

Microsoft Defender for Identity (MDI)

Introduction and Technical Overview

Liju Varghese
Sr. CSA-Engineering



Conditions and Terms of Use

Microsoft Confidential

This training package is proprietary and confidential, and is intended only for uses described in the training materials. Content and software is provided to you under a Non-Disclosure Agreement and cannot be distributed. Copying or disclosing all or any portion of the content and/or software included in such packages is strictly prohibited.

The contents of this package are for informational and training purposes only and are provided "as is" without warranty of any kind, whether express or implied, including but not limited to the implied warranties of merchantability, fitness for a particular purpose, and non-infringement.

Training package content, including URLs and other Internet Web site references, is subject to change without notice. Because Microsoft must respond to changing market conditions, the content should not be interpreted to be a commitment on the part of Microsoft, and Microsoft cannot guarantee the accuracy of any information presented after the date of publication. Unless otherwise noted, the companies, organizations, products, domain names, e-mail addresses, logos, people, places, and events depicted herein are fictitious, and no association with any real company, organization, product, domain name, e-mail address, logo, person, place, or event is intended or should be inferred.

Copyright and Trademarks

© 2016 Microsoft Corporation. All rights reserved.

Microsoft may have patents, patent applications, trademarks, copyrights, or other intellectual property rights covering subject matter in this document. Except as expressly provided in written license agreement from Microsoft, the furnishing of this document does not give you any license to these patents, trademarks, copyrights, or other intellectual property.

Complying with all applicable copyright laws is the responsibility of the user. Without limiting the rights under copyright, no part of this document may be reproduced, stored in or introduced into a retrieval system, or transmitted in any form or by any means (electronic, mechanical, photocopying, recording, or otherwise), or for any purpose, without the express written permission of Microsoft Corporation.

For more information, see Use of Microsoft Copyrighted Content at

<http://www.microsoft.com/en-us/legal/intellectualproperty/Permissions/default.aspx>

DirectX, Hyper-V, Internet Explorer, Microsoft, Outlook, OneDrive, SQL Server, Windows, Microsoft Azure, Windows PowerShell, Windows Server, Windows Vista, and Zune are either registered trademarks or trademarks of Microsoft Corporation in the United States and/or other countries. Other Microsoft products mentioned herein may be either registered trademarks or trademarks of Microsoft Corporation in the United States and/or other countries. All other trademarks are property of their respective owners.

Agenda

**Microsoft
Defender for
Identity
General
Overview**

**How Does
Microsoft
Defender for
Identity
Work?**

**Microsoft
Defender for
Identity
And
Technical
Overview**

**Questions and
Answers**



The Problem

Traditional IT security tools are typically:



Complex

Initial setup, fine-tuning, and the creation of rules, thresholds, and baselines can take a long time



Prone to false positives

You receive too many reports in a day with false positives that require valuable time that you do not have.



Designed to help protect the perimeter

When user credentials are stolen and attackers are inside the network, your current defenses provide limited protection.

Start with the right assumptions!

Your **ARE** a **TARGET**

You **CANNOT DEFEND** against **EVERYTHING**

Your infrastructure **IS**, or **WILL BE**, **COMPROMISED**

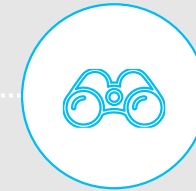
Assume Compromise!

Based on all of this information,
what should you assume?

How do I detect **compromised credentials**?



How do I **detect attackers** moving laterally in my environment?



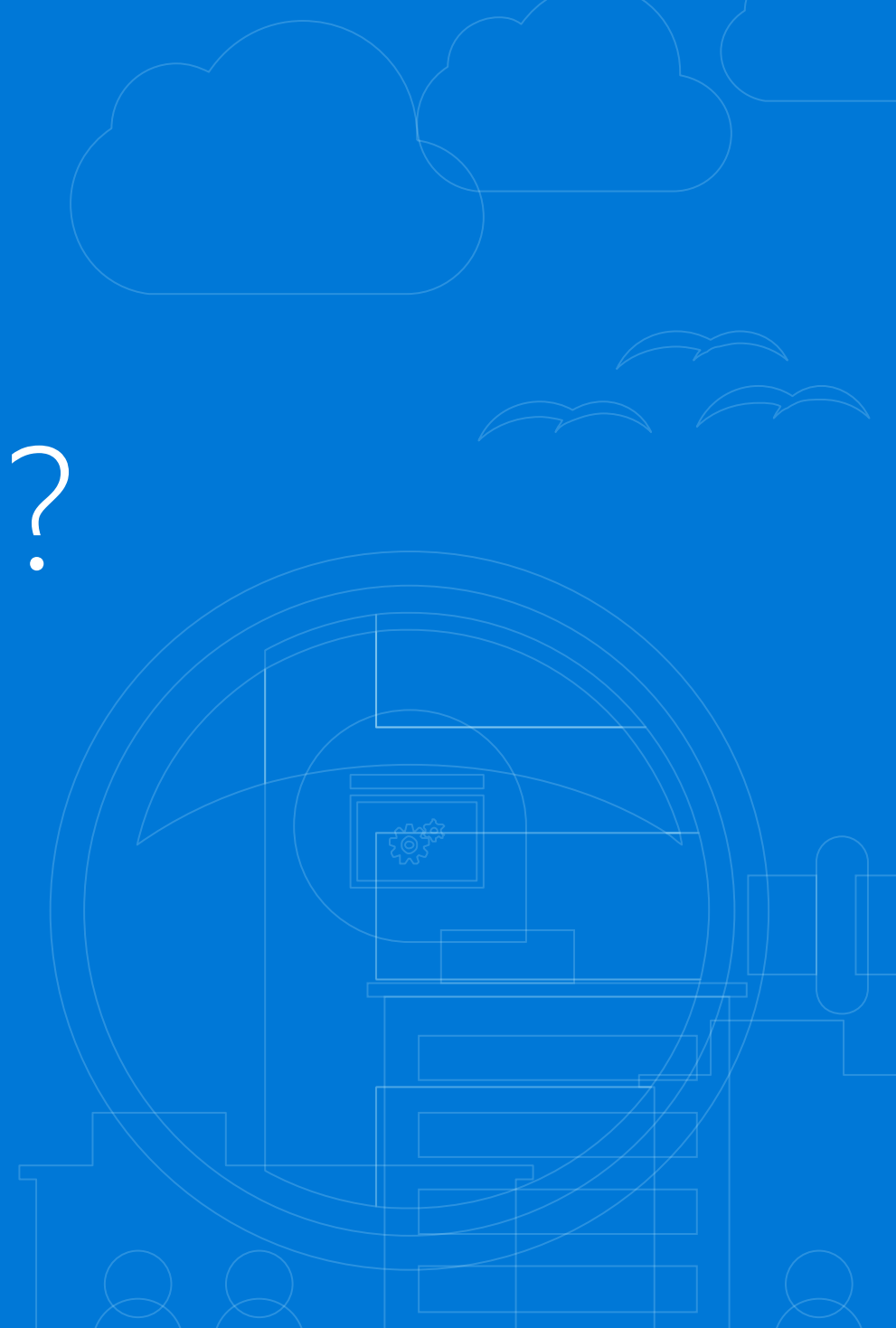
How do I **detect Pass-the-Hash?**
Pass-the-Ticket?



Aren't **rule-based security solutions** enough?



What is the solution?



Microsoft Defender for Identity



User and Entity Behavior Analytics (UEBA)

Monitors behaviors of users and other entities by using **multiple data-sources**

Profiles behavior and detects anomalies by using **machine learning** algorithms

Evaluates the activity of users and other entities to detect **advanced attacks**

“

Enterprises successfully use **UEBA** to detect malicious and abusive behavior that otherwise went unnoticed by existing security monitoring systems, such as SIEM and (DLP) .

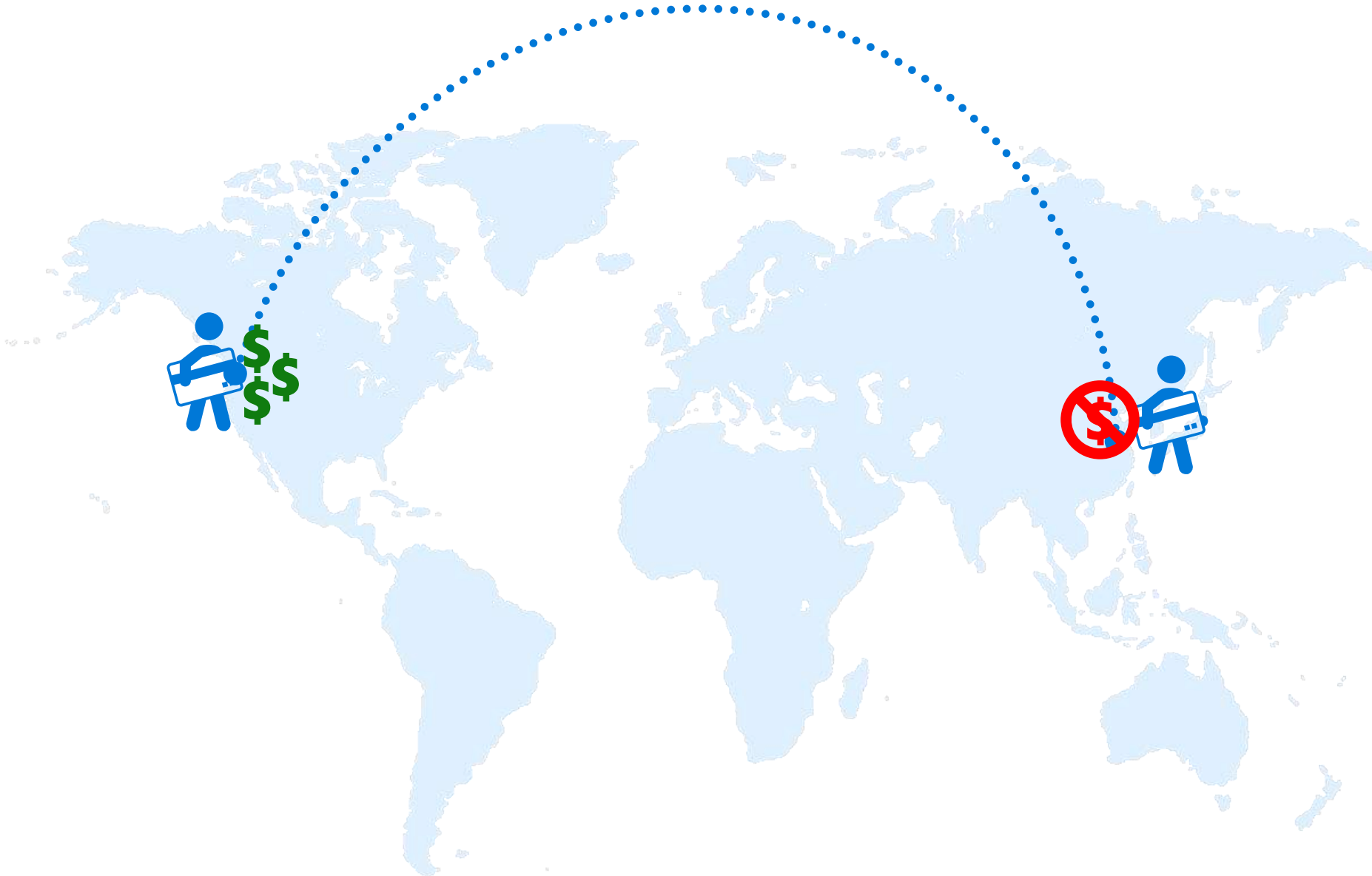
”

Gartner[®]

SIEM: Security Information and Event Management

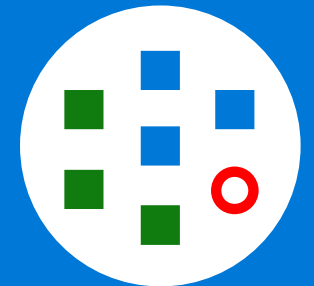
DLP: MDI loss prevention

Behavior Analytics In Practice



Credit card companies monitor cardholders' behavior.

By observing purchases, they learn what is typical behavior for each buyer.



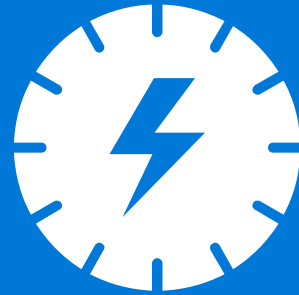
If there is any abnormal activity, they will notify the cardholder to verify charge.

Microsoft Defender for Identity

A platform to identify advanced security attacks ***before*** they cause damage



Behavioral
Analytics

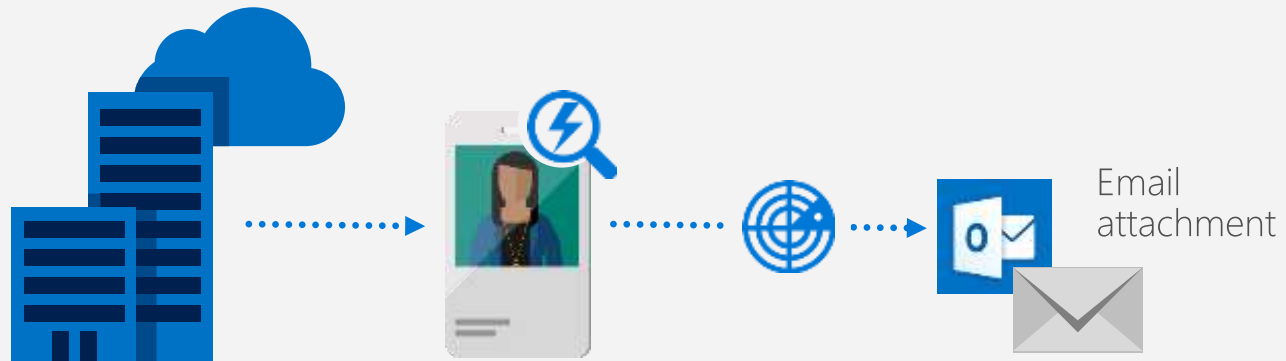


Detection for known
attacks and issues



Microsoft Defender
for Identity

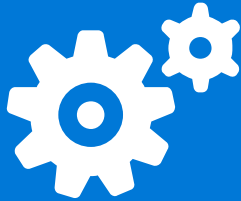
Microsoft Defender for Identity brings the behavioral analytics concept to IT and the organization's users.



Benefits of Microsoft Defender for Identity



Detect threats fast with Behavioral Analytics



Adapt as fast as your enemies



Focus on what is important by using the simple attack timeline



Reduce the fatigue of false positives



Prioritize and plan for next steps

Microsoft Defender for Identity: Differentiating Factors



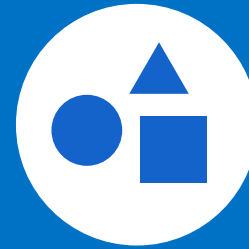
It is fast

- No need to create rules, thresholds, or baselines
- Straightforward and fast deployment



It is reliable

- Takes advantage of unique data sources, combines entity contextual deep packet inspection (DIP) and logs
- Consistent learning and abnormal behavior identification
- Detection of human and non-human service accounts
- Network name resolution



It provides clear information

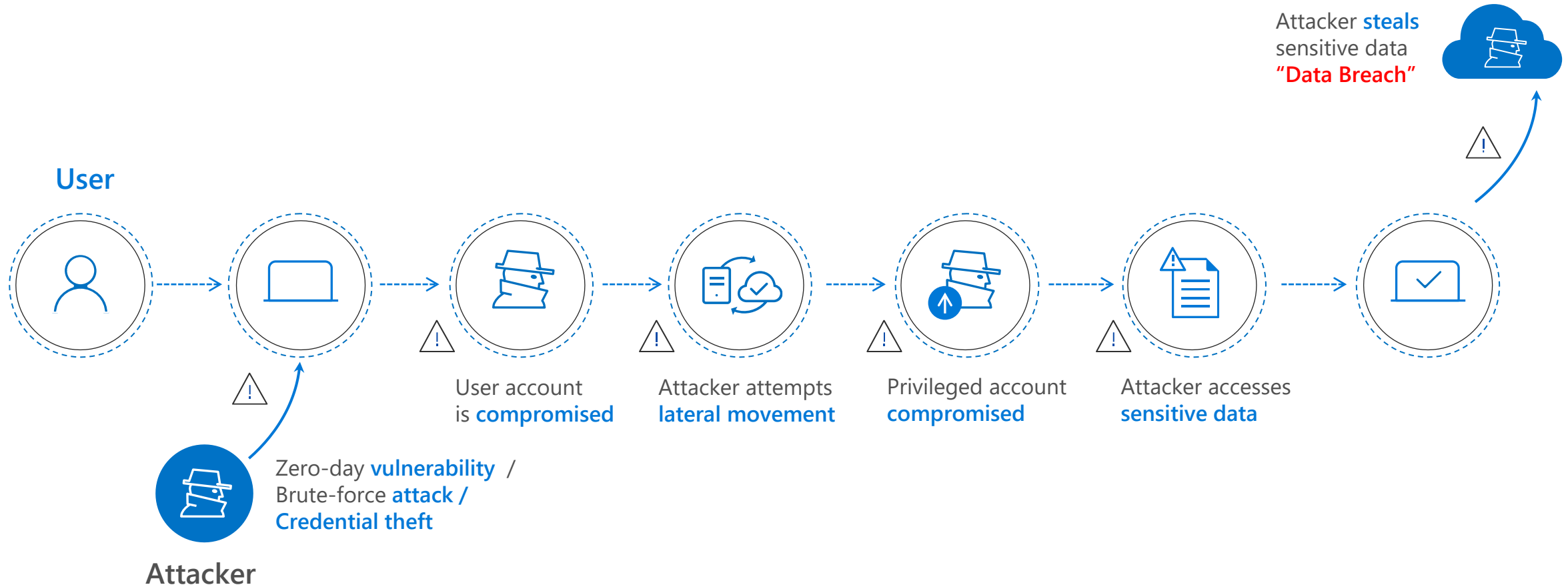
- Functional, clear, and actionable attack timeline, that shows the who, what, when, and how in near real time
- Continuously updated reports



It is innovative

- Patented technology
- Combines deterministic and machine learning based algorithms
- The UEBA product that allows user input

The anatomy of an attack

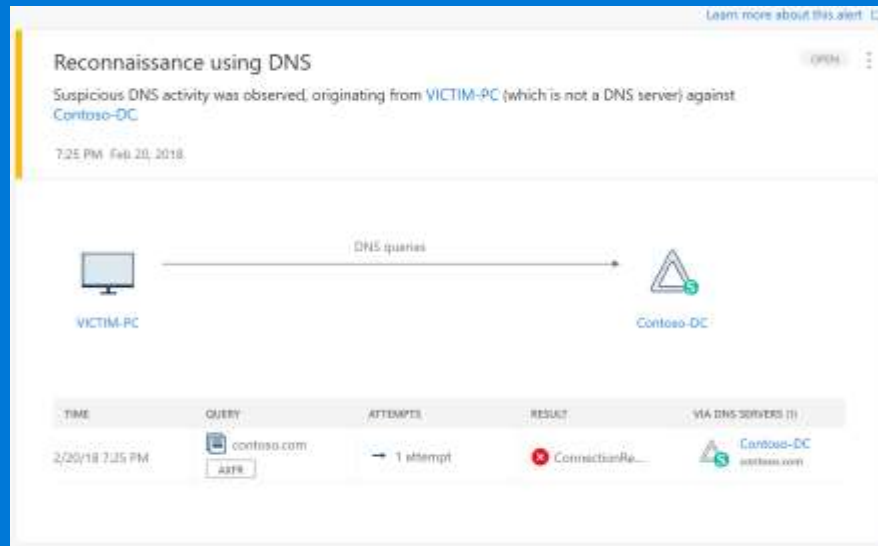


Anomalous user behavior
Unfamiliar sign-in location



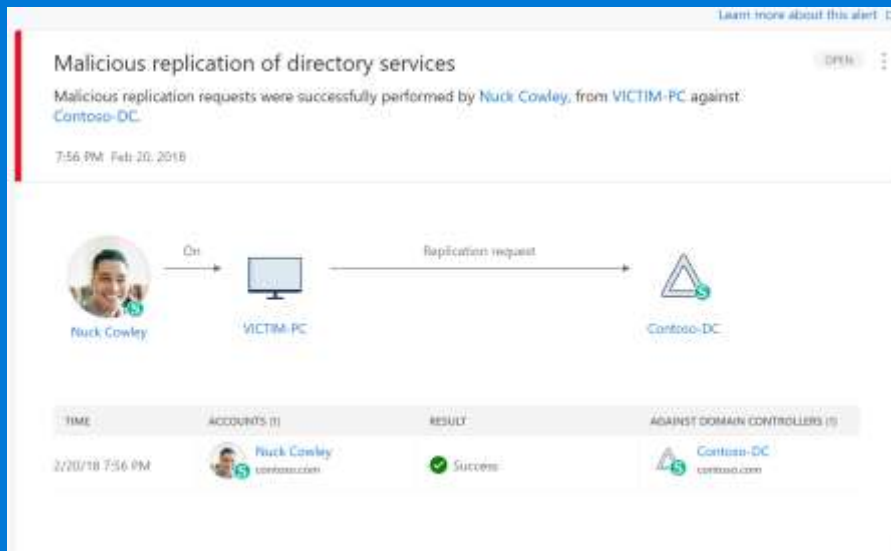
Lateral movement attacks
Escalation of privileges
Account impersonation

Detected Threats



Reconnaissance and brute force suspicious activities:

- Account enumeration reconnaissance
- Active Directory attributes reconnaissance (LDAP)
- Network mapping reconnaissance (DNS)
- Security principal reconnaissance (LDAP)
- User and Group membership reconnaissance (SAMR)
- User and IP address reconnaissance (SMB)
- Suspected Brute force attacks (LDAP, Kerberos, SMB)



Identity theft suspicious activities:

- Pass-the-ticket
- Pass-the-hash
- Over-Pass-the-hash
- Skeleton key
- MS11-013 Elevation of Privilege
- Forged PAC (MS14-068)
- Golden ticket
- Remote execution
- Malicious DPAPI Request
- Suspicious communications

Detected Threats

Remote code execution attempt

The following remote code execution attempts were performed on Contoso-DC from VICTIM-PC:

- Successful remote scheduling of one or more tasks.
- Successful remote execution of one or more WMI methods by Nuck Cowley.

7:52 PM Feb 20, 2018

TIME ACCOUNTS (1) CREATED RESULT VIA DOMAIN CONTROLLERS (1)

2/20/18 7:52 PM	Nuck Cowley contoso.com	Unknown W...	Success	Contoso-DC contoso.com
2/20/18 7:52 PM	Nuck Cowley contoso.com	Unknown Task adsisapi.com...	Success	Contoso-DC contoso.com

Honeytoken activity

The following activities were performed by Lydia Alexander:

- Attempted to login to VICTIM-PC via Contoso-DC.

21:17 20 Feb 2018

TIME FROM (1) ACCESSSED RESULT VIA DOMAIN CONTROLLERS (1)

20/02/2018 21:17	VICTIM-PC contoso.com Kerberos (Traffic)	contoso.com to KRB5TGT Login	Failure	Contoso-DC contoso.com
------------------	--	------------------------------------	---------	---------------------------

Abnormal behavior suspicious activities:

- Abnormal behavior based on authentication, authorization, and working hours (machine learning algorithm)
- Abnormal modification of sensitive groups
- Massive object deletion

Security issues:

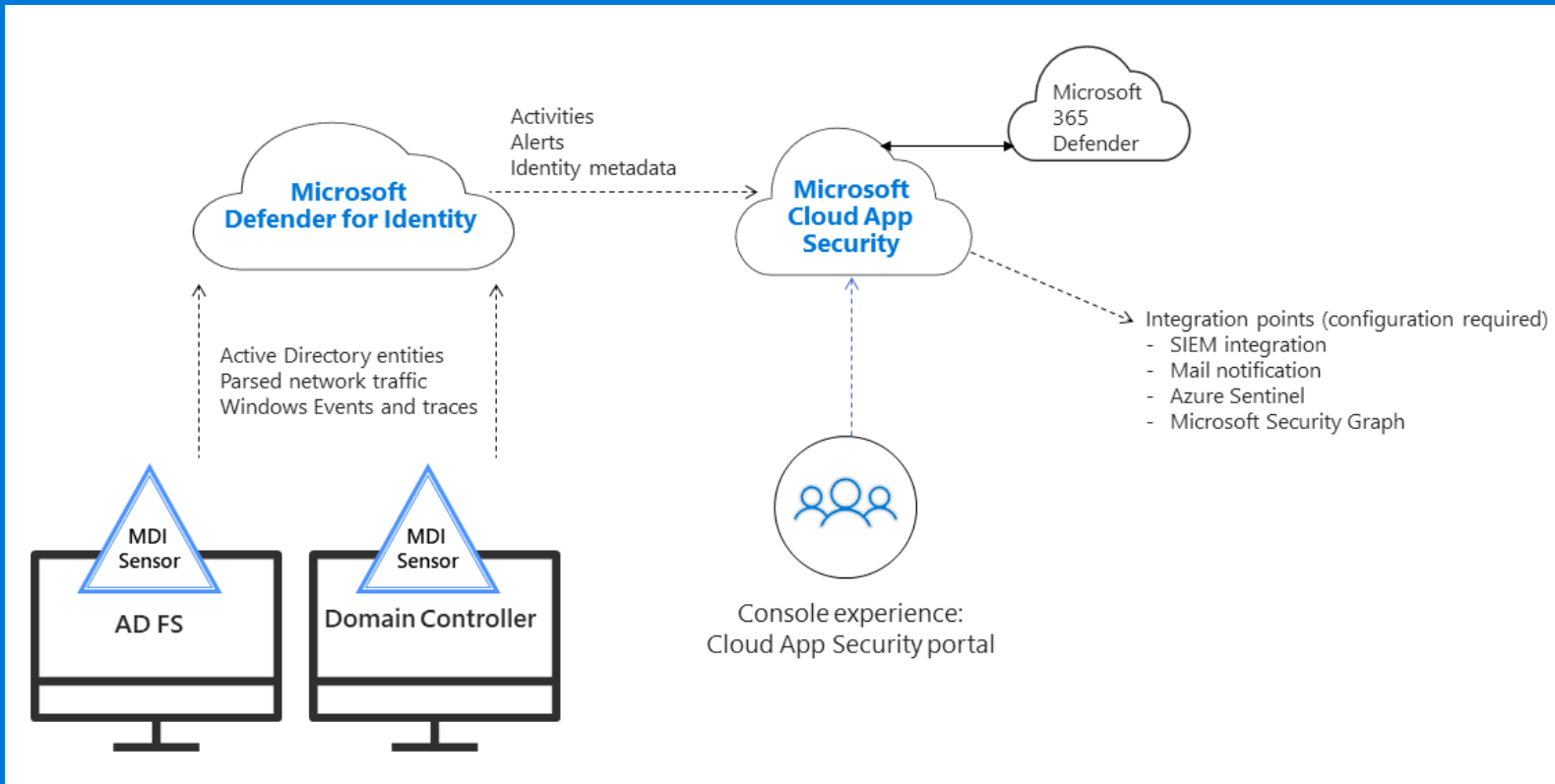
- Sensitive account exposed in plain text authentication
- Service exposing accounts in plain text authentication
- Remote Execution attempts
- Honey token accounts suspicious activity
- Malicious replication requests
- Computer account broken trust
- Data exfiltration over SMB

How Does MDI Work?



How MDI Works

1. Analyze



After installation:

- Install MDI sensor on DCs or ADFS servers to monitor their traffic directly, without the need for a dedicated server or configuration of port mirroring.
- Or configure a dedicated server that monitors the traffic from your domain controllers using either port mirroring or a network TAP.

Note: MDI Sensor uses an agent, rather than port-mirroring

How MDI Works

2 Learn



MDI :

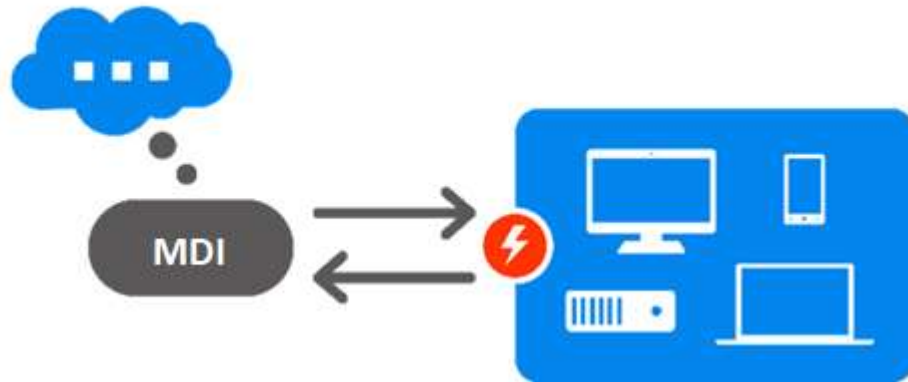
- Automatically starts learning and profiling entity behavior
- Identifies normal behavior for entities
- Learns continuously to update the activities of the users, devices, and resources

What is an entity?

An entity represents users, devices, or resources

How MDI Works

3 Detect



Microsoft Defender for Identity:

- Looks for abnormal behavior and identifies suspicious activities
- Only raises red flags if abnormal activities are contextually aggregated
- Uses world-class security research to detect security risks and attacks in near real time, based on attackers' Tactics, Techniques, and Procedures (TTPs)

MDI not only compares the entity's behavior to its own, but also to the behavior of other entities in the **interaction path**.

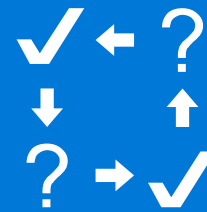
How MDI Works

4 Alert

MDI reports all suspicious activities on a simple, functional, usable attack timeline



MDI identifies
Who?
What?
When?
How?

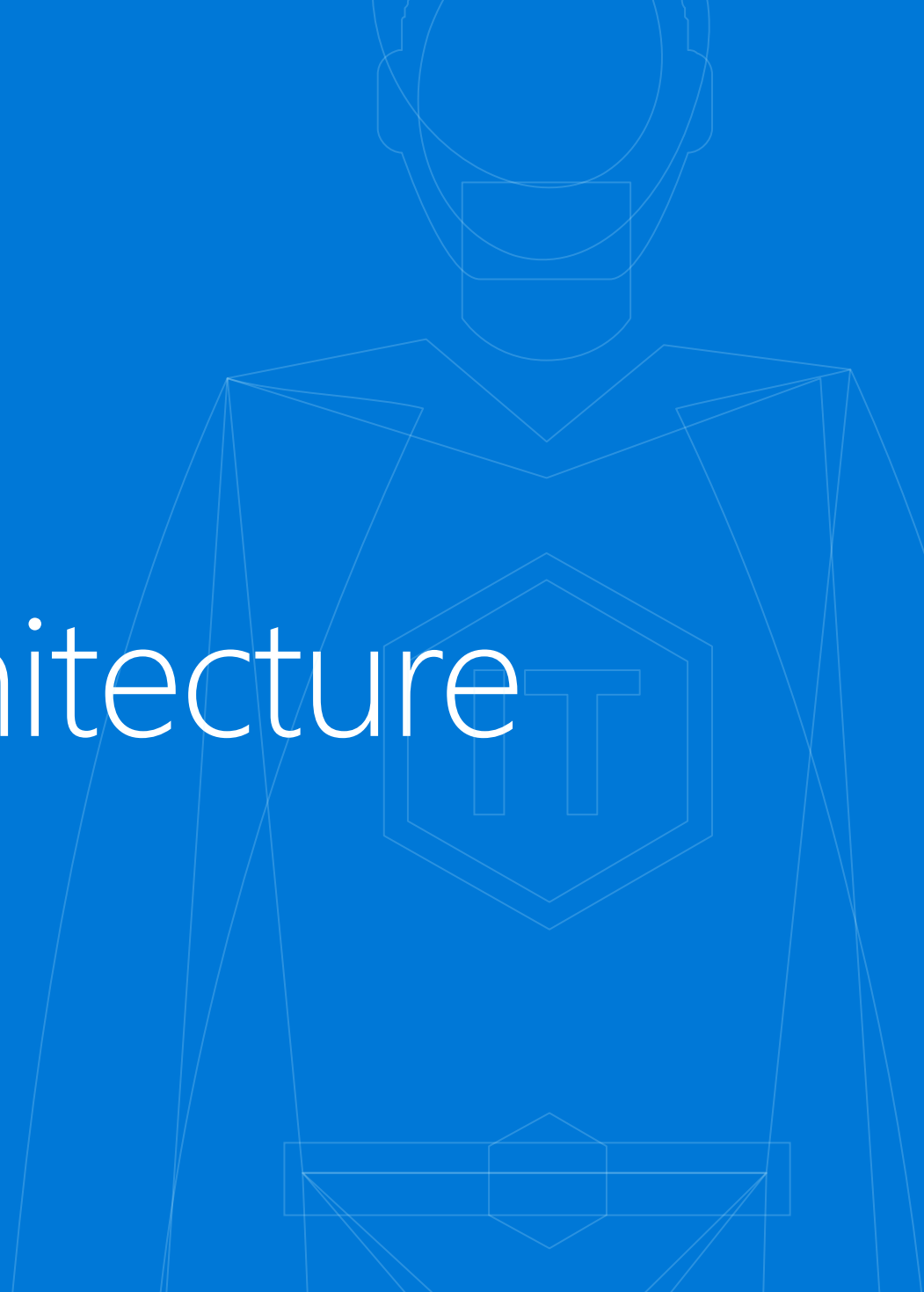


For each suspicious activity, MDI provides recommendations for the investigation and remediation

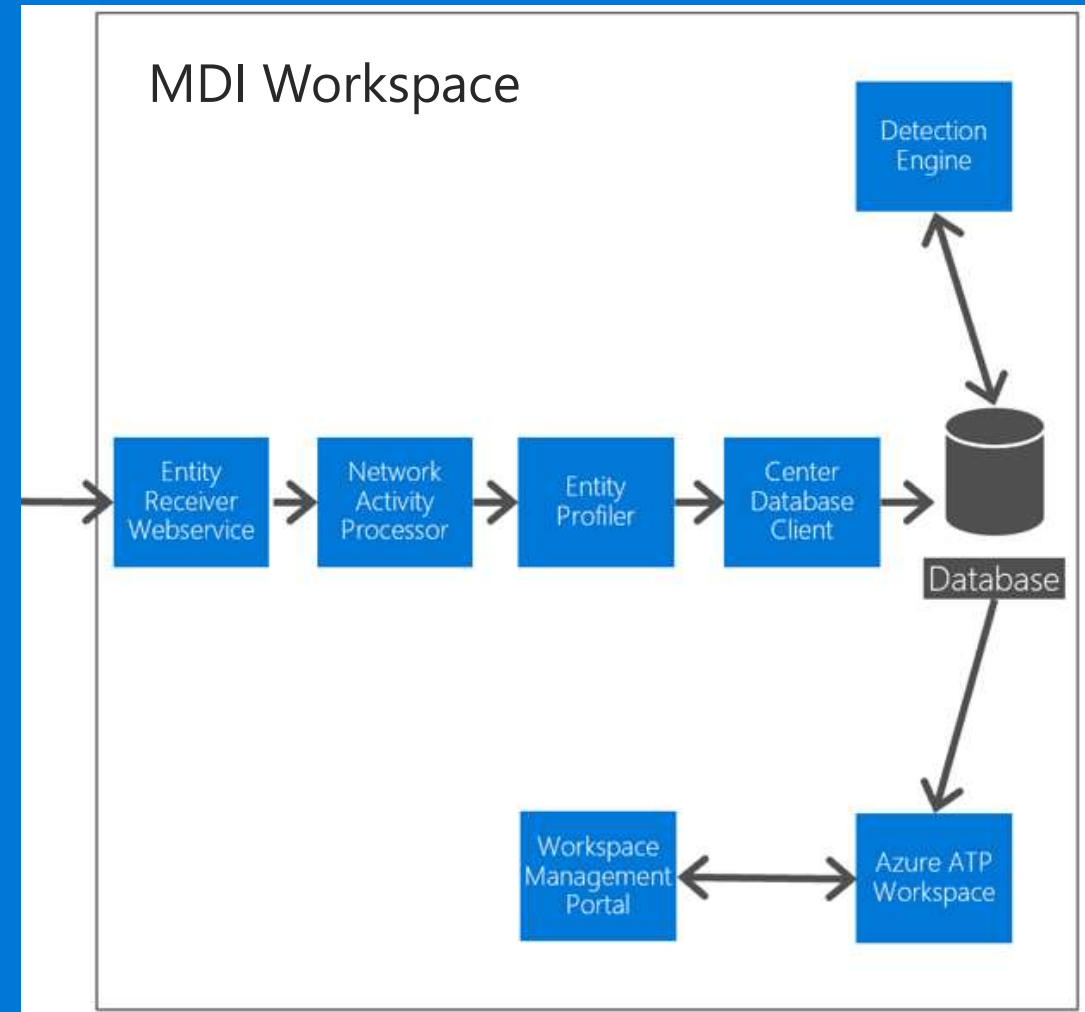
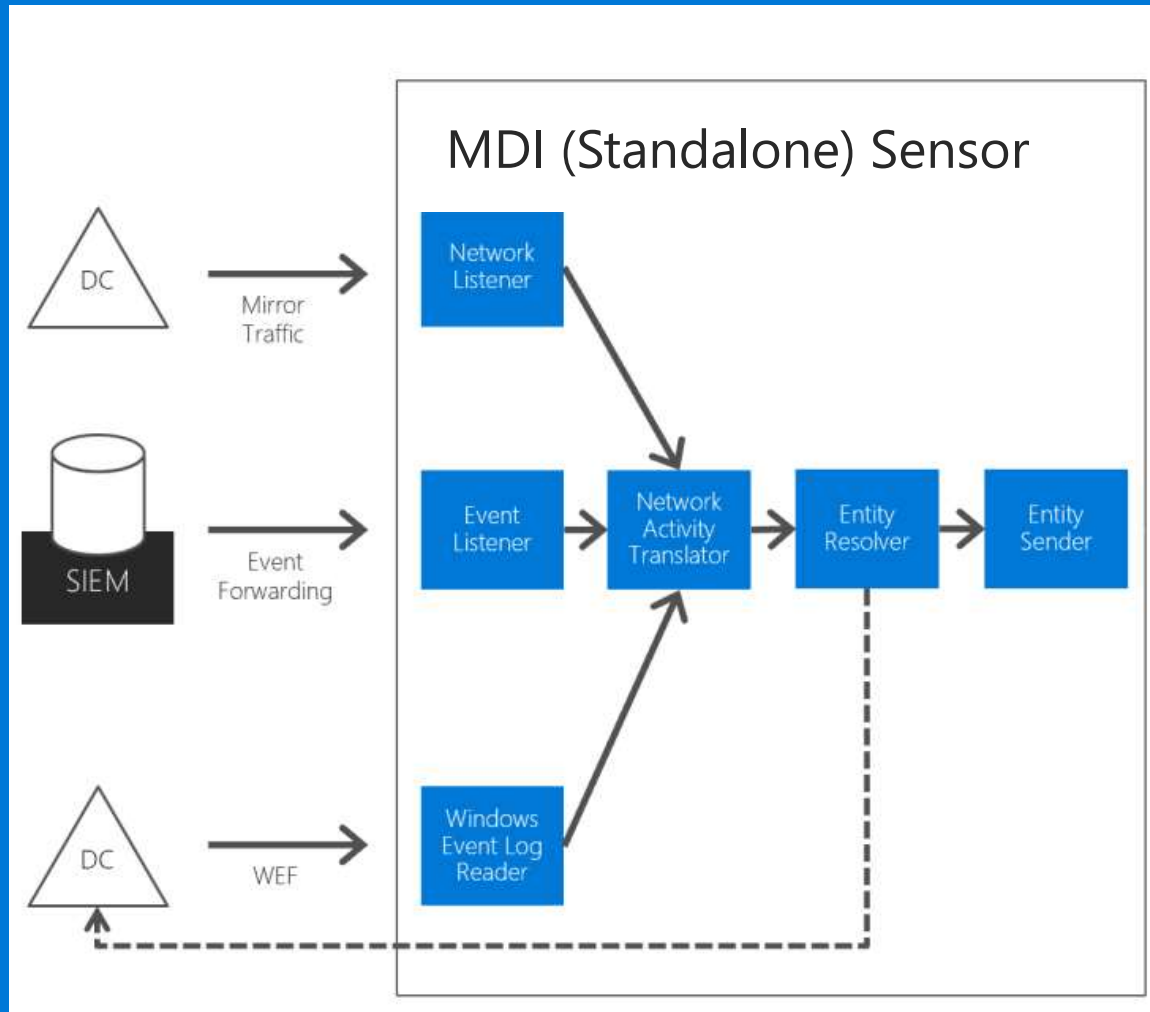




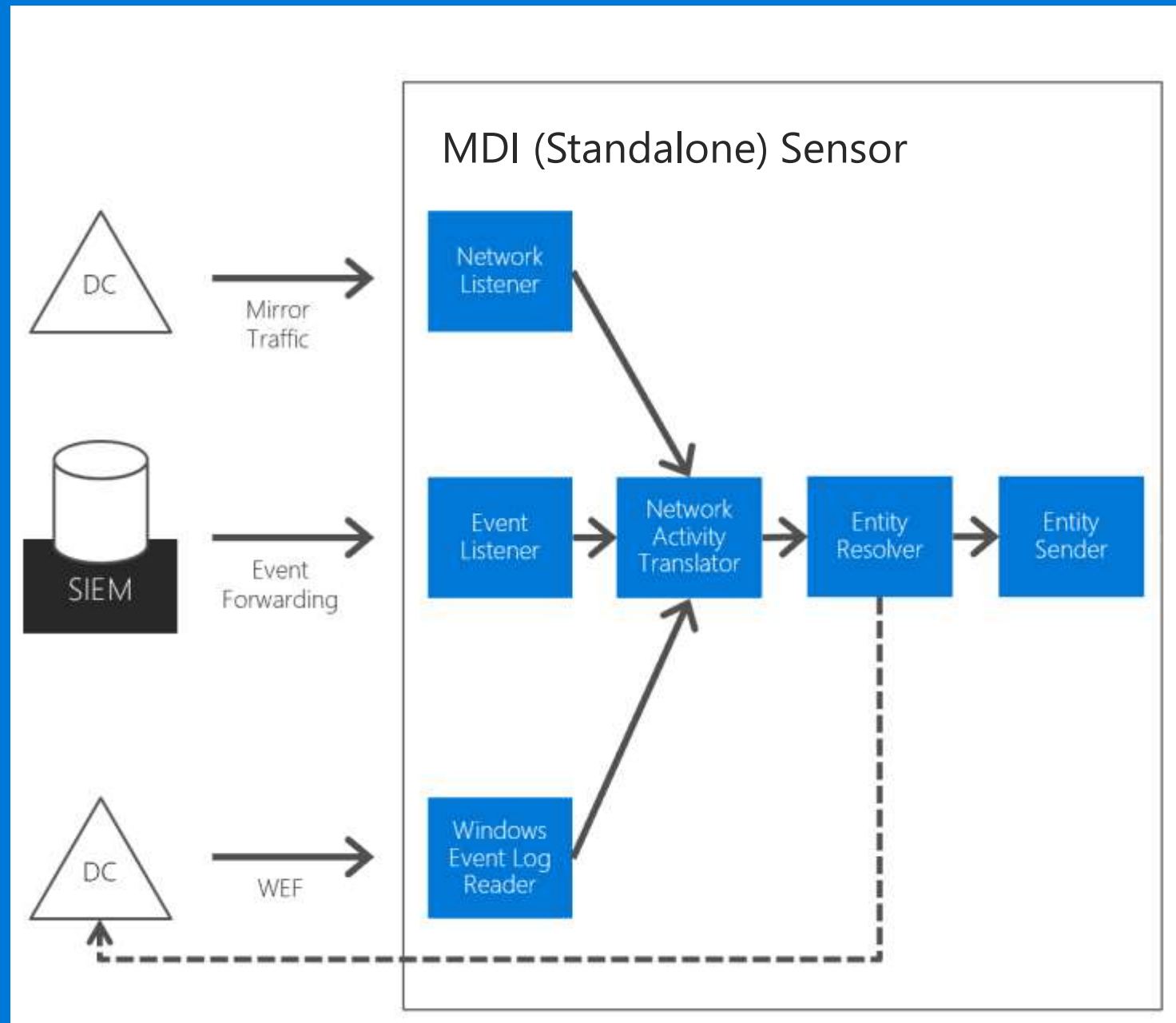
MDI Technical Overview and Architecture



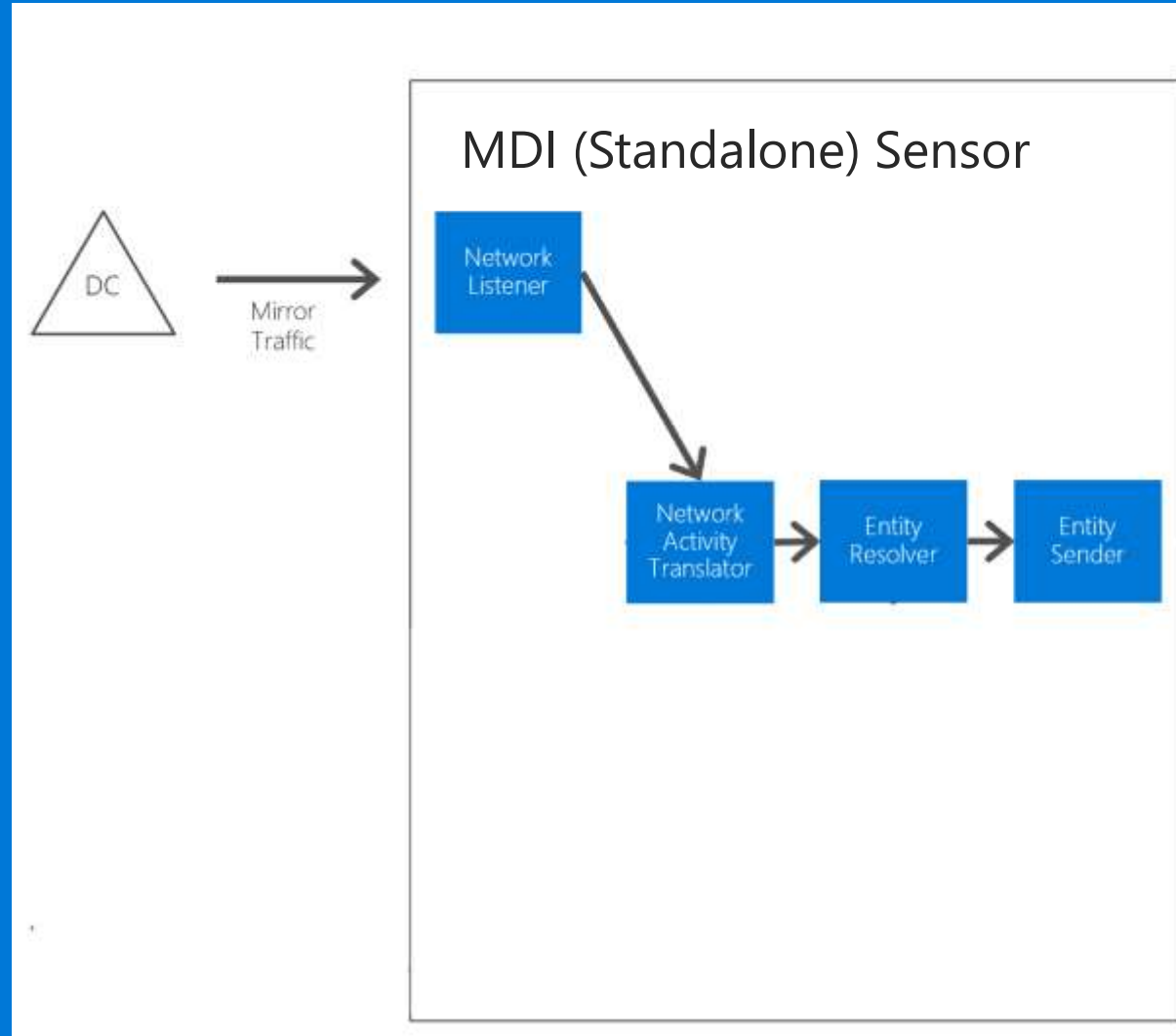
Overview: Entire MDI Architecture



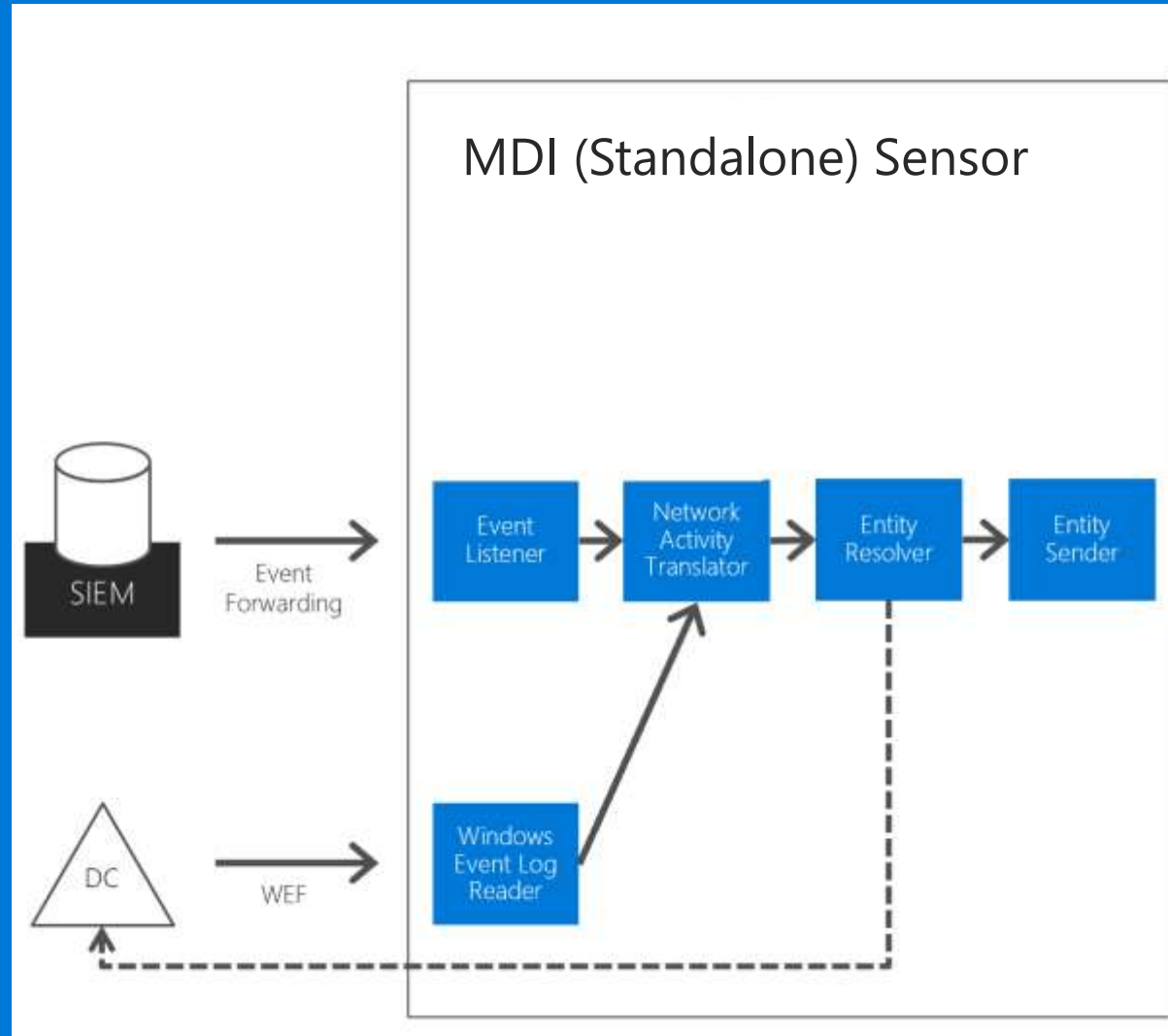
MDI Sensor Architecture



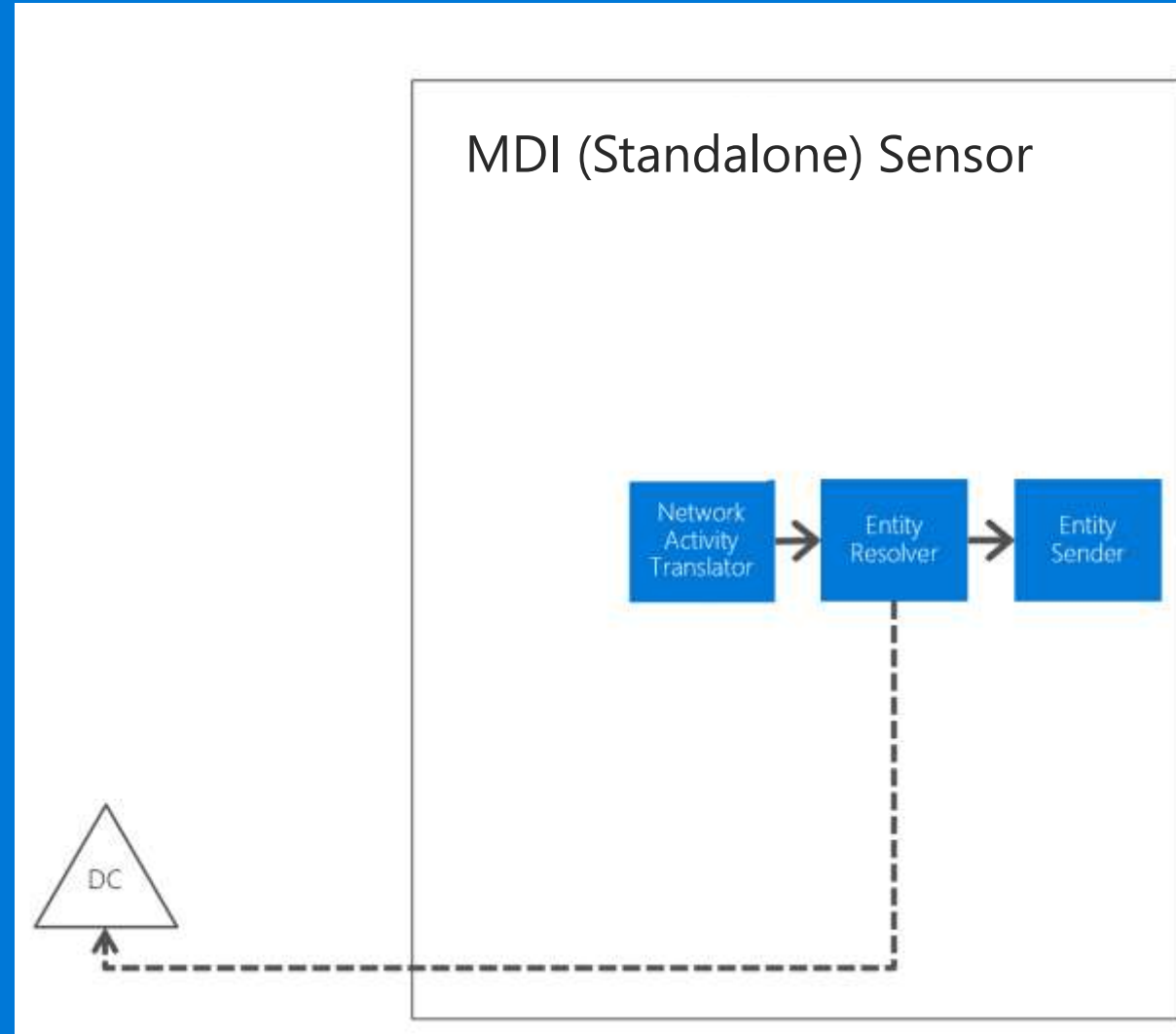
MDI Sensor: Network Activity Collection



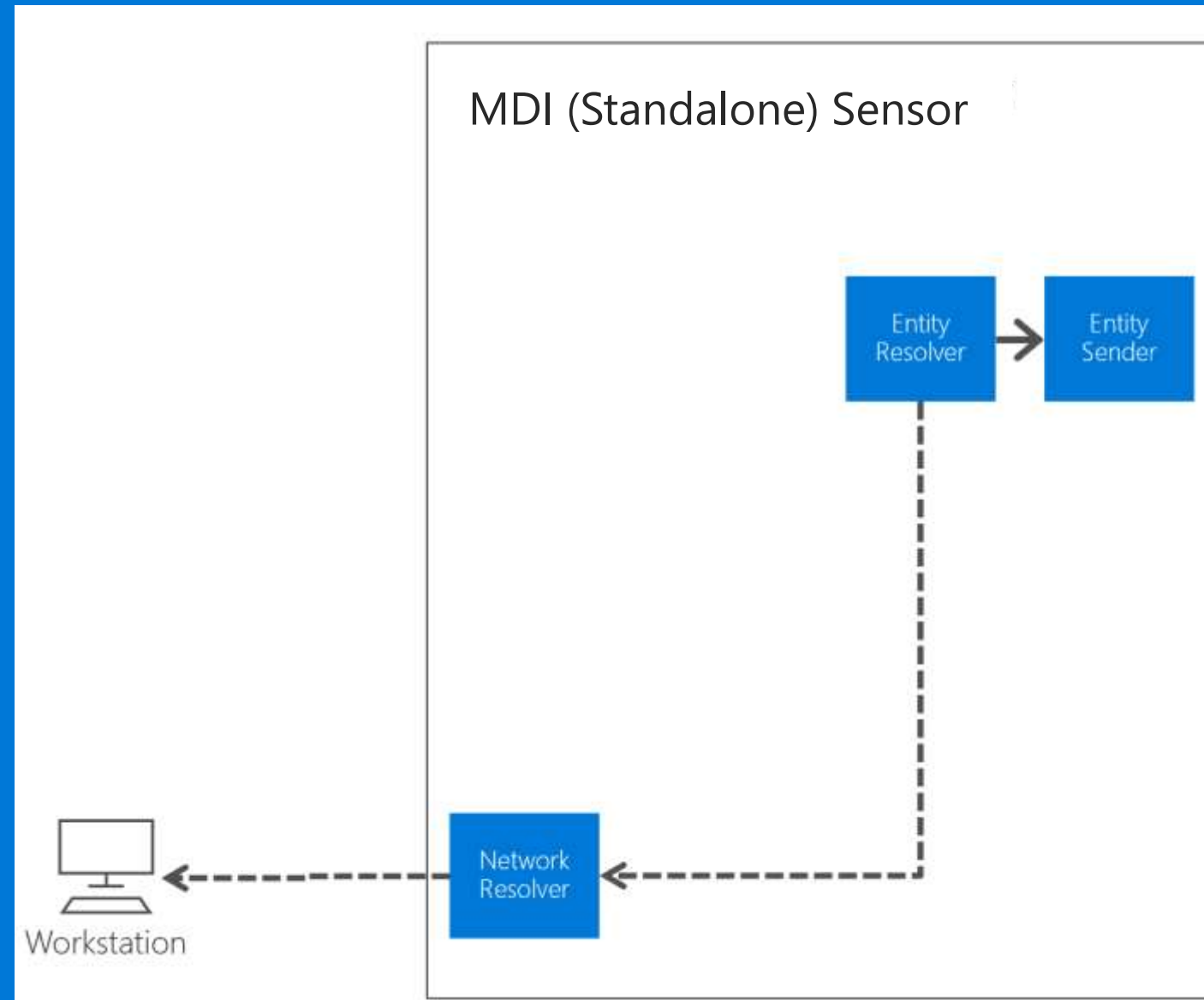
MDI Sensor: SIEM and Event Collection



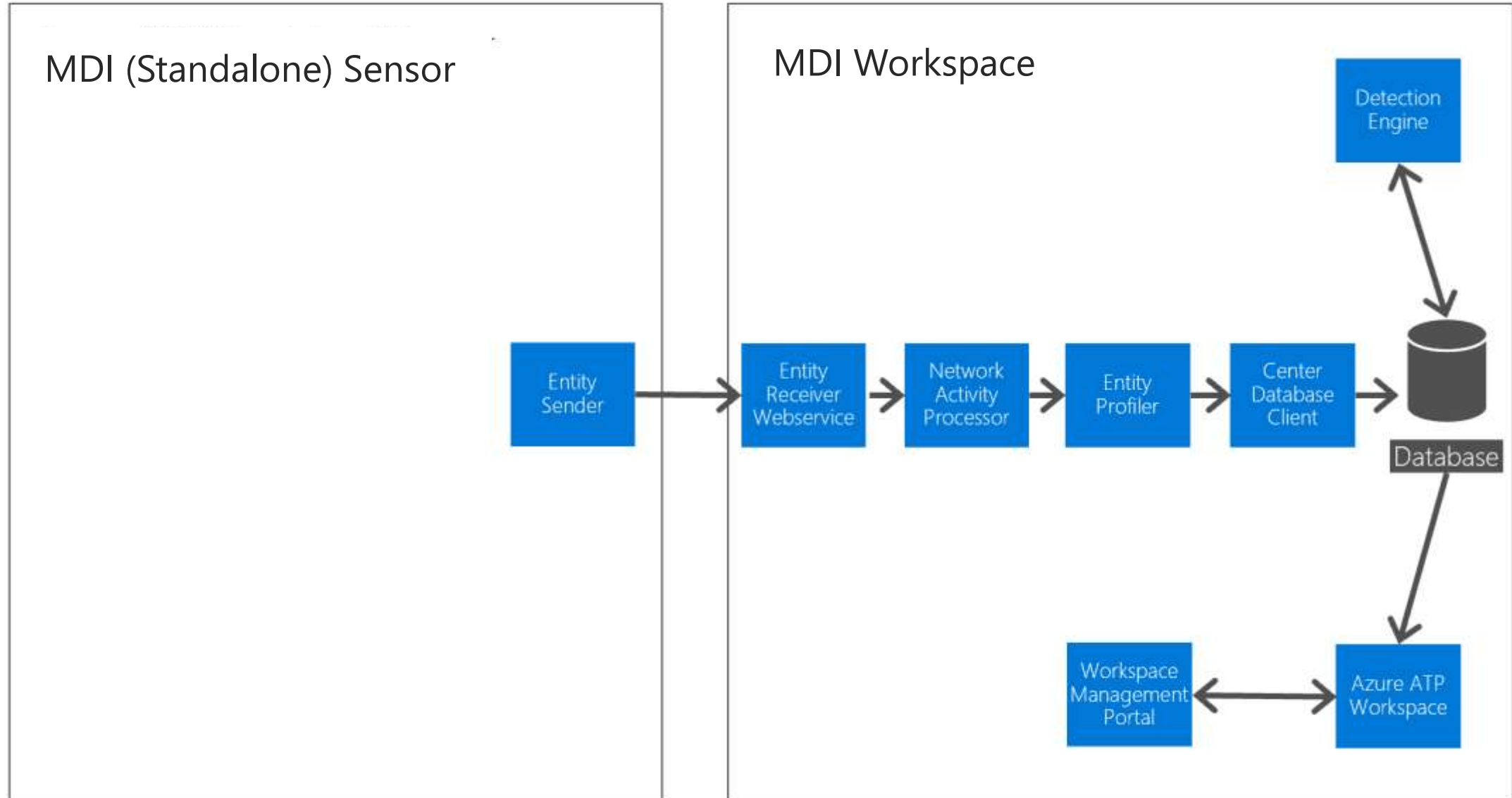
MDI Sensor: Directory Services Collection



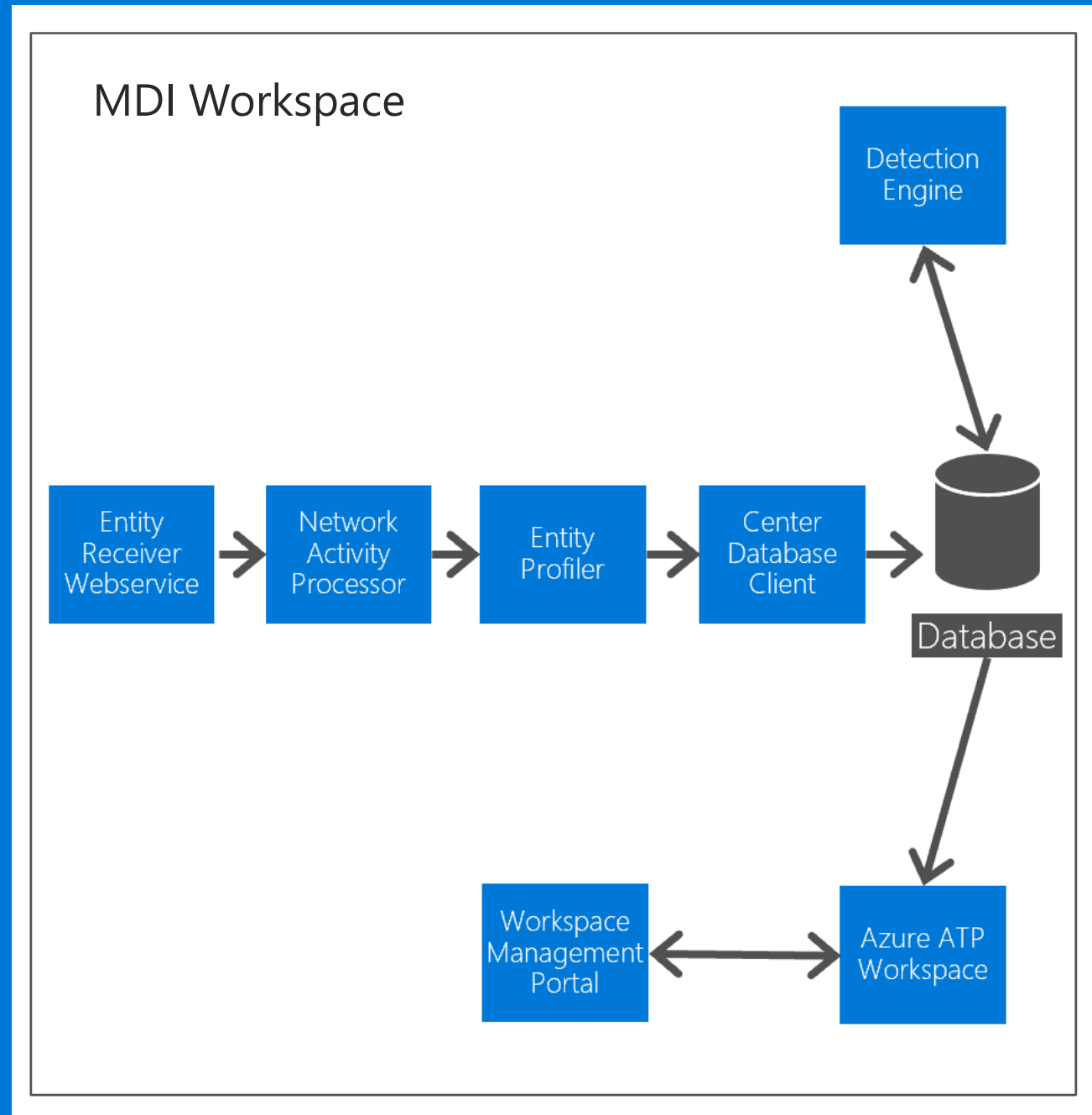
MDI Name Resolution Collection



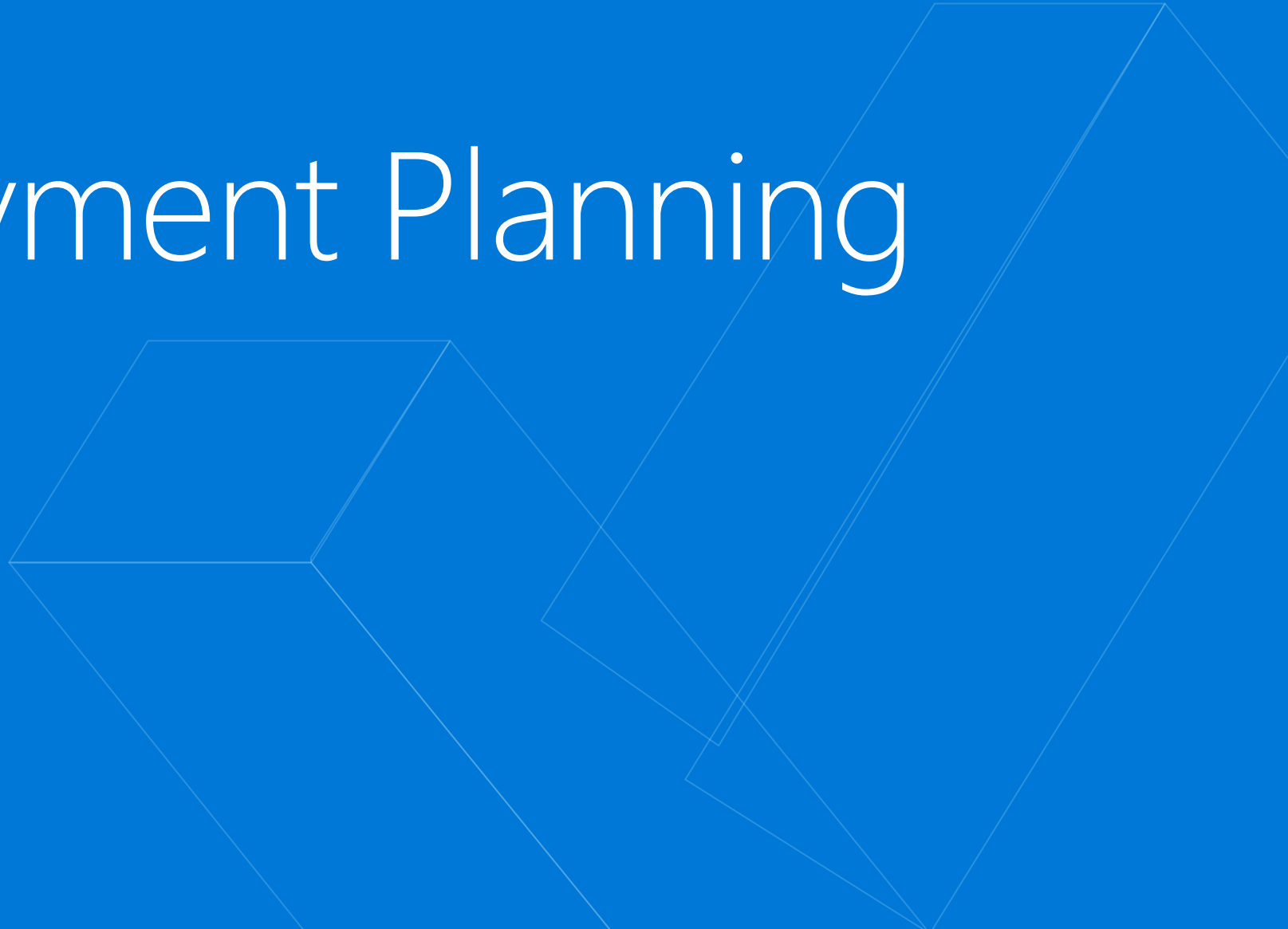
MDI sensor: MDI Sensor to MDI Webservice Communication



MDI Cloud Architecture



MDI Deployment Planning



Preparing for MDI

- MDI Workspace
- MDI Sensor Types
- Port mirroring configuration
- Off domain / On domain (Standalone Sensor only)
- Active Directory Domain Services (AD DS) user accounts
- Proper auditing on DCs and ADFS servers
- Honey token account

Preparation for MDI

1. Create an Active Directory Domain Services (AD DS) account for the MDI Sensor to use
2. Create the MDI Detection mailbox (Optional)
3. Create a honey token account in AD (Optional)
4. Configure and validate port mirroring (domain controller = source, MDI Standalone Sensor = destination)
5. Enable relevant Audit policy
6. Procure Enterprise Mobility + Security E5 and enable for the correct tenant

MDI Cloud service Network Port Requirements

- Communication between the MDI Cloud service and the MDI Sensor is encrypted by using SSL on port 443 and the configuration endpoints over port 80
- The MDI Portal is secured by using SSL on port 443

MDI Network Port Requirements

Protocol	Transport	Port	To/From	Direction
SSL (MDI Communications)	TCP	443	MDI Sensor	Outbound
SMTP (optional)	TCP	25	MDI Sensor/SMTP server	Outbound
SMTPS (optional)	TCP	465	MDI Sensor/SMTP server	Outbound
Syslog (optional)	TCP	514	MDI Sensor/SIEM server	Outbound
Syslog (optional)	TCP/UDP	514	MDI Sensor/SIEM server	Inbound
LDAP	TCP and UDP	389	Domain controllers	Outbound
LDAPS (optional)	TCP	636	Domain controllers	Outbound
DNS	TCP and UDP	53	DNS servers	Outbound
Kerberos (optional if domain joined)	TCP and UDP	88	Domain controllers	Outbound
Netlogon (optional if domain joined)	TCP and UDP	445	Domain controllers	Outbound
Windows Time (optional if domain joined)	UDP	123	Domain controllers	Outbound

MDI Pre-requisite Script

- By running the MDI Audit Script, you can verify that the domain controller are having the correct Audit settings

MDI Sensor Administrative Requirements

- Configured by using the MDI Cloud Service and install package downloaded to MDI Sensor server
- Requires an Active Directory account with read-only access (does not need interactive sign in) used to enumerate users and devices for event correlation and behavioral analysis in the MDI Cloud service
- Nothing special added, not even an administrative local group
- Requires read-only access on Deleted Objects container and ADFS database

MDI Standalone Sensor Requirements

- **Operating system:** Windows Server 2012 R2 or Windows Server 2016 or 2019 (includes server core). OS can be a domain or workgroup member.
- **Hardware:** An MDI Standalone Sensor can support monitoring multiple domain controllers, depending on the amount network traffic to and from the domain controllers.
- **Networking:** Two or more NICs
 - **Management Adapter**
 - **Capture Adapter**

Configure a static non-routable IP address on the capture adapter with no default gateway and no DNS server addresses. For example, 1.1.1.1/8

MDI Sensor Requirements for DCs

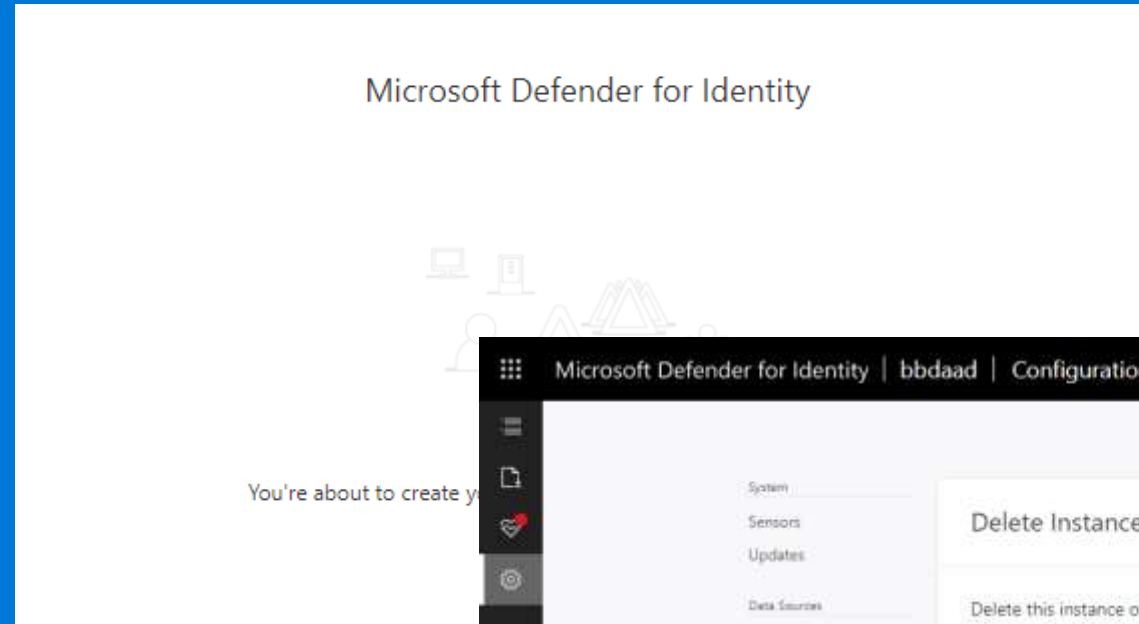
- **Operating system:** Windows Server 2012 or above (includes server core).
- **Roles:** AD Domain Controller only. ADFS and DC roles should not co-exist on target server.
- **Domain Controller:** Branch or RODCs are supported.
- **.NET:** During installation, if .NET Framework 4.7 or later isn't installed, the .NET Framework 4.7 is installed and might require a reboot of the server.

MDI Sensor Requirements for ADFS Servers

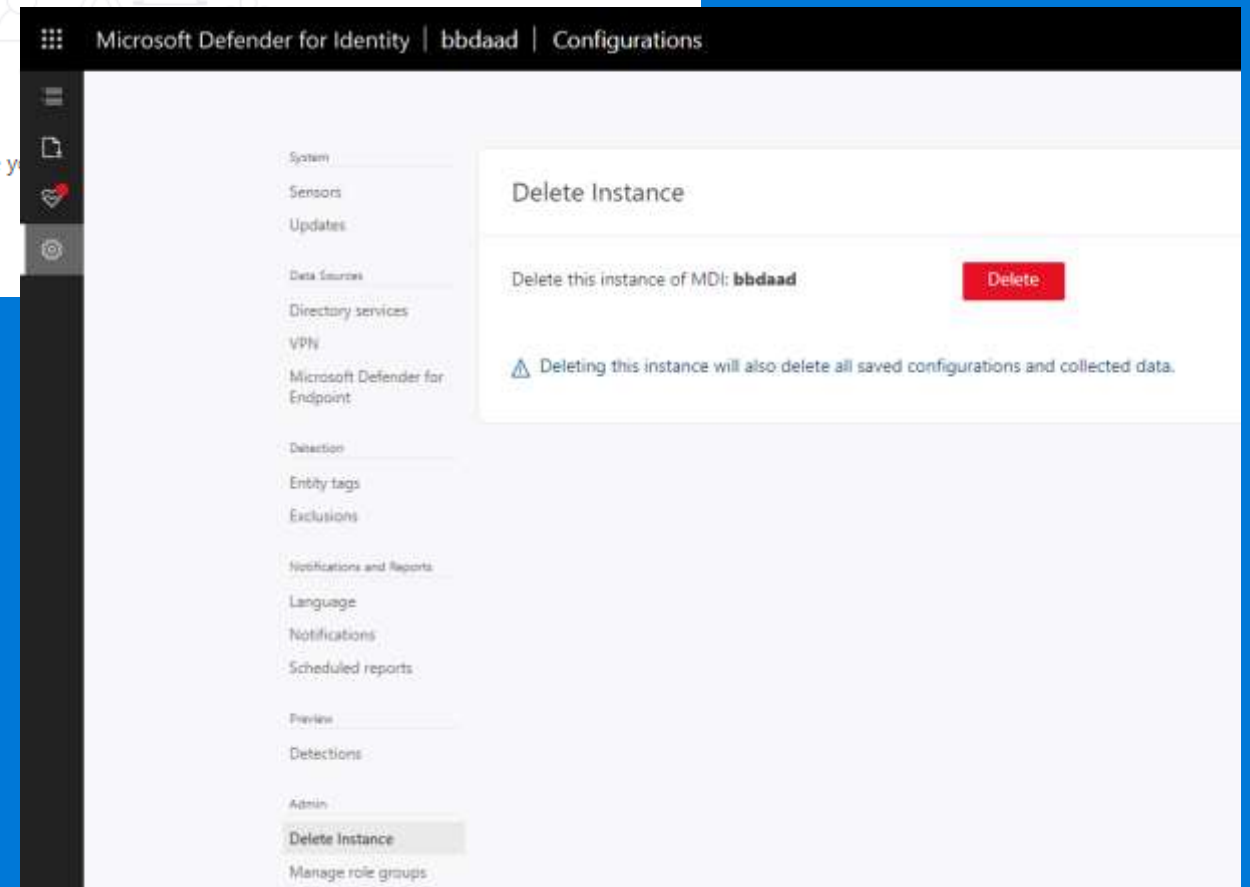
- **Operating system:** Windows Server 2016 or 2019
- **Roles:** AD Federation Services only. ADFS and DC roles should not co-exist on target server.
- **ADFS Database:** Connect, log in, read, and select permissions to the AdfsConfiguration database.
- **.NET:** During installation, if .NET Framework 4.7 or later isn't installed, the .NET Framework 4.7 is installed and might require a reboot of the server.

Microsoft Defender for Identity Configuration

Enabling MDI

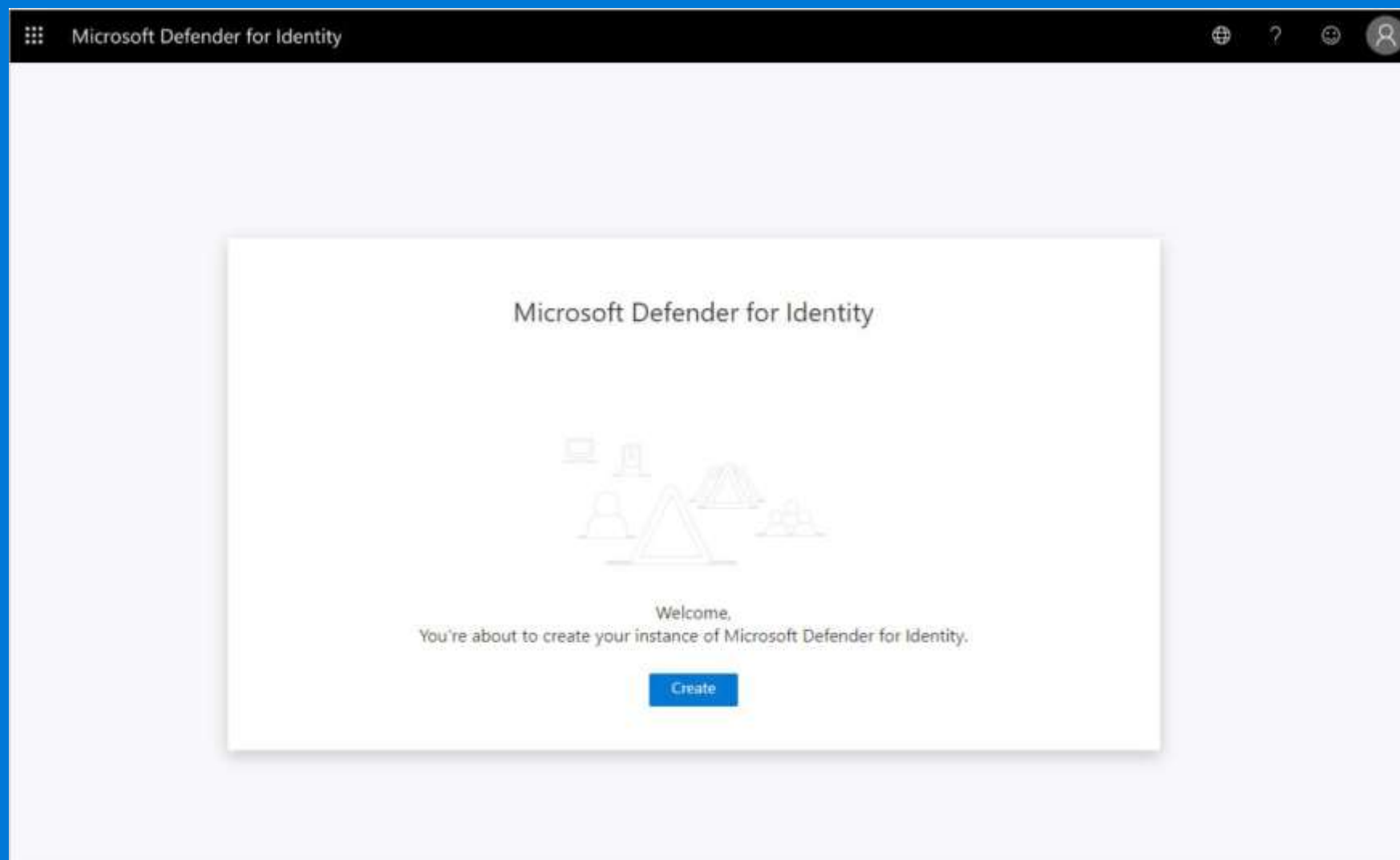


Deleting MDI Workspace



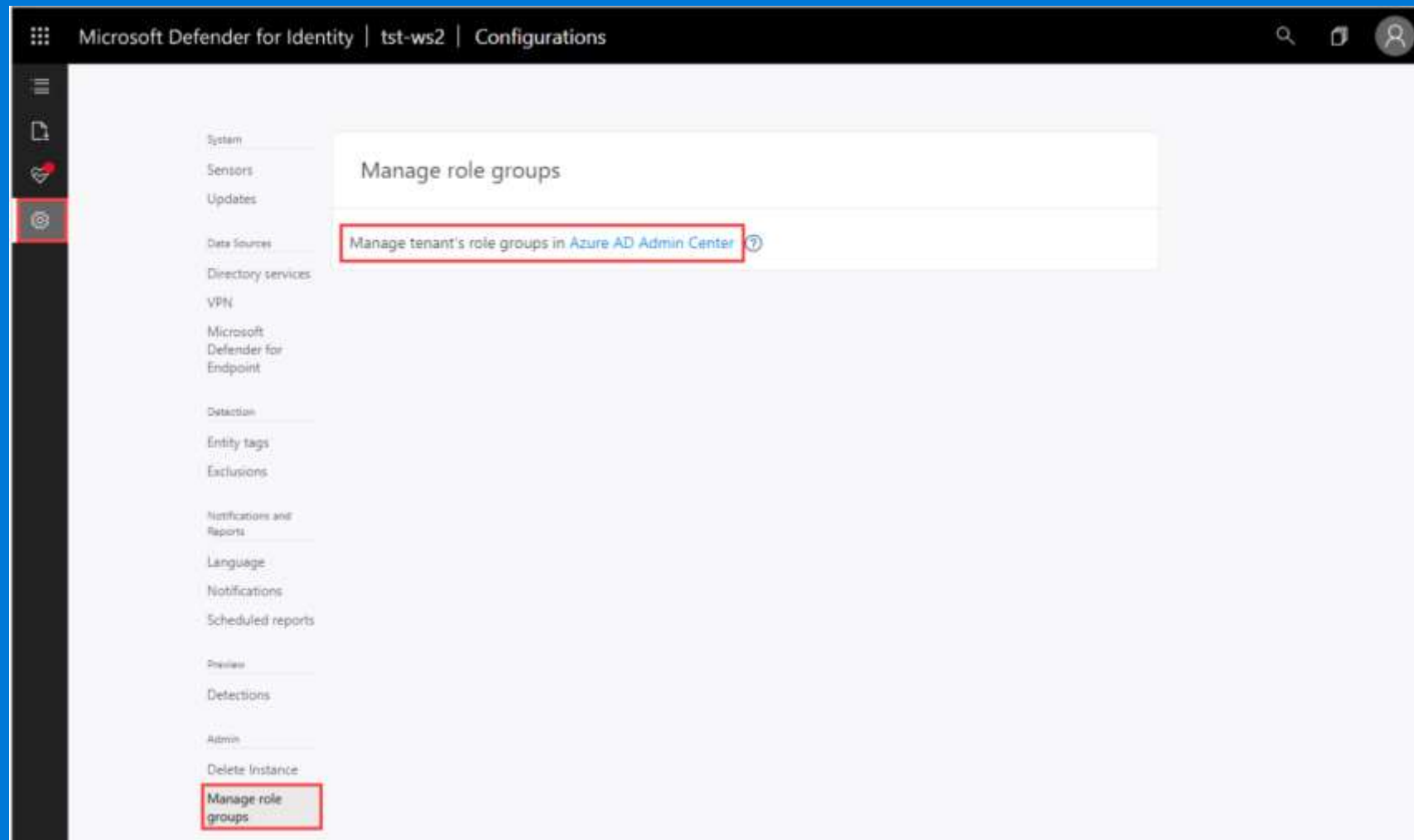
Microsoft Defender for Identity Configuration

- Creating a workspace



Microsoft Defender for Identity Configuration

- Assign necessary delegations



Read-Only AD User Account

- MDI uses this to read from Active Directory Domain Services and correlate network activity to the Active Directory object. gMSA is recommended

System
Sensors
Updates
Data Sources
Directory services
VPN
Microsoft Defender for Endpoint
Detection
Entity tags
Exclusions
Notifications and Reports
Language
Notifications
Scheduled reports
Preview
Detections
Admin
Delete Instance
Manage role groups

Directory services

ⓘ Before transferring to another page, remember to save the changes you made to the configuration

contoso.com\mdi

Username

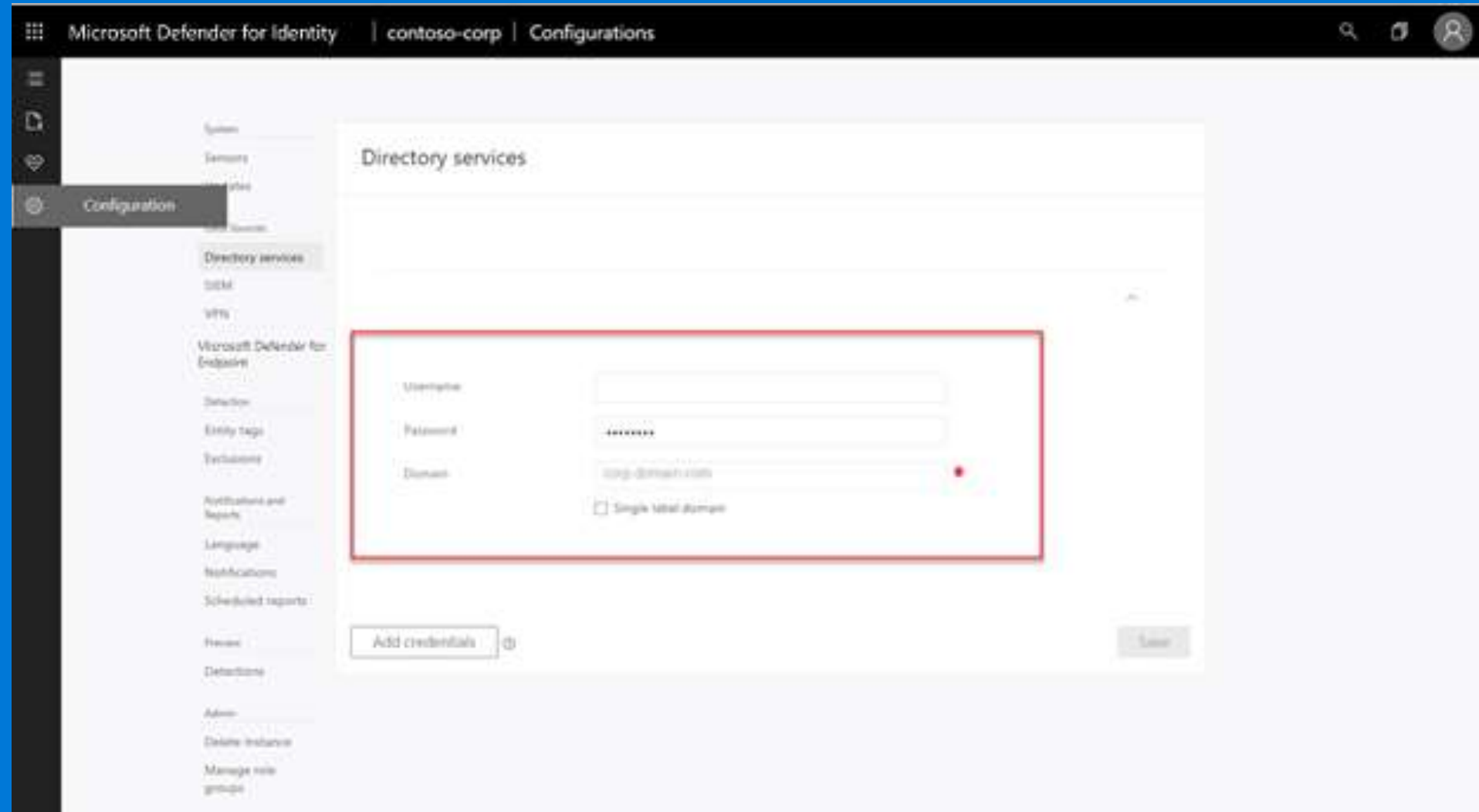
☐ Group managed service account ⓘ

Password

Domain

☐ Single label domain

Data sources



MDI Sensor Installation

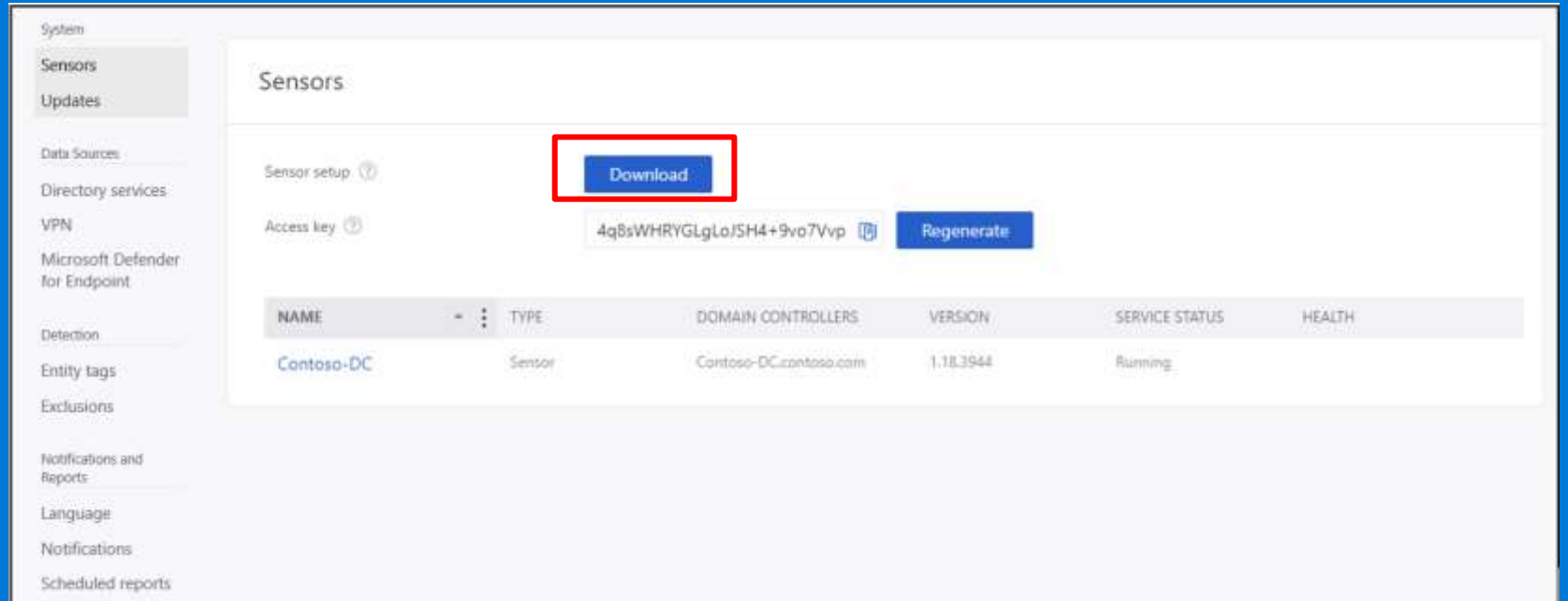


MDI Sensor Installation

- The MDI sensor can be installed in different ways
- -MDI Standalone Sensor
- -MDI Sensor (installed on Domain Controller or ADFS servers)

MDI Sensor Installation

- The MDI sensor installation packet



The screenshot shows the Windows Security app interface. On the left is a navigation pane with the following items: System, Sensors (selected), Updates, Data Sources, Directory services, VPN, Microsoft Defender for Endpoint, Detection, Entity tags, Exclusions, Notifications and Reports, Language, Notifications, and Scheduled reports. The main content area is titled 'Sensors'. It contains a 'Sensor setup' section with a 'Download' button highlighted by a red rectangle. Below this is an 'Access key' section showing the key '4q8sWHRYGLgLoJSH4+9vo7Vvp' and a 'Regenerate' button. At the bottom is a table with the following data:

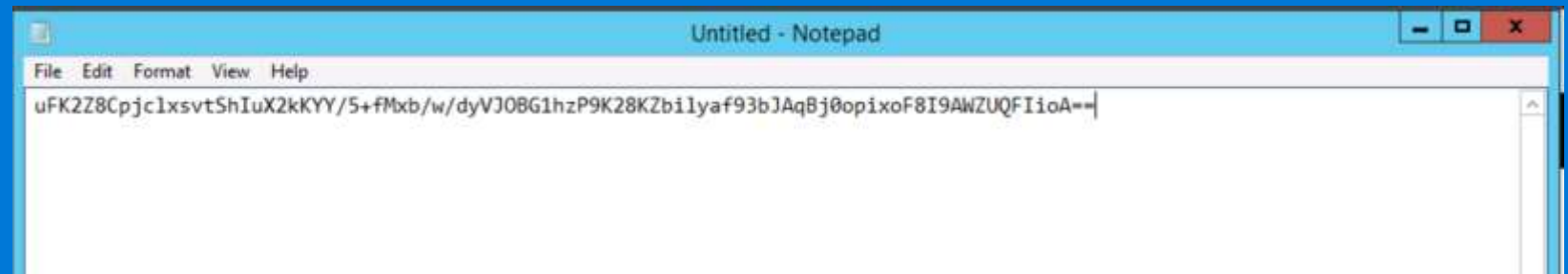
NAME	TYPE	DOMAIN CONTROLLERS	VERSION	SERVICE STATUS	HEALTH
Contoso-DC	Sensor	Contoso-DC.contoso.com	1.18.3944	Running	

MDI Sensor Installation

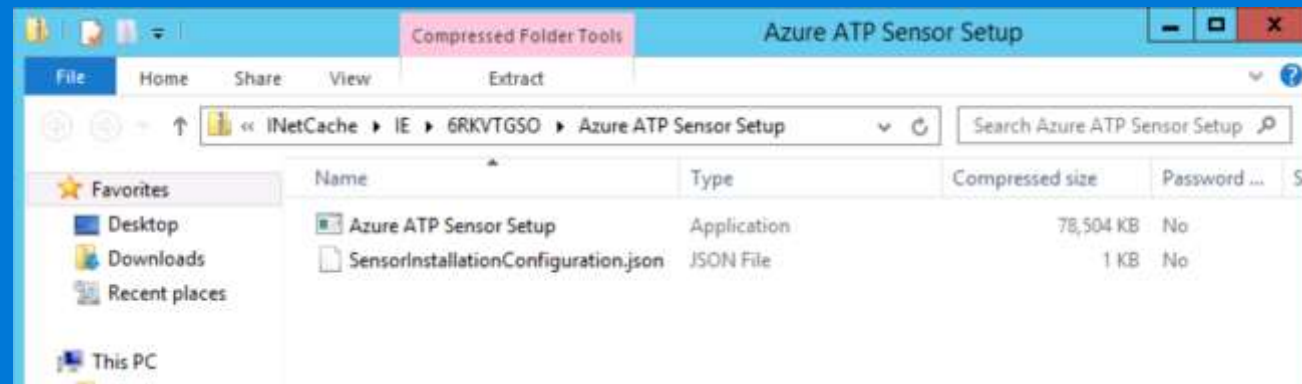
- Download the MDI sensor installation packet to the machine from a browser



- Copy the access key



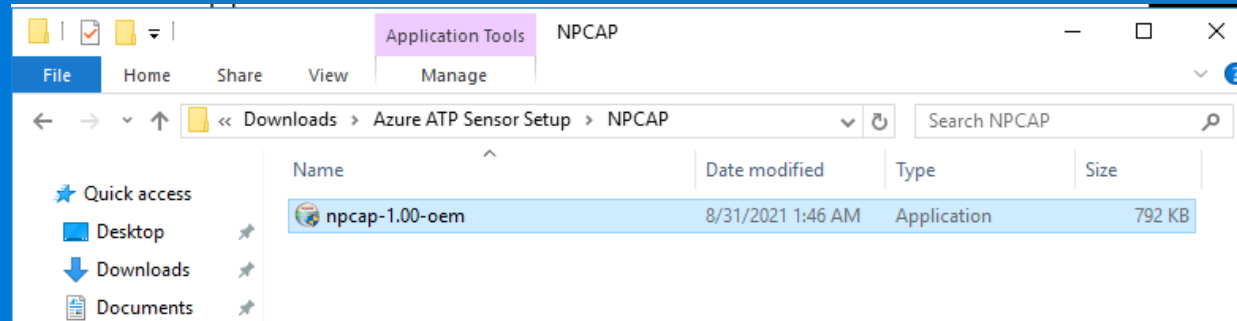
- Extract the setup files



MDI Sensor Installation

Install the NPCAP application

- Install the NPCAP application



MDI Sensor Installation

- Start the MDI sensor installation

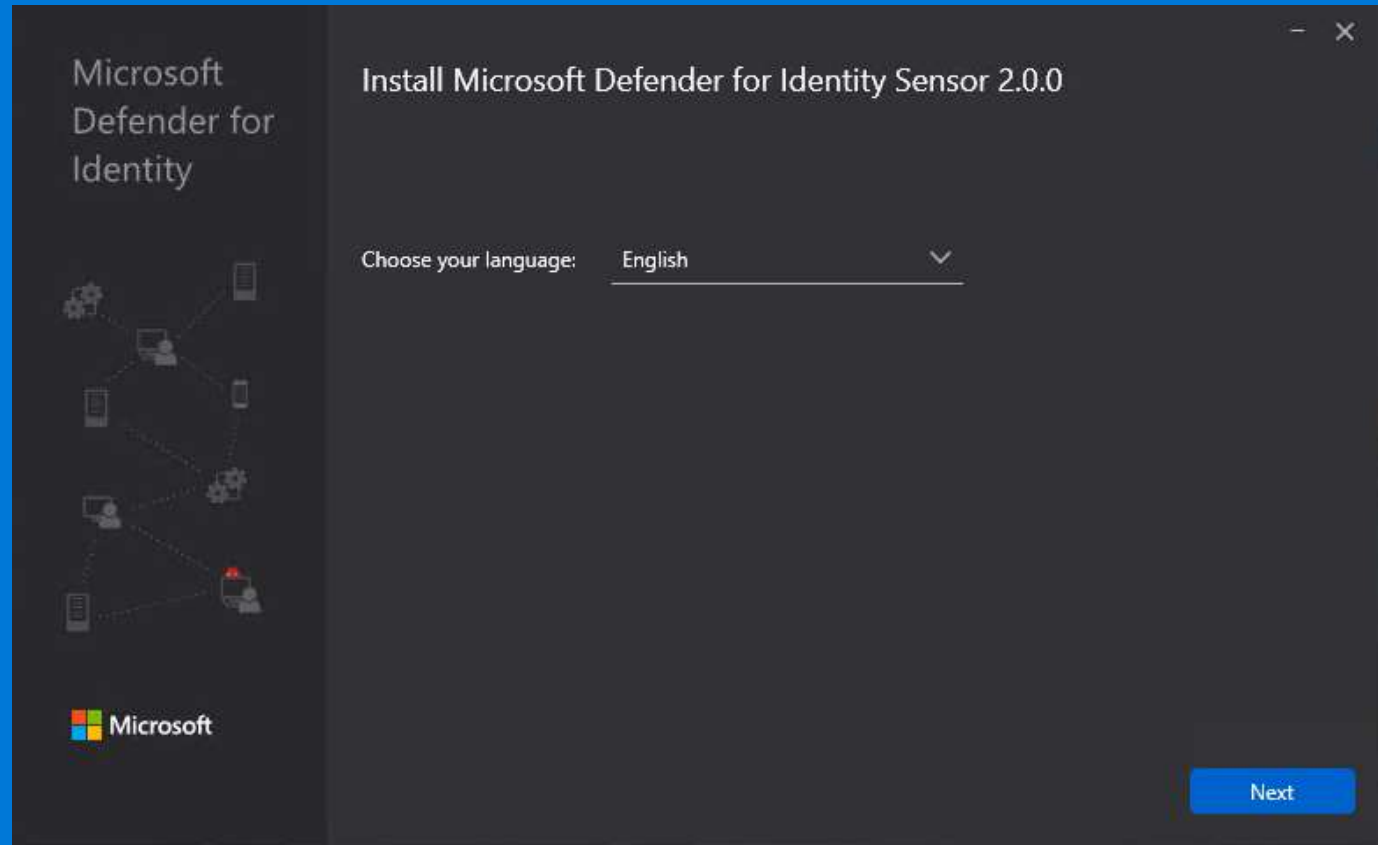


- MDI will install the right version of .NET framework if it is not installed



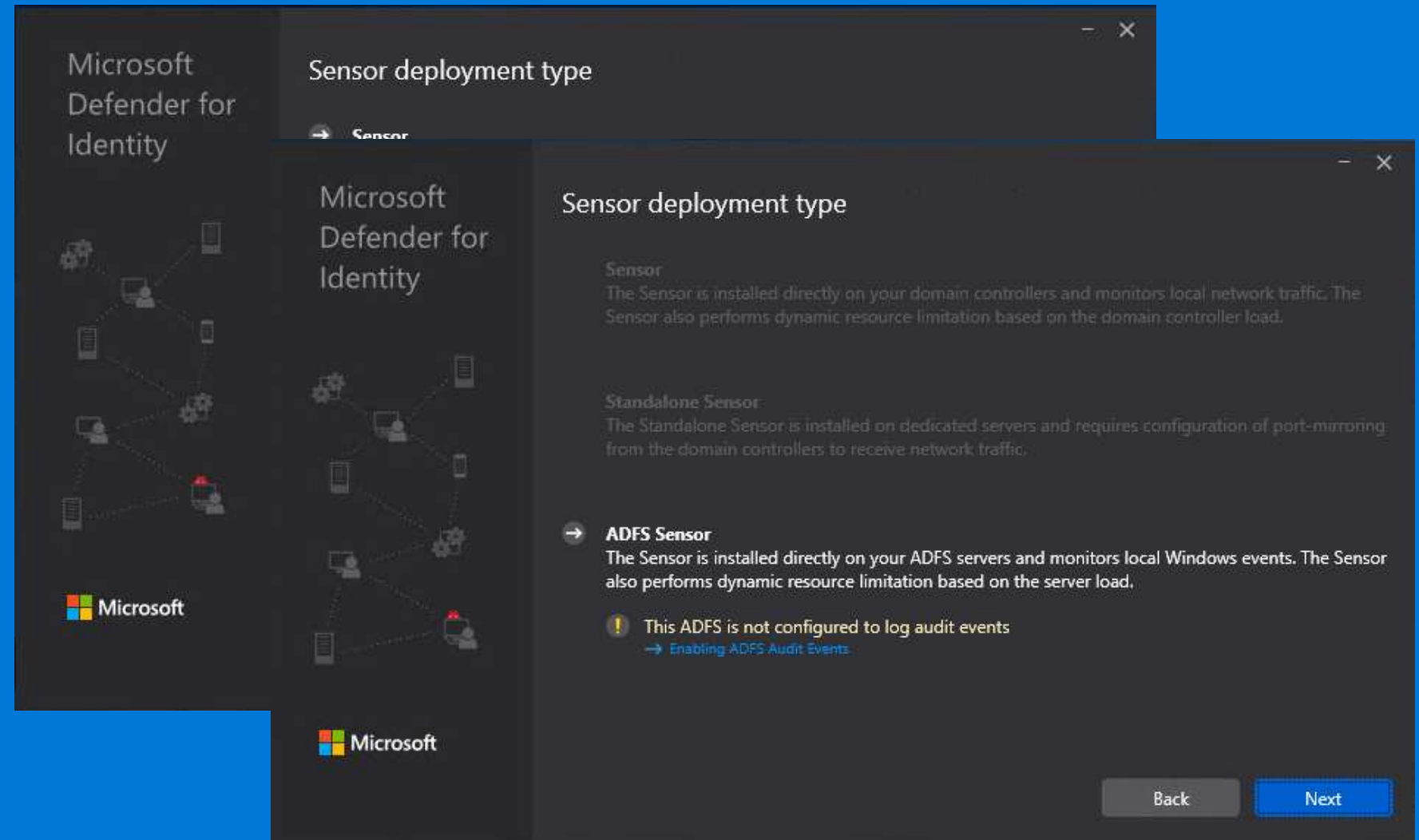
MDI Sensor Installation

- Choose language to install

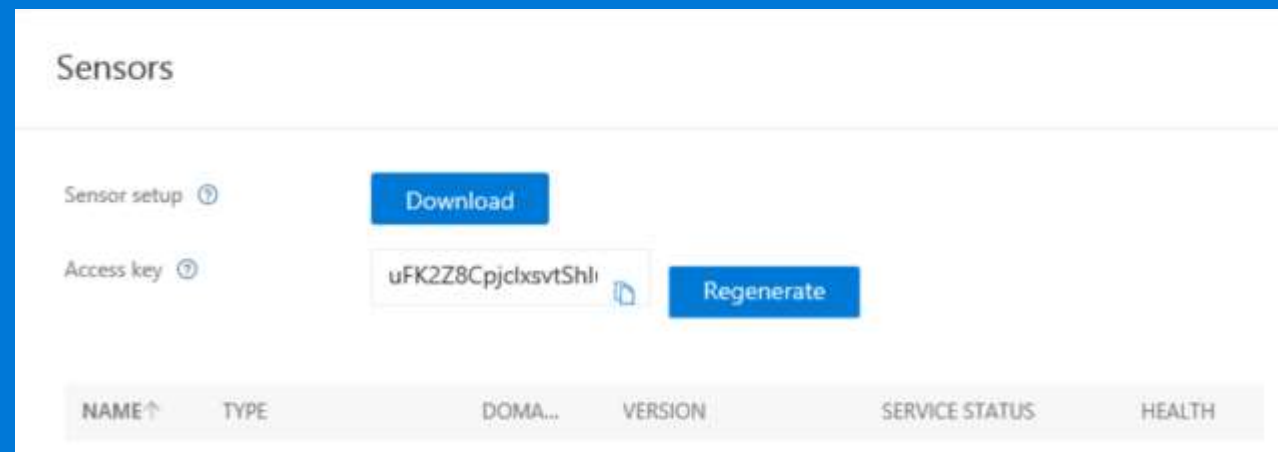
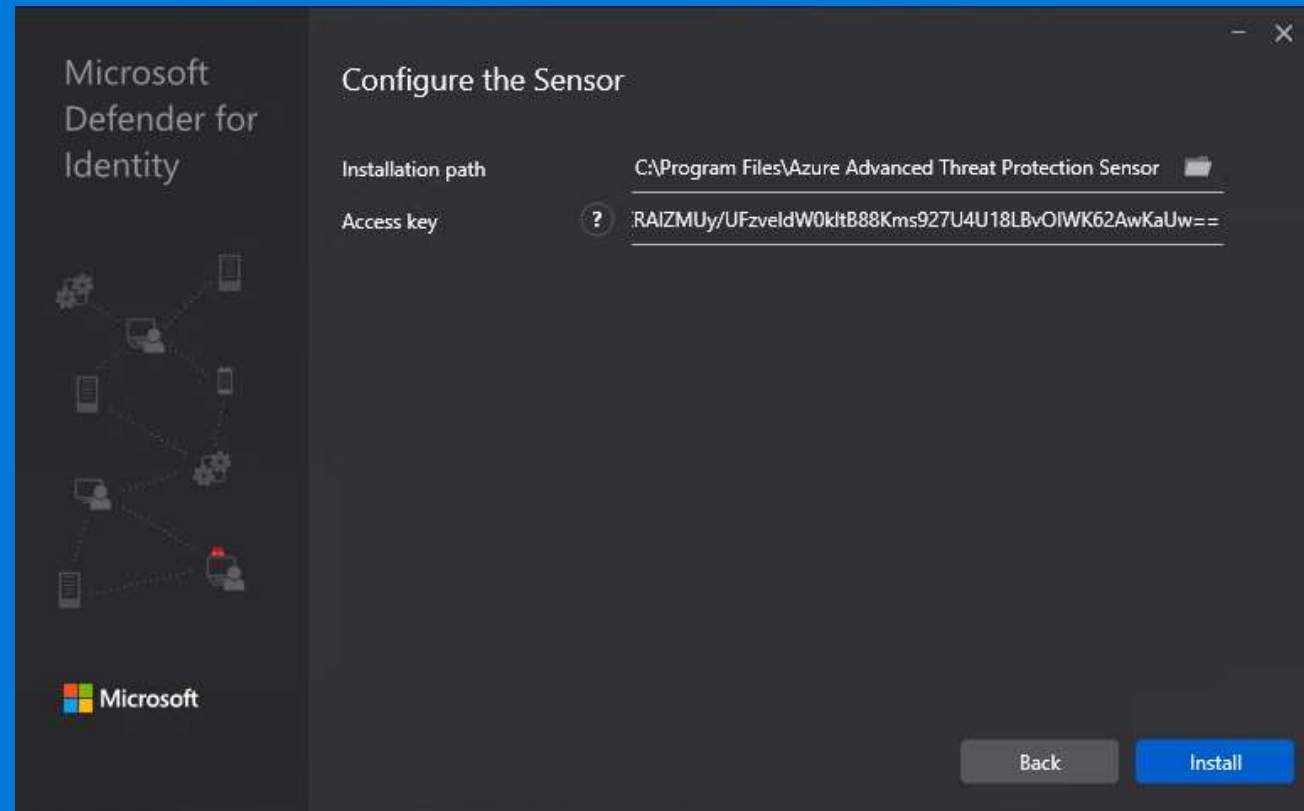


MDI Sensor Installation

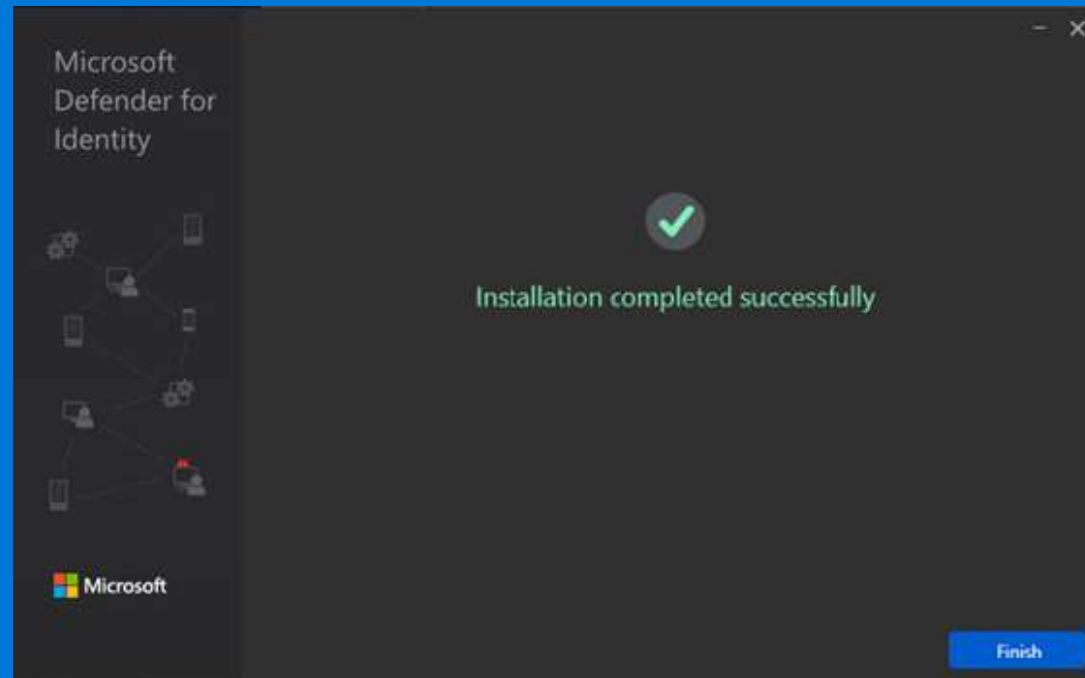
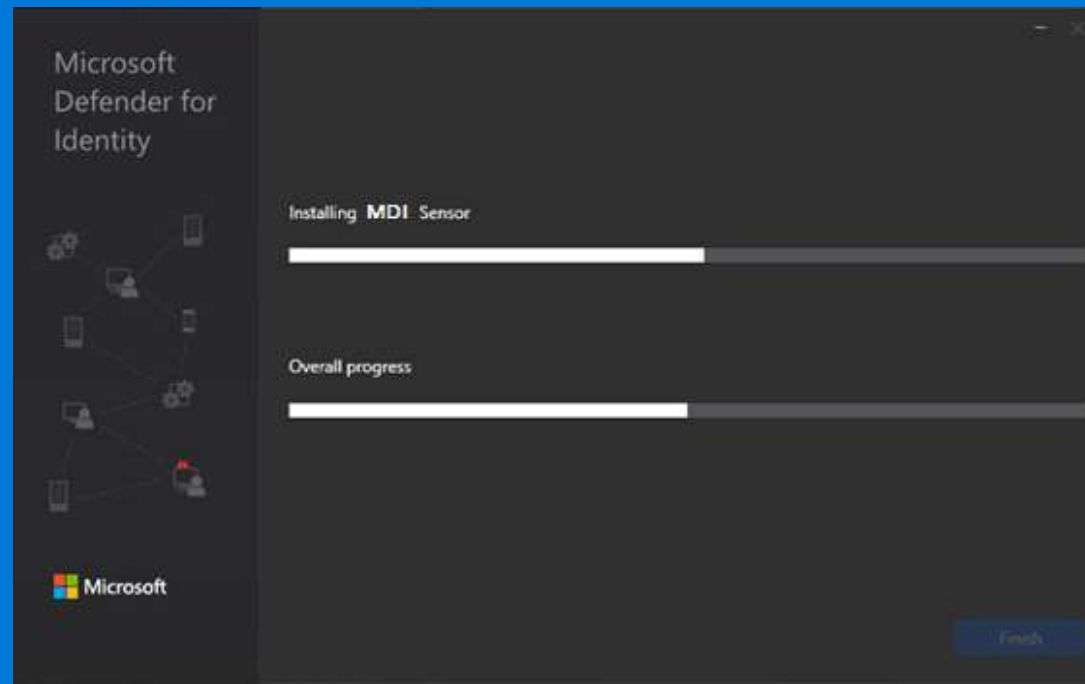
- MDI Sensor



MDI Sensor Installation



MDI Sensor Installation



Installing the MDI Sensor

- Scripted installation can be done via Sensor Setup
- Install
`'D:\Azure ATP Sensor Setup.exe' /quiet`
`NetFrameworkCommandLineArguments="/q"`
`AccessKey= <YourMDIWorkspaceAccessKey>`
- Uninstall
`Azure ATP Sensor Setup.exe [/quiet] [/Uninstall] [/Help]`

MDI Sensor Installation

Sensors

Sensor setup ⓘ

Download

Access key ⓘ

uFK2Z8CpjclxsvtSh ⓘ

Regenerate

NAME	TYPE	DOM...	VERSION	SERVICE STATUS	HEAL...
WIN-T...	Sensor	WIN-TV...	2.45.5337	Running	

Configuration Options






Configuring MDI












1. Set up the MDI Service
2. Configure detection options (honey token account)
3. Configure alerting options (mail integration, syslog integration)
4. Configure the MDI Sensor settings within the MDI configuration
5. Download the MDI Sensor Setup package, transfer to the MDI Sensor, and run setup
6. Configure each MDI Sensor accordingly
7. When the MDI Sensor configuration completes, wait for MDI to learn about the Active Directory environment

Group for Administering Microsoft Defender for Identity (MDI)

- To configure the MDI portal, you must be a member of either the Global Administrator role or the Security Administrator role on the tenant where the service is going to be installed.

 Profile	ROLE 
 Directory role	<input type="checkbox"/> Global administrator

- MDI security groups can be used to delegate the administration to other users after the initial setup

		 New group  Refresh  Columns	
 All groups		Name <input type="text" value="Search groups"/>	
Settings			
 General			
 Expiration			
Activity			
 Access reviews			
		NAME	GROUP TYPE
		 Azure ATP oaaatp Administrators	Security
		 Azure ATP oaaatp Users	Security
		 Azure ATP oaaatp Viewers	Security

Data sources

SIEM/Syslog Listener

- ✓ Already enabled on Standalone Sensors
- ✓ Supports below solutions
 - HP Arcsight
 - Splunk
 - RSA Security Analytics
 - Snare
 - Qradar

Data sources

The screenshot shows a web-based configuration interface for VPN settings. On the left is a vertical sidebar with a list of menu items: System, Sensors, Updates, Data Sources, Directory services, VPN (highlighted), Microsoft Defender for Endpoint, Detection, Entity tags, and Exclusions. The main content area is titled 'VPN' and contains a toggle switch for 'RADIUS Accounting' which is currently turned off. Below the toggle is an informational message starting with an 'i' icon, explaining that enabling RADIUS Accounting allows for suspicious VPN connection detection and adds VPN locations to the entity profile. A 'Save' button is located in the bottom right corner of the main content area.

System

Sensors

Updates

Data Sources

Directory services

VPN

Microsoft Defender for Endpoint

Detection

Entity tags

Exclusions

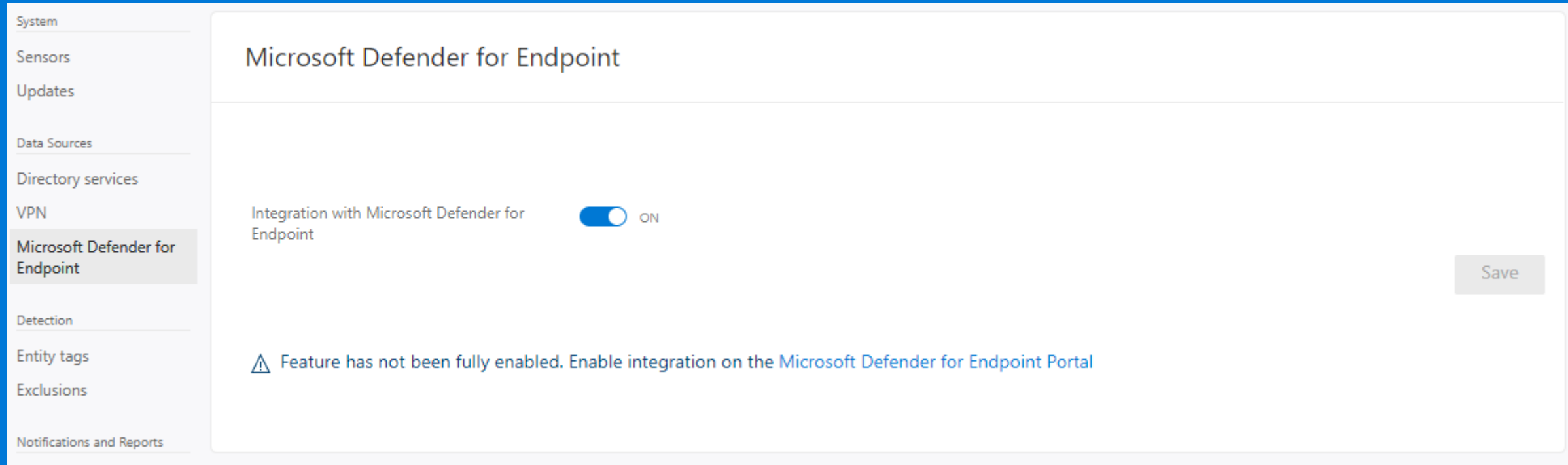
VPN

RADIUS Accounting ⓘ ☐ OFF

ⓘ Configuring Radius Accounting enables the [Suspicious VPN connection](#) detection and enriches the entity profile page with VPN locations.

Save

Data sources



The screenshot shows a management console interface for Microsoft Defender for Endpoint. On the left is a vertical sidebar with a list of navigation items: System, Sensors, Updates, Data Sources, Directory services, VPN, Microsoft Defender for Endpoint (which is highlighted), Detection, Entity tags, Exclusions, and Notifications and Reports. The main content area is titled "Microsoft Defender for Endpoint". It contains a toggle switch for "Integration with Microsoft Defender for Endpoint", which is currently turned ON. To the right of the toggle is a "Save" button. Below the toggle, there is a warning message: a yellow triangle icon followed by the text "Feature has not been fully enabled. Enable integration on the Microsoft Defender for Endpoint Portal".

System

Sensors

Updates

Data Sources

Directory services

VPN

Microsoft Defender for Endpoint

Detection

Entity tags

Exclusions

Notifications and Reports

Microsoft Defender for Endpoint

Integration with Microsoft Defender for Endpoint ☒ ON

Save

⚠ Feature has not been fully enabled. Enable integration on the [Microsoft Defender for Endpoint Portal](#)

Configure Exclusions

From the Exclusions tab on the Configuration page:

The screenshot shows the Windows Security Configuration page, specifically the Exclusions tab. The left sidebar contains a list of configuration categories: System, Sensors, Updates, Data Sources, Directory services, VPN, Microsoft Defender for Endpoint, Detection, Entity tags, Exclusions (highlighted), Notifications and Reports, Language, Notifications, Scheduled reports, and Overview. The main content area is titled 'Exclusions' and includes a link 'Learn about MDI security alerts' with an external link icon. Below the title, there are three expandable sections. The first section, 'Suspected overpass-the-hash attack (Kerberos)', is expanded and shows two exclusion categories: 'IP addresses and subnets' with the value '157.54.208.0/24 or 3FFE:FFFF:0:C000::/6' and a plus icon, and 'Computers' with the value 'JOHN-PC' and a plus icon. The second section, 'Suspected NTLM authentication tampering', shows '1 User' and a downward arrow. The third section, 'Suspicious additions to sensitive groups', also shows a downward arrow.

System

Sensors

Updates

Data Sources

Directory services

VPN

Microsoft Defender for Endpoint

Detection

Entity tags

Exclusions

Notifications and Reports

Language

Notifications

Scheduled reports

Overview

Exclusions

[Learn about MDI security alerts](#)

Suspected overpass-the-hash attack (Kerberos) ^

IP addresses and subnets 157.54.208.0/24 or 3FFE:FFFF:0:C000::/6 +

Computers JOHN-PC +

Suspected NTLM authentication tampering 1 User v

Suspicious additions to sensitive groups v

Configure Exclusions

Or from suspicious activity itself:

Reconnaissance using DNS OPEN

Suspicious DNS activity was observed, originating from [WIN-62GIMJT315](#) [WIN-A1LGI2OQR7F](#).

2:29 PM Jan 12, 2018

DNS queries

[WIN-62GIMJT315](#)

- Close**
Close now but alert if it recurs
- Suppress**
Ignore ongoing activity, but alert if it resumes after 7 days
- Close and exclude WIN-62GIMJT315** [?](#)
Close now and do not alert again for this activity from WIN-62GIMJT315
- Download Details**
- Share**
- Delete**
Delete this suspicious activity

TIME	QUERY	ATTEMPTS	RESULT	VIA DNS SERVERS (1)
1/12/18 2:29 PM	contoso.com	→ 1 attempt	ConnectionRefus...	WIN-A1LGI2OQR...

Detection Settings

- Configure exclusions from suspicious activity itself, or from the Exclusions tab on the Configuration page.
- Account enumeration reconnaissance
- Network mapping reconnaissance (DNS)
- gMSA Password retrieval
- User and IP address reconnaissance (SMB)
- User and group membership reconnaissance (SAMR)
- Suspected brute force attack (Kerberos, NTLM)
- Suspected brute force attack (LDAP)
- Honeytoken activity
- Suspected WannaCry ransomware attack
- Suspected brute force attack (SMB)
- Suspected use of Metasploit hacking framework
- Suspected overpass-the-hash attack (Kerberos)
- Malicious request of Data Protection API master key
- Suspicious VPN connection
- Suspected over-pass-the-hash attack (encryption downgrade)
- Suspected golden ticket usage (encryption downgrade)

Detection Settings

- Configure exclusions from suspicious activity itself, or from the Exclusions tab on the Configuration page.
- Suspected skeleton key attack (encryption downgrade)
- Suspected identity theft (pass-the-hash)
- Suspected identity theft (pass-the-ticket)
- Suspected golden ticket usage (forged authorization data)
- Suspicious modification of sensitive groups
- Suspicious service creation
- Suspected golden ticket usage (time anomaly)
- Suspected golden ticket usage (nonexistent account)
- Suspected DCSync attack (replication of directory services)
- Remote code execution attempt
- Suspected DCShadow attack (domain controller promotion)
- Suspected DCShadow attack (DC replication request)
- Suspicious communication over DNS

Configuring Entity Tags

System

Sensors

Updates

Data Sources

Directory services

VPN

Microsoft Defender for Endpoint

Detection

Entity tags

Exclusions

Notifications and Reports

Language

Notifications

Scheduled reports

Preview

Detections

Admin

Delete Instance

Manage role groups

Entity tags

Honeytoken

Honeytoken accounts

user1 or JOHN-PC

+

Sensitive

1 group

Sensitive accounts

user1 or JOHN-PC

+

Sensitive groups

group1

+

Tier 0 Admins

-

Exchange Servers

JOHN-PC

+

Notifications: Alerts

- MDI will send email alerts for events:
- Required Items
- Additional Options
- Data Options

Questions & Answers

GEEK



