Silverfort and Netskope's risk intelligence integration

Organizations face growing challenges in maintaining real-time visibility for user risk across cloud and hybrid environments. Often, security tools and inconsistent identity signals are isolated, which can lead to security blind spots in detecting threats like compromised credentials and lateral movement. To address this challenge, Silverfort and Netskope developed a seamless integration that enhances access decisions using identity risk signals exchanged between the two platforms via API.

Enforcing access with shared real-time risk context

Through the integration between Silverfort and Netskope, organizations strengthen their ability to make risk-based access decisions across cloud apps and web traffic based on identity risk. Silverfort provides user-specific identity risk assessments via its API, which are consumed and normalized by a Cloud Risk Exchange (CRE) plugin in Netskope. These identity risk signals are then used to dynamically adjust Netskope's User Confidence Index (UCI), allowing access decisions to reflect users' real-time behavior and security posture.

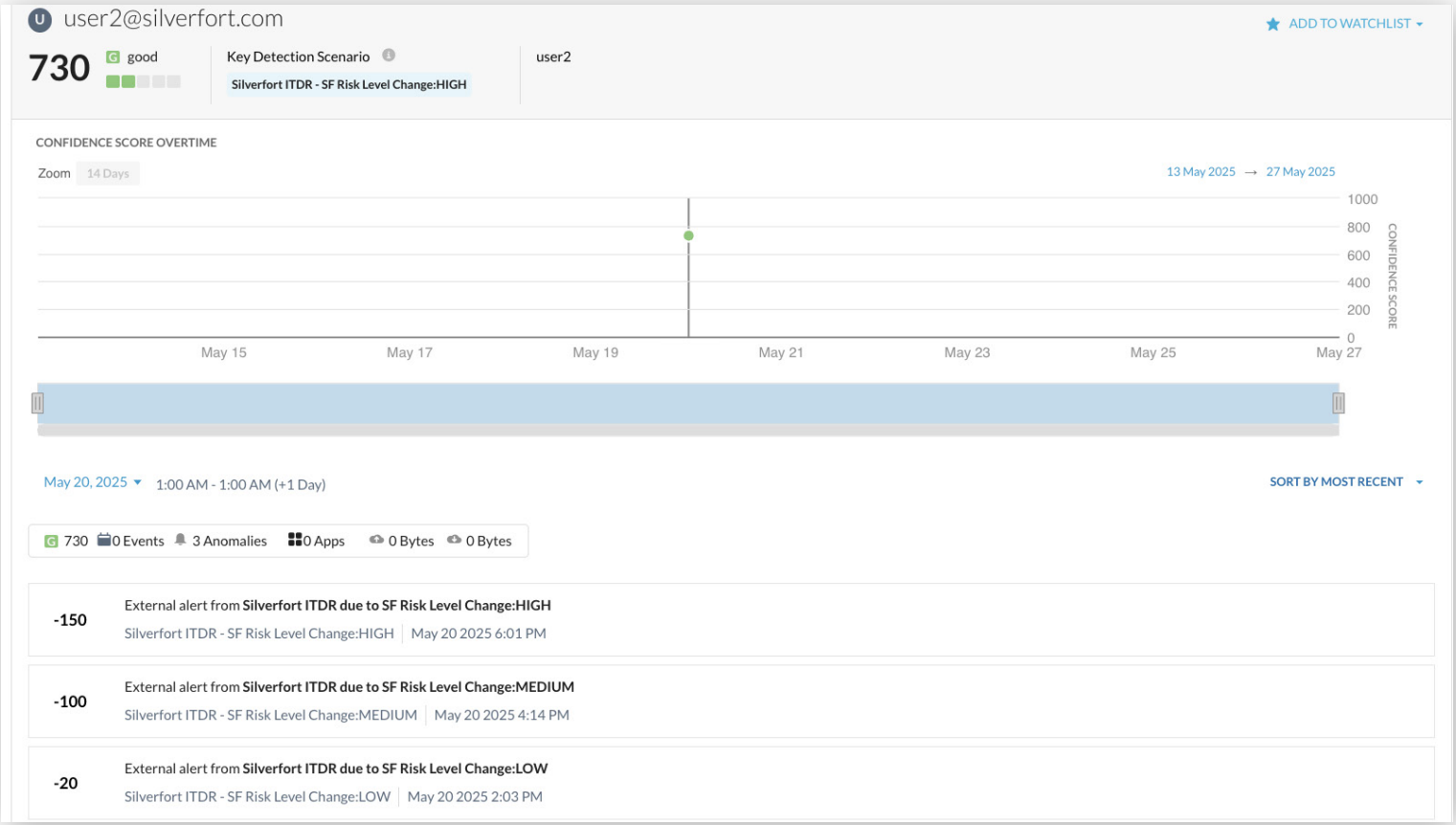
How Silverfort and Netskope's integration works

Silverfort and Netskope customers must choose a single direction for risk signal exchange, either ingesting risk signals from Netskope into Silverfort, or from Silverfort into Netskope.

- **When ingesting risk from Silverfort into Netskope**, Silverfort shares user-specific risk levels that are mapped to Netskope's UCI. These values guide Netskope's enforcement of adaptive policy controls, including access permissions and authentication requirements.
- **When ingesting risk from Netskope into Silverfort**, Netskope pushes its updated risk evaluations—typically derived from UCI thresholds—back to Silverfort. These updates inform Silverfort's downstream access decisions, enhancing identity-aware access enforcement across the environment.

This integration enables adaptive and contextual risk-based access enforcement and contributes to a stronger overall security posture. A feedback loop is maintained within the chosen direction, ensuring policies remain aligned with evolving identity signals.

Note: Full simultaneous bidirectional support is planned for a future release, targeting **Silverfort version 6.2**, which will allow both platforms to exchange risk data continuously and enrich enforcement capabilities even further.



Example of a security alert generated by Netskope, containing severity and a unique identifier, sent to Netskope's UCI for investigation and response.

Key benefits

Risk-based access control
Reduce exposure to active threats by instantly adjusting user access based on identity risk signals.

Enhanced threat response
Automatically enforce strict access policies when risky behavior is detected.

Unified visibility across environments
Get a centralized view of identity and access risk across cloud, on-prem, and hybrid environments.

Operational efficiency
Streamline policy enforcement by integrating identity intelligence directly into Netskope's access control decisions.

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.