Silverfort | Microsoft

Enhancing Microsoft's ability to protect leaked credentials with Silverfort

With Microsoft's real-time credential leak detection and Silverfort's Conditional Access policies, Entra ID can block any malicious access to resources and environments.

More than 80% of organizations have experienced a breach involving compromised credentials, which are often used to move laterally across environments and to other resources. To prevent these attacks, Silverfort has integrated with Microsoft Entra ID to deliver unmatched real-time detection and prevention of identity threats across all resources and environments.

Detecting and preventing lateral movement attacks

Microsoft and Silverfort's integration provides organizations with real-time detection and prevention capabilities.

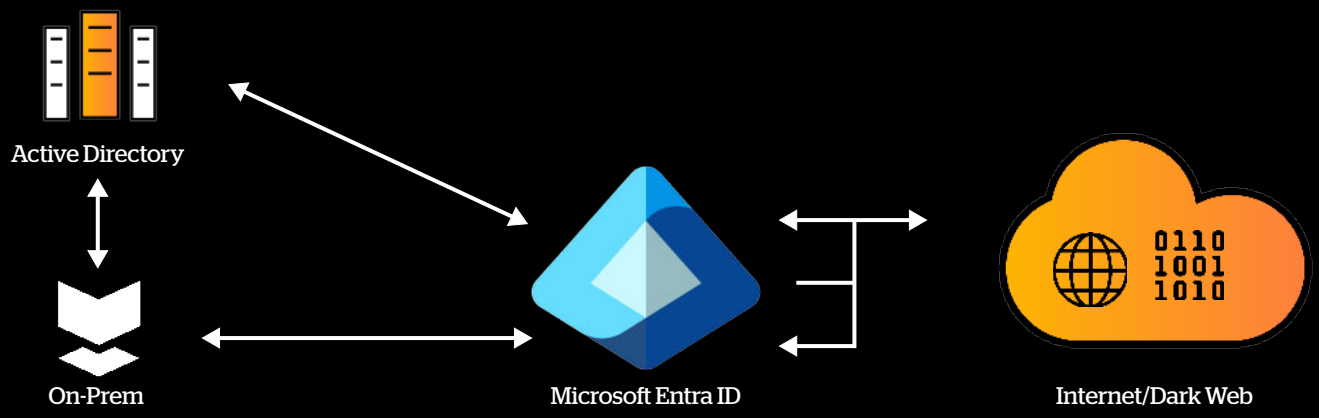
Microsoft's risk indicators detect if a user's credentials have been compromised, while Silverfort responds by enforcing deny access or MFA policies. This blocks malicious actors from using compromised credentials in real time, while reducing the rate of false positives. By adding another level of protection to the identity layer, organizations strengthen their resilience to evolving identity threats and have the proper security controls in place to prevent lateral movement.

How Silverfort adds real-time prevention to Microsoft's risk indicators

If Microsoft detects that a user's credentials may have been compromised, it calculates the detection in offline mode and compares the credentials to values in external databases. These are then checked against the Entra users' current valid credentials. If the credentials are compromised, the user risk level is raised, and an Entra ID Conditional Access policy is triggered. Silverfort automatically extends this policy to on-prem authentication as well as non-Entra ID authentication.

By applying the Conditional Access policy, when the compromised credentials are next used, the access request will be denied, preventing lateral movement within the environment.

How does it work



1. Password hashes are synced from AD to Entra ID
2. Entra ID compares hashes to leaked credentials from internet databases
3. Entra ID checks the list of leaked credentials against Entra ID accounts and on-prem accounts (through the password hash sync)
4. The user's risk level is updated if a compromised credential is found
5. MFA/Blocking can be enforced for on-prem authentication through Silverfort using Entra ID Bridging or Silverfort's risk-based policies.

Key benefits

Protect the 'Unprotectable'

Extend Entra ID MFA and access policies to any resource, including on-prem servers, legacy apps, IT infrastructure, and command-line tools.

Response without disruption

Block compromised users from accessing resources while allowing legitimate users to prove their identity and avoid disruption.

Prevent lateral movement

Proactively prevent lateral movement attacks and ransomware propagation.

Hybrid Attack Protection

Detect and prevent advanced lateral movement attacks that connect between the on-prem and cloud environments.

About Silverfort

Silverfort secures every dimension of identity. We deliver end-to-end identity security that is easy to deploy and won't disrupt business operations, resulting in better security outcomes with less work. Discover every identity, analyze exposures, and enforce protection inline to stop lateral movement, ransomware, and other identity threats.