Silverfort | IBM QRadar

Silverfort and IBM Security QRadar Integration

As cyber attacks become more complex, identity remains the primary entry point for adversaries. Attackers routinely exploit compromised credentials to move laterally, escalate privileges, and evade detection across hybrid environments.

To detect and contain these identity-driven threats, security teams require enriched identity intelligence with their existing SIEM workflows. Silverfort transforms authentication activity and identity risk into high-fidelity security signals that IBM QRadar can correlate, prioritize, and act on – enabling SOC teams to detect and stop identity-based attacks.

Rapid and efficient detection of identity threats

The Silverfort integration with IBM Security QRadar enables security teams to aggregate and correlate concrete identity threat signals directly within their SIEM workflows. Instead of manually reviewing authentication logs from Active Directory or cloud identity providers such as Entra ID, Okta, or Ping, analysts receive enriched identity telemetry that includes user risk scores, authentication context, and enforcement outcomes.

This enables QRadar to detect identity-driven attacks such as:

- Account takeovers
- Pass-the-Hash and Kerberoasting
- Brute force attempts
- Suspicious service account activity
- Lateral movement

By correlating Silverfort's identity intelligence with network, endpoint, and cloud activity inside QRadar, security teams can identify compromised users and systems faster, reduce investigation time, and focus on the most critical incidents.

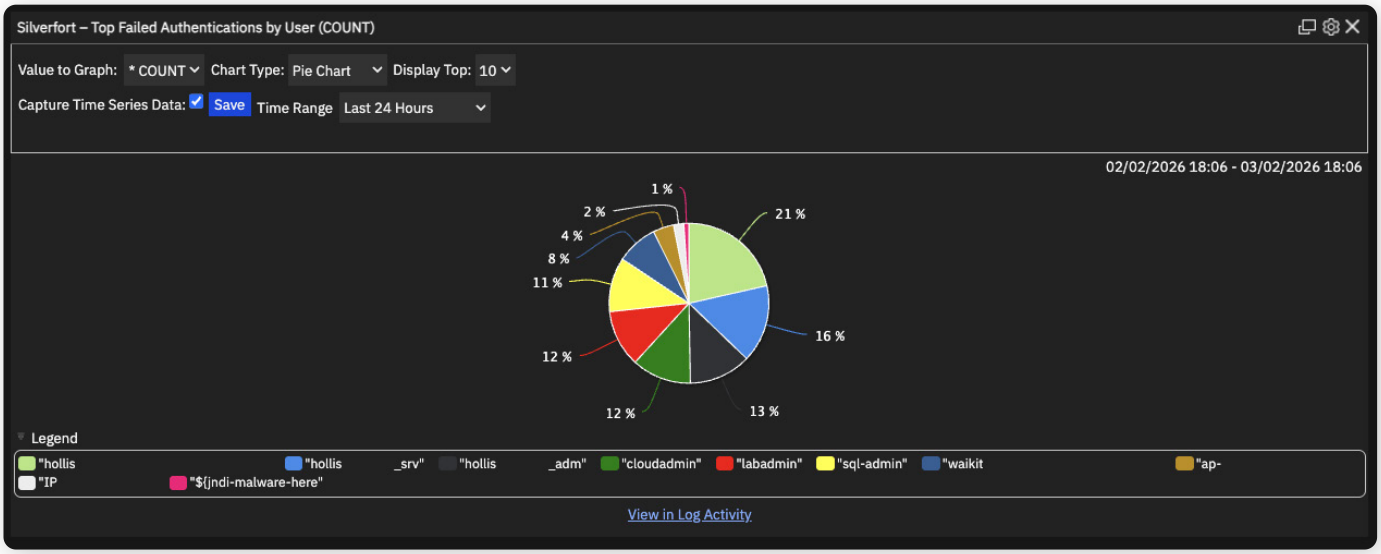
How it works

Silverfort continuously monitors and analyzes authentication and access activity across hybrid environments. Identity risk scores, authentication events, and enforcement decisions are forwarded via Syslog to IBM QRadar, where the Silverfort DSM parses and normalizes the data for structured analysis.

QRadar's correlation engine and anomaly detection capabilities then combine identity telemetry with other enterprise security data sources. This enables security teams to:

- Detect anomalous user behavior and compromised credentials
- Identify risky service account activity
- Prioritize threats based on both identity risk and asset criticality
- Investigate incidents from a centralized, single-pane view

By extending QRadar's visibility into the identity layer, organizations gain richer context, faster triage, and improved detection of both known and unknown threats.



Key benefits

Automated risk enrichment

Leverage Silverfort's real-time user and entity risk scoring within QRadar correlation rules to improve detection accuracy.

Actionable identity threat detection

Surface concrete alerts for identity-driven attacks such as credential misuse, lateral movement, and privilege abuse.

Faster investigation and response

Accelerate incident triage with granular authentication data, user behavior insights, and enforcement outcomes.

Prioritized incident management

Enrich QRadar security incidents with identity risk context to focus investigations on the most critical threats.

Centralized SOC visibility

Provide SOC teams with identity intelligence directly within their existing QRadar workflows with no additional tools required.

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.