configure policy settings
- • Preset security policies for quick deployment
- • Simple checkbox policies
- » Configuration analyzer for policy tuning
- » Advanced delivery for phishing simulations and SecOps mailboxes

4. Detailed and actionable reporting
- • Priority Account Protection tracks critical users
- • Reports uncover configuration gaps
- • Enriched details for SOC effectiveness
- • APIs to create customized detection reports

5. Powerful campaign analysis
- • Big-picture views of entire email campaigns
- • Easy identification of configuration flaws, vulnerable users
- • Integrated with automated investigation and response

6. Threat investigation & hunting
- • Advanced tools that reduce investigation time by 92%
- • Detailed email analysis tools with API access
- » Ability for SecOps to submit emails, URLs, files to Microsoft for analysis

7. Automated response
- » Automated response playbooks integrated across Office 365
- • Trigger automated investigations manually
- » Integrated investigation and response across Microsoft 365 Defender workloads

8. Compromise detection & response
- » Based on anomalous email patterns and Office 365 activities
- • Configurable sending limits to limit scope of breach
- » Disable external forwarding automatically
- » Powerful automation for quicker remediation

9. Built-in simulation & awareness training
- » Powerful phishing simulation using direct injection
- » No whitelisting required of IP's and URLS
- • Assign end user training based on simulation results
- • Detailed reporting of clicks, IPs, devices and browsers used
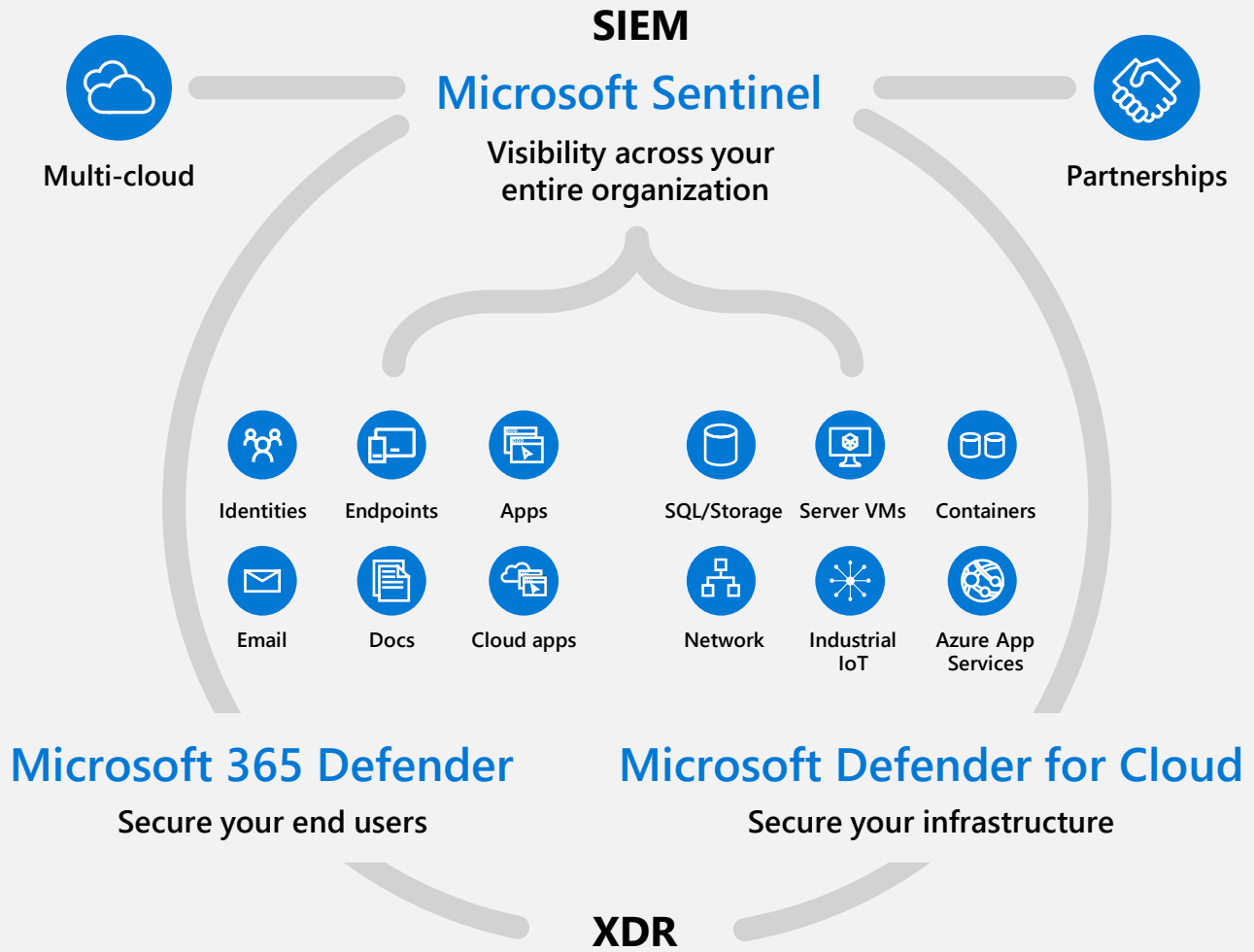- • Outlook report message add-on integration

10. Microsoft 365 Defender
- » XDR integration to amplify prevention, detection, and response across Microsoft products
- » Automated Investigation and response integration across Defender for Office 365, Defender for Endpoint, Defender for Identity, Defender for Cloud Apps, and Azure Active Directory
- » Powerful advanced hunting across the digital estate

Stay ahead of attackers with a unified SecOps experience

Microsoft Defender for Office 365 is part of an integrated set of threat protection solutions from Microsoft that offer a holistic view of security for your organization.

Microsoft 365 Defender and Microsoft Defender for Cloud deliver the most comprehensive XDR solution on the market and Microsoft Sentinel is an innovative cloud-native SIEM. With the integration of these tools, defenders have more actionable context than ever so they can focus on stopping threats across the entire enterprise.

SIEM
Microsoft Sentinel
Visibility across your entire organization

Multi-cloud

Partnerships

Identities   Endpoints   Apps   SQL/Storage   Server VMs   Containers

Email   Docs   Cloud apps   Network   Industrial IoT   Azure App Services

Microsoft 365 Defender
Secure your end users

Microsoft Defender for Cloud
Secure your infrastructure

XDR

Microsoft Defender for Office 365 has been named a Leader in The Forrester Wave™: Email Security, Q2 2021.[1]

"Without being an email security expert, I managed to configure it for effective usage within less than a day. Not only does it run on its own automatically with little intervention from me—it also provides great forensic value."

Gabriel Necula
Security Operations Lead
UiPath

"The incident detection and response capabilities we get with Defender for Office 365 give us far more coverage than we've had before. This is a really big deal for us."

Jason Youngers
Director and Information Security Officer
Ithaca College

Total Economic Impact study of moving from a competitor to Defender for Office 365[2]

Improved blocking
of malicious links by
95%

Improved
investigation time by
92%

Reduced risk
of breach by
29%

Exchange Online Protection
Prevents broad volume-based and known attacks.

Defender for Office 365 Plan 1
Protects email **and collaboration** from targeted malware, phish, and business email compromise attacks.

Defender for Office 365 Plan 2
Post-breach investigation, hunting and response. Includes automation, attack simulation training, and XDR integration.

Learn more:
aka.ms/DefenderO365

Stay up to date:
aka.ms/MDOblog

Get started:
aka.ms/MDOdocs