doan
COPYWRITING

Article for ISDecisions.com

UserLock vs Silverfort: A Comprehensive Comparison

Alternate Titles

UserLock vs Silverfort: MFA Solutions for Your Network Setup

UserLock vs Silverfort: On-Premises and Cloud Security Solutions

UserLock vs Silverfort: AD Protection for Different IT Environments

Meta Description:

Compare UserLock vs Silverfort to find the right MFA solution for your infrastructure, from Windows-focused to hybrid AD security environments.

The security landscape demands different approaches to Active Directory security, especially between on-premises and hybrid infrastructures. UserLock vs Silverfort exemplifies this choice:

UserLock provides agent-based comprehensive security and MFA for Windows AD environments, with granular authentication control. Silverfort, developed in partnership with Microsoft, delivers an agentless platform for enterprise environments, deeply integrating with both on-premises AD and Azure AD (now Microsoft Entra ID). While Silverfort's enterprise pricing starts higher, this difference narrows above 500 users.

Organizations must choose based on their environment needs—Windows-focused or requiring broader platform support. In this guide, we look at how each authentication solution can address Windows authentication, access management, compliance, and legacy system protection.

Detailed Use Case Comparisons UserLock vs Silverfort

A strong MFA comparison helps organizations strengthen AD access management through user authentication. Both solutions offer zero-trust security features that match different IT environments.

Let's examine how UserLock and Silverfort protect user accounts, cloud applications, and existing systems based on your organization's infrastructure setup.

1) Multi-Factor Authentication (MFA) for Windows Logins

UserLock

A November 2022 ransomware attack on logistics companies in Ukraine and Poland exposed how attackers exploit privileged credentials to breach Windows systems. MFA protection for Windows login security stops unauthorized access through stolen credentials.

UserLock seamlessly integrates MFA capabilities within Windows Active Directory environments through micro-agents deployed on workstations. The solution provides MFA protection for Windows login security, RDP sessions, and network access points without cloud dependencies.

Silverfort

With Silverfort, you don't need to modify your endpoints for agentless MFA functionality across Windows, Linux, and cloud platforms. The solution functions through a virtual appliance deployed on-premises, enabling unified authentication security across diverse systems.

2) Access Management for Active Directory (AD)

UserLock

Using specific restrictions based on geographical location and IP address, UserLock enhances AD access management. The solution enforces role-based limitations aligned with existing AD user groups and organizational unit policy settings. Organizations maintain detailed monitoring over network sessions, concurrent logins, and time-based access through native AD infrastructure integration.

Silverfort

Integrated identity providers allow Silverfort to manage access across AD and non-AD systems. The platform extends Active Directory security to legacy applications while supporting hybrid and multi-cloud infrastructures. Organizations planning cloud migration gain unified security policies across diverse environments.

Organizations staying on-premises due to compliance requirements, cost constraints, or bandwidth limitations benefit from UserLock's on-premises-first approach. Companies moving toward cloud infrastructure or using Entra ID find value in Silverfort's cloud-first strategy, which bridges legacy systems with modern cloud resources.

3) Zero Trust Security and Conditional Access

UserLock

UserLock implements Zero Trust security through AD-integrated contextual policies based on IP restrictions and time controls. Organizations maintain their established role-based access controls through AD users, groups, and organizational units without duplicating identity management in the cloud. The solution keeps authentication within the data center, avoiding the complexity of hybrid identity scenarios that need AD FS and Entra Connect infrastructure.

Silverfort

Using Silverfort, you can assess real-time risk and analyze behavior in real-time. The platform requires integrating cloud-based identity providers like Entra ID or Okta, creating a "half in, half out" approach. Organizations must manage additional infrastructure and synchronization tools while gaining advanced behavioral analytics.

4) Compliance and Auditing

UserLock

Detailed AD-focused logging allows UserLock to monitor Windows system activities, access attempts, and MFA events. The solution tracks administrator actions and privileged account behavior to meet advanced compliance requirements like CMMC. Organizations maintain Zero Trust security through meticulous audit trails, generating detailed reports for HIPAA, SOX, and GDPR compliance within AD environments.

Silverfort

Silverfort aggregates access data across multiple platforms and cloud infrastructures. The platform creates unified compliance reports spanning hybrid environments, tracking authentication events beyond Windows systems. Organizations receive consolidated audit trails for PCI DSS, NIST, and CMMC through cross-platform monitoring that maintains centralized visibility.

5) Legacy System Protection

UserLock

Organizations running legacy systems face mounting security risks—94% of data breaches involve compromised credentials in outdated infrastructure. UserLock protects Windows-based systems through native protocol integration and AD authentication methods. The platform secures access through Windows protocols without requiring cloud components, delivering complete security controls within the Microsoft ecosystem.

Silverfort

Besides providing agentless protection, Silverfort extends hybrid environment security to legacy systems and non-AD resources. The solution operates independently of native protocols, managing authentication through a virtual appliance. Large organizations gain broad platform coverage but must consider Entra ID and Silverfort licensing costs.

6) Third-Party Security Integration

UserLock

A recent study shows that 41% of organizations suffered security incidents caused by third-party integrations in 2023. As a Silverfort alternative, UserLock extends beyond AD-centric tools through strong API and PowerShell support. The solution enhances user security awareness through .NET API for custom applications and PowerShell cmdlets for automation.

Organizations can create:

- Custom .NET applications interfacing with UserLock service
- Automated responses to authentication events
- SIEM system integration for security monitoring
- PowerShell automation for access management

- Enhanced AD activity visibility

Silverfort

With Silverfort, you can connect to SIEM, EDR, and identity providers across a variety of security ecosystems. The platform requires configuration to integrate with multiple security tools and cloud services. Organizations must manage various integration points while gaining broad compatibility across hybrid environments.

Companies focused on Windows environments benefit from UserLock's straightforward development tools. Organizations needing multi-platform integration gain Silverfort's extensive third-party support, provided they can handle the added configuration complexity.

7) Air-Gapped Network Security

UserLock

With UserLock, you can create air-gapped networks using offline-capable micro-agents that communicate with an on-premises server. The solution supports multiple authentication methods, like TOTP/HOTP hardware tokens and smartphone authenticator apps, maintaining all access policies without internet connectivity.

Organizations gain granular session controls and real-time monitoring while meeting compliance requirements through complete audit logging.

Silverfort

With Silverfort, you can deploy a virtual appliance on-premises in an isolated environment. The platform enables agentless MFA using FIDO2 hardware tokens without endpoint modifications. Organizations receive behavioral analysis and risk assessment features while maintaining air gap integrity.

Environmental Fit Analysis Between UserLock vs Silverfort

Selecting between UserLock vs Silverfort requires evaluating your organization's infrastructure setup, from on-premises Active Directory to hybrid environment security needs. Let's examine the factors guiding you toward the right authentication solution for your organization.

On-Premises AD Environments

Recent data shows that 86% of breaches involve stolen credentials in on-premises environments.

UserLock enhances Active Directory security through native integration, syncing with AD every 5 minutes for real-time monitoring. The solution streamlines AD access management without requiring cloud components or additional infrastructure.

Organizations maintain complete visibility over authentication events and access patterns within their Windows environment. UserLock's focused approach reduces deployment complexity and administrative overhead compared to Silverfort's broader platform requirements.

Hybrid/Multi-Platform Environments

Silverfort's architecture is specifically designed for complex infrastructures requiring unified security across diverse platforms and authentication protocols. The solution's deployment complexity is balanced against its ability to provide comprehensive hybrid environment security and coverage across hybrid environments, though this requires more extensive initial configuration and planning.

Budget Considerations

The cost difference stands out when comparing UserLock's pricing models to Silverfort's. UserLock charges $1.75 per user monthly, totaling $4,200 yearly for 200 users, with a 20% discount available on three-year subscriptions.

Silverfort's pricing reaches $50,000 annually for 100-250 users, reflecting its broader platform coverage and enterprise focus. Organizations need to carefully evaluate whether these expanded capabilities justify the higher investment, particularly for small to mid-sized companies or those primarily operating in Windows environments. Additional implementation costs through third-party vendors should also be considered.

Feature Comparison Matrix - UserLock vs Silverfort

Here's a summarized overview of Userlock vs Silverfort:

Features	UserLock	Silverfort
Authentication Methods	Provides MFA through push notifications, hardware tokens, and authenticator apps specifically designed for Windows AD environments. It also has native protocol support for offline authentication.	It offers agentless MFA across multiple platforms, including cloud and on-premises, and supports various authentication protocols through a virtual appliance.
Access Controls	Enforces granular restrictions based on time, location, and device within Windows environments, with real-time AD synchronization every 5 minutes.	Implements AI-driven risk analysis and adaptive policies across platforms, requiring cloud connectivity for full feature functionality.
Deployment Model	Deploys through micro-agents on Windows endpoints with direct AD integration, supporting air-gapped networks without cloud dependencies.	Requires virtual appliance installation and cloud identity provider integration, with optional on-premises deployment mode.
Infrastructure	Connects with SIEM systems and Windows-native tools through REST API, focusing on AD-centric security infrastructure.	Integrates with multiple security platforms, identity providers, and cloud services, requiring additional configuration for each integration point.

Start Securing Your AD Access with UserLock

The choice between UserLock and Silverfort depends primarily on your infrastructure complexity and security coverage needs across platforms. Organizations must evaluate their requirements for cross-platform support, legacy system protection, and integration capabilities. While UserLock specializes in Windows environments, Silverfort serves diverse infrastructure needs with broader platform coverage.

Implementation planning should balance immediate security requirements with long-term evolution plans. Consider your existing technology investments and organizational security strategy when choosing between UserLock's focused Windows security approach and Silverfort's comprehensive multi-platform protection. Book a consultation today to determine which solution best fits your infrastructure needs.