Microsoft Defender

Article • 09/21/2023

Microsoft 365 Defender

Microsoft 365 Defender is a unified pre- and post-breach enterprise defense suite that natively coordinates detection, prevention, investigation, and response across endpoints, identities, email, and apps to provide integrated protection against sophisticated attacks.

FastTrack provides remote guidance for:

- Providing an overview of the Microsoft 365 security center.
  - Providing an overview of cross-product incidents, including focusing on what's critical by ensuring the full attack scope, impacted assets, and automated remediation actions that are grouped together.
  - Demonstrating how Microsoft 365 Defender can orchestrate the investigation of assets, users, devices, and mailboxes that might have been compromised through automated self-healing.
  - Explaining and providing examples of how customers can proactively hunt for intrusion attempts and breach activity affecting your email, data, devices, and accounts across multiple data sets.
  - Showing customers how they can review and improve their security posture holistically using Microsoft Secure Score.

Out of scope

- Deployment guidance or education on:
  - How to remediate or interpret the various alert types and monitored activities.
  - How to investigate a user, computer, lateral movement path, or entity.
  - Custom threat hunting.
- Security information and event management (SIEM) or API integration.

Microsoft advanced deployment guides

Microsoft provides customers with technology and guidance to assist with deploying your Microsoft 365, Microsoft Viva, and security services. We encourage our customers to start their deployment journey with these offerings.

For non-IT admins, see Microsoft 365 Setup .

Microsoft Defender for Cloud Apps

Microsoft Defender for Cloud Apps is a multi-purpose software-as-a-service (SaaS) security solution that combines SaaS security posture management, data loss prevention, app-to-app protection, and integrated threat protection to ensure holistic coverage for your apps. By adopting a SaaS security approach, you can easily identify misconfigurations to improve your overall app posture, implement policies to protect sensitive data, and protect app-to-app scenarios to ensure that only apps have the acceptable permissions to access other app data. By natively integrating into Microsoft 365 Defender, organizations like yours benefit from using the signal from SaaS to actively hunt in their environments and combat incidents across their apps, devices, identities, and email.

FastTrack provides remote guidance for:

- Configuring the portal, including:
  - Importing user groups.
  - Managing admin access and settings.
  - Scoping your deployment to select certain user groups to monitor or exclude from monitoring.
  - How to set up IP ranges and tags.
  - Personalizing the end-user experience with your logo and custom messaging.
- Integrating first-party services including:
  - Microsoft Defender for Endpoint.
  - Microsoft Defender for Identity.
  - Microsoft Entra Identity Protection.
  - Microsoft Purview Information Protection.
- Setting up cloud discovery using:
  - Microsoft Defender for Endpoints.
  - Zscaler.
  - iboss.
- Creating app tags and categories.
- Customizing app risk scores based on your organization's priorities.
- Sanctioning and unsanctioning apps.
- Reviewing the Defender for Cloud Apps and Cloud Discovery dashboards.
- Enabling app governance.

    - Guide the customer through the overview page and create up to five (5) app governance policies.
- Connecting featured apps using app connectors.
- Protecting apps with Conditional Access App Control in the Conditional Access within Microsoft Entra ID and Defender for Cloud Apps portals.
- Deploying Conditional Access App Control for featured apps.
- Reviewing SaaS Security Posture Management (SSPM) capabilities in Secure Score recommendations for available apps.
- Using the activity and file logs.
- Managing OAuth apps.
- Reviewing and configuring policy templates.
- Providing configuration assistance with the top SaaS use cases (including the creation or updating of up to six (6) policies).
- Understanding incident correlation in the Microsoft 365 Defender portal.

Out of scope

- Discussions comparing Defender for Cloud Apps to other Cloud Access Security Broker (CASB) or SaaS security offerings.
- Configuring Defender for Cloud Apps to meet specific compliance or regulatory requirements.
- Deploying the service to a non-production test environment.
- Deploying Cloud App Discovery as a proof of concept.
- Setting up the infrastructure, installation, or deployment of automatic log uploads for continuous reports using Docker or a log collector.
- Creating a Cloud Discovery snapshot report.
- Blocking app usage using block scripts.
- Adding custom apps to Cloud Discovery.
- Connecting custom apps with Conditional Access App Control.
- Onboarding and deploying Conditional Access App Control for any app.
- Integrating with third-party identity providers (IdPs) and data loss prevention (DLP) providers.
- Training or guidance covering advanced hunting.
- Automated investigation and remediation including Microsoft Power Automate playbooks.
- SIEM or API integration (including Microsoft Sentinel).

Microsoft advanced deployment guides

Microsoft provides customers with technology and guidance to assist with deploying your Microsoft 365, Microsoft Viva, and security services. We encourage our customers to start their deployment journey with these offerings.

For non-IT admins, see Microsoft 365 Setup .

Microsoft Defender for Endpoint

Microsoft Defender for Endpoint is a platform designed to help enterprise networks prevent, detect, investigate, and respond to advanced threats.

FastTrack provides assistance with the following:

- Assessing the OS version and device management approach (including Microsoft Intune, Microsoft Endpoint Configuration Manager, Group Policy, and third-party configurations) as well as the status of your Windows Defender AV services or other endpoint security software.
- Onboarding Microsoft Defender for Endpoint P1 and P2 using:
  - Local script.
  - Group Policy.
  - Intune.
  - Configuration Manager.
  - Defender for Endpoint security settings management.
- Providing recommended configuration guidance for Microsoft traffic to travel through proxies and firewalls, restricting network traffic for devices that are not able to connect directly to the internet.
- Enabling the Defender for Endpoint service by explaining how to deploy an endpoint detection and response (EDR) agent profile using one of the supported management methods.
- Deployment guidance, configuration assistance, and education on:
  - Vulnerability management core features.
  - Attack surface reduction.[1]
  - Next-generation protection.
  - Endpoint detection and response.
  - Automated investigation and remediation.
  - Secure score for devices.
  - Microsoft Defender SmartScreen configuration using Intune.

    - Device discovery.[2]
- Reviewing simulations and tutorials (like practice scenarios, fake malware, and automated investigations).
- Overview of reporting and threat analytics features.
- Integrating Microsoft Defender for Office 365, Microsoft Defender for Identity, and Defender for Cloud Apps with Defender for Endpoint.
- Conduct walkthroughs of the Microsoft 365 Defender portal.
- Onboarding and configuration of the following operating systems:
    - Windows 10/11, including Windows 365 Cloud PCs.
    - Windows Server 2012 R2.[3]
    - Windows Server 2016.[3]
    - Windows Server 2019.[3]
    - Windows Server 2022.[3]
    - Windows Server 2019 Core Edition.[3]
    - Supported macOS versions (see System requirements for more details).
    - Android.[4]
    - iOS.[4]

[1]Only attack surface reduction rules, controlled folder access, and network protection are supported. All other attack surface reduction capabilities aren't in scope. See the following **Out of scope** section for more details.

[2]Only some aspects are device discovery are supported. See the following **Out of scope** section for more details.

[3]Windows Server 2012 R2 and 2016 support is limited to onboarding and configuration of the unified agent. The servers must be managed by a supported version of Configuration Manager.

[4]See the following **Out of scope** section for mobile threat defense details.

Out of scope

- Onboarding and enablement guidance for preview features.
- Troubleshooting issues encountered during engagement (including devices that fail to onboard).
- Supporting Microsoft Defender for Business.
- Onboarding or configuration for the following Defender for Endpoint agents:
    - Windows Server 2008.

  - Linux.
  - Virtual Desktop Infrastructure (VDI) (persistent or non-persistent), including Azure Virtual Desktop and third party VDI solutions.
- Server onboarding and configuration:
  - Configuring a proxy server for offline communications.
  - Configuring Configuration Manager deployment packages on down-level Configuration Manager instances and versions.
  - Servers not managed by Configuration Manager.
  - Integrating Defender for Endpoint with Microsoft Defender for Servers (Microsoft Defender for Cloud).
- macOS onboarding and configuration:
  - JAMF-based deployment.
  - Other mobile device management (MDM) product-based deployment.
  - Manual deployment.
- Mobile threat defense onboarding and configuration (Android and iOS):
  - Unmanaged bring your own devices (BYOD) or devices managed by other enterprise mobility management systems.
  - Set up app protection policies (like mobile app management (MAM)).
  - Android devices admin-enrolled devices.
  - Assistance with co-existence of multiple VPN profiles.
  - Onboarding devices to Intune. For more information on onboarding assistance, see Microsoft Intune.
- Configuration of the following attack surface reduction capabilities:
  - Hardware-based app and browser isolation (including Application Guard).
  - App control, including AppLocker and Windows Defender Application Control.
  - Device control.
  - Exploit protection.
  - Network and endpoint firewalls.
- Configuration or management of account protection features like:
  - Credential Guard.
  - Local user group membership.
- Configuration or management of BitLocker.

> **Note**
>
> For information on BitLocker assistance with Windows 11, see **Windows 11**.

- Configuration or management of network device discovery.

- Configuration or management of the following device discovery capabilities:
  - Onboarding of unmanaged devices not in scope for FastTrack (like Linux).
  - Configuring or remediating internet-of-things (IoT) devices including vulnerability assessments of IoT devices through Defender for IoT.
  - Integration with third-party tooling.
  - Exclusions for device discovery.
  - Preliminary networking assistance.
  - Troubleshooting network issues.
- Attack simulations (including penetration testing).
- Enrollment or configuration of Microsoft Threat Experts.
- Configuration or training guidance for API or SIEM connections.
- Training or guidance covering advanced hunting.
- Training or guidance covering the use of or creation of Kusto queries.
- Training or guidance covering Defender SmartScreen configuration using Group Policy Objects (GPOs), Windows Security, or Microsoft Edge.
- Defender Vulnerability Management Add-on.
- Defender Vulnerability Management Standalone.

Contact a Microsoft Partner for assistance with these services.

Microsoft advanced deployment guides

Microsoft provides customers with technology and guidance to assist with deploying your Microsoft 365, Microsoft Viva, and security services. We encourage our customers to start their deployment journey with these offerings.

For non-IT admins, see Microsoft 365 Setup .

Microsoft Defender for Identity

Microsoft Defender for Identity is a cloud-based security solution that leverages your on-premises Active Directory signals to identify, detect, and investigate advanced threats, compromised identities, and malicious insider actions directed at your organization.

FastTrack provides remote guidance for:

- Running the sizing tool for resource capacity planning.
- Creating your instance of Defender for Identity.
- Configuring Windows event collection.

- Managing admin access with role groups.
- Downloading, deploying, and configuring the sensor on your domain controllers for both single and multiple forest environments.
- Portal configuration, including:
  - Tagging sensitive accounts, devices, or groups.
  - Email notifications for health issues and security alerts.
  - Alert exclusions.
  - Scheduled reports.
- Providing deployment guidance, configuration assistance, and education on:
  - Identity Security Posture Assessment reports within Microsoft Secure Score.
  - User Investigation Priority Score and User Investigation ranking reports.
  - Inactive user reports.
  - Remediation options on a compromised account.
- Facilitating the migration from Advanced Threat Analytics (ATA) to Defender for Identity (if applicable).

Out of scope

- Deploying Defender for Identity as a proof of concept.
- Deploying or performing the following Defender for Identity sensor activities:
  - Manual capacity planning.
  - Deploying the standalone sensor.
  - Deploying to Active Directory Federation Services (AD FS) servers.
  - Deploying the sensor using a Network Interface Card (NIC) Teaming adaptor.
  - Deploying the sensor through a third-party tool.
  - Connecting to the Defender for Identity cloud service through a web proxy connection.
- Creating and configuring directory service accounts or manage action accounts in Active Directory including group managed service accounts (gMSA).
- Creation and management of honeytokens accounts or devices.
- Enabling Network Name Resolution (NNR).
- Enabling and configuration of the Deleted Objects container.
- Deployment guidance or education on:
  - Remediating or interpreting various alert types and monitored activities.
  - Investigating a user, computer, lateral movement path, or entity.
  - Threat or advanced hunting.
  - Incident response.
- Providing a security alert lab tutorial for Defender for Identity.

- Providing notification when Defender for Identity detects suspicious activities by sending security alerts to your syslog server through a nominated sensor.
- Configuring Defender for Identity to perform queries using security account manager remote (SAMR) protocol to identify local admins on specific machines.
- Configuring VPN solutions to add information from the VPN connection to a user's profile page.
- SIEM or API integration (including Microsoft Sentinel).

Source environment expectations

- Aligned with Defender for Identity prerequisites.
- Active Directory deployed.
- The domain controllers you intend to install Defender for Identity sensors on have internet connectivity to the Defender for Identity cloud service.
  - Your firewall and proxy must be open to communicate with the Defender for Identity cloud service (*.atp.azure.com port 443 must be open).
- Domain controllers running on one of the following:
  - Windows Server 2012.
  - Windows Server 2012 R2.
  - Windows Server 2016.
  - Windows Server 2019 with KB4487044 (OS Build 17763.316 or later).
  - Windows Server 2022.
- Microsoft .NET Framework 4.7 or later.
- A minimum of six (6) GB of disk space is required and 10 GB is recommended.
- Two (2) cores and six (6) GB of RAM installed on the domain controller.

Microsoft advanced deployment guides

Microsoft provides customers with technology and guidance to assist with deploying your Microsoft 365, Microsoft Viva, and security services. We encourage our customers to start their deployment journey with these offerings.

For non-IT admins, see Microsoft 365 Setup .

Microsoft Defender for Office 365

Microsoft Defender for Office 365 safeguards your organization against malicious threats posed by email messages, links (URLs), attachments and collaboration tools like Microsoft

Teams, SharePoint and Outlook. With real-time views of threats and tools like Threat Explorer, you can hunt and stay ahead of potential threats. Use attack simulation training to run realistic attack scenarios in your organization. These simulated attacks can help you identify and find vulnerable users before a real attack impacts your bottom line.

FastTrack provides remote guidance for:

- Reviewing the Configuration analyzer and/or Defender for Office 365 Recommended Configuration Analyzer (ORCA).
- Setting up evaluation mode.
- Enabling preset policies, Safe Links (including Safe Documents), Safe Attachments, anti-malware, anti-phishing, anti-spam, anti-spoofing, impersonation, and quarantine policies.
- Enabling Teams protection.
- Configuring user-reported message settings.
- Using Attack Simulator and configuring an advanced delivery policy
- Overview of Tenant Allow/Block List (TABL) submissions, email entity page, reporting, campaigns, threat explorer, and threat analytics.
- Overview of zero-hour auto purge (ZAP) automation and investigation and response (AIR).
- Understanding incident correlation in the Microsoft 365 Defender portal.
- Transitioning from a third-party provider following the Microsoft best practice guidance with the exception of creating an inventory of your current settings, moving features that modify messages into Microsoft 365, and configuring enhanced filtering for connectors.

Out of scope

- Discussions comparing Defender for Office 365 to other security offerings.
- Deploying Defender for Office 365 as a proof of concept.
- Mail flow analysis.
- Enhanced filtering.
- Training or guidance covering advanced hunting.
- Integration with Microsoft Power Automate playbooks.
- SIEM or API integration (including Microsoft Sentinel).

Source environment expectations

In addition to FastTrack core onboarding, Exchange Online must also be configured.

Microsoft advanced deployment guides

Microsoft provides customers with technology and guidance to assist with deploying your Microsoft 365, Microsoft Viva, and security services. We encourage our customers to start their deployment journey with these offerings.

For non-IT admins, see Microsoft 365 Setup .