Silverfort

Identity-first incident response

Accelerate and optimize incident response in AD environments.

Silverfort's Identity Security Platform core capabilities

Visibility, MFA and access blocking on all AD authentications

Enforce MFA and deny access policies on any AD authentication, regardless of protocol (NTLM/Kerberos/LDAP) and access method (PsExec, PowerShell, Lmpacket, etc.). Silverfort's proprietary Runtime Access Protection (RAP) technology natively integrates with AD, delivering consolidated visibility and inline protection, in one.

Rapid deployment in the most demanding environments

In incident response, time matters most. The Silverfort Identity Security Platform deploys within hours, even in complex multi-domain environments with hundreds of DCs. Gain visibility into all user accounts' activities, and start applying MFA and deny access enforcement capabilities immediately after deployment.

Empowering IR teams with unpredecented speed and efficiency

Detect and contain compromised accounts in a rapid, semi-automated process with Silverfort. Starting with compromised users and working back from there can fundamentally accelerate and optimize the entire IR operation.

Immediate attack containment

Enforce a complete lockdown on any lateral movement attempt with simple MFA or deny access policies on all users. Enabling this policy will put an immediate halt to lateral movement by blocking the attacker from accessing any additional servers or workstations.

Automatically detect compromised accounts

Once MFA policies are enabled, compromised accounts will begin to reveal themselves with no investigation or effort from your side. Every access attempt rejected by the actual user indicates that it was actually initiated by a compromised account.

Accelerated attack trail discovery

The presence of a compromised account is a clear indication that the machine it's logged in to is also compromised. Tracing the lateral movement path of these accounts and pinpointing patient (or patients) zero becomes a trivial task.

Secure recovery and environment hardening

Silverfort highlights all the identity security weaknesses that enabled the attack to spread. Use this visibility to amend any AD and user misconfigurations, malpractices, and insecure features to elevate your environment's resilience against future attacks.

Identity-first IR process drill down

Containment

1 Enforce MFA or deny access policies on all user accounts

Halt all malicious spread within minutes, without needing to know the compromised machines or accounts.

Investigation

Remediation

2 Detect compromised accounts & machines

Any malicious access attempt will trigger an MFA violation, disclosing the identity of the compromised account or machine.

→ **Reset passwords, isolate machines & kick off forensics**

Inform the identity team of the compromised accounts so they can revoke access. Take suspected machines offline and kick off forensic activity to identify malicious files, processes and outbound network traffic.

3 Confirm malicious presence has been eliminated

Validate suspicious accounts were disabled or had passwords reset. Ensure infected machines have no other activity indicating compromise.

→ **Gradually release lockdown**

Replace the block access policies with MFA so users can return to business as usual in a secure manner.

4 Trace lateral movement path

Use Silverfort's log screen filters to display the compromised account's authentication trail sources and destinations, disclosing the compromised machines in the attack's route.

→ **Isolate machines and acquire artifacts**

Quarantine suspected machine and conduct the standard forensic activity to pinpoint the malicious files, processes, and outbound network traffic.

5 Identify patient zero

Keep tracing attacker's movement until you reach the machine where initial access took place.

→ **Validate and mitigate initial compromise vector**

Apply your standard forensic tools to determine how the initial malicious access into the environment was carried out and apply mitigations against any future occurrence.

6 Detect exploited identity weaknesses

Finally, use Silverfort's Logs and Insights to map identity weaknesses used by attackers to gain access, escalate privileges and move laterally.

→ **Harden environment against future attacks**

Provide the IAM team with full insights into your findings so they can fix misconfigurations, malpractices, and legacy settings across the entire user inventory and DCs.

Recovery

7 Restore operations to affected environment and configure access policies to prevent attackers from repeating similar attack patterns. Provide SecOps team with accounts that should be closely monitored for policy violations as well as suspicious activity.

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.