Defend Against Threats with Microsoft 365 Defender

Microsoft 365 Defender combines protection, detection, investigation, and response to email, collaboration, identity, device, and cloud app threats, in a central place. The Microsoft 365 Defender portal emphasizes quick access to information, simpler layouts, and bringing related information together for easier use.

Business Outcomes:

- Incidents & alerts
- Hunting
- Actions & submissions
- Threat analytics
- Secure score
- Learning hub
- Trials
- Partner catalog

Approach:

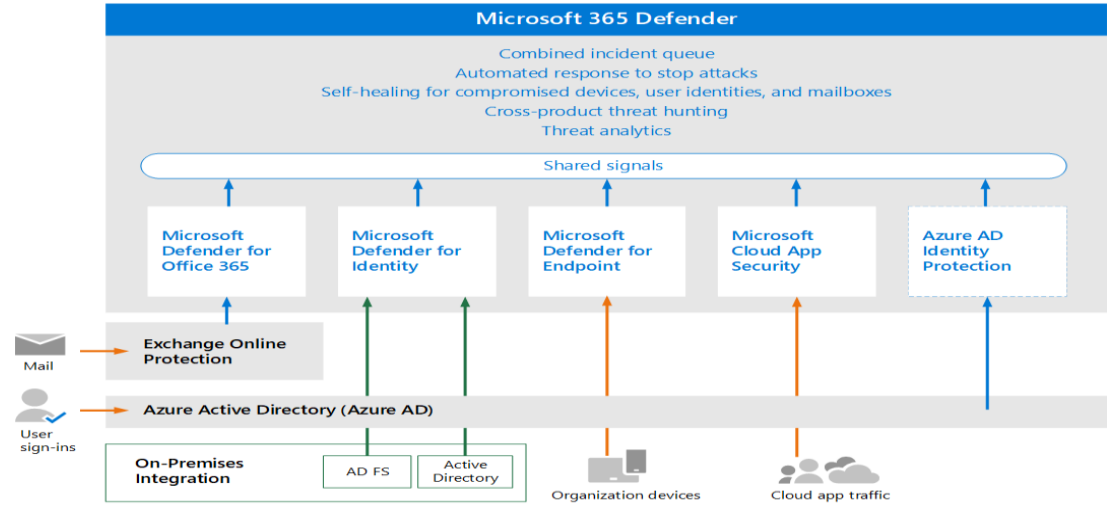
- Microsoft 365 Defender operations readiness to Provide situational awareness of modern threats
- Perform a SOC integration readiness assessment using the Zero Trust Framework
- Plan for Microsoft 365 Defender integration with your SOC catalog of services
- Define Microsoft 365 Defender roles, responsibilities, and oversight
- Develop and test use cases
- Identify SOC maintenance tasks
- Investigate and respond
- Configure automated investigation and remediation capabilities

> **Get closer than ever to your customers. So close that you'll know what they need well before they realize it themselves**
>
> **Steve Jobs**

Microsoft Business Group

© 2022 Cognizant

Microsoft defender Architecture



Microsoft Defender for Identity

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

Microsoft Defender for Office 365

Protects email and collaboration from zero-day malware, phish, and business email compromise. Adds post-breach investigation, hunting, and response, as well as automation, and simulation

Microsoft Defender for Cloud Apps

Microsoft Defender for Cloud Apps is a Cloud Access Security Broker (CASB) that supports various deployment modes including log collection, API connectors, and reverse proxy.

Microsoft Defender for EndPoints

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

cognizant