

Extended Detection and Response with Microsoft Defender XDR



Vlad Catrinescu

Microsoft MVP | Independent Consultant

@vladcatrinescu | VladTalksTech.com | YouTube.com/@VladTalksTech

Overview



Microsoft Defender for Endpoint

Microsoft Defender for Office 365

Microsoft Defender for Identity

Microsoft Defender Vulnerability Management

Microsoft Defender Threat Intelligence

Microsoft Security Copilot





Microsoft Defender for Endpoint



Microsoft Defender for Endpoint

Microsoft Defender for Endpoint is a platform designed to help enterprise networks protect endpoints including laptops, phones, tablets, PCs, access points, routers, and firewalls. It does so by preventing, detecting, investigating, and responding to advanced threats.



Microsoft Defender for Endpoint Key Areas

**Core Defender
Vulnerability
Management**

**Attack surface
reduction**

**Next-generation
protection**

**Endpoint detection
and response**

**Automated
investigation and
remediation**

**Microsoft Threat
Experts**



Core Defender Vulnerability Management



Risk-based approach to

- Discovery
- Prioritization
- And remediation of endpoint vulnerabilities

Uses sensors for real-time discovery

- No agents/scans needed



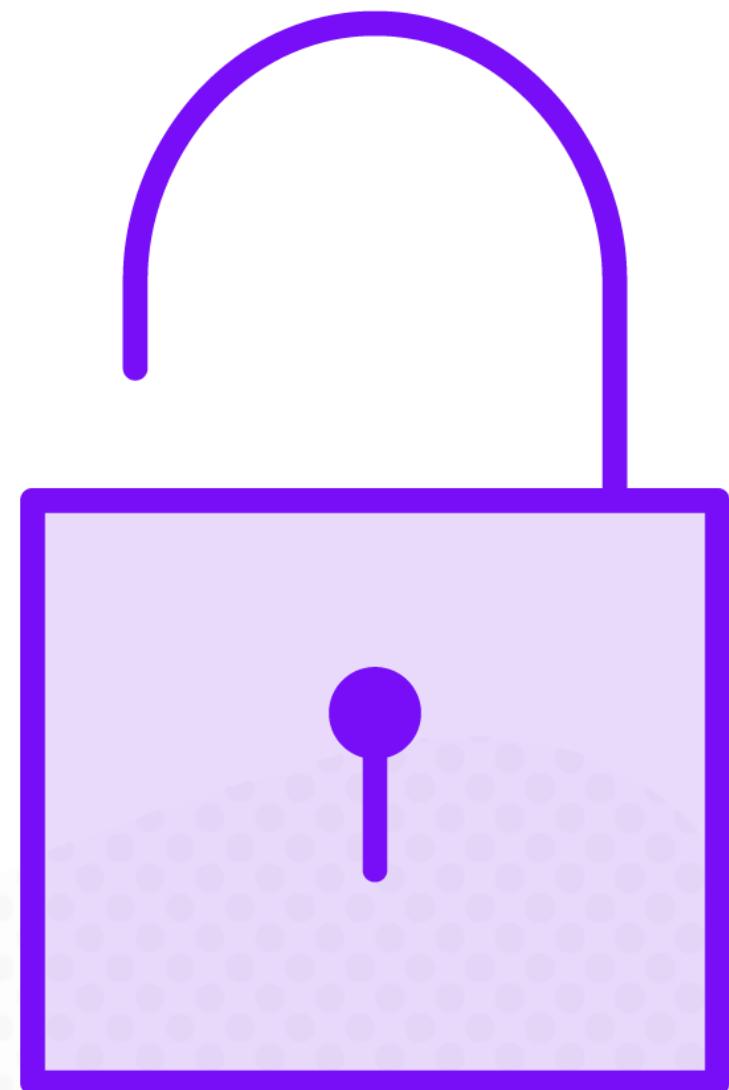
Attack Surface Reduction

**Reduce the places where your organization
is vulnerable**

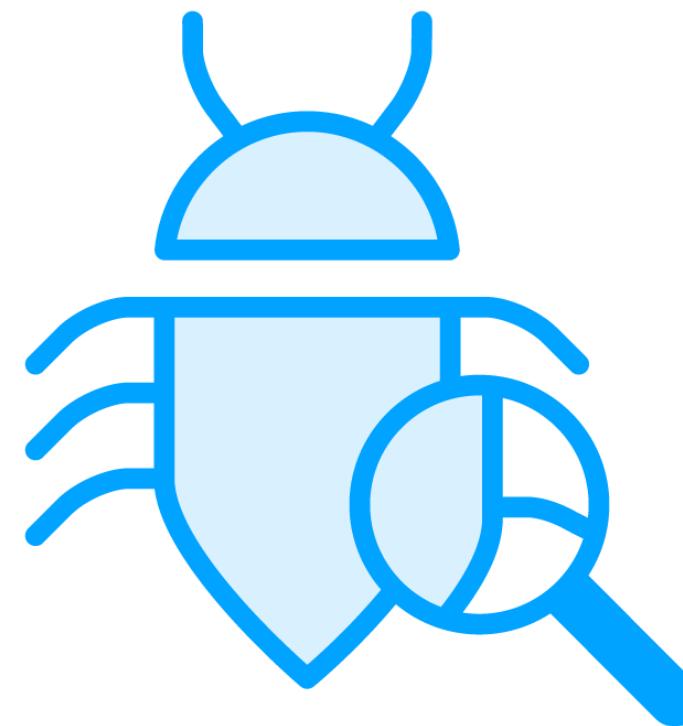
Provides a first line of defense

Ensures configurations are properly set

Network and web protection



Next-generation Protection



Microsoft Defender Antivirus

- Behavior-based and real-time antivirus protection
- Cloud-delivered protection
- Protection and product updates



Endpoint Detection and Response

Advanced attack detection

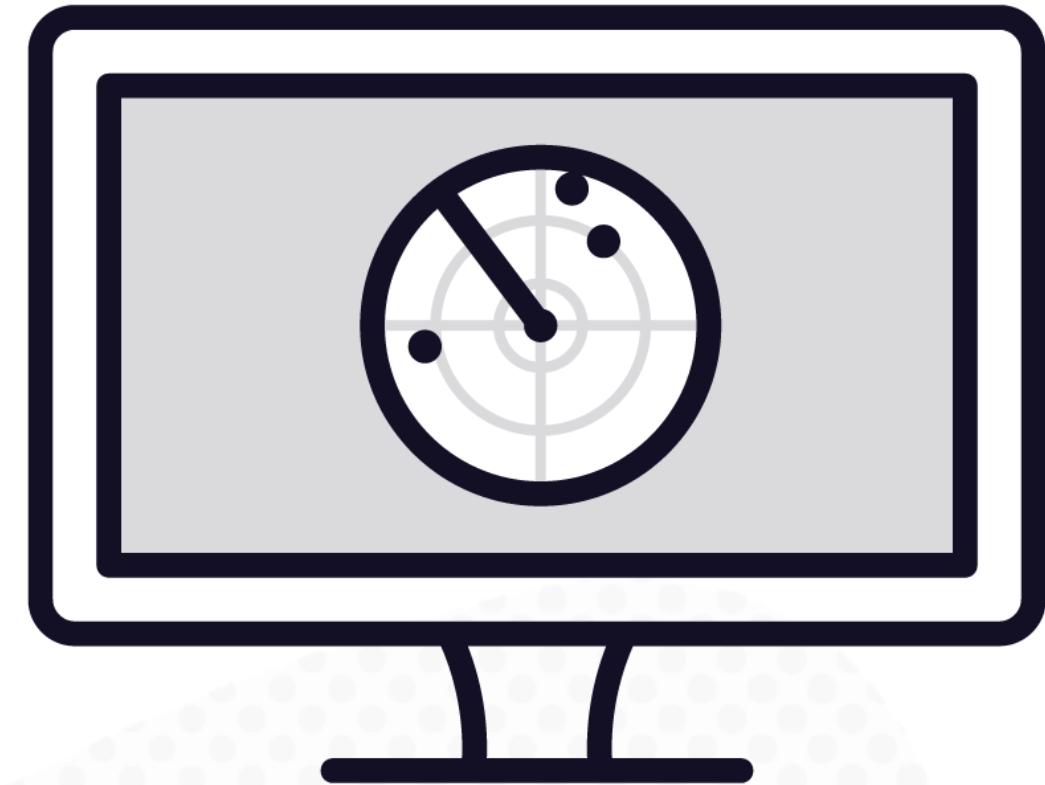
Near real-time

Actionable

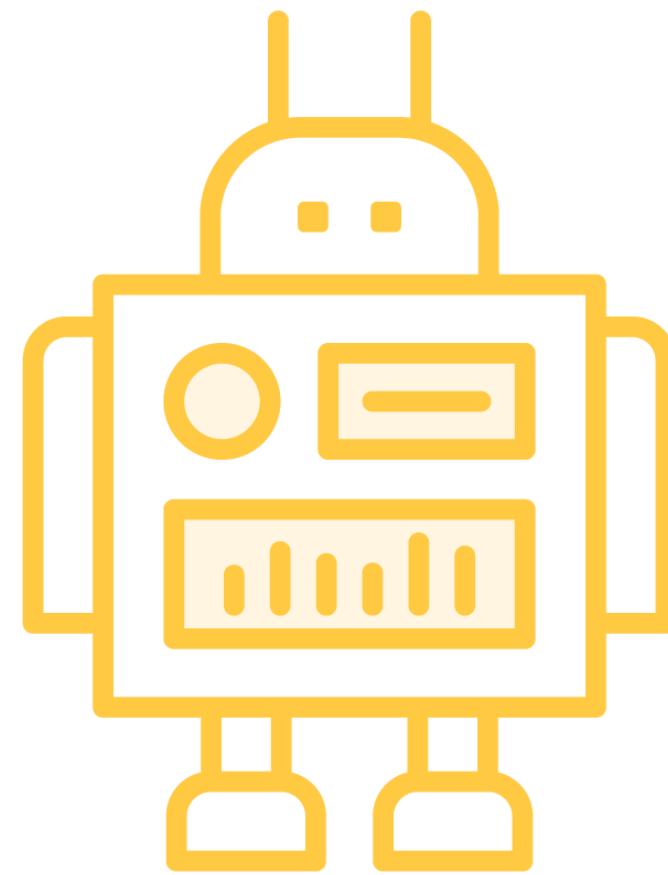
Prioritize alerts and gain visibility into the full scope of a breach

Alerts with same technique/attacker are aggregated into an incident

Easier to investigate and respond to a threat



Automated Investigation and Remediation (AIR)



Inspection algorithm and processes to examine alerts and take quick remediation

Remediation can occur automatically or only upon approval

- Depending on your organization configuration



Microsoft Threat Experts

Managed threat hunting service

Expert level monitoring and analysis

Targeted attack notification

Access to experts on demand

Customers need to apply for the Microsoft Threat Experts program

Extra cost



Other Features

Microsoft Secure Score for Devices

Dynamically assess the security state of your enterprise network, identify unprotected systems, and take recommended actions to improve the overall security of your organization

Management and APIs

Offers an API model designed to expose entities and capabilities through a standard Microsoft Entra ID-based authentication and authorization model





Microsoft Defender for Office 365



Microsoft Defender for Office 365

Microsoft Defender for Office 365 , safeguards your organization against malicious threats posed by email messages, links , and collaboration tools, including Microsoft Teams, SharePoint Online, OneDrive for Business, and other Office clients



Microsoft Defender for Office 365 Key Areas

Threat protection policies

Reports

Threat investigation and response capabilities

Automated investigation and response capabilities



Threat Protection Policies

Safe Attachments

Provides zero-day protection to safeguard your messaging system, by checking email attachments for malicious content

Safe Links

Provides time-of-click verification of URLs, for example, in emails messages and Office files

Anti-phishing protection

Detects attempts to impersonate your users and internal or custom domains

Safe Attachments for SharePoint, OneDrive, and Teams

Protects your organization when users collaborate and share files, by identifying and blocking malicious files in document libraries



Microsoft Defender for Office 365 Reports

Real-time reports to monitor performance

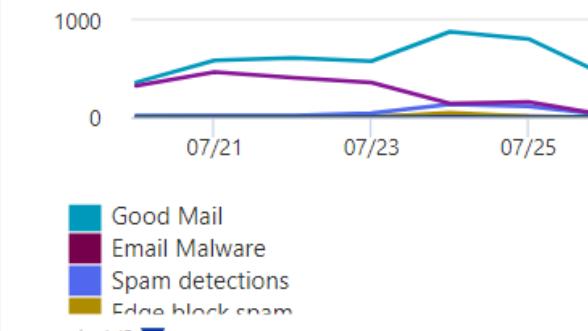
URL protection report

Threat protection status

User reported messages

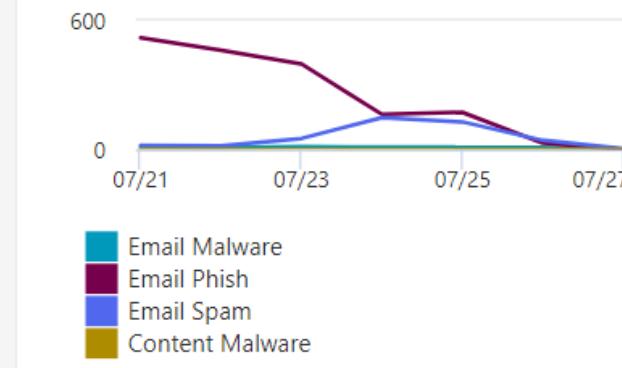
Email & collaboration reports

Mailflow status summary



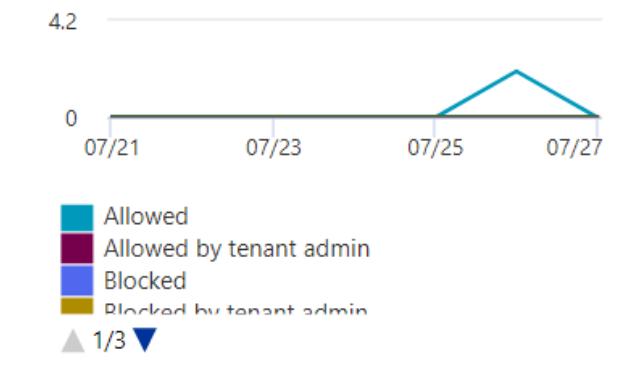
[View details](#)

Threat protection status



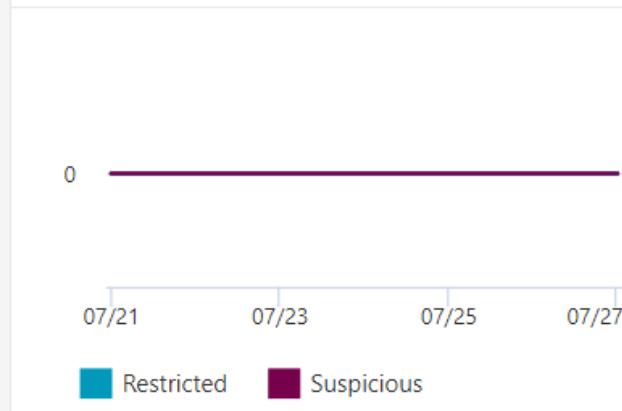
[View details](#)

URL protection report



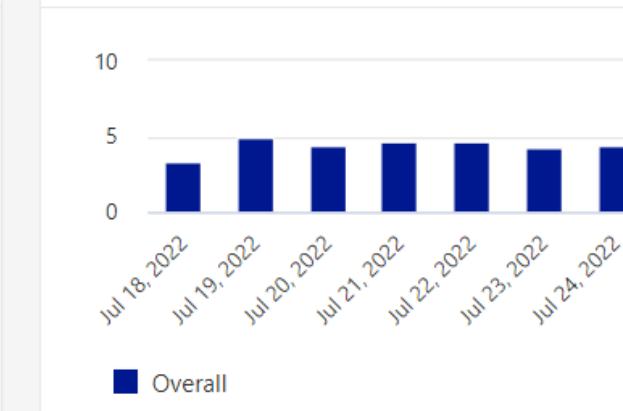
[View details](#)

Compromised users



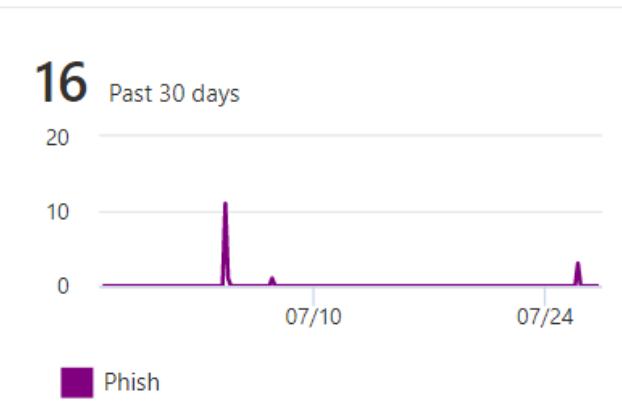
[View details](#)

Mail latency report



[View details](#)

User reported messages



[View details](#)

[Go to Submissions](#)



Threat Investigation and Response Capabilities



Threat trackers

Threat explorer/real-time detections

- Identify and analyze recent threats

Attack simulator

- Run realistic attack scenarios in your organization
 - Spear phishing
 - Attachment attack
 - Password spray



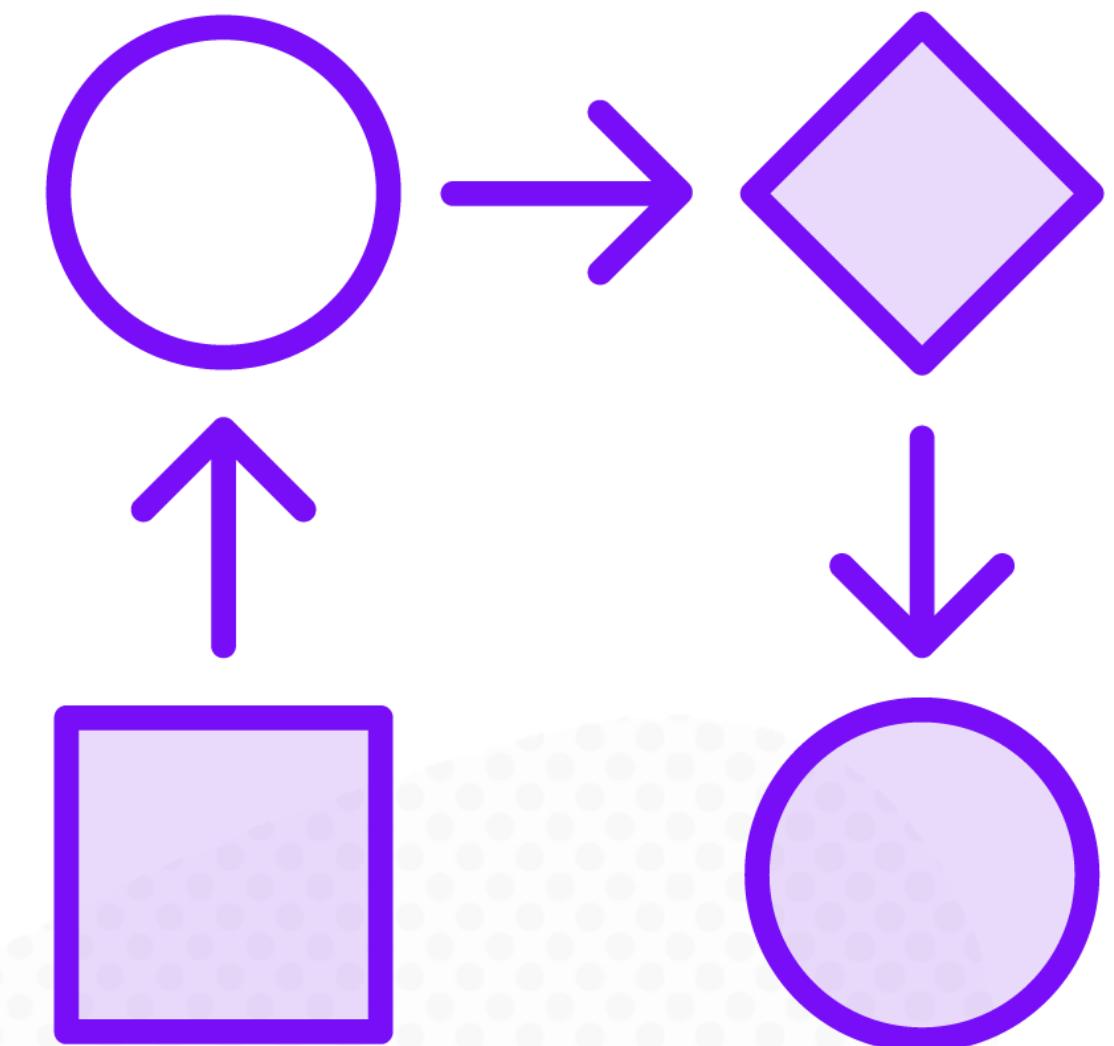
Automated Investigation and Response (AIR)

Set of security playbooks

Can be launched manually or automatically

Remediation actions are proposed

Security team approves or rejects them





Microsoft Defender for Identity



Microsoft Defender for Identity

Microsoft Defender for Identity is a cloud-based security solution that helps secure your identity monitoring across your organization. Defender for Identity is fully integrated with Microsoft Defender XDR, and leverages signals from both on-premises Active Directory and cloud identities to help you better identify, detect, and investigate advanced threats directed at your organization.



Microsoft Defender for Identity Key Areas

Monitor and profile user behavior and activities

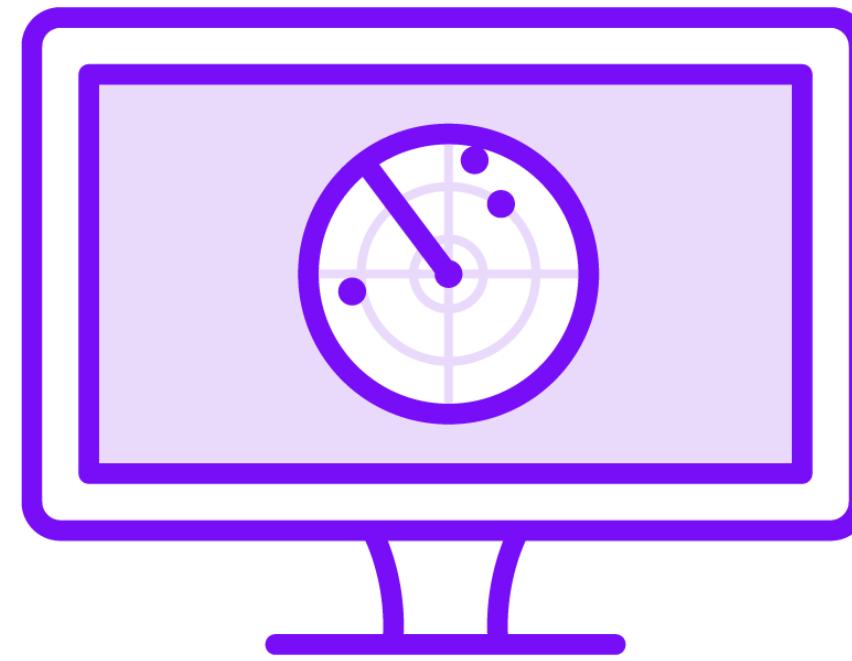
Protect user identities and reduce the attack surface

Identify suspicious activities and advanced attacks across the cyber-attack kill-chain

Investigate alerts and user activities



Monitor and Profile User Behavior and Activities



Monitors and analyzes

- User activities
- Permissions
- Group membership

Creates a behavioral baseline for each user

Identify anomalies in user behavior

- Insights into suspicious activities and events



Protect User Identities and Reduce the Attack Surface

Insights on identity configurations and security best practices

Reduce your organizational attack surface

Visual Lateral Movement Paths

Quickly understand how attackers can move laterally inside your network

Security reports to identify users and devices authenticating with clear-text passwords



Identify Suspicious Activities and Advanced Attacks

Reconnaissance

Identify rogue users and attackers' attempts to gain information

Compromised credentials

Identify attempts to compromise user credentials using brute force attacks, failed authentications, and other methods

Lateral movements

Detect attempts to move laterally inside the network to gain further control of sensitive users

Domain dominance

Highlighting attacker behavior if domain dominance is achieved, through remote code execution on the domain controller and other methods



Investigate Alerts and User Activities



Provide only relevant security alerts
Real-time organizational attack timeline



Microsoft Defender Vulnerability Management



Microsoft Defender Vulnerability Management

Defender Vulnerability Management delivers asset visibility, intelligent assessments, and built-in remediation tools for Windows, macOS, Linux, Android, iOS, and network devices.

Leveraging Microsoft threat intelligence, breach likelihood predictions, business contexts, and devices assessments, Defender Vulnerability Management rapidly and continuously prioritizes the biggest vulnerabilities on your most critical assets and provides security recommendations to mitigate risk.

<https://learn.microsoft.com/en-us/microsoft-365/security/defender-vulnerability-management/defender-vulnerability-management>



Microsoft Defender Vulnerability Management Key Areas

Continuous asset discovery and monitoring

Risk-based intelligent prioritization

Remediation and tracking



Continuous Asset Discovery and Monitoring



Visibility into software and vulnerabilities



Network share assessment



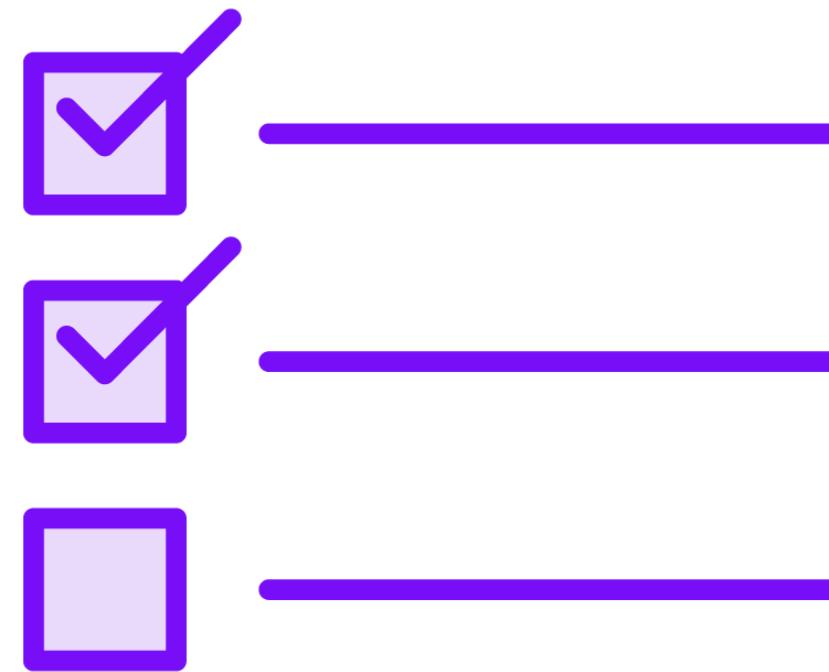
Browser extensions assessment



Digital certificates assessment



Risk-based Intelligent Prioritization



Prioritizes recommendations for your assets to reduce the biggest vulnerabilities

- From multiple sources including Microsoft's threat intelligence



Remediation and Tracking

Create remediation tasks in Microsoft Intune

Block vulnerable applications for specific device groups

Configure mitigations

Real-time monitoring of remediation activities



Microsoft Defender Vulnerability Management Dashboard

Microsoft 365 Defender

Search

Filter by device groups (72/72)

Microsoft Secure Score for Devices

Your score for devices: 50%

This score reflects the collective security configuration posture of your devices across OS, Application, Network, Accounts and Security Controls. Score is potentially impacted by active exceptions.

544/1079 points achieved

Category	Score
Application	7/52
OS	116/259
Network	72/122
Accounts	35/87
Security controls	314/559

Score for devices over time

51.6% 49.2% 03/28 04/11

Improve score

Microsoft Defender Vulnerability Management dashboard

Organization exposure score

Exposure score

This score reflects the current exposure associated with devices in your organization. Score is potentially impacted by active exceptions.

23/100

Low 0-29 Medium 30-69 High 70-100

Exposure score over time

Improve score

View vulnerability details

Threat awareness

15 devices exposed to CVE-2021-44228 (Log4j)

The Log4j vulnerability affects a Java logging component used in many software products. Devices running various apps and platforms with the vulnerable component might be exposed to remote code execution, which can lead to full attacker control.

Category	Count
Devices - onboarded	13
Devices - not onboarded	2
Vulnerable files	173
Vulnerable software	4

Top security recommendations

Recommendation	Exposed devices	Threats	Impact	Tags
Update Microsoft Windows 10 (OS and built-in applic...	21	🕒 🚨	▼ 5.11	
Update Microsoft Office	30	🕒 🚨	▼ 4.38	
Block untrusted and unsigned processes that ru...	54	🕒 🚨	▼ 4.01 + 9.00	+1

Show more Show exceptions

Top events (7 days)

Date (UTC)	Event	Originally impacted devices (%)
4/13/2022	Microsoft Windows 10 has 67 new vulnerabilities, impacting 21 devices	21 (11%)

Device exposure distribution

Exposure distribution

Exposed devices are easy targets for cybersecurity attacks. Ensure that these devices can receive security updates, have

Top remediation activities

Remediation activities

This table lists top activities that were generated from security recommendations



Microsoft Defender Threat Intelligence



Microsoft Defender Threat Intelligence (Defender TI)

Microsoft Defender Threat Intelligence (Defender TI) is a platform that streamlines triage, incident response, threat hunting, vulnerability management, and cyber threat intelligence analyst workflows when conducting threat infrastructure analysis and gathering threat intelligence.

Analysts spend a significant amount of time on data discovery, collection, and parsing, instead of focusing on what actually helps their organization defend themselves--deriving insights about the actors through analysis and correlation.



Defender TI articles

Narratives by Microsoft
that provide insights into:

- Threat actors
- Tooling
- Attacks
- Vulnerabilities

Link to actionable content
and key indicators of
compromise

The screenshot shows the Microsoft Defender Intel explorer interface. The left sidebar contains a navigation menu with items like Home, Incidents & alerts, Hunting, Actions & submissions, Threat intelligence, Threat analytics, Intel profiles, Intel explorer (which is selected), Intel projects, Learning hub, Trials, Partner catalog, Exposure management, Overview, and Attack surface. The main content area is titled "Intel explorer" and features a search bar with "All" and "Search" dropdowns. Below the search bar is a "Featured" section with two cards. The first card, titled "Diamond Sleet compromises TeamCity servers", includes a "Diamond Sleet" tag. The second card, titled "Flax Typhoon using legitimate software to quietly access...", includes a "Flax Typhoon" tag. Both cards have a small "Featured" badge.

Indicators

Microsoft Defender Threat Intelligence

Home > Goot to Loot—How a Gootloader Infect...

4 days ago

Goot to Loot—How a Gootloader Infection Led to Credential Access - ReliaQuest

OSINT Gootloader JavaScript CredentialTheft SystemBC RAT

Description Public indicators (21) Defender TI indicators (2)

Public indicators

Type	Name
URL	http://ddman-vpn.ddns.net/wordpress/xmlrpc.php
URL	https://airjust.de/xmlrpc.php
URL	https://anevaz.com.br/xmlrpc.php

Home > RiskIQ: New ManaTools Panel Identified

14 days ago

RiskIQ: New ManaTools Panel Identified

RiskIQ Malware AgentTesla ManaTools

Description Public Indicators (34) Defender TI Indicators (447)

Defender TI Indicators

Type	Name
MD5 Hash	1add7d2346cdfc5704a96626270f6df VirusTotal, ANY.RUN, Hybrid Analysis
MD5 Hash	1c70294dba38efa1cc674e36f259b3ef VirusTotal, ANY.RUN, Hybrid Analysis
MD5 Hash	67b07b9ff1e24ea2aabfc0d36e82f1c4 VirusTotal, ANY.RUN, Hybrid Analysis
MD5 Hash	7fb2c4b42d87a373d926f12485b8bd6f VirusTotal, ANY.RUN, Hybrid Analysis

Defender TI includes a database of CVE

Common vulnerabilities and exposures

Allows you to quickly find information on CVE including key context and priority score

Intel Explorer > CVE-2023-41721

Vulnerability search

CVE-2023-41721

Priority score : 53 Medium | CVSS 2 : No score | CVSS 3 : 5.3 Medium | Published : October 25, 2023

Description Affected components (1)

Description

Instances of UniFi Network Application that (i) are run on a UniFi Gateway Console, and (ii) are versions 7.5.176 and earlier, implement device adoption with improper access control logic, creating a risk of access to device configuration information by a malicious actor with preexisting access to the network.

Affected Products: UDM UDM-PRO UDM-SE UDR UDW

Mitigation: Update UniFi Network to Version 7.5.187 or later.

References (advisories, solutions, and mitigation)

This information is provided "as is". Microsoft recommends that you validate applicability before implementing in your own environment.

- <https://community.ui.com/releases/Security-Advisory-Bulletin-036-036/81367bc9-2a64-4435-95dc-bbe482457615>

Intelligence

POC Available

Chatter observed

Active exploitation observed

Published POCs (0)



Data sets give you access to search for any domain, IP and find information from a wide variety of sources

Defender TI provides reputation scoring and analyst insights

The screenshot shows a detailed analysis page for a domain or IP address. At the top, a red box highlights the 'Malicious (Score : 100)' status. Below this, a navigation bar includes tabs for Summary, Resolutions, WHOIS, Certificates, Trackers, Components, Host pairs, Cookies, Services, Reverse DNS, and Articles. The WHOIS tab is currently selected. A large section below displays 'Reputation' details, including two entries: 'MDTI Intel Article' (Severity: Red Diamond) and 'ASN' (Severity: Orange Square). The 'Analyst insights' section is also highlighted with a red box. At the bottom, three status indicators are shown: 'Blocklisted by Third Party', 'Open Port Last Detected 1 day...', and 'Hosts a Web Server'. A note states 'Not triggered: Not a Tor Exit Node, Not a Proxy'.

Malicious (Score : 100)

First seen: 2015-03-30 | Last seen: 2023-06-27 | Netblock: ASN: Organization:

Summary Resolutions WHOIS Certificates Trackers Components Host pairs Cookies Services Reverse DNS Articles

Reputation: Malicious (Score: 100)

Severity	Rule	Description
Red Diamond	MDTI Intel Article	Ruby Sleet targeting government and defense entities with job description-themed lures and malicious .scr
Orange Square	ASN	Infrastructure hosted by this ASN frequently exhibits suspicious behavior

Analyst insights

Blocklisted by Third Party Open Port Last Detected 1 day... Hosts a Web Server

Not triggered: Not a Tor Exit Node, Not a Proxy

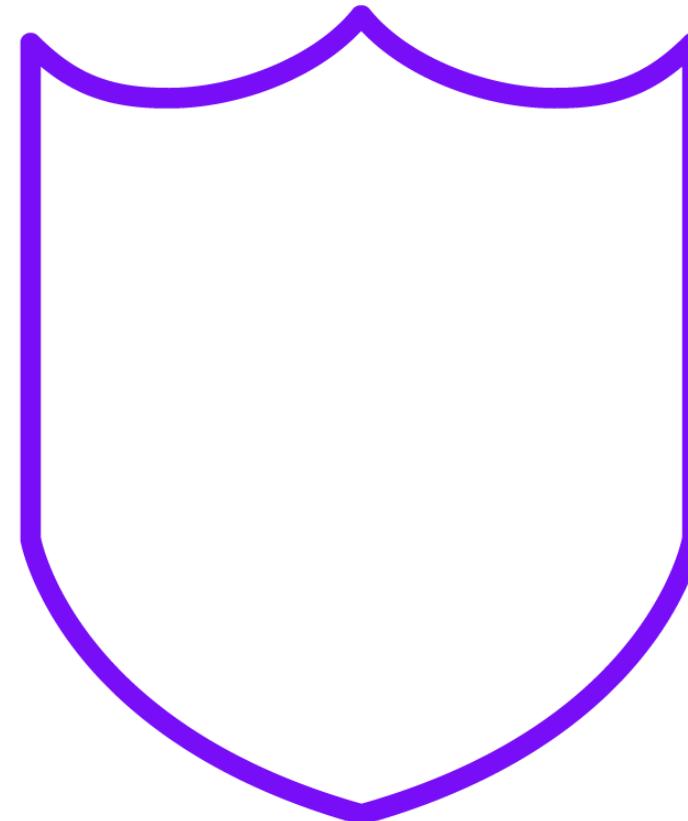




Microsoft Security Copilot



Microsoft Security Copilot



Amplify your security team with the power of AI

Combines the power of large language models (LLMs) with a security-specific model from Microsoft

- Security specific model is trained by Microsoft and over 65 trillion daily signals

Integrates with Microsoft Defender XDR and Microsoft Sentinel



Incident Response

<Vlad will insert MS provided short video in post editing similar as in Copilot course>



Threat Hunting

<Vlad will insert MS provided short video in post editing similar as in Copilot course>



Security Reporting

<Vlad will insert MS provided short video in post editing similar as in Copilot course>



Reverse Engineering

Reverse-engineer exploits

Promptbook that grabs exploit(s) and reverse-engineers them.

If present, reverse engineer the script that downloaded the exploit. Explain the capabilities of the script and give each section a short heading and a one-sentence description for each point.

Produce a visual to explain the activity of the download, the exploit and how it moved through the incident.

Produce a visual to explain the activity of the download, the exploit and how it moved through the incident.

12:40 PM

</>

```
graph LR; US((Unknown source)) --> DT((Devon Torres)); DT --> WB[WorkstationB]; WB --> ON[OneNote.exe]; SalesLeads[SalesLeads (1).onepkg] --> WScript[WScript.exe]; WScript --> P1[Powershell.exe]; P1 --> ID[Invoke DoorBreach.ps1]; ID --> DE[Doorbreach.exe.exe]; DE --> DC01[DC01.contoso...]; DE --> P2[Powershell.exe]; DE --> MW[Malicious Website]; DE --> C2[C2 Server];
```

Module Conclusion



Microsoft Defender for Endpoint

Microsoft Defender for Office 365

Microsoft Defender for Identity

**Microsoft Defender Vulnerability
Management**

Microsoft Defender Threat Intelligence

Microsoft Security Copilot



Up Next:

Discover and Control Shadow IT with Defender for Cloud Apps

