Silverfort | Google Cloud

Silverfort and Google Security Operations SOAR Integration

Identity is the fastest-moving layer in any attack, and the hardest one for security teams to act on in the moment. Risk signals often reach the SOC in real time, but the response to them often lags; the SOC sees the threat before it has the means to stop it.

To respond to identity-driven threats at runtime, security teams need identity risk context and enforcement controls within their existing SOAR workflows. Silverfort brings live identity risk and access controls into the Google Security Operations SOAR platform that analysts can enrich, automate, and act on, enabling security teams to move from identity detection to identity response in a single workflow.

Faster containment of identity threats

The Silverfort integration with the Google SecOps SOAR platform enables security teams to act on identity risk directly within their SOAR playbooks. Instead of pivoting to a separate solution to assess identity risk or apply a policy change mid-incident, analysts can pull real-time Silverfort risk context into the case, raise the identity risk level, and update users' access-based and service account virtual fencing policies as part of the response workflow.

This enables security teams to automate identity response actions such as:

- Enriching alerts with real-time Silverfort risk context before assigning priority
- Raising the identity risk level in Silverfort to enforce stronger security controls within the existing access-based policies
- Reviewing protected service accounts and updating their virtual fencing policies (risk thresholds, protocol scope, allowed sources and destinations)
- Retrieving, enabling, disabling, and partially updating access-based policies during active response

By bringing Silverfort's identity risk and access controls into the Google SecOps SOAR platform, security teams can contain identity threats faster, automate response across hybrid environments, and focus on the most critical incidents, without leaving the SOAR workflow.

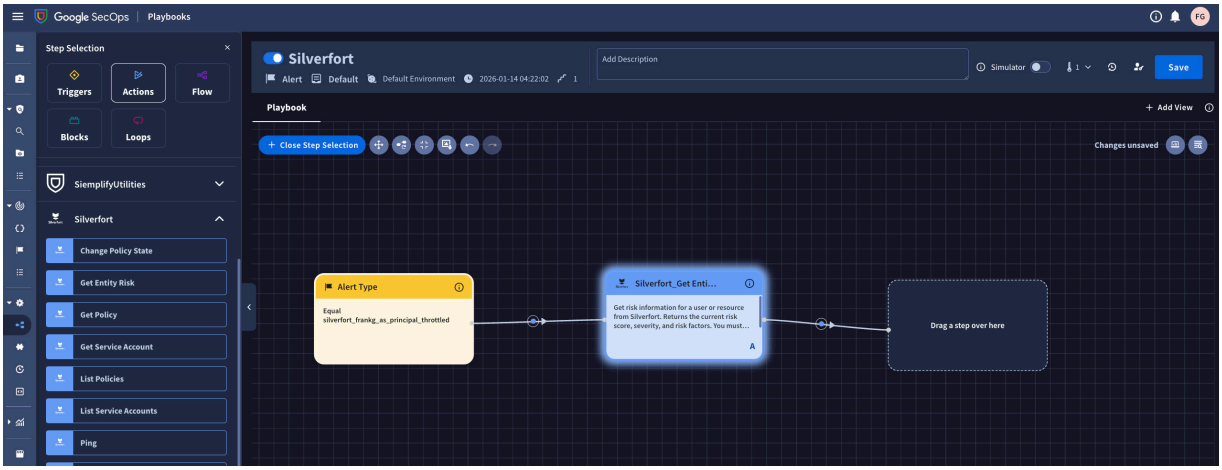
How it works

Google SecOps SOAR initiates API calls to Silverfort as part of playbook execution. Silverfort returns real-time identity risk context or applies one of the requested changes: raising an identity risk level, updating a service account's virtual fencing policy, or adjusting an access-based policy. Silverfort applies the updated policy to every subsequent authentication, reaching even legacy protocols like NTLM, Kerberos, and LDAP.

The integration covers three Silverfort APIs (Risk, Service Accounts, and Policies), giving security teams full coverage of identity response from a single integration:

Contain service account compromise directly from the response workflow	Operate access-based policies without leaving Google SecOps	Start with minimal, risk-only enrichment and expand to full automation over time	Maintain a clean audit trail with permissions scoped per API family

By bringing Silverfort's runtime access protection into the SOAR workflow, security teams gain real-time identity context, faster containment, and consistent enforcement across hybrid environments.



Key benefits

Better decisions on every alert

Enrich Google SecOps alerts with real-time Silverfort risk context to focus triage on the most critical threats.

Automatic tightening of controls

Raise identity risk from a SOAR playbook to enforce stronger security controls in real time, reaching even legacy protocols like NTLM, Kerberos, and LDAP.

Service account protection from the SOC workflow

Update virtual fencing policies (risk thresholds, protocol scope, allowed sources and destinations) to contain compromised service accounts directly from the response workflow.

Policy control without context switching

Adjust Silverfort access-based policies from Google SecOps as the incident unfolds.

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.