Microsoft 365 Defender

examlabpractice.com

REFERENCE: https://learn.microsoft.com/en-us/microsoft-365/security/defender/microsoft-365-defender?view=o365-worldwide

What is Microsoft 365 Defender?

- Microsoft 365 Defender serves as a comprehensive enterprise defense suite that seamlessly combines pre- and post-breach security measures.
- It inherently orchestrates the identification, prevention, examination, and action in response to security incidents across endpoints, user identities, email communications, and applications.
- This holistic approach delivers integrated security, guarding against advanced and intricate cyber threats.

The Different Defender Services

- Microsoft Defender for Endpoint
- Microsoft Defender for Office 365
- Microsoft Defender for Identity
- Microsoft Defender for Cloud Apps
- Microsoft Defender Vulnerability Management
- Microsoft Entra ID Protection
- Microsoft Data Loss Prevention
- App Governance

Microsoft Defender for Endpoint

Endpoint Behavioral Sensors:

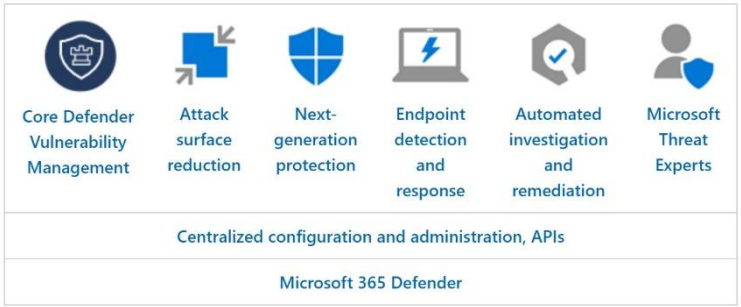
- Integrated within Windows 10, these sensors capture and process behavioral data from the operating system. This data is then transmitted to your private and isolated cloud instance of Microsoft Defender for Endpoint.

Cloud Security Analytics:

- Harnessing the power of big data, machine learning, and Microsoft's extensive insights into the Windows ecosystem, enterprise cloud services (like Office 365), and online resources, behavioral data is transformed into valuable insights, detections, and recommended responses to sophisticated threats.

Threat Intelligence:

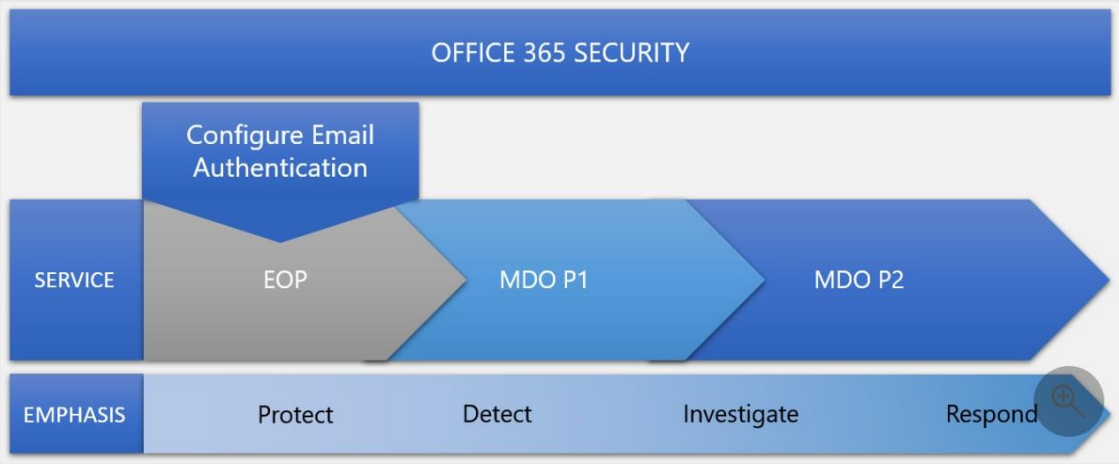
- Derived from Microsoft's dedicated security experts and teams, further enriched by threat intelligence contributions from trusted partners, this valuable resource empowers Defender for Endpoint to recognize attacker tactics, techniques, and procedures. It triggers alerts when these are identified within the collected sensor data.



Microsoft Defender for Office 365

EOP	Defender for Office 365 P1	Defender for Office 365 P2
Prevents broad, volume-based, known attacks.	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 (for training).

But in terms of architecture, let's start by thinking of each piece as cumulative layers of security, each with a security emphasis. More like this:



Microsoft Defender for Identity

Microsoft Defender for Identity is a security solution based in the cloud, designed to enhance the security of identity monitoring across your entire organization.

This solution is seamlessly integrated with Microsoft 365 Defender and utilizes data from both your on-premises Active Directory and cloud-based identities to assist you in more effectively recognizing, identifying, and investigating advanced threats targeting your organization.

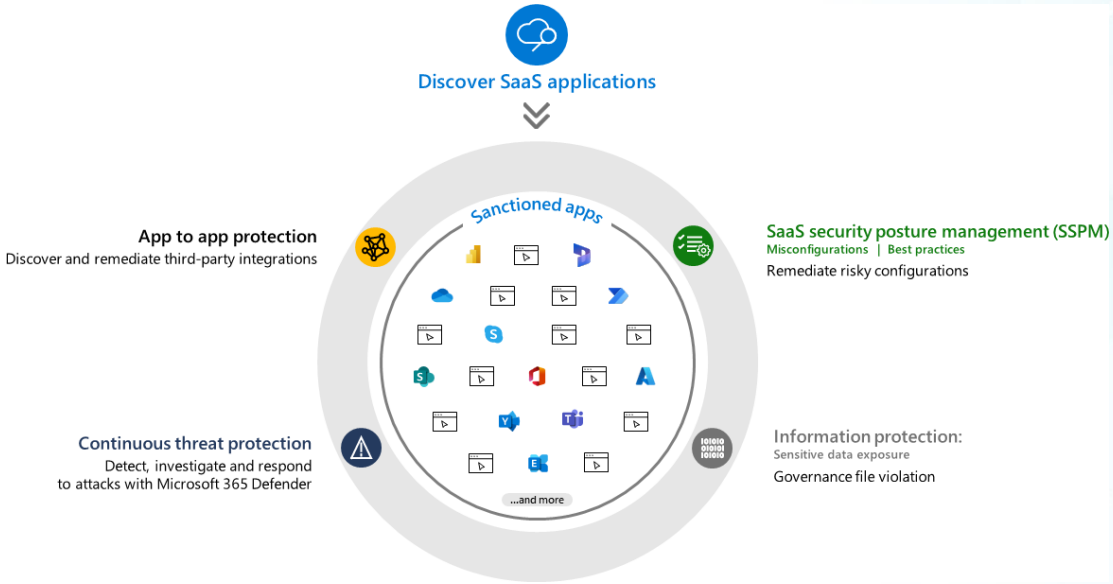
By implementing Defender for Identity, you empower your Security Operations (SecOps) teams to provide state-of-the-art identity threat detection (ITDR) capabilities across hybrid environments. This includes:

- Proactively preventing breaches by conducting security posture assessments for identities.
- Real-time detection of threats through advanced analytics and data intelligence.
- In-depth investigation of suspicious activities, with actionable incident information.
- Swift response to attacks by automating responses to compromised identities.

It's worth noting that Defender for Identity was formerly known as Azure Advanced Threat Protection (Azure ATP).

Microsoft Defender for Cloud Apps

Safeguarding Software as a Service (SaaS) applications and their vital data is a growing challenge in hybrid work environments. With increased app usage and remote access, new attack vectors emerge. To counter these threats effectively, security teams need to extend their protection beyond traditional cloud access security brokers (CASBs)."

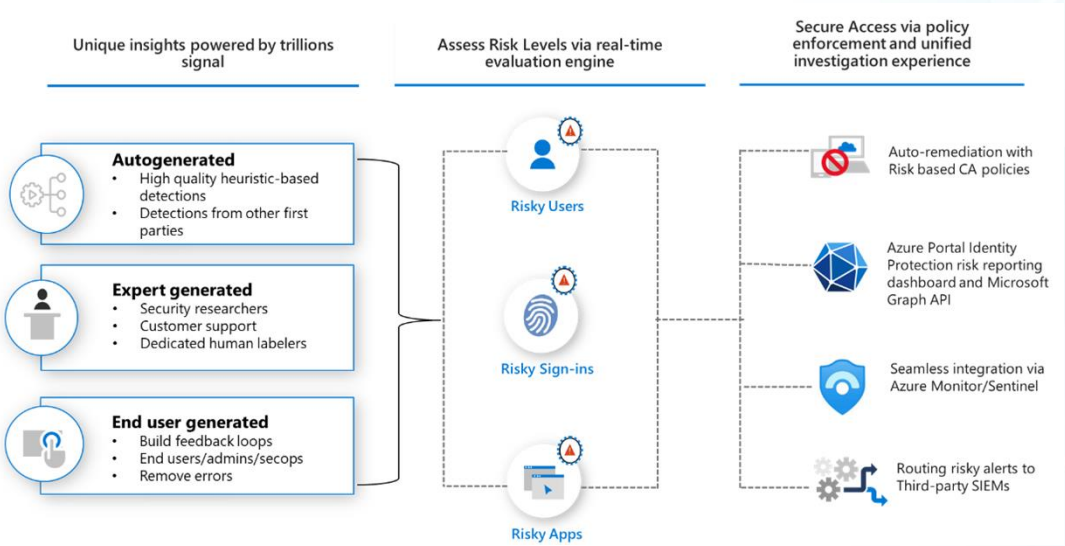


Microsoft Defender Vulnerability Management

- Defender Vulnerability Management offers comprehensive asset visibility, intelligent evaluations, and integrated remediation features across Windows, macOS, Linux, Android, iOS, and network devices.
- Powered by Microsoft's threat intelligence, breach likelihood predictions, business context insights, and device assessments, Defender Vulnerability Management swiftly and consistently ranks the most significant vulnerabilities on your vital assets.
- It also offers security guidance to mitigate potential risks.

Microsoft Entra ID Protection

- Microsoft Entra ID Protection aids organizations in identifying, probing, and addressing identity-related risks.
- These risks can be seamlessly integrated into tools such as Conditional Access for access control decisions or shared with a security information and event management (SIEM) solution for deeper scrutiny and correlation.

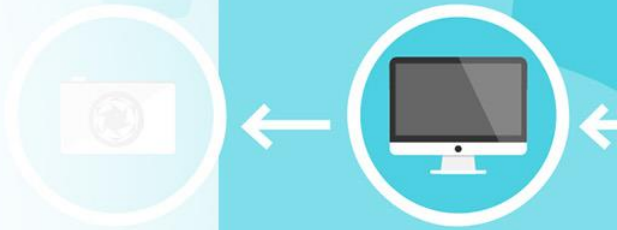


Microsoft Data Loss Prevention

Organizations manage a wealth of sensitive information, including financial data, proprietary content, credit card details, health records, and social security numbers. To safeguard this data and mitigate the risk of overexposure, they require a means to prevent users from inadvertently sharing sensitive information with unauthorized individuals. This practice is known as Data Loss Prevention (DLP).

In Microsoft Purview, DLP is implemented through the formulation and application of DLP policies. These policies enable the identification, monitoring, and automated protection of sensitive assets across various platforms, including:

- Microsoft 365 services like Teams, Exchange, SharePoint, and OneDrive accounts.
- Office applications such as Word, Excel, and PowerPoint.
- Endpoints running Windows and macOS (recent versions).
- Non-Microsoft cloud applications.
- On-premises file repositories and on-premises SharePoint.
- Power BI.



App Governance

Defender for Cloud Apps offers app governance, a suite of security and policy management tools tailored for OAuth-enabled apps registered on Entra ID (formerly Azure AD), Google, and Salesforce.

App governance insights empower you to make informed decisions regarding the management of apps that pose substantial risks to your organization. For instance:

- **Insights:** Gain a comprehensive overview of all non-Microsoft apps registered with Azure Active Directory, Google, or Salesforce within your organization, all from a single dashboard. Monitor app status and activities, and take responsive actions.
- **Governance:** Establish proactive or reactive policies to address app and user behaviors, protecting against noncompliant or malicious app usage and restricting access to risky apps.
- **Detection:** Receive alerts and notifications when unusual app activities occur, including the use of noncompliant, malicious, or risky apps.
- **Remediation:** In addition to automatic remediation capabilities, promptly employ remediation controls to address detected abnormal app activities.""and identifies the users who have authorized access to their accounts.