Securing Active Directory Domain Services (AD DS) with Microsoft Defender for Identity

Identify, detect, and investigate advanced cyber threats using intelligence from Active Directory

Detect Advanced Threats in Hybrid Environments

Bad actors looking to compromise user credentials will look for every way possible to carry out an attack. Starting with reconnaissance, successful cybercriminals can end up with domain dominance. With Microsoft Defender for Identity, you can protect your organization against threats at all stages across your modern identity environment.

Defender for Identity enables SecOp analysts and security professionals to

- ☑ Monitor users, entity behavior, and activities with learning-based analytics

- ☑ Identify and investigate suspicious user activities and advanced attacks throughout the cyber-attack kill-chain

- ☑ Protect user identities and credentials stored in Active Directory

- ☑ Provide clear incident information on a simple timeline for fast triage

Get implementation steps and learn best practices for configuring Defender for Identity for on-prem AD Domain Controllers and/or AD Federation Services and/or AD Certificate Service during this three-week implementation.

As part of securing your identity, Bulletproof will:

Enable Microsoft Defender for Identity.

Install Sensor on Domain Controllers.

Configure Windows Event Collection, Microsoft Defender for Identity action accounts, sensitive users, Honeytoken accounts, SAM-R to enable lateral movement path detection, and domain service account DSA or GMSA.

If needed, configure endpoint proxy and Internet connectivity settings, enable Azure Sentinel Data Connector, integrate MDI and other Defender solutions, and configure required permissions for the Microsoft 365 Defender experience and Role Groups.

Plan capacity for Microsoft Defender for Identity deployment.

Customers who will benefit the most out of this implementation

Have E5 or Microsoft Defender for Identity standalone licenses who need help in implementation

Are exploring the use of Microsoft Sentinel, and need to enable all the Defender suite solutions to get full value of the Microsoft Defender suite

Need to know what are the benefits of using Microsoft Defender for Identity

Provide clear incident information on a simple timeline for fast triage

About Bulletproof

With locations across North America and around the globe, Bulletproof, a GLI company has decades of IT, security, and compliance expertise. Bulletproof works with various industries of all sizes and leverages its extensive industry experience to mitigate risk and improve client processes, systems, and business infrastructure.

Named Microsoft's global Security Partner of the Year in 2021 for delivering excellence and innovative end-to-end security solutions, Bulletproof is also a member of the Microsoft Intelligent Security Association (MISA).

Microsoft Intelligent Security Association

Microsoft

Microsoft Verified Managed XDR Solution

Microsoft Partner

2021 Partner of the Year Security Award

Microsoft