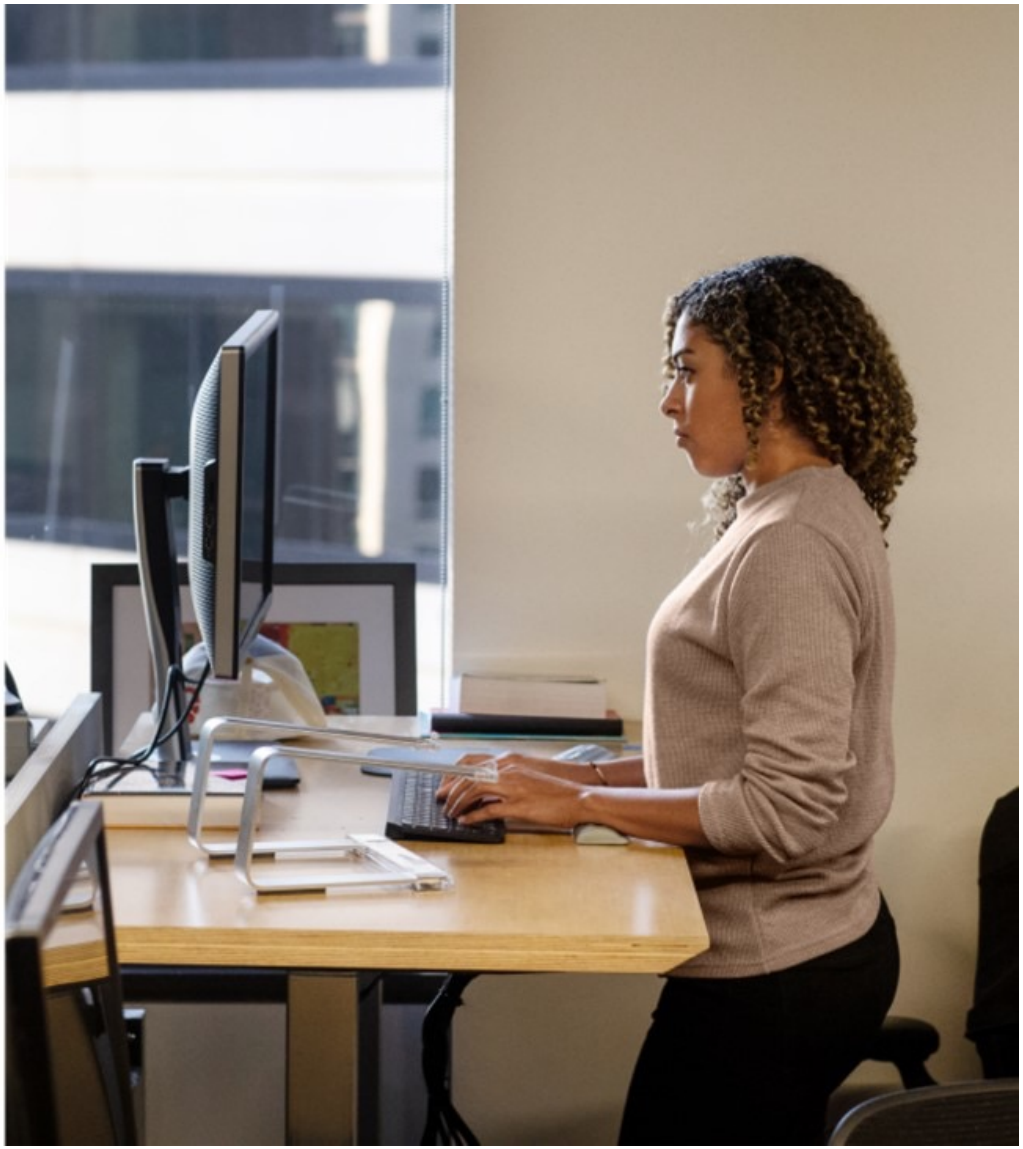
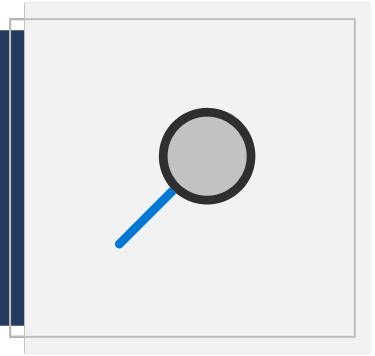
Microsoft 365

Microsoft 365 Defender for endpoint



Explore threat intelligence in Microsoft 365 Defender



Introduction

This module examines how to manage the Microsoft 365 threat intelligence features that provide organizations with insight and protection against the internal and external cyber-attacks that threaten their tenants.

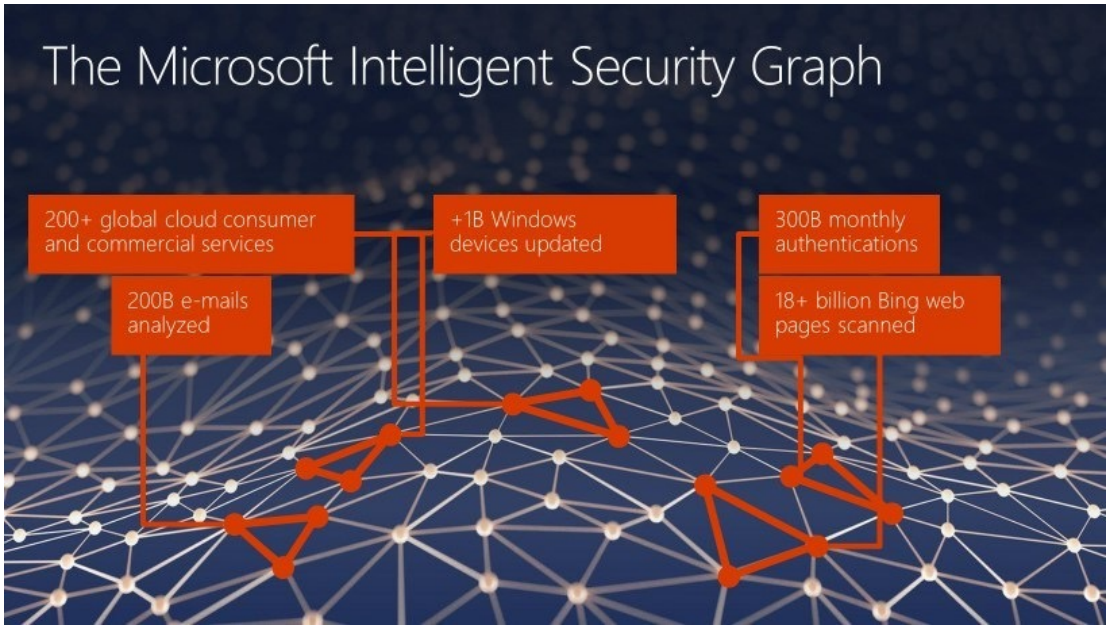
- Microsoft Intelligent Security Graph
- How Microsoft 365 Defender uses alerts
- Automated investigation and response
- Threat hunting
- Threat analytics

Explore Microsoft Intelligent Security Graph

To help customers focus on breach prevention and spend less on breach recovery, Microsoft has created the Microsoft Intelligent Security Graph

The Microsoft Intelligent Security Graph powers threat intelligence in Microsoft 365 by consuming billions of signals

The signals that are obtained from the Intelligent Security Graph, plus additional third-party feeds, are fed into Microsoft's three major platforms: Windows, Azure, and Microsoft 365

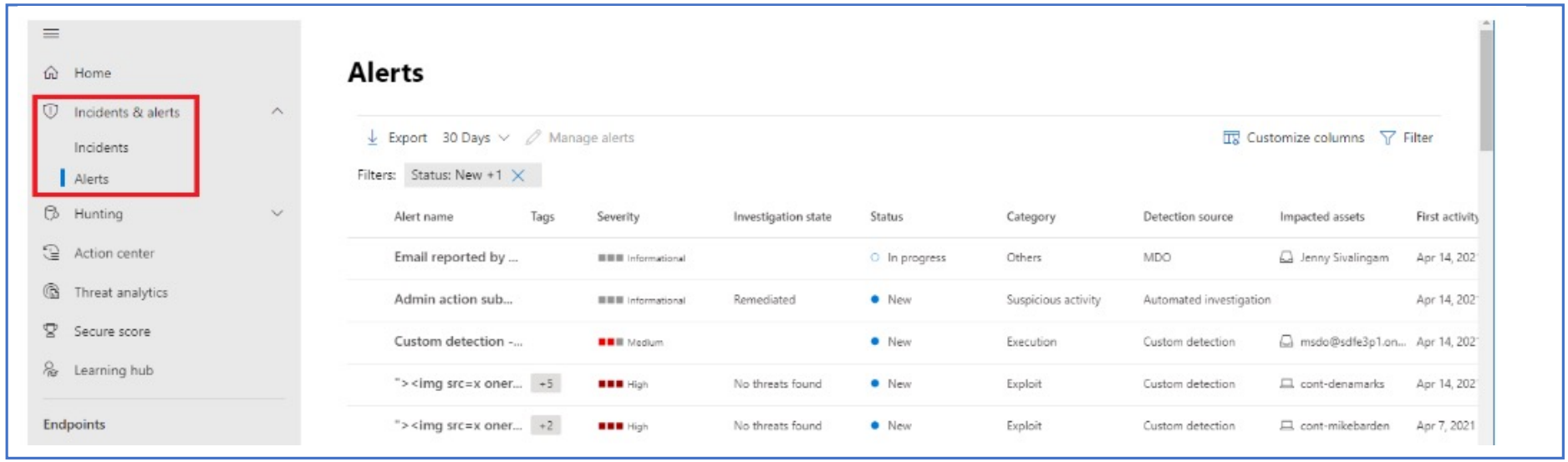


Explore alert policies in Microsoft 365

Alerts are the basis of all incidents and indicate the occurrence of malicious or suspicious events in your environment

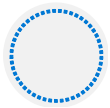
Alerts are typically part of a broader attack and provide clues about an incident

The Microsoft 365 Defender portal enables you to analyze, manage, and resolve alerts

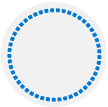


Run automated investigations and responses

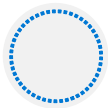
Automated investigation and response (AIR) capabilities enable organizations to automatically investigate well-known threats



Security operations teams can feel overwhelmed by the sheer volume of threats they must monitor and protect against



AIR capabilities enable security teams to dramatically increase their company's capacity to deal with security alerts and incidents

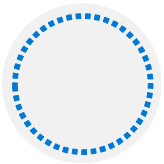


AIR capabilities help security operations teams complete the following steps:

1. Determine whether a threat requires action.
2. Take or recommend any necessary remediation actions against the identified threat.
3. Determine whether other investigations should occur, and what they should do.
4. Repeat the process as necessary for other alerts.

Not every alert triggers an automated investigation, and not every investigation results in automated remediation actions - It depends on how AIR is configured for an organization

Explore threat hunting with Microsoft Threat Protection

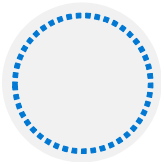


What is threat hunting?

Cyberthreat hunting is a proactive cybersecurity activity

Its goal is to find threats that are either buried under massive quantities of security signals and alert data, or aren't flagged by security products

Threat hunting lets analysts work with established baselines and highlight behavior that may be interesting or suspicious



Threat hunting in Microsoft Threat Protection

The threat hunting capabilities in Microsoft Threat Protection enable you to find threats across your users, endpoints, email, productivity tools, and apps

Microsoft Threat Protection itself is made possible by the power of the Azure cloud coupled with insights from the Microsoft Intelligent Security Graph

Microsoft Threat Protection's threat hunting capabilities enable security analysts to:

- Effectively access and handle large sets of data
- Automate monitoring of interesting matches to new data

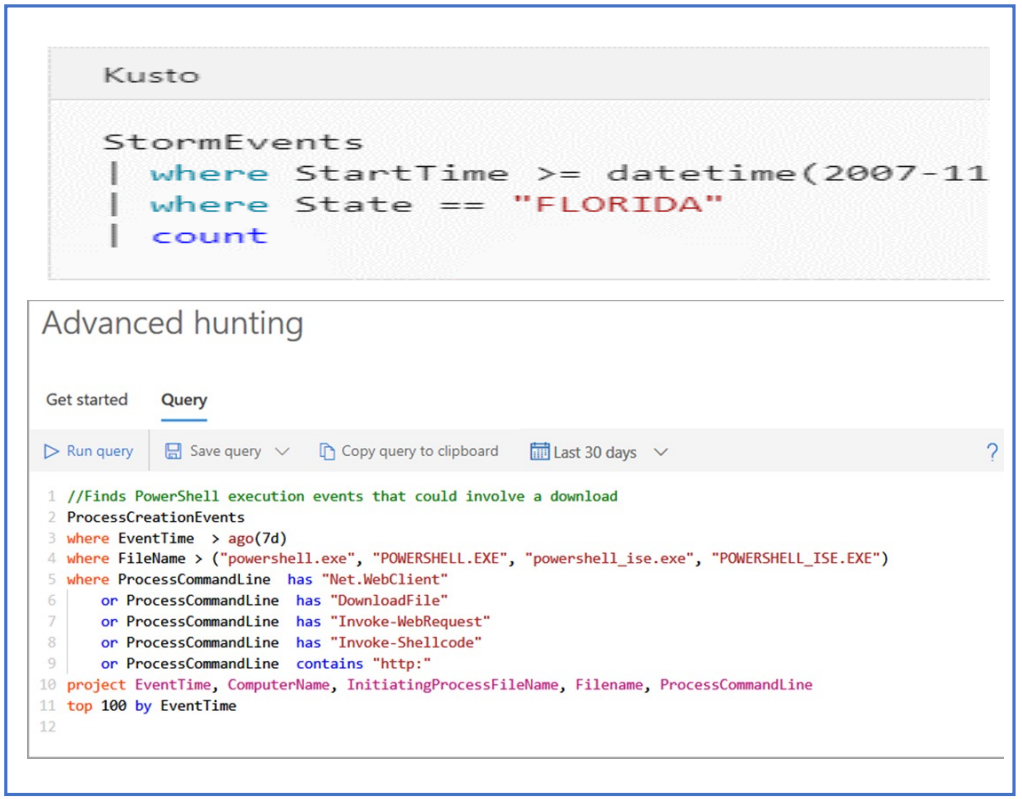
Explore advanced threat hunting in Microsoft 365 Defender

Advanced hunting in Microsoft 365 Defender is a query-based threat-hunting tool that lets you explore up to 30 days of raw data

Advanced hunting data can be categorized into two distinct types:

- Event or activity data
- Entity data

Advanced hunting is based on the Kusto query language



Explore threat analytics in Microsoft 365

View the threat analytics dashboard

The threat analytics dashboard summarizes the threats in the following sections:

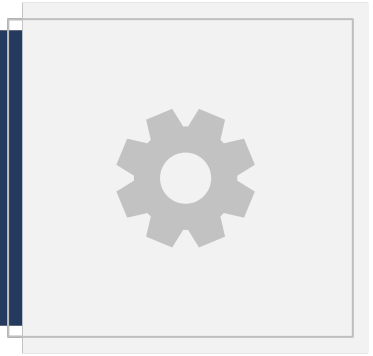
- Latest threats
- High-impact threats
- Highest exposure

View a threat analytics report

Each threat analytics report provides information in several tabs:

- Overview
- Analyst report
- Related incidents
- Impacted assets
- Prevented email attempts
- Exposure & mitigations

Implement endpoint protection by using Microsoft Defender for Endpoint



Introduction

This module examines the following key features of Microsoft Defender for Endpoint, which is an industry-leading, cloud-powered endpoint security solution:

- Threat and vulnerability management
- Attack surface reduction
- Next generation protection
- Endpoint detection and response
- Auto investigation and remediation

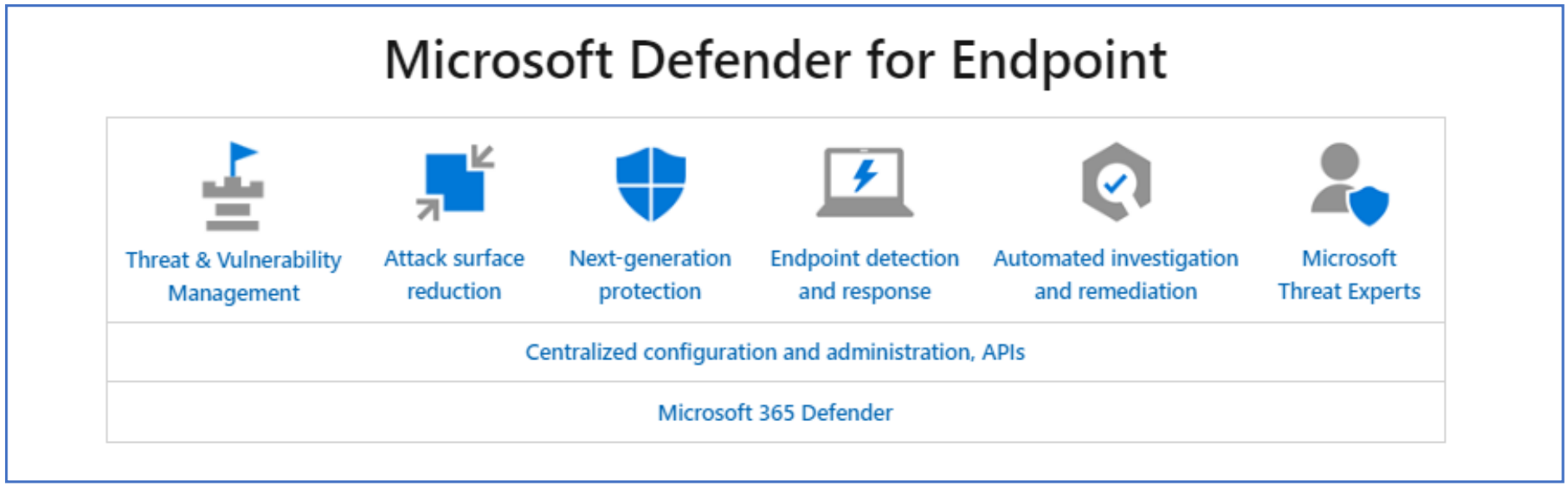
Explore Microsoft Defender for Endpoint

Combination of technologies:

- Endpoint behavioral sensors
- Cloud security analytics
- Threat intelligence

Plan your Microsoft Defender for Endpoint deployment:

- Identify your architecture
- Select the deployment method
- Configure Endpoint capabilities



Configure Microsoft Defender for Endpoint in Microsoft Intune

To be successful, you'll use the following configurations in concert:

- Establish a service-to-service connection between Microsoft Intune and Microsoft Defender for Endpoint
- Use a device configuration profile to onboard devices with Microsoft Defender for Endpoint
- Use a device compliance policy to set the level of risk you want to allow
- Use a conditional access policy to block users from accessing corporate resources from devices that are noncompliant

Onboard devices in Microsoft Defender for Endpoint

Examine the following steps to onboard devices and configure compliance and conditional access policies:

- Onboard devices that run Android, iOS/iPadOS, and Windows 10/11
- Use compliance policies to set device risk levels
- Use conditional access policies to block devices that exceed your expected risk levels
- Android and iOS/iPadOS, use app protection policies that set device risk levels. App protection polices work with both enrolled and unenrolled devices

Manage endpoint threats and vulnerabilities

Microsoft's Threat and Vulnerability Management module is a component of Microsoft Defender for Endpoint. It effectively identifies, assesses, and remediates endpoint weaknesses.

- Bridging the workflow gaps
- Intelligence-driven prioritization
- Seamless remediation
- Threat and Vulnerability Management walk-through
- Dashboard insights - threat and vulnerability management

Manage device discovery and vulnerability assessment

Microsoft Defender for Endpoint provides a device discovery capability that enables organizations to discover:

- Enterprise endpoints (workstations, servers and mobile devices) that aren't yet onboarded to Microsoft Defender for Endpoint
- Network devices like routers and switches
- IoT devices like printers and cameras

The device discovery feature includes:

- Discovery methods
- Device inventory
- Network device discovery
- Device discovery integrations
- Configure device discovery
- Exclude devices from being actively probed in standard discovery
- Select networks to monitor
- Configure the network monitor state
- Explore devices in the network
- Get information on a device
- Vulnerability assessment on discovered devices
- Advanced hunting on discovered devices
- Query network related information

Reduce your threat and vulnerability exposure

An organization's exposure score reflects how vulnerable it is to cybersecurity threats

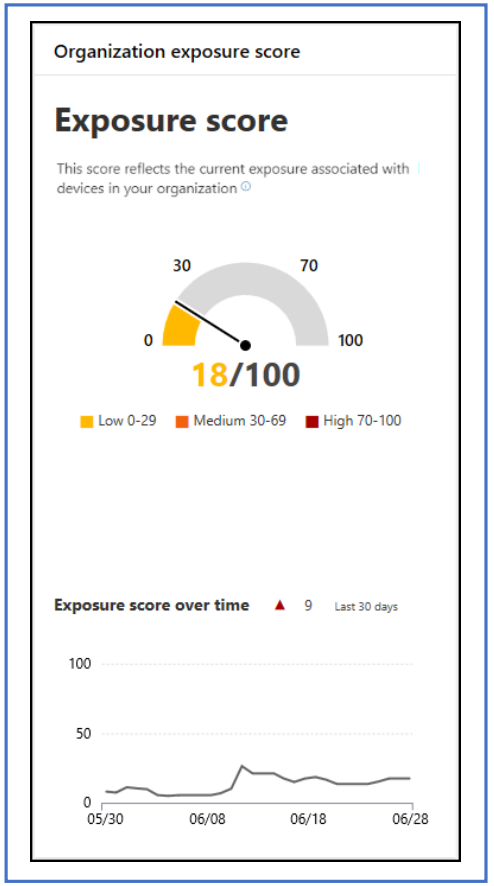
The score is displayed in the Threat and Vulnerability dashboard of the Microsoft 365 Defender portal

Each device in an organization is scored based on three factors:

- Threat
- Breach likelihood
- Business value

The Microsoft 365 Defender portal includes:

- Security recommendations with remediation actions
- Changes in device exposure or effect
- File exceptions for security recommendations
- Report an inaccurate recommendation




Microsoft
THANK YOU
Q & A