SILVERFORT | IS4U

Why Silverfort is Essential

Traditional identity controls fall short of providing complete coverage, leaving critical resources exposed to malicious access. With Silverfort, organizations can solve the critical identity security risks they've been struggling with for years – **because we go where identity protection has never gone before.**

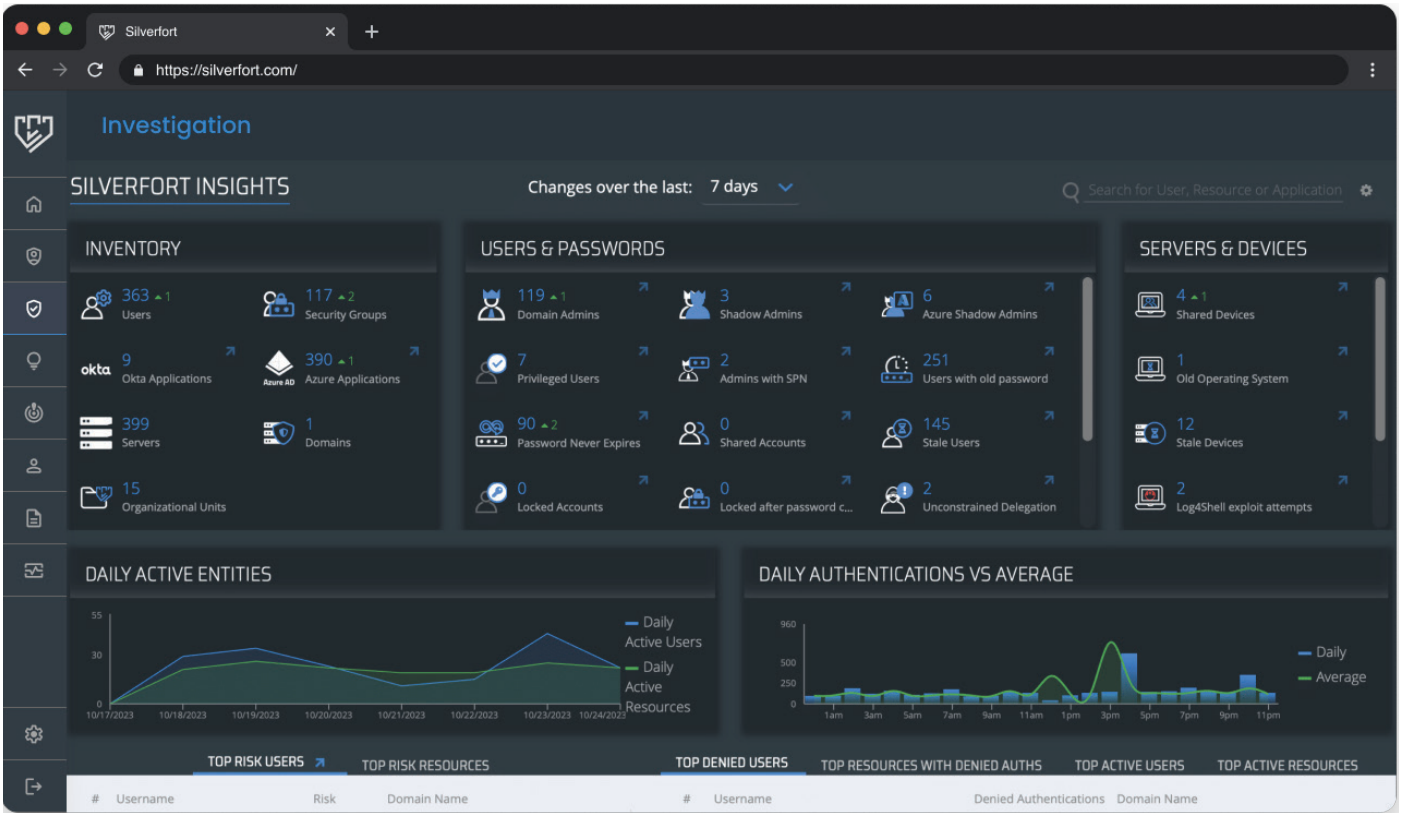
Solve the Identity Protection Challenges That Matter Most

Visibility of User Activity & Authentication

Monitor all identity traffic and authentication activities in one place. Silverfort provides centralized visibility into every authentication and access request across all users and resources in the hybrid environment, thanks to its native integrations with all identity providers.

With complete visibility across all user activity, Silverfort's analysis engine can determine the risk of every authentication, so organizations can detect and respond to potential security threats in real time — including blocking the access of any accounts that display anomalous behavior.

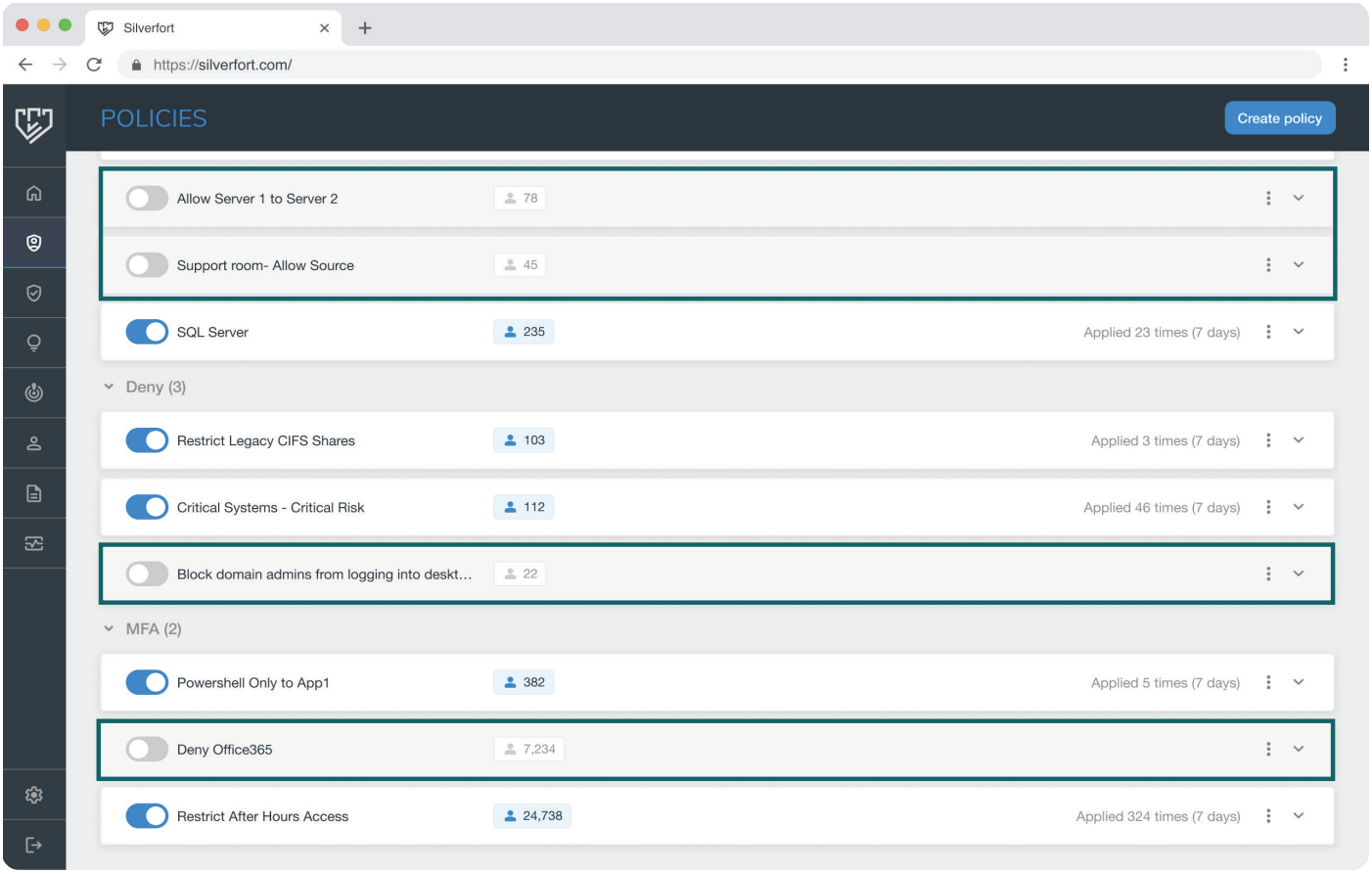
Silverfort provides you with an in-depth identity inventory that displays the types of users and resources in your environment as well as weaknesses in your security. With continuous visibility and actionable insights into everything identity-related, Silverfort allows you to take a more proactive approach to your identity security posture management with just a few clicks.



Silverfort's Insight Screen

Blocking Risky Access

Don't underestimate the power of blocking access. Silverfort can block access requests for every type of user, service account, access method, and resource in real time, effectively halting any unauthorized access from occurring.

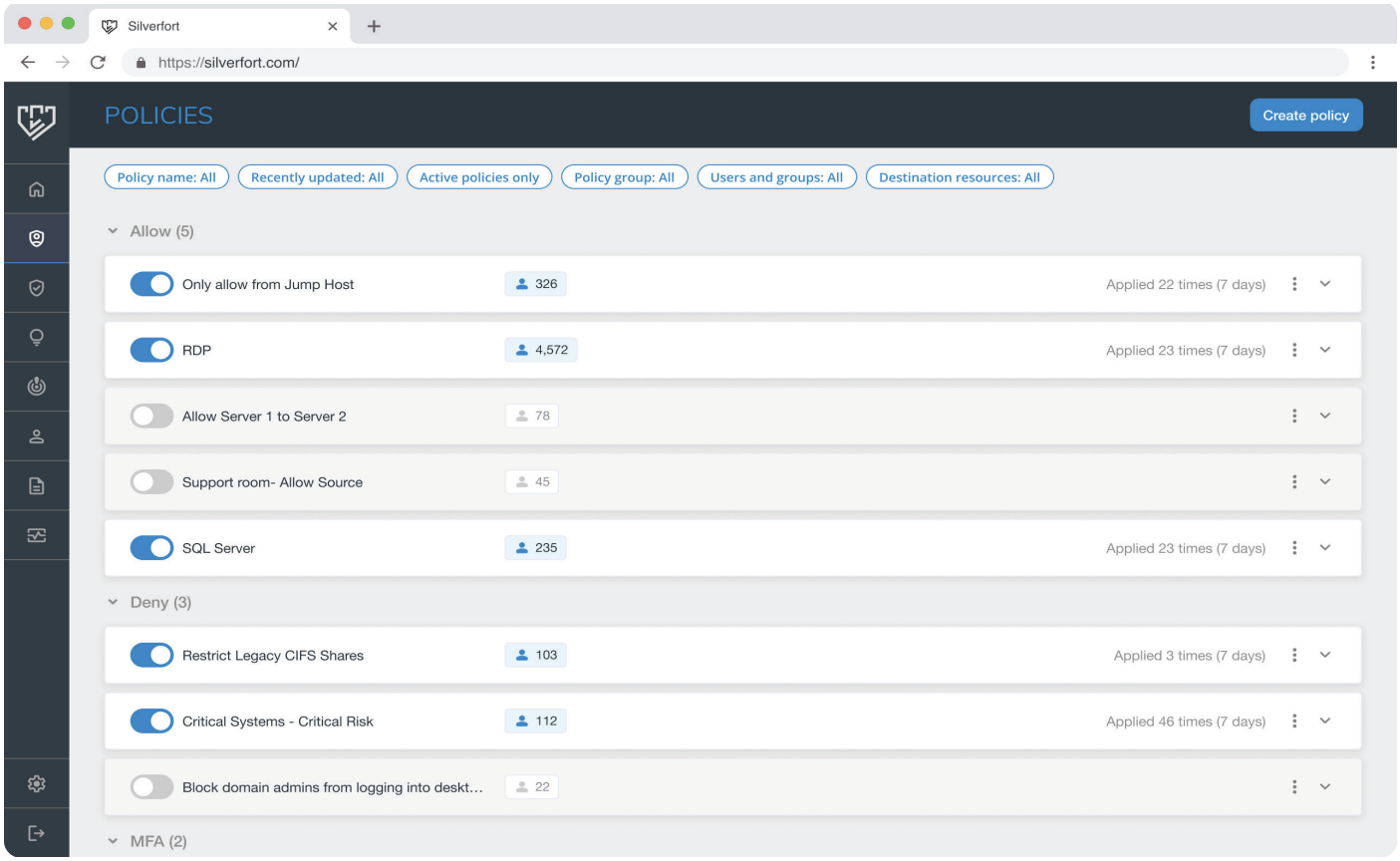


Silverfort policy screen displays all the deny policies

In addition, Silverfort can enforce policies to either require MFA or block access to any privileged account – including service accounts – that attempts to access a resource. Administrators can choose which sources, destinations, and authentication protocols policies should be applied to and what actions the system should take if users deviate from their standard behaviour.

Lateral Movement Prevention

Silverfort prevents lateral movement by enforcing adaptive authentication and MFA on all administrative interfaces, including low-level CLI interfaces such as PsExec, PowerShell, WMI, and CIFS/SMB. As Silverfort extends MFA protection to core enterprise resources, including on-prem applications and servers, attackers would still need to pass an additional authentication step, even if they have compromised credentials, making unauthorized access significantly more difficult. This eliminates an attacker's ability to use compromised credentials to move laterally across an environment.

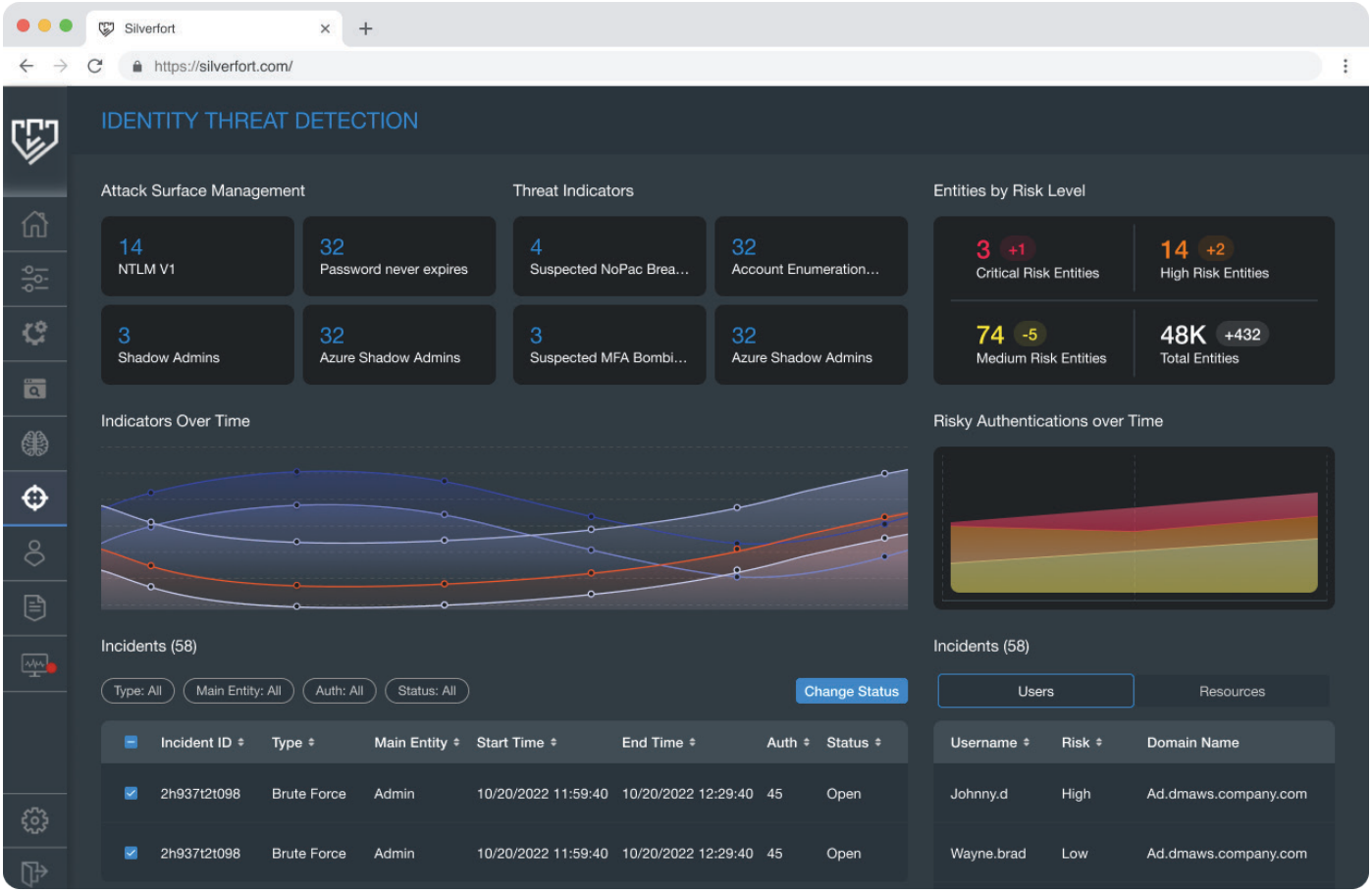


In Silverfort's policy screen, you can create and apply access policies in your environment to stop lateral movement attacks

Additionally, Silverfort's risk engine provides continuous monitoring and risk assessment to detect anomalies that may indicate lateral movement. When an access request is deemed untrustworthy, Silverfort can immediately block it, preventing the malicious actor from logging in. This real-time protection is key to stopping lateral movement attacks as they happen.

Identity Threats Incident Response

Silverfort is the first solution to provide IT teams with incident response capabilities at the identity layer in a single, easily deployable solution.



Silverfort's ITDR screen

Alongside its aggregated view of all authentications and access attempts, Silverfort also assists IT teams by blocking attackers from advancing through an environment and by restoring things to their original state. With Silverfort's IR capabilities, the environment's security architecture can be fully prepared to handle any identity infrastructure compromise, as well as detect and block malicious access to compromised accounts.

Meet Cyber Insurance MFA and Privileged Access Requirements

Though cyber insurance requirements are stricter than ever, they will empower enterprises to be much better prepared against cyberattacks. Silverfort helps organizations to fast-track the cyber insurance renewal process by complying with every MFA, PAM, and service account protection requirement from underwriters. The most stringent requirement is to apply MFA protection on all admin users across various resources in the environment. Silverfort is the only solution that enforces MFA on all admins without agents or proxies – resulting in full compliance with MFA protection requirements for cyber insurance.

With Silverfort, companies can also automatically discover, secure, and monitor all service accounts in their environment, and gain real-time insights into their activities and level of risk.

With ready-to-use access policies tailored to each service account, any deviation from its standard behavior will result in either blocked access or an alert sent to the SOC team.

Implementing MFA and service account protection with Silverfort across all resources and protecting all privileged accounts are essential steps toward an improved security posture. Uncover your security gaps, qualify for cyber insurance, and eliminate the threat of ransomware. Silverfort makes this quick and easy.

Silverfort's Cyber Insurance Report