Silverfort

Identity Threat Detection and Response (ITDR)

Secure your environment against credential access, privilege escalation, and lateral movement, with unparalleled detection accuracy and real-time prevention.

Eliminate your blind spots.

Silverfort leverages its patented Runtime Access Protection (RAP) to analyze every authentication and access attempt in real time and disclose malicious identity-related TTPs that aims to compromise, manipulate, or utilize user credentials for malicious access.

With our unique visibility into the authentication process, Silverfort can spot anomalies in protocols, access patterns, and user behavior, while also sharing threat signals with XDR, SIEM, SOAR, and other components of the security stack. Moreover, we can trigger MFA and block access, helping you to move beyond alerting to automated prevention.

Detect threats with accuracy. Block with confidence.

High precision

Employ multiple risk engines that combine real-time analysis of the authentication, with the user's overall context and security posture to increase accuracy and avoid false positives.

Real-time prevention

Trigger MFA upon detected malicious access attempts over any remote command-line or screen sharing tool, eliminating adversaries from using them for malicious access.

Streamline investigation

Empower your SecOps team to easily discover the access trail of compromised user accounts all the way to patient zero by filtering any account that violated the MFA or block access policy.

Integrate seamlessly with XDR, SIEM, and SOAR.

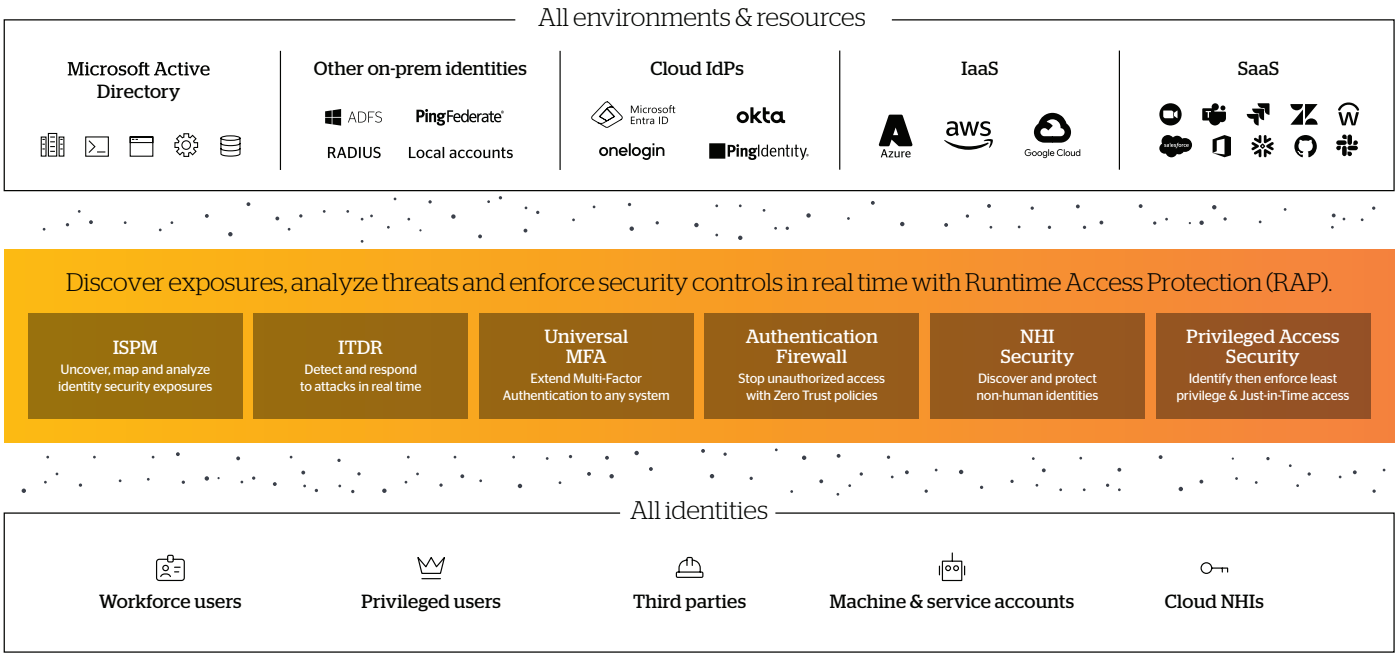
Silverfort ITDR integrates with the core components in your security stack, filling a critical blind spot across three key MITRE tactics: credential access, privilege escalation, and lateral movement.

- **XDR:** Share detected threats and ingest endpoint, network, and other telemetries to enrich context and increase accuracy.
- **SIEM:** Exchange data with the mutual correlation of risk signals to enhance insight into each user accounts' involvement in active attacks.
- **SOAR:** Provide context of compromised accounts and machines, and trigger MFA and block access to quickly eradicate malicious presence.

86%

of data breaches involve the use of compromised credentials, and number continues to increase. This makes the ability to detect and block all the related TTPs in real time a critical part of every security architecture.

The Silverfort Identity Security Platform



Identity security: mitigate the risk of compromised credentials

ITDR is a key part in Silverfort's mission to deliver comprehensive identity security and mitigate the risk of malicious access with compromised credentials.

The Silverfort Identity Security Platform achieves this with its three core capabilities:

Continuous discovery of every user account in the enterprise environment.

Risk analysis of every account's security posture and every authentication and access attempt.

Real-time enforcement that blocks unauthorized and malicious access.

Silverfort implements these capabilities across all users, all resources, and all on-prem and cloud environments, so organizations can secure their entire identity attack surface with a single, easy-to-deploy solution.

About Silverfort

Finally, the identity security platform you deserve. Silverfort connects to your entire infrastructure to protect it from within. By breaking down silos and eliminating blind spots, Silverfort is the first to give businesses visibility into their whole network of identities and secure every identity, every resource, and every environment—all the time.