Silverfort and SentinelOne

Identity Threat Protection

The evolving threat landscape and the sophistication of attack methods have forced security stakeholders to continuously rethink how to deliver sound protection to their organizations. Lateral movement and ransomware propagation are increasing in volume with compromised credentials and file-less malware as the most frequently used attack vectors. To address this challenge, SentinelOne and Silverfort join forces in providing a new integration that protects the endpoint and identity attack surfaces.

SentinelOne and Silverfort Protecting User Identity and Endpoints

The integration of SentinelOne and Silverfort empowers organizations to expand the protection they get from the Singularity XDR platform to the identity control plane. SentinelOne blocks the execution of exploits, malware, and fileless attacks in real-time, and Silverfort prevents any attack that utilizes compromised credentials to access targeted resources on-prem and in the cloud. Bringing together leading XDR and identity protection solutions increases resilience against today's threat landscape.

How SentinelOne and Silverfort Prevent Incoming Attacks

Mutual customers benefit by integrating SentinelOne and Silverfort to provide unified protection against endpoint and identity attacks. Silverfort alerts SentinelOne about identity-based threats, like brute force attacks, account takeovers, lateral movement attacks, and more. Silverfort identifies user data such as user risk and denied authentications and shares this data with SentinelOne, which triggers its autonomous response process on all the machines this user is logged in to. Additionally, when SentinelOne detects malicious execution on an endpoint, the integration between both platforms updates the risk level of all users due to this malicious activity and shares this data with Silverfort. Silverfort identity protection now automatically enforces security policies for all user activity including block policies for critical assets, critical users and MFA protection.

KEY BENEFITS

Prevent Lateral Movement
Gain proactive prevention of lateral movement attacks and ransomware propagation.

Investigate with Full Context
Get comprehensive and granular visibility to both process execution and user authentications.

Respond without Disruption
Prevent compromised users from accessing resources with MFA verification.

Enhanced Threat Hunting
Detection of hidden malicious presence and activity by analyzing both users' authentication trail and their respective process activity.

Identity Zero Trust
Enforce granular access policies upon each access request to an organization resource.