SILVERFORT | Microsoft

Unified XDR & Identity Threat Protection

Enable Entra MFA and Conditional Access as a real-time response to Microsoft Defender's detected threats in legacy on-prem environments

Today's data breaches and ransomware attacks often include two key components – exploiting the endpoint and using compromised credentials to move laterally to additional resources. Silverfort and Microsoft have joined forces to deliver unmatched real-time detection and prevention of identity threats in a unified manner, across all resources and environments.

Microsoft 365 Defender & Silverfort: Stopping Identity Attacks

The integration of Microsoft 365 Defender and Silverfort enables organizations to complement their existing identity threat detection capabilities with real-time prevention.

Microsoft 365 Defender detects malicious activity that targets the enterprise's endpoints, identities, Office 365, and cloud apps, while Silverfort responds by blocking detected identity threats in real time. This collaboration of leading XDR and Identity Threat Detection and Response capabilities enables organizations to increase their resilience against today's evolving threats, including account takeover, lateral movement, and ransomware propagation, while preventing them in real-time without disrupting the business.

KEY BENEFITS

Extend Entra MFA

To on-prem legacy applications, command line access to workstations and servers, IT/OT infrastructure and other resources that couldn't be protected with MFA before.

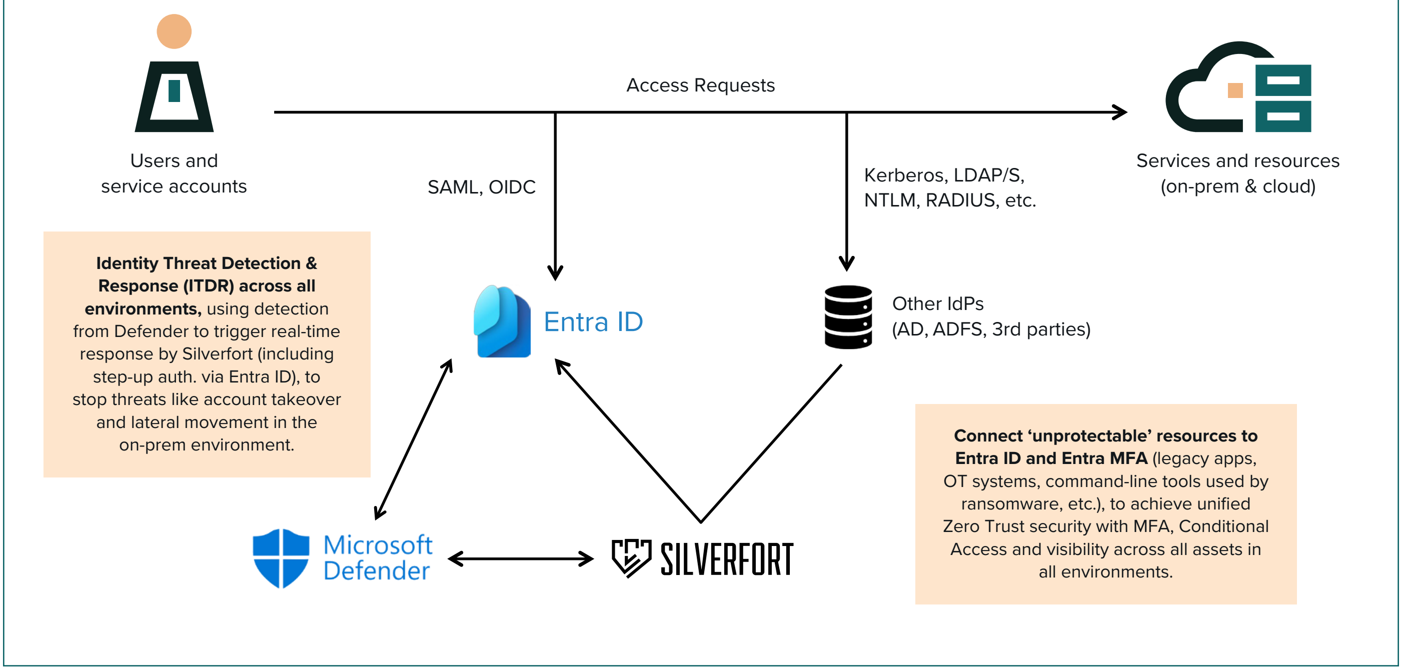
Response Without Disruption

Prevent compromised users from accessing resources, while allowing legitimate users to prove their identity and avoid interruption.

Identity Zero Trust

Enforce granular authentication and access policies for any access to corporate resources, based on the user's risk.

Silverfort & Microsoft Integrations



Users and service accounts
Access Requests
Services and resources (on-prem & cloud)
SAML, OIDC
Kerberos, LDAP/S, NTLM, RADIUS, etc.
Entra ID
Other IdPs (AD, ADFS, 3rd parties)
Microsoft Defender
SILVERFORT

Identity Threat Detection & Response (ITDR) across all environments, using detection from Defender to trigger real-time response by Silverfort (including step-up auth. via Entra ID), to stop threats like account takeover and lateral movement in the on-prem environment.

Connect 'unprotectable' resources to Entra ID and Entra MFA (legacy apps, OT systems, command-line tools used by ransomware, etc.), to achieve unified Zero Trust security with MFA, Conditional Access and visibility across all assets in all environments.

How the Microsoft 365 Defender and Silverfort Integration Works

When Microsoft 365 Defender detects a threat, for example, compromised credentials being used in a Pass the Hash attack, it raises the user risk level and triggers an Entra ID (formerly Azure AD) Conditional Access policy, while Silverfort extends this policy to on-prem and non-Entra ID authentications in real-time. This helps prevent attacks that are utilizing access interfaces that don't support MFA or modern authentication, such as command-line tools (including those used by ransomware), file shares and critical IT/OT infrastructure.

In addition to stopping attacks in real-time, this unique integration enables security teams to dramatically reduce false positive alerts by utilizing MFA as the ideal least intrusive protection capability. The use of MFA offloads the initial threat response from the security team while providing its security analysts with concrete, actionable information to easily spot the malicious activity and eradicate its presence.

Microsoft
Co-Sell Ready
Partner

Microsoft preferred solution

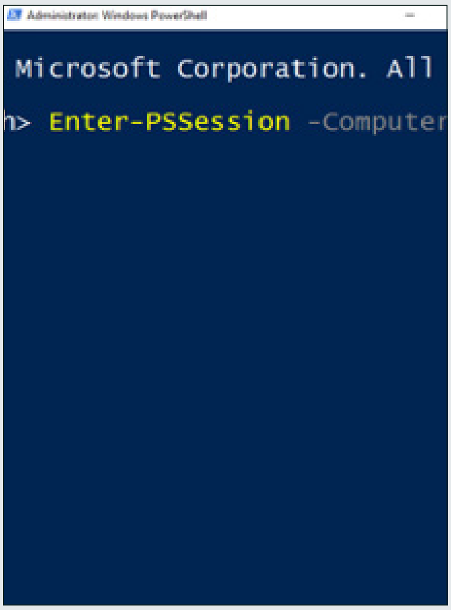
Microsoft Security 2023
'Zero Trust Champion' Winner

Microsoft Top Tier Partner

Extended Entra MFA User Experience: How it Works

1

Attempted access via remote PowerShell

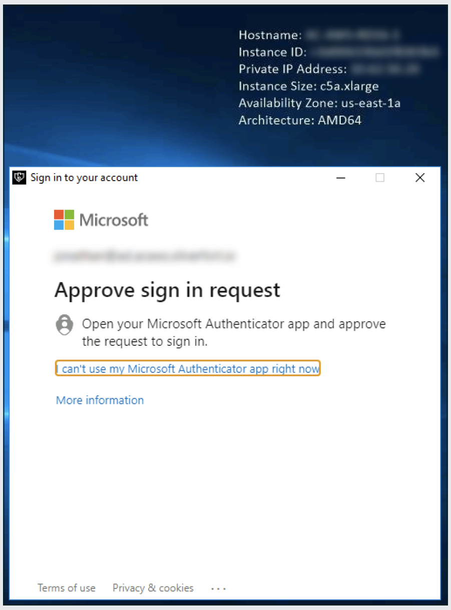


```
Administrator: Windows PowerShell
Microsoft Corporation. All
h> Enter-PSSession -Computer
```

PowerShell remote access interface that doesn't natively support MFA

2

Microsoft sign-in pop up



```
Hostname: [redacted]
Instance ID: [redacted]
Private IP Address: [redacted]
Instance Size: c5a.xlarge
Availability Zone: us-east-1a
Architecture: AMD64
```

Sign in to your account

Microsoft

[redacted]

Approve sign in request

Open your Microsoft Authenticator app and approve the request to sign in.

I can't use my Microsoft Authenticator app right now

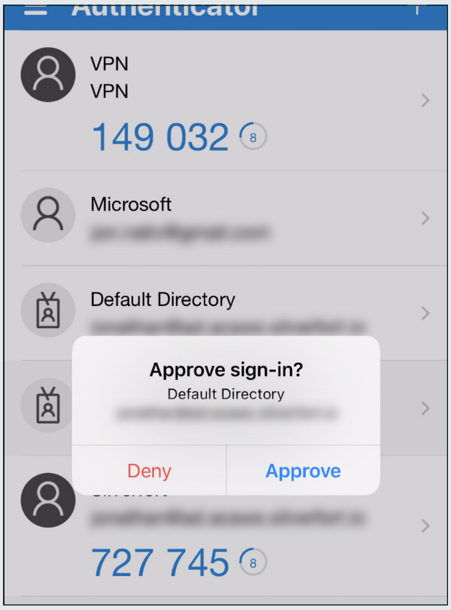
More information

Terms of use Privacy & cookies ...

With Silverfort integration, PowerShell now triggers a Microsoft sign-in request

3

Microsoft Authenticator verification



Authenticator

VPN
VPN
149 032 8

Microsoft
[redacted]

Default Directory
[redacted]

Approve sign-in?
Default Directory
[redacted]

Deny Approve

[redacted]
727 745 8

PowerShell access is now protected with MFA

> "The integration with Silverfort allows customers to extend the power and flexibility of Entra ID to many additional resources and applications across hybrid and multi-cloud environments, and unify their identity management and protection on Entra ID."
>
> *Sue Bohn, Partner Director, Microsoft Identity Division*

To learn more about Silverfort's integration with Microsoft 365 Defender, please reach out to microsoft@silverfort.com