Windows Defender Guide

Microsoft 365 Defender

Previously, you learned about system hardening and critical elements in security architecture. In this reading, you will learn how Microsoft 365 Defender can be used within an organization for expanded security services and tools. You will also learn about User Account Control (UAC) and its importance in endpoint security.

Microsoft 365 Defender services

Preventing threats across an enterprise environment can be challenging for IT Support professionals. Microsoft 365 Defender can help to simplify this responsibility. Defender provides enterprise-wide security through an integrated suite of tools. It offers tools to prevent attacks, detect threats, investigate security breaches, and coordinate effective response strategies. The Defender portal also offers an action center for monitoring incidents and alerts, as well as for threat hunting and analytics.

Microsoft 365 Defender protection and services include:

- **Defender for Endpoint:** Protects network endpoints including servers, workstations, mobile devices, and IoT devices. Provides preventative safeguards, breach detections, automated analyses, and threat response services.
- **Defender Vulnerability Management:** Protects assets including, hardware, software, licenses, networks, and data. Provides asset inventory, vulnerability discovery, configuration assessment, risk-based prioritization, and remediation tools.
- **Defender for Office 365:** Protects Microsoft 365 (formerly Office 365), including Exchange, Outlook, files, and attachments. Guards against malicious threats entering from email messages, links (URLs), and collaboration tools.
- **Defender for Identity:** Protects user identities and credentials. Detects, identifies, and investigates advanced threats, compromised identities, and malicious actions performed using stolen user identities or by internal threats.
- **Azure Active Directory Identity Protection:** Protects cloud-based identities in Azure by automating detection and resolutions for identity risks.

- **Defender for Cloud Apps:** Protects cloud applications by providing deep visibility searches, robust data controls, and advanced threat protection.

Using Microsoft 365 Defender

As an IT Support professional in an organization, you might use Microsoft 365 Defender to monitor your enterprise's IT security. You can customize the Defender portal Home page by job roles. Various security cards can be selected to appear on the Home page for your role. For example, you might see cards for monitoring:

- **Identities:** Monitor user identities for suspicious or risky behaviors.
- **Data**: Track user activity that is risky to data security.
- **Devices**: See alerts, breach activity, and other threats on devices connected to the organization's network.
- **Apps**: Observe how cloud apps are being used in your organization.
- **Incidents:** Review attacks through compiled comprehensive incident data.
- **Alerts:** View alerts compiled from across the Microsoft 365 suite.
- **Advanced hunting:** Scan for suspicious files, malware, and risky activities.
- **Threat Analytics:** View information about current cybersecurity threats.
- **Secure score:** Get a calculated score for your security configuration and recommendations on how to improve your score.
- **Learning hub:** Easily access Microsoft 365 security tutorials and other learning materials.
- **Reports:** Obtain information to help you better protect your organization.

Microsoft 365 Defender aggregates and organizes this monitoring data to provide IT Support professionals details on where attacks began, which malicious tactics were used, the scope of the attacks, and other related incident information.

Microsoft 365 Defender in action

The following are examples of how a cyberattack might penetrate and infect an enterprise network. For each type of malicious attack, a potential Microsoft 365 Defender response follows, illustrating how the security suite could respond:

- **A phishing attempt enters through email:** An employee in an organization receives an email from a business that appears to be legitimate, like a bank. The email might claim that there is a problem with the employee's account and that they must click on a given link to resolve the

problem. However, the phishing email actually contains a link to a malicious website that a cybercriminal disguised to look like a real bank. If the employee clicks on the link to view the website, the site requests that the user enter their account credentials or other sensitive information. This information is then transmitted to the cybercriminal.
Microsoft Defender for Office 365 detects the emailed phishing scam by monitoring Exchange and Outlook. Both the employee and the IT Support team are alerted about this attempted phishing attack.

- **Malware enters through social media:** An employee clicks on an enticing link posted on their favorite social media app. The link triggers an automatic download of a malware file to the employee's laptop.
  Microsoft Defender for Endpoint monitors the employee's laptop for suspicious malware signatures. Upon detecting the malware, Defender for Endpoint alerts the employee and the organization's IT Support team about the malware and discloses its endpoint location.
- **A cybercriminal intercepts an employee's work login credentials:** An employee accesses their work account using their laptop and an open Wi-Fi access point in a busy coffee shop. A cybercriminal is in the same coffee shop to intercept and collect unprotected information flowing through the open Wi-Fi access point. The cybercriminal obtains the employee's user account credentials and uses them to hijack the employee's work account. The cybercriminal then begins a malicious attack on the employer's network.
  Microsoft Defender for Identity can detect the sudden change in activity on the employee's user account. Defender for Identity alerts the employee and the IT Support team about the compromised user identity.
- **A virus enters a cloud drive through a file upload:** An employee unknowingly uploads an file that is infected with a virus to their work cloud storage drive. When the employee opens the file from the cloud drive, the virus is activated and begins changing the security settings on the other files in the employees cloud drive.
  Microsoft Defender for Cloud Apps detects the unusual pattern of activity and alerts the employee and IT Support team of the suspicious activity in the cloud account.

User Account Control (UAC)

User Account Control (UAC) allows IT administrators to create standard user accounts with limited access rights and privileges for end users. This configuration can prevent users from installing unauthorized programs, changing system settings, tampering with firewalls, and more. In order to perform these types of tasks, administrator credentials must be provided. For less restrictive controls, UAC provides the option to grant end users local administrative privileges for approved activities that require administrative privileges. For more restrictive controls, UAC can require global administrator credentials be entered for each and every administrative change the user attempts to make.

Resources for more information

To learn more about Microsoft Defender through the Microsoft learning portal, please visit:

- Microsoft Learn: Introduction to Microsoft 365 Defender - Microsoft's self-paced course for Microsoft 365 Defender
- Protect your organization with Microsoft 365 Defender - An interactive guide to Microsoft 365 Defender and how it detects security risks, investigates attacks, and prevents harmful activities.
- Microsoft Defender for Endpoint - Gives an overview of product, services, architecture, and training opportunities.
- Microsoft Defender Vulnerability Management - Provides information about the services and tools available to find and fix vulnerabilities.
- Microsoft Defender for Office 365 - Lists included services and tools for various product levels, as well as the types of threats it protects against.
- Microsoft Defender for Identity - Offers product information, how-to guides, tutorials, and reference information.
- Microsoft Defender for Cloud Apps - Provides product overview, quickstart reference guide, tutorials, best practices, and additional resources.
- How User Account Control works - User Account Control (UAC) is a fundamental component of Microsoft's overall security vision. UAC helps mitigate the impact of malware.