

# Introduction to Microsoft Defender XDR



**Vlad Catrinescu**

Microsoft MVP | Independent Consultant

@vladcatrinescu | [VladTalksTech.com](http://VladTalksTech.com) | [YouTube.com/@VladTalksTech](https://YouTube.com/@VladTalksTech)

# Overview



**Introduction to Microsoft Defender XDR**

**Microsoft Defender portal**

**Microsoft Secure Score**



# Introduction to Microsoft Defender XDR



# Microsoft Defender XDR

**Microsoft Defender XDR is a unified pre- and post-breach enterprise defense suite that natively coordinates detection, prevention, investigation, and response across endpoints, identities, email, and applications to provide integrated protection against sophisticated attacks.**

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



**Microsoft Defender XDR was previously named Microsoft 365 Defender. You might still see references to the old name it in documentation today.**



# Microsoft Defender XDR Services

**Microsoft Defender  
for Endpoint**

**Microsoft Defender  
for Office 365**

**Microsoft Defender  
for Identity**

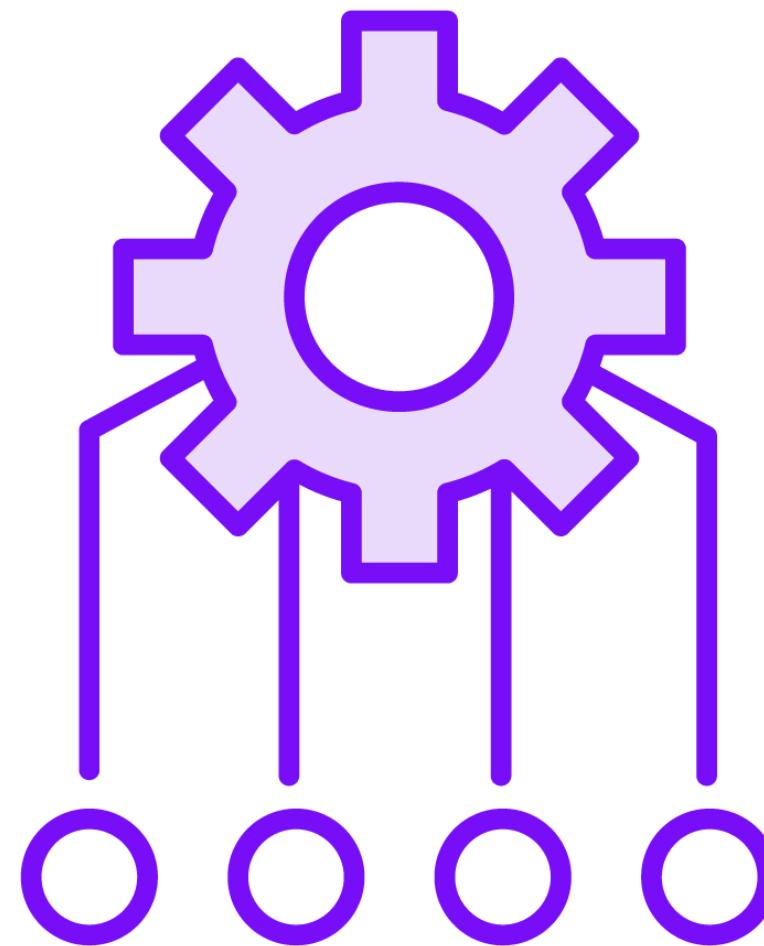
**Microsoft Defender  
Vulnerability  
Management**

**Microsoft Defender  
Threat Intelligence**

**Microsoft Defender  
for Cloud Apps**



# An Integrated Solution



**Microsoft Defender XDR is an integrated – cross domain solution**

- Stiches together signals from
  - Endpoints
  - Identities
  - Data
  - Applications
- Groups signals from all domains in incidents
  - Allows security teams to see the full picture



# Microsoft Defender XDR Incident

Microsoft Defender

Search

Incidents & alerts

Incidents

Alerts

Hunting

Actions & submissions

Threat intelligence

Learning hub

Trials

Partner catalog

Exposure management

Overview

Attack surface

Exposure insights

Secure score

Assets

Devices

Identities

Incidents > Multi-stage incident involving Initial access & Exfiltration on multiple endpoints reported by multiple sources

## Multi-stage incident involving Initial access ...

Ask Defender Experts Activity log

Attack story Alerts (611) Assets (206) Investigations (0) Evidence and Response (12) Summary

Alerts and categories

Active alerts 611/611 Tactics 6 Other categories 1

InitialAccess 565 / 611

DefenseEvasion 3 / 611

CredentialAccess 1 / 611

View all categories

Scope

Top impacted assets

Impacted devices 2 Impacted users 3

Entity	Risk level/inve...	Tags
vhcal4hci		
prd00010		
ranjitsawant@microsoft.com		
wprietogomez@microsoft.com		
nialdaag@microsoft.com		

Incident information

Guided Response

Associated Incidents

This incident might be associated with other incidents.

Incident ID	Reason	Entity
58571	TimeSeries	
58571	SameUserCred...	
58571	SameUserCred...	
53628	TimeSeries	

View all associated incidents

# Microsoft Defender XDR Incident

Microsoft Defender

Search

Incidents > Multi-stage incident involving Initial access & Exfiltration on multiple endpoints reported by multiple sources

## Multi-stage incident involving Initial access ...

Attack story   Alerts (611)   Assets (206)   Investigations (0)   Evidence and Response (12)   Summary

Alerts

611/611 Active alerts

Nov 29, 2023 2:38 AM • New  
TI map IP entity to SigninLogs  
Partner Demo

Nov 29, 2023 3:38 AM • New  
TI map IP entity to SigninLogs  
Partner Demo

Nov 29, 2023 5:38 AM • New  
TI map IP entity to SigninLogs  
Partner Demo

Nov 29, 2023 7:38 AM • New  
TI map IP entity to SigninLogs  
Partner Demo

Nov 29, 2023 10:38 AM • New  
TI map IP entity to SigninLogs  
Partner Demo

Incident graph

Layout Group similar nodes

2 Users

4 IPs

24.210.46.253

Azure Portal

pdemo

Microsoft 365

vhcalal4hci

newspouser

162 Users

Communication Association

MDTI Suspicious

Manage incident   Activity log

Incident details

Assigned to Unassigned   Incident ID 60716

Classification Not set   Categories Initial access, Defense evasion, Credential access

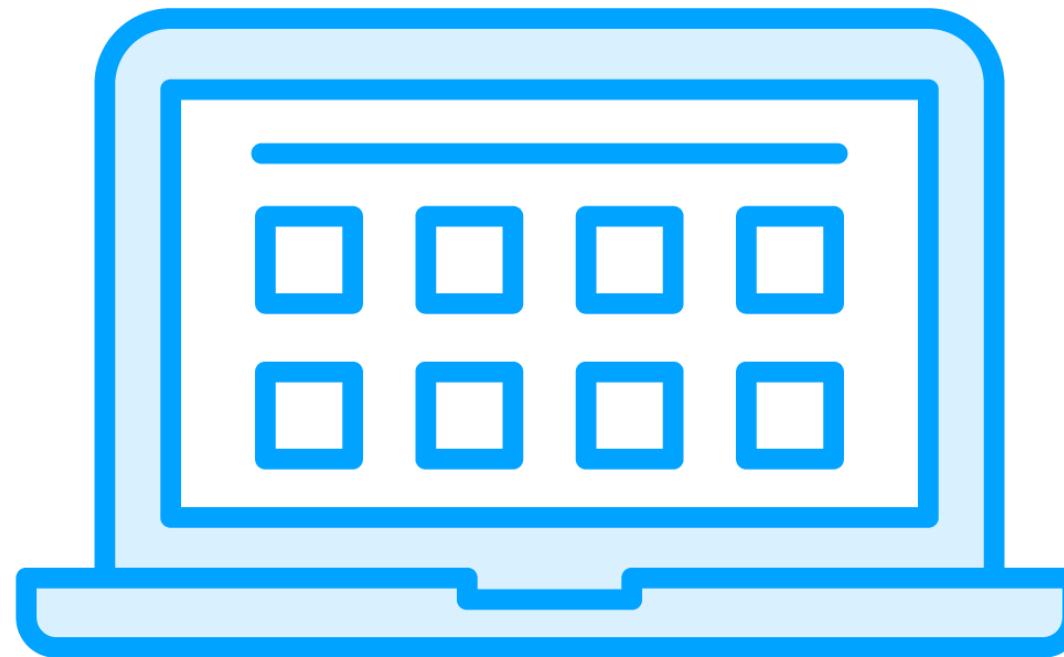
The screenshot shows the Microsoft Defender XDR interface for managing incidents. On the left, a navigation sidebar lists various security modules like Alerts, Hunting, Threat intelligence, and Assets. The main area displays a detailed view of a specific incident titled 'Multi-stage incident involving Initial access ...'. It includes a timeline of five active alerts from November 29, 2023, all related to 'TI map IP entity to SigninLogs' and attributed to 'Partner Demo'. To the right is an 'Incident graph' showing connections between various entities: users, IP addresses, and cloud services like Azure Portal and Microsoft 365. Nodes are color-coded by risk level: red for High and blue for Active. A legend indicates that red dots represent 'High' risk and blue dots represent 'Active'. Below the graph, incident details are listed, including the status of assigned users and the incident ID. The bottom right corner features a circular navigation element.



# The Microsoft Defender Portal



# The Microsoft Defender Portal



**Central location for monitoring and managing security services**

- Identities
- Data
- Devices
- Apps
- Infrastructure

Accessible at <https://security.microsoft.com>



# Only Certain Roles Have Access to the Defender Portal

Global Administrator

Security Administrator

Security Operator

Security Reader



# Microsoft Defender Portal

Microsoft Defender

Search

Home

Incidents & alerts

Hunting

Actions & submissions

Threat intelligence

Learning hub

Trials

Partner catalog

Exposure management

Overview

Attack surface

Exposure insights

Secure score

Assets

Devices

Identities

Endpoints

Defender Experts

Updated 2023-12-13 11:58am

**0 incidents** require your action

**Your service is working**

Our analysts are gathering insights from your network

[View report](#)

Connected SaaS apps

Defender for Cloud Apps protects your SaaS apps with security configuration recommendations, threat protection and information protection. [Learn more](#)

SaaS app connectors by health status

Healthy	Needs attention	Connection errors
8	0	1

[Connect your SaaS apps](#)

Threat analytics

**11 threats require action**

**High-impact threats** ⓘ

Technique profile: Brute-force attacks 29,953 / 29,953

Threat overview: Cloud identity abuse 9,959 / 10,148

Active Alerts Resolved Alerts No Alerts

Highest exposure threats

Actor profile: Citrine Sleet 0

Microsoft Secure Score

**Secure Score: 56.77%**

910.59/1604 points achieved

Microsoft Secure Score is a representation of your organization's security posture, and your opportunity to improve it.

Score last calculated 12/12

Identity 75.11%

Data 88.89%

Device 53.1%

Apps 58.48%

[Improve your score](#) [View history](#)

Users at risk

**155 users at risk**

View all users

Security news feed

Tweets from @msftsecurity

Follow

Discovered devices to onboard

# Microsoft Defender Portal: Customization

X

## Customize your navigation pane

X

Show or hide navigation items in your navigation pane. Other admins won't see your changes.

### Selected items appear in the navigation pane

Don't worry, you can find these hidden items by selecting **Show all** from the navigation pane.

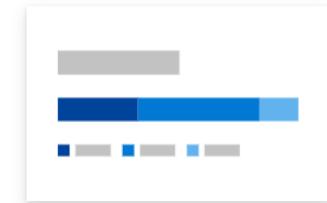
- Select all
- Incidents & alerts
- Hunting
- Actions & submissions
- Threat intelligence
- Learning hub
- Trials
- Partner catalog
- Overview
- Attack surface
- Exposure insights
- Secure score
- Devices
- Identities
- Vulnerability management

**Save** **Cancel**

## Add cards to your home page



### Attack simulation training



### Devices with active malware

Intune-managed devices with active, unresolved malware. If a device has multiple malware detections, it may be counted more than once.



### Device health



### Devices discovered in the last 7 days



### Microsoft Sentinel integration



# Microsoft Secure Score

Quick way to understand your security posture

Helps prioritize actions based on potential to reduce risk

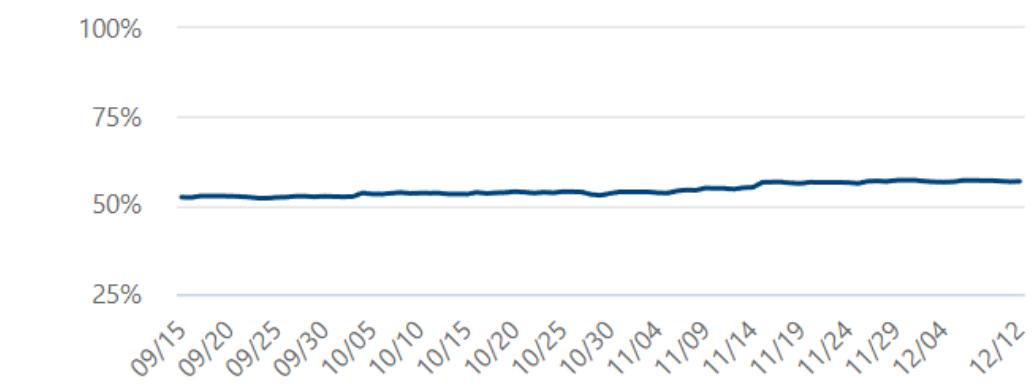
Bigger the security impact – more points

Your secure score

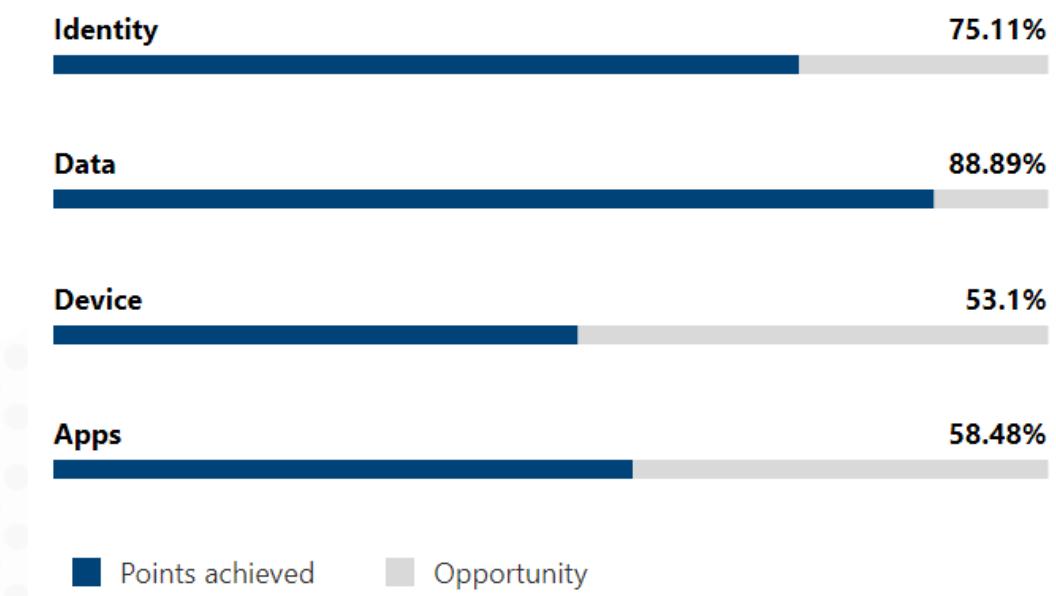
Include ▾

**Secure Score: 56.77%**

910.59/1604 points achieved



Breakdown points by: Category ▾



# Microsoft Secure Score Recommendation

The screenshot shows the Microsoft Defender interface with the 'Secure score' section selected. A specific recommendation is highlighted: 'Ensure multifactor authentication is enabled for all users in administrative roles'. This recommendation has a score of 2.32 / 10 and is categorized under Identity and Azure Active Directory, protecting against Password Cracking, Account Breach, and Elevation of Privilege.

**Microsoft Secure Score**

There are new permissions options available for Secure Score. You can now choose to enable or disable them.

Actions you can take to improve your Microsoft Secure Score. Score updated 1 hour ago.

Export

Rank	Recommended action
1	Turn on Firewall in macOS
2	Turn on Microsoft Defender Antivirus real-time protection
33	Ensure multifactor authentication is enabled for all users in administrative roles
111	Turn on Microsoft Defender for Endpoint sensor
112	Fix Microsoft Defender for Endpoint sensor data collection
113	Fix Microsoft Defender for Endpoint impaired communication
119	Update Microsoft Defender for Endpoint core components
120	Fix Microsoft Defender for Endpoint impaired communication
121	Fix Microsoft Defender for Endpoint sensor data collection
143	Turn on real-time protection

**Description**

Requiring multifactor authentication (MFA) for administrative roles makes it harder for attackers to access accounts. Administrative roles have higher permissions than typical users. If any of those accounts are compromised, your entire organization is exposed. At a minimum, protect the following roles:

- Global administrator
- Authentication administrator
- Billing administrator
- Conditional Access administrator
- Exchange administrator
- Helpdesk administrator
- Security administrator
- SharePoint administrator
- User administrator

**Implementation status**

You have 76 out of 99 users with administrative roles that aren't registered and protected with MFA.

**User impact**

First, users with administrative roles need to register for MFA. After each admin is registered, your policies then determine when they're prompted for the additional authentication factors.

Manage in Microsoft Azure Share

**Details**

- Points achieved: 2.32 / 10
- History: 2 events
- Category: Identity
- Product: Azure Active Directory
- Protects against: Password Cracking, Account Breach, Elevation of Privilege

## Products included in Secure Score

Currently there are recommendations for the following products:

- App governance
- Microsoft Entra ID
- Citrix ShareFile
- Microsoft Defender for Endpoint
- Microsoft Defender for Identity
- Microsoft Defender for Office
- Docusign
- Exchange Online
- Github
- Microsoft Defender for Cloud Apps
- Microsoft Information Protection
- Microsoft Teams
- Okta
- Salesforce
- ServiceNow
- SharePoint Online
- Zoom

**Secure Score includes recommendations for both Microsoft and third-party products**

**Microsoft keeps adding supported products**

**Check out the latest available products at**

- <https://learn.microsoft.com/en-us/microsoft-365/security/defender/microsoft-secure-score#products-included-in-secure-score>



# Demo



**Microsoft Defender portal**  
**Microsoft Secure Score**



# Module Conclusion



## Introduction to Microsoft Defender XDR

- Microsoft Defender for Endpoint
- Microsoft Defender for Office 365
- Microsoft Defender for Identity
- Microsoft Defender Vulnerability Management
- Microsoft Defender Threat Intelligence
- Microsoft Defender for Cloud Apps

## Microsoft Defender Portal

- Central location to manage the security settings of your organization

## Microsoft Secure Score

- Quick way to understand your security posture



**Up Next:**

# **Extended Detection and Response with Microsoft Defender XDR**

---

