Microsoft Security

Securing the hybrid identity infrastructure

Martin Schvartzman
Senior Product Manager @ Microsoft Defender for Identity
@martin77s

Threats related to identities

Benjamin Delpy @gentilkiwi · Sep 16

A new #mimikatz release with #zerologon / CVE-2020-1472 detection, exploit, DCSync support and a lots of love inside ❤️

It now uses direct RPC call (fast and supports unauthenticated on Windows)

> github.com/gentilkiwi/mim...

Thank you: @SecuraBV

March 25, 2022

Okta Notifies Customers of LAPSUS$ Attack

LinkedIn Facebook Twitter Send Embed

Okta, which markets itself as a "leading provider of identity" in the healthcare, public sector, energy, financial services, technology, travel and hospitality, and nonprofit industries, has notified some of its customers that data may have been accessed by cybercriminal group Lapsus$. (Late breaking news—Lapsus$ may be a teenager living in the U.K.). According to Okta, in late January it "detected an attempt to compromise the account of a third party customer support engineer working for one of our subprocessors." According to the forensic investigation, an attacker had access to the support engineer's laptop for five days in January.

WRITTEN BY:

Robinson+Cole Data Privacy + Security Insider

Contact + Follow

Linn Freedman + Follow

PUBLISHED IN:

Cyber Attacks + Follow

Abusing Exchange: One API call away from Domain Admin

11 minute read

In most organisations using Active Directory and Exchange, Exchange servers have such high privileges that being an Administrator on an Exchange server is enough to escalate to Domain Admin. Recently I came across a blog from the ZDI, in which they detail a way to let Exchange authenticate to attackers using NTLM over HTTP. This can be combined with an NTLM relay attack to escalate from any user with a

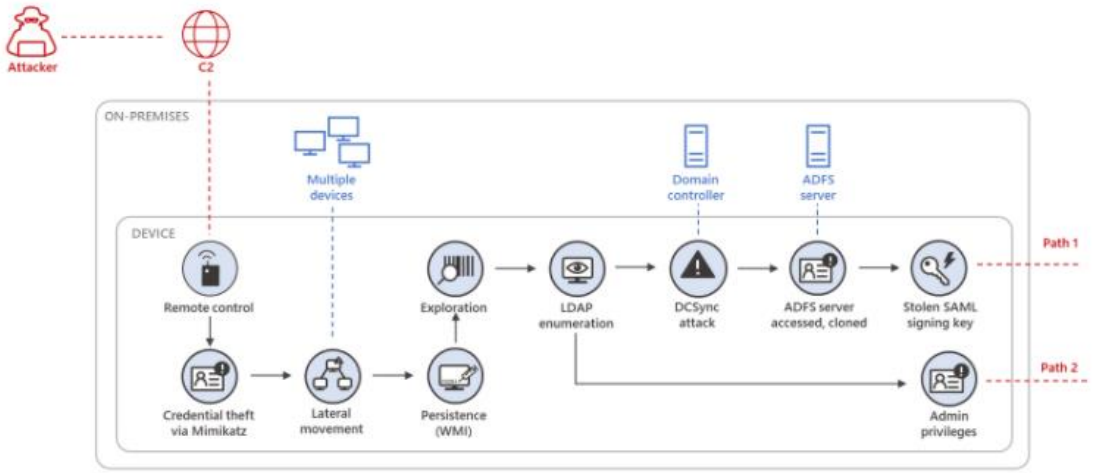
This phishing attack uses an unusual trick to spread further

Attackers enroll Outlook on BYO devices with Azure AD and then spread SharePoint PDF lures.

Written by **Liam Tung, Contributor** on **Jan. 27, 2022**

Solorigate

...after gaining administrative privileges in the organization's on-premises network, and with access to the AD FS server itself, the attacker access and extract the SAML signing certificate. *[December 28 2020]*



PrintNightmare exploit

CVE-2021-1675 / CVE-2021-34527 exploit.

Reflective Dll implementation of the PrintNightmare PoC by Cornelis de Plaa (@Cneelis). The exploit was originally created by Zhiniang Peng (@edwardzpeng) & Xuefeng Li (@lxf02942370).

- It can be used as Remote Code Execution (RCE) exploit (screenshot 1),
- It can be used for Privilege Escalation (screenshot 2).

This implementation has some advantages compared to other public exploits:

- It uses MS-PAR protocol instead of MS-RPRN (credits @cube0x0).
- It is in Reflective DLL form, so can be used directly from Cobaltstrike or other C2 framework.
- It automatically finds the path of the printer driver.

What is the PrintNightmare Vulnerability?

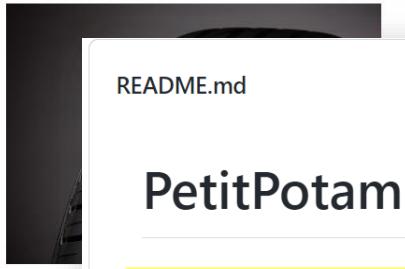
The vulnerability exists on all devices running Windows 7 or higher. It resides in the Windows Print Spooler service and affects the Windows Print Queue. To be more precise, the Print Queue service doesn't restrict access to the RpcAddPrinterDriverEx function, which enables an attacker to run malicious programs on a users' device. An attacker who successfully exploits this vulnerability is able to perform operations with system-level privileges, which means they can access, edit and delete sensitive data, install programs and create new privileged accounts.

Microsoft Fixes Azure Active Directory Issue Exposing Private Key Data

By Kurt Mackie | 11/18/2021

Microsoft **announced on Wednesday** that it fixed an Azure Active Directory private key data storage gaffe that affects Azure application subscribers, but affected organizations nonetheless should carry out specific assessment and remediation tasks.

Affected organizations were notified via the Azure Service Health Notifications message center, Microsoft indicated.



README.md

PetitPotam

PoC tool to coerce Windows hosts to authenticate to other machines via MS-EFSRPC EfsRpcOpenFileRaw or other functions :)

The tools use the LSARPC named pipe with inteface c681d488-d850-11d0-8c52-00c04fd90f7e because it's more prevalent. But it's possible to trigger with the EFSRPC named pipe and interface df1941c5-fe89-4e79-bf10-463657acf44d. It doesn't need credentials against Domain Controller :D

Disabling the EFS service seems not to mitigate the "feature".

Attacking tools are available for all

Downloading BloodHound Binaries

Pre-Compiled BloodHound binaries can be found here.

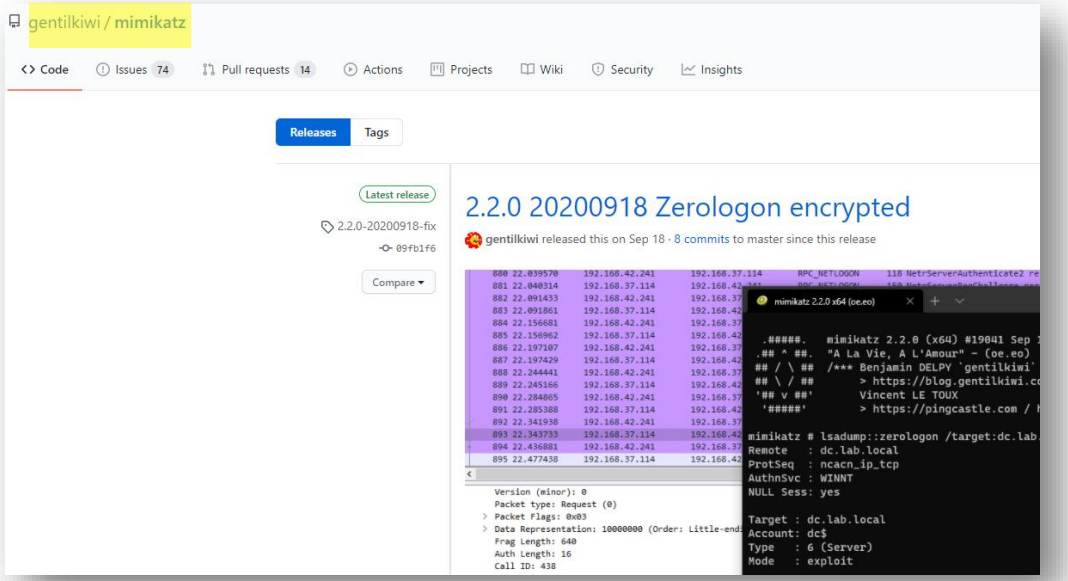
The rolling release will always be updated to the most recent source. Tagged releases are considered "stable" but will likely not have new features or fixes.

About BloodHound

To get started with BloodHound, check out the BloodHound docs.

BloodHound is a single page Javascript web application, built on top of Linkurious, compiled with Electron, with a Neo4j database fed by a C# data collector.

BloodHound uses graph theory to reveal the hidden and often unintended relationships within an Active Directory environment. Attackers can use BloodHound to easily identify highly complex attack paths that would otherwise be impossible to quickly identify. Defenders can use BloodHound to identify and eliminate those same attack paths. Both blue and red teams can use BloodHound to easily gain a deeper understanding of privilege relationships in an Active Directory environment.



ADFSpoof

A python tool to forge AD FS security tokens.

Created by Doug Bienstock (@doughsec) while at Mandiant FireEye.

Detailed Description

ADFSpoof has two main functions:

1. Given the EncryptedPFX blob from the AD FS configuration database and DKM decryption key from Active Directory, produce a usable key/cert pair for token signing.
2. Given a signing key, produce a signed security token that can be used to access a federated application.

This tool is meant to be used in conjunction with ADFSDump. ADFSDump runs on an AD FS server and outputs important information that you will need to use ADFSpoof.

If you are confused by the above, you might want to read up on AD FS first. For more information on AD FS spoofing I will post a link to my TROOPERS 19 talk and slides when they are released.

kerberoast

Kerberoast is a series of tools for attacking MS Kerberos implementations. Below is a brief overview of what each tool does.

Extract all accounts in use as SPN using built in MS tools

```
PS C:\> setspn -T medin -Q */*
```

Request Ticket(s)

One ticket:

```
PS C:\> Add-Type -AssemblyName System.IdentityModel
PS C:\> New-Object System.IdentityModel.Tokens.KerberosRequestorSecurityToken -ArgumentList "HTTP/web01.medin.
```

All the tickets

README.md

RiskySPNs

RiskySPNs is a collection of PowerShell scripts focused on detecting and abusing accounts associated with SP
(Service Principal Name). This module can assist blue teams to identify potentially risky SPNs as well as red te
escalate privileges by leveraging Kerberos and Active Directory.

For detailed information: http://www.cyberark.com/blog/service-accounts-weakest-link-chain/

Usage

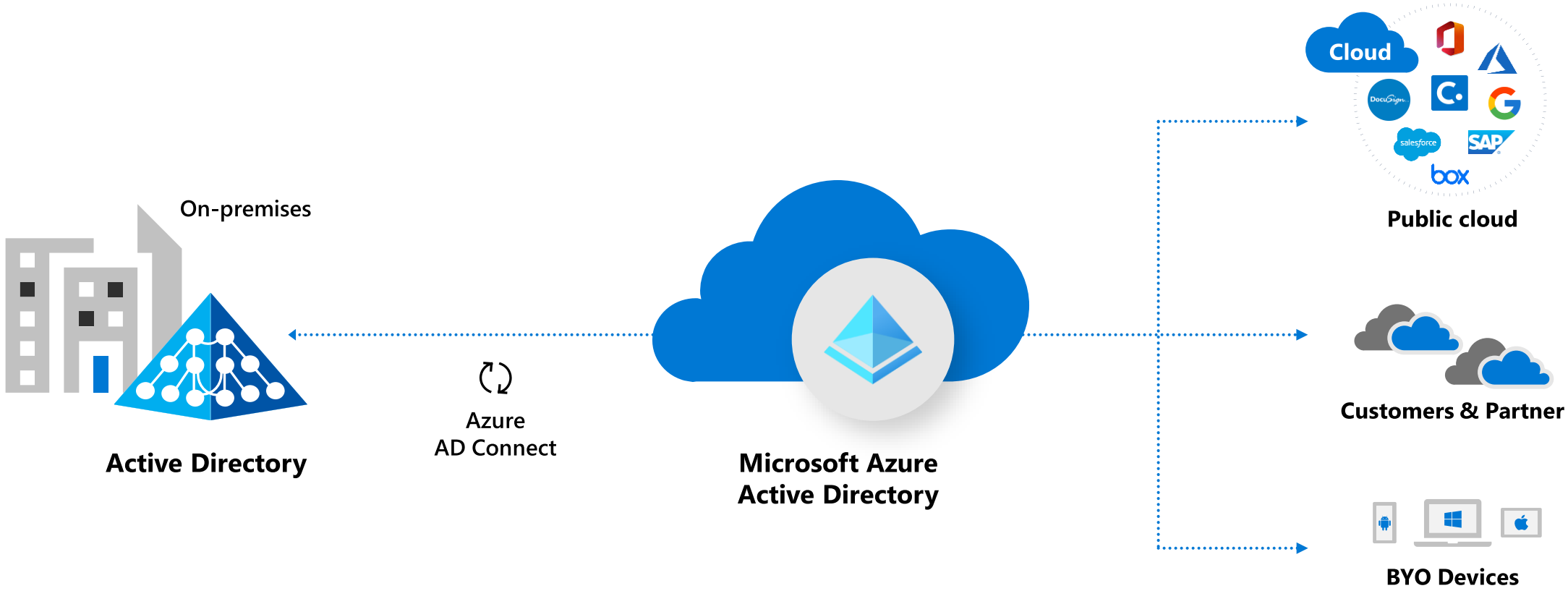
Install the module

Challenges with securing identities

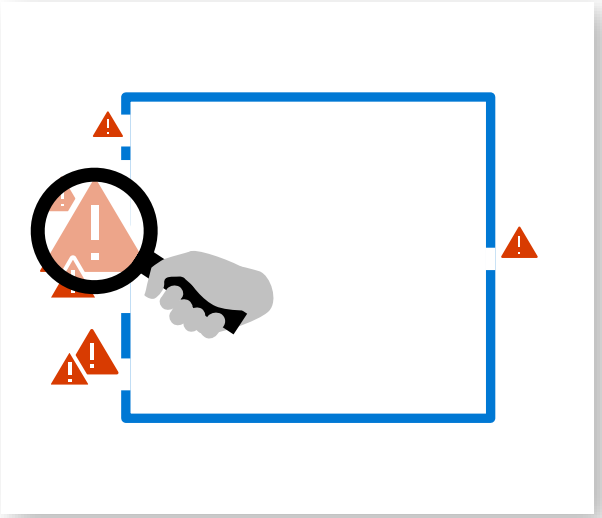
- On-premises and cloud identity platforms
- Identities aren’t just humans
- Establishing baselines for prevention
- Multi-cloud and app explosion
- Identity and security tools are fragmented

The Complexity of the Enterprise Identity Security Landscape

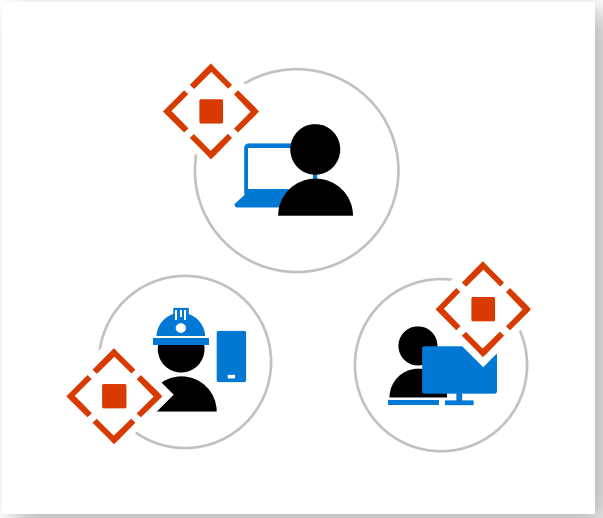
Enterprise security environments are complex and include both on-premises and cloud assets



A Broad Array of Identity Security Risks



It's easy to miss risky configurations . . .



Threats can originate anywhere . . .

Activity volume makes prioritization difficult . . .

It’s a team sport

Identity admin

- MFA and SSO
- Real-time adaptive access
- PAM & identity governance

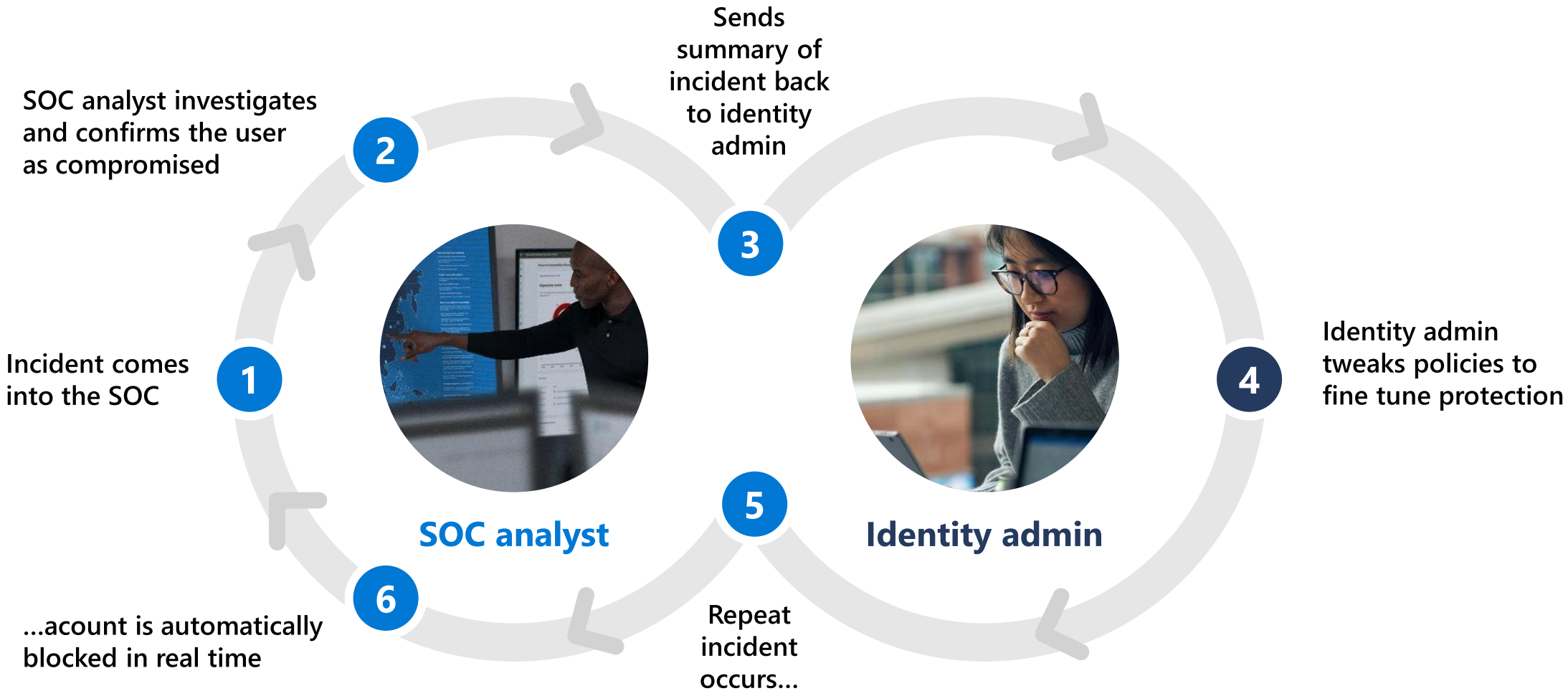
SOC analyst

- Detection and Investigation
- Response
- Automation

Common responsibilities:

Posture management | Policy configuration | Inventory

Identity admin and SOC analyst feedback loop



Microsoft's approach

Secure accounts and infrastructure

- Protect human and workload identities
- Modernization of identity infrastructure
- Proactive posture assessments
- Reconnaissance monitoring
- Highlight riskiest lateral movement paths

Detect attacks with industry-leading intel

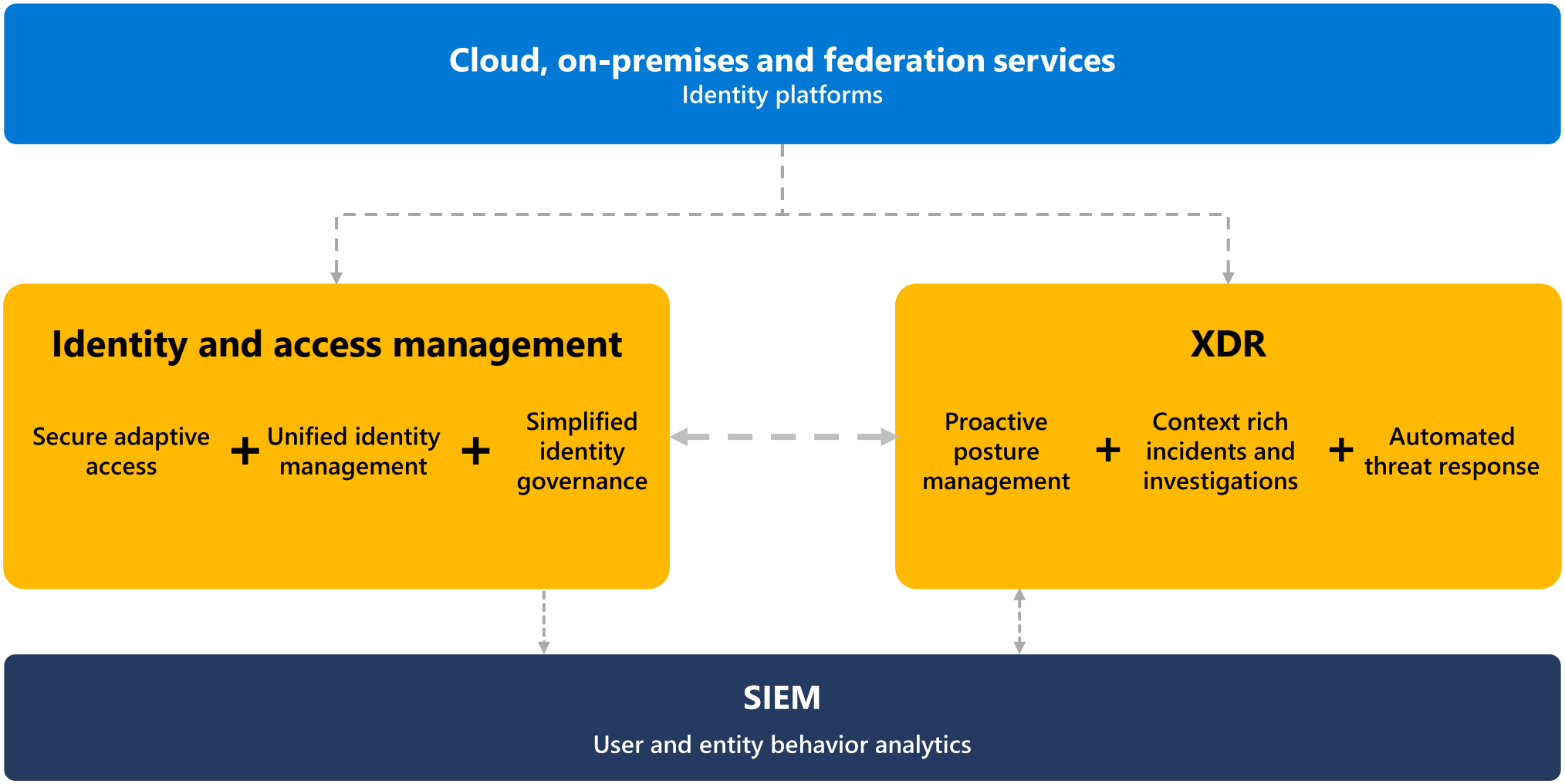
- Real-time ML-based risk detections
- Revoke access in near real-time for critical events
- Cross-platform attack detections
- Role change alerts for privileged accounts
- Honeytoken account deception

Tailored and unified experiences

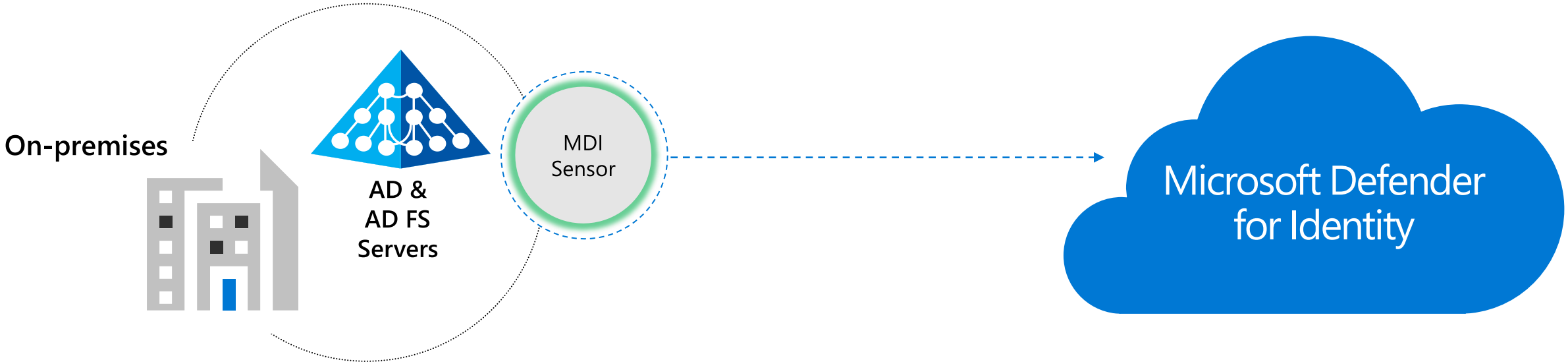
- Visualize investigations using all your signals
- Utilize cross-workload hunting and custom detections
- Combine identity sources into a single view
- Fine-tune policy configuration based on insights from incidents
- Improve effectiveness of response with pre-built risk workbooks

Cloud, on-premises and federated identity platforms

Unified threat protection architecture



MDI Data Sources and Technologies



Network traffic analytics

NTLM, Kerberos, LDAP, RPC, DNS, SMB

Security events and event tracing

Security Events
Event Tracing (ETW)
Profile AD entities

User behavior analytics

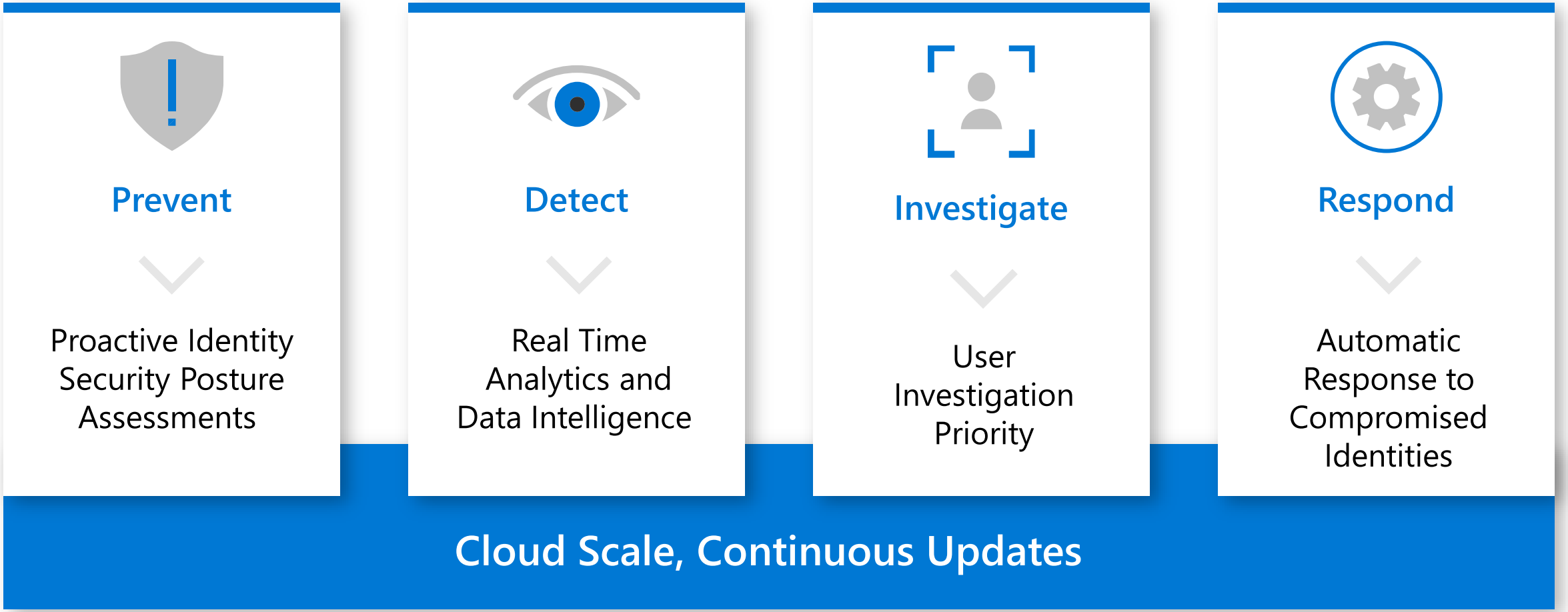
Profile users & entities behavior, identify behavior anomalies

Cloud based real-time detections

Data enrichment and correlation in the cloud, for real time detections

Microsoft Defender for Identity for Identity Protection

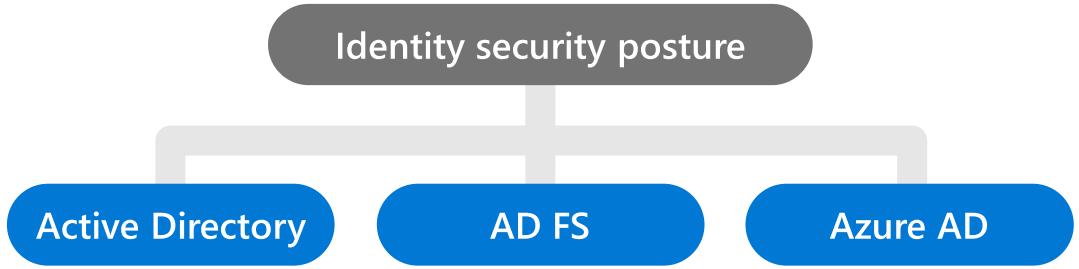
Microsoft Defender for Identity helps protect user identity as part of on-premises and cloud enterprise environments.



Identity security posture

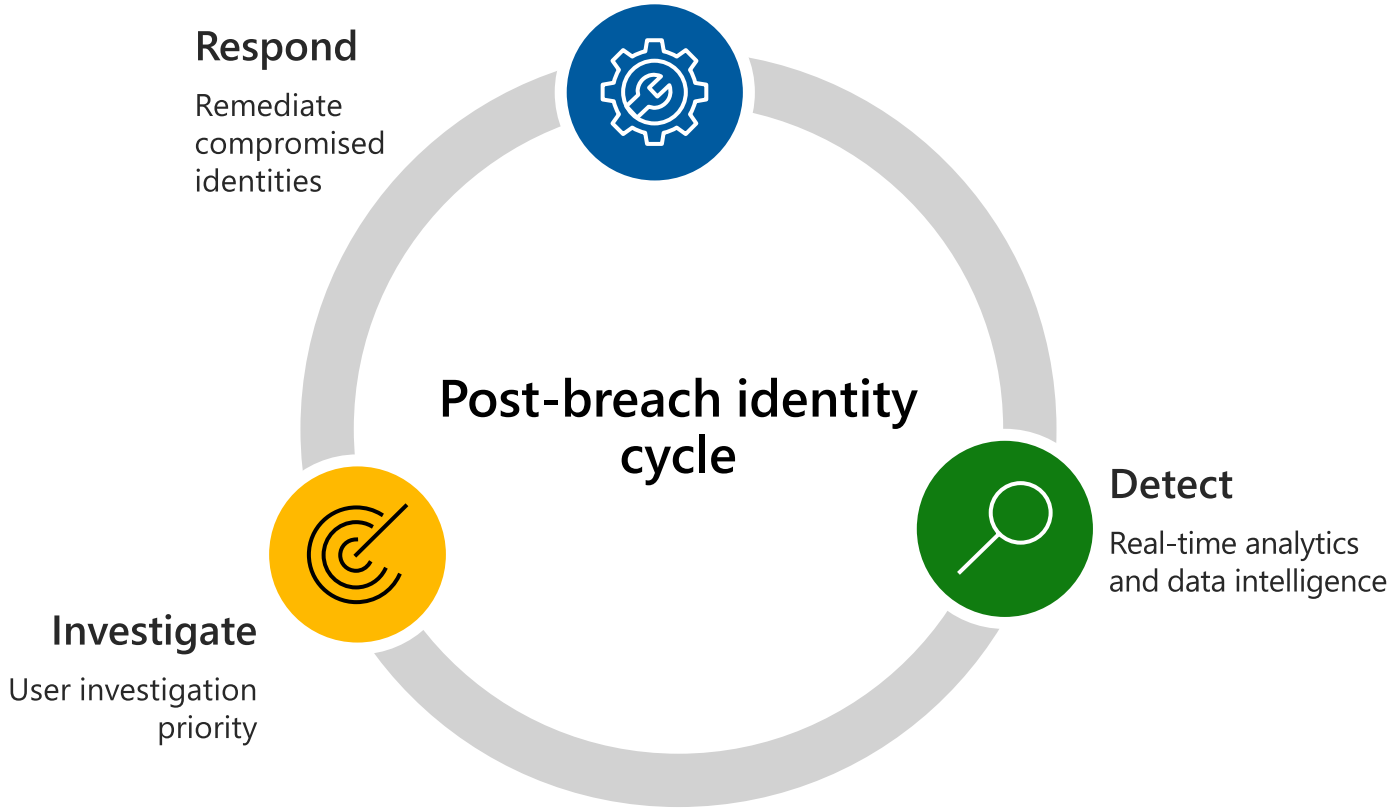
Top improvement actions

- Enable MFA for Admins
- Dormant entries in sensitive groups
- Clear text credentials in place
- Use limited administrative roles
- Reduce risky lateral movement paths



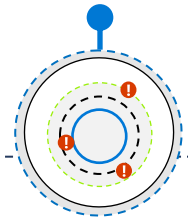
Secure Score

▲ **49.86%**


Respond
Remediate compromised identities
Post-breach identity cycle
Detect
Real-time analytics and data intelligence
Investigate
User investigation priority

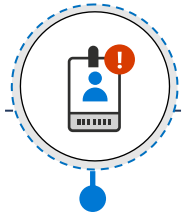
Detection of Identity related attacks

Discovery



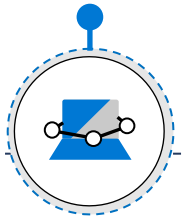
- Security principal enumeration (LDAP)
- Users group membership enumeration
- Users & IP address enumeration
- Hosts & server name enumeration (DNS)
- Resource access suspicious activities
- Reconnaissance by targeted entity attributes

Initial access



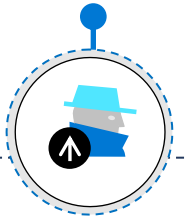
- Brute force attempts via ADFS
- Suspicious VPN connection
- Honey Token account suspicious activities
- Logon/Failed logon & resource access suspicious activities
- Suspected Kerberos SPN exposure
- Suspicious DC Password change using NetLogon (CVE-2020-1472)

Lateral movement



- NTLM Relay & NTLM tampering
- Pass-the-Ticket
- Pass-the-Hash, Overpass-the-Hash
- Suspicious groups membership changes
- Suspicious SID history injection
- Suspicious rogue certificate

Persistence

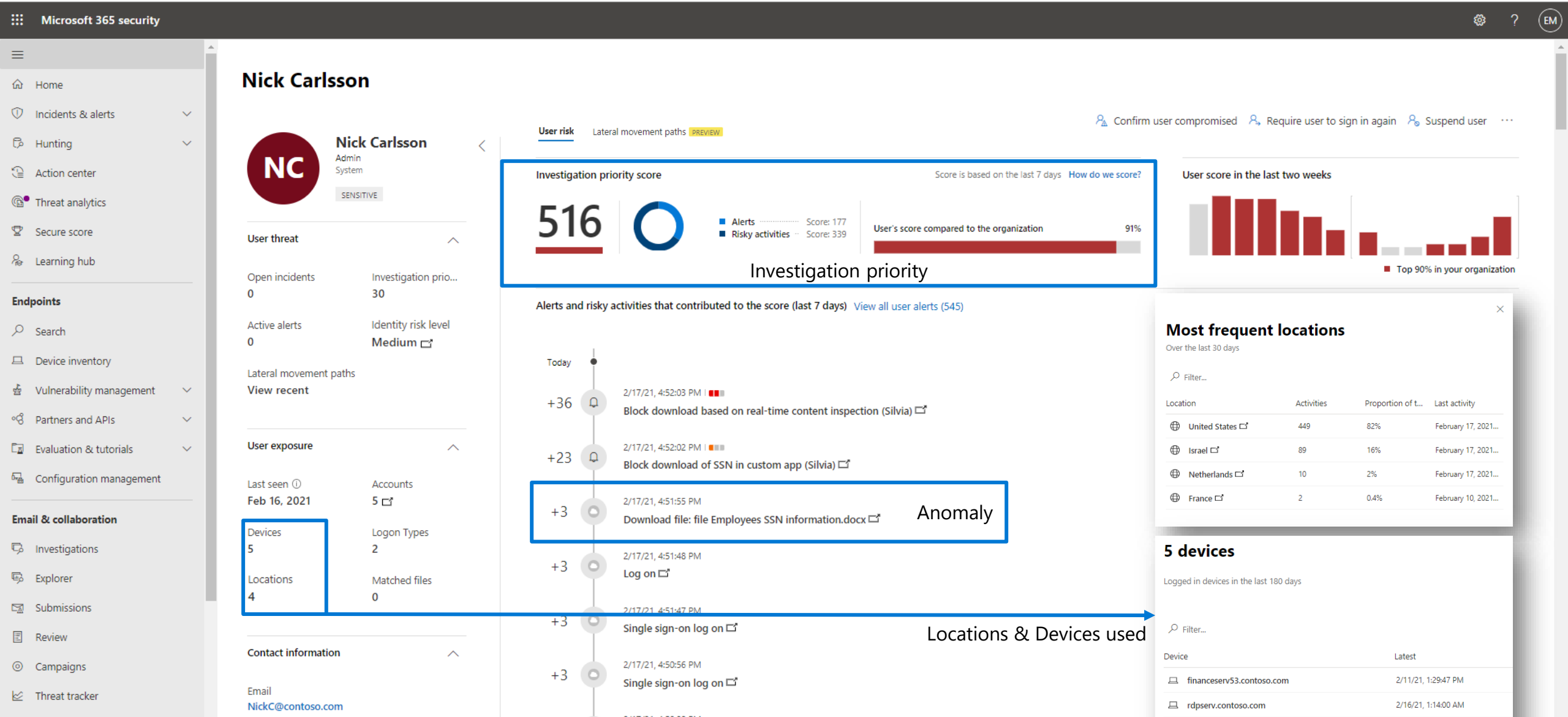


- ADFS Dump Activity
- Suspicious new ADFS trusted domain
- Golden ticket attack
- DCShadow, DCSync
- AD Objects & hashes exfiltration (NTDS.DIT)
- Code execution/Service creation on DC and ADFS
- SMB packet manipulation
- Skeleton Key
- Golden ticket leveraging RBCD
- DNS Remote code execution attempt (CV 2020-1305)

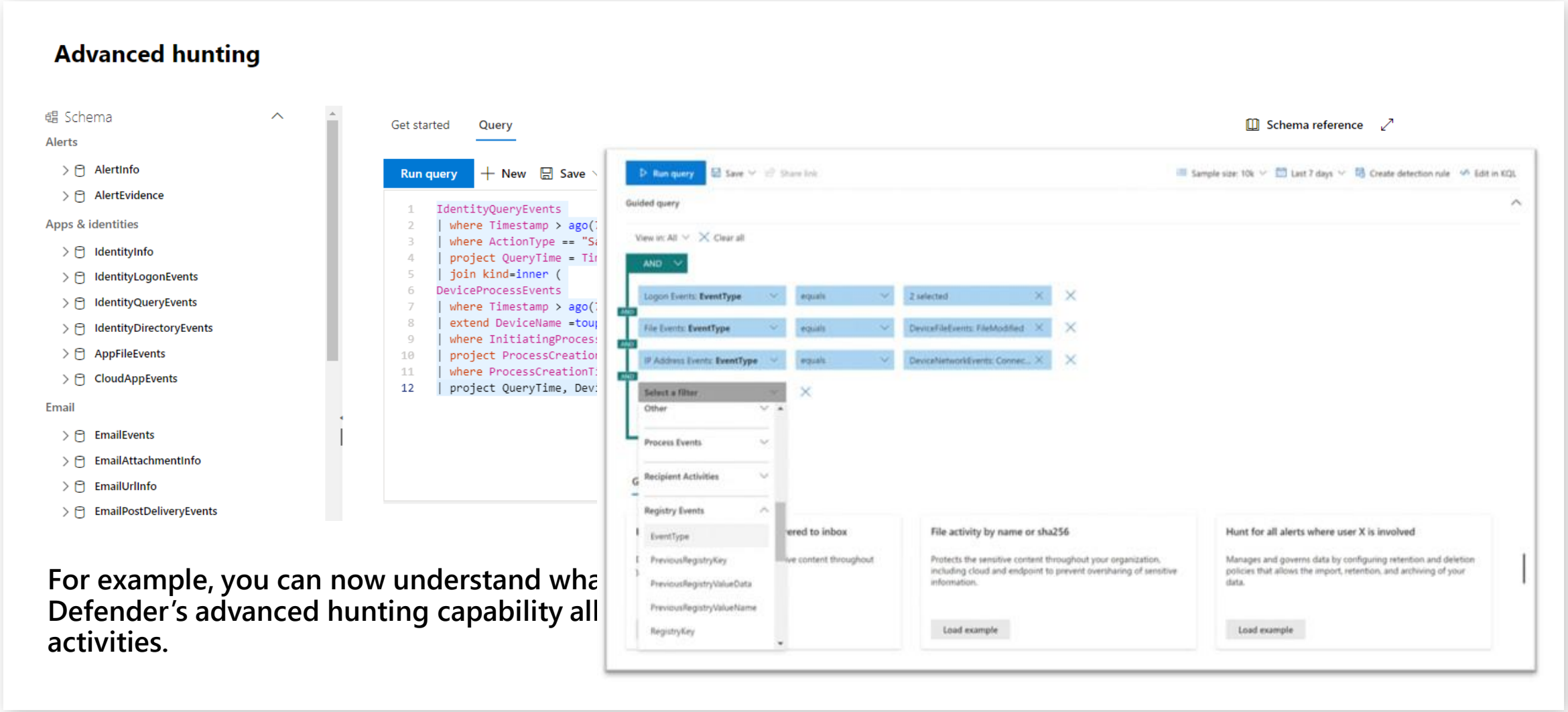
Activity Behavior Analysis by User, Peers, and Organization

- Login to devices
- Access to on-premises resources
- Remote connections to servers
- Access to cloud applications
- Usage of SharePoint Online sites
- User agent, location & ISP analytics
- Mailbox behavior
- Failed logins behavior

User Entity page & User Investigation Priority



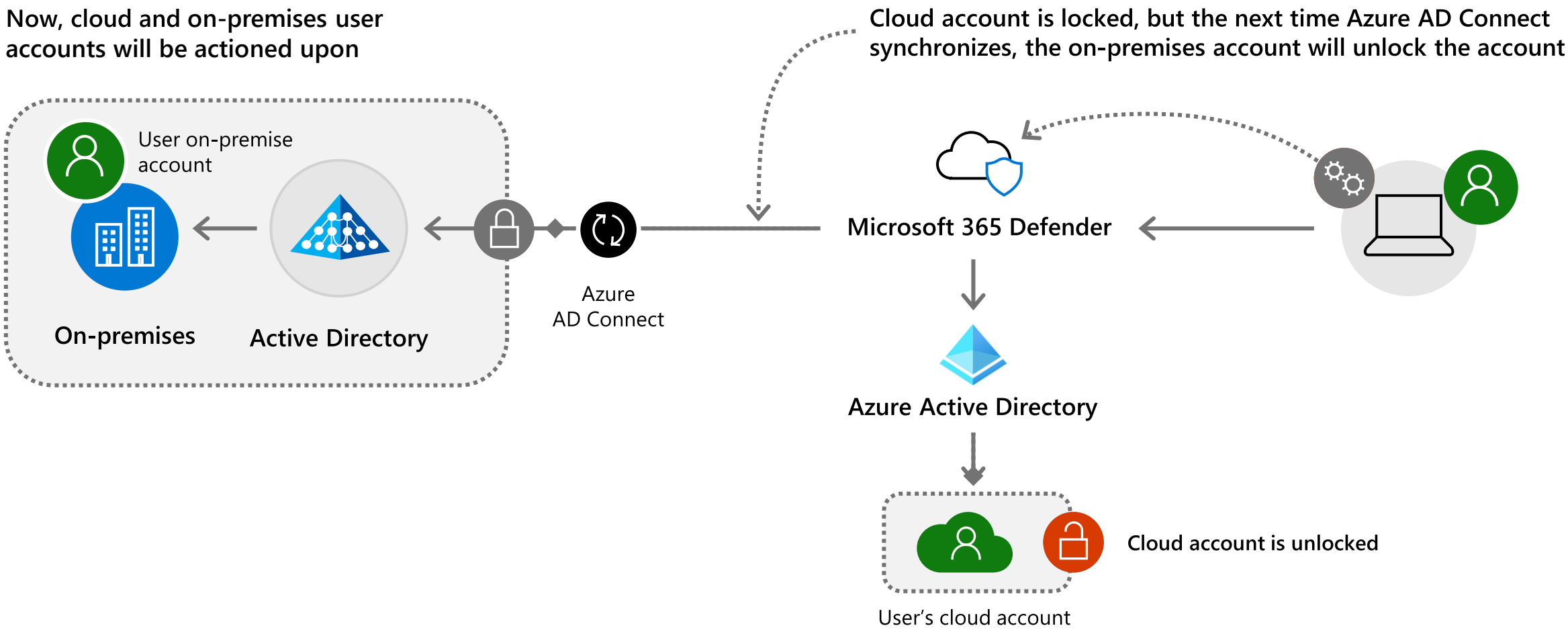
Advanced hunting in Microsoft 365 Defender



For example, you can now understand wha
Defender's advanced hunting capability all
activities.

Response and remediation actions

Enabling cloud and on-premises accounts to be protected immediately



Red vs Blue

To provide a safe playing field for a SOC team to improve investigating, managing and hunting for incidents generated in real time against a real-life environment.

The environment has onboarded devices, mailboxes, users and AAD accounts that resemble a corporate environment. Basic network and system information is shared.

Red team's mission

- **Execute attacks against the blue team's environment, following paths and tactics and using tools taken from real world breach cases. Infiltrating the environment, move laterally and compromises assets until they get to their final goal.**

Blue team's mission

- **Analyze and investigate incidents and alerts, hunt for red team's activities, and report their findings at the end of the game.**

At the end of the event, both teams meet. The red team is walking the blue team through the attack scenario in detail, while the blue team is sharing feedback on how they investigated and what challenges they faced during their investigation.