Silverfort | Microsoft

Silverfort and Microsoft Defender for Endpoint (MDE)

As the threat landscape evolves and cyberattacks become more complex, security teams need more integrated and proactive approaches to threat detection and response. With identity now as the entry point to most attacks, adversaries routinely exploit credential-based access to infiltrate environments, evade detection, and move laterally without being noticed.

To counter these threats, Silverfort and Microsoft Defender for Endpoint (MDE) deliver a powerful integration that extends identity risk intelligence into the endpoint layer. Silverfort adds deep authentication visibility across users, devices, and access protocols, while MDE provides endpoint detection and response capabilities. Together, they enhance endpoint investigations by incorporating real-time identity risk context, enabling smarter prioritization, streamlined response workflows, and earlier containment of identity-driven threats.

Identity-driven risk synchronization for endpoint protection

The integration between MDE and Silverfort extends threat detection into the identity layer while leveraging Defender's endpoint protection capabilities. Silverfort's Identity Threat Detection and Response (ITDR) continuously monitors authentication activity across hybrid environments and synchronizes identity risk signals directly to MDE.

Risk synchronization occurs from Silverfort to Microsoft Defender for Endpoint:

Silverfort assigns dynamic risk scores to monitored identities and devices. These risk levels are synchronized to MDE by automatically adding or removing machine tags based on the associated identity or host risk level.

Tag synchronization follows defined thresholds:

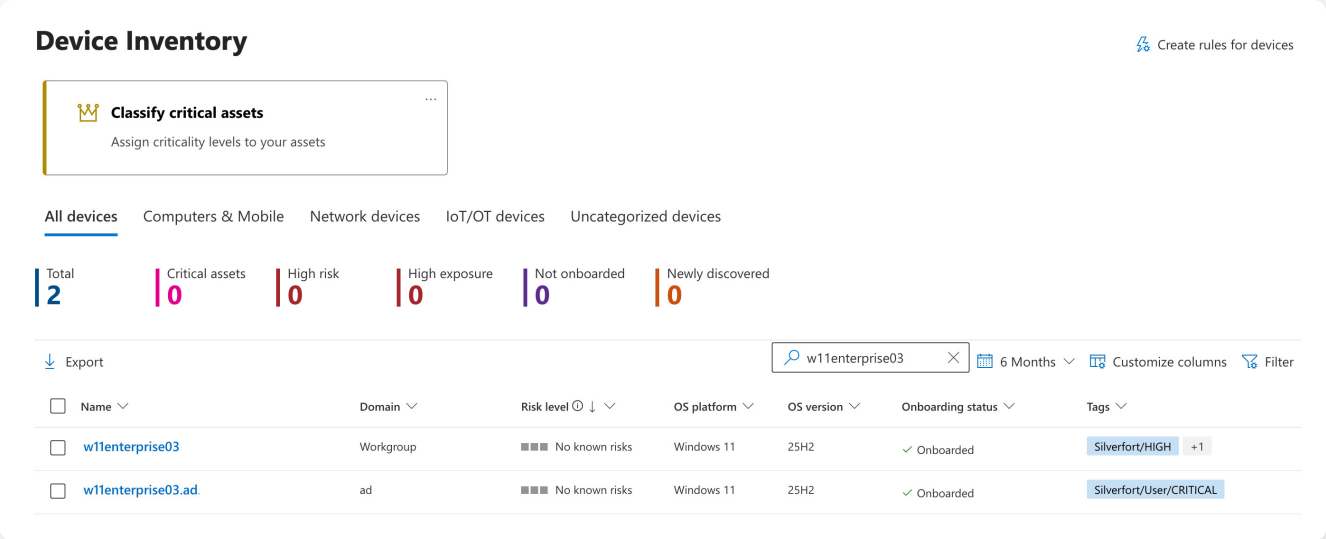
- **Critical risk** → Critical tag applied
- **High or above** → High/Critical tag applied
- **Medium or above** → Medium/High/Critical tag applied
- Tags are automatically removed when risk levels fall below the configured threshold

This enables security teams to filter, prioritize, and automate Defender workflows based on identity-driven risk.

How it works

The Silverfort and MDE integration enhances endpoint visibility with real-time identity intelligence, enabling security teams to act faster and more effectively. When Silverfort identifies risky behavior, such as abnormal login attempts, lateral movement, or use of compromised credentials, it flags the associated users or devices. These risk levels are synchronized to MDE by applying machine tags that reflect the current identity risk level. Endpoint analysts can immediately identify devices associated with high-risk identities, prioritize investigations, and apply conditional workflows or automated actions with MDE.

By combining Silverfort's deep identity intelligence with MDE's advanced threat protection capabilities, organizations gain enriched endpoint context and improved prioritization of identity-driven threats.



Key benefits

Enhanced threat hunting

Link anomalous login behavior to suspicious endpoint activity to improve hunt accuracy.

Investigate with full identity context

Correlate user authentication activity with endpoint detections for faster, more precise investigations.

User-centric risk propagation

Automatically apply identity risk across all active user sessions and devices – not just the initially compromised endpoint.

Lateral movement prevention

Detect and contain identity-driven threats before attackers can pivot across systems or escalate privileges.

Automated workflow prioritization

Use synchronized risk tags to filter, group, and trigger Defender-based workflows aligned with identity risk levels.

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.