silent4business

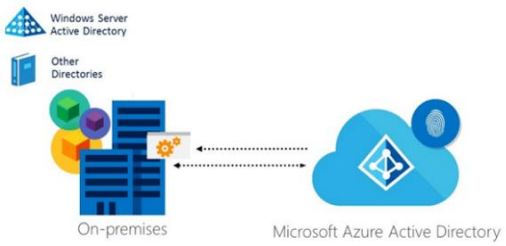
Microsoft Security

On-premise Identities

Defender for identity

Protect user accounts and credentials in on-premises environments from risky access and anomalous activity.

SILENT4BUSINESS and Microsoft Defender for Identity enable detection and response to identity compromises in accounts hosted in on-premises Active Directory. The service monitors domain controllers, identifies lateral movement, privilege escalation attempts, and credential misuse, automating threat responses to prevent unauthorized access and safeguard organizational resources.



- Continuous analysis of network traffic and Active Directory activity in real time.
- Identification of compromised accounts, privilege abuse, and exposed credentials.
- Detection of attacks such as Pass-the-Ticket, Pass-the-Hash and Golden Ticket.
- Correlation of events to understand the context of each threat.

70+ Suspicious activities detected per day in on-premises environments protected with Defender for Identity.

92% of internal identity threats in on-premises Active Directory are detected within the first 24 hours with Microsoft Defender for Identity.

Benefits of Defender for Identity for On-premise Identities

Detect internal threats such as lateral movement, privilege abuse, or the use of stolen credentials.

Strengthen domain security against advanced persistent attacks.

Respond proactively to anomalous behavior patterns in the local environment.

SILENT4BUSINESS implements Microsoft Defender for Identity to protect on-premises environments from the core: your Active Directory. We detect suspicious patterns, block threats in real time, and provide actionable insights to prevent breaches and insider attacks.

Contact us today.

gerardo.garibay@silent4business.com

https://silent4business.com/

55 7823 3000