COMPETITIVE ANALYSIS

Analog Informatics vs. Silverfort - Competitive Analysis

Compare AIC and Silverfort for identity protection, privileged work and air-gapped deployment. See local MFA, secret control and customer fit.

Analysis date: November 17, 2026 | Revised: November 20, 2026

Analog Informatics Corporation

Copyright © 2026 Analog Informatics Corporation. All rights reserved.

Deployment options and who operates them

Compare where the management software runs, who operates it and which functions remain local. A local connector, an outage cache and a customer-operated air-gapped installation have different dependencies.

Deployment option	AIC	Silverfort
On-premises management	Yes. Install and operate the management software on customer infrastructure.	Yes. Silverfort offers a full on-premises virtual appliance. Verify which modules your order includes.
Management in your own cloud account	Yes. Install and manage AIC in a cloud account and region you choose.	Cloud deployment is offered. Obtain confirmation of which management components are supported in your own cloud account.
Hybrid operation	Yes. Customer-managed local and cloud components can serve the chosen systems and applications.	Yes. Hybrid deployment is offered. Establish the location and dependencies of each selected module.
Vendor-operated SaaS	No mandatory AIC-operated SaaS management service. The customer or its authorized provider operates the installation.	Yes. SaaS is offered alongside on-premises and hybrid deployments. Establish responsibilities for the selected service.
Air-gapped or disconnected operation	Yes. Supported local credential and session functions run with required local services and a valid license. Install, license and update without a network connection to AIC.	Yes for documented local MFA: an on-premises appliance uses FIDO2 hardware tokens in an air-gapped network. Verify additional modules for the selected deployment.
Secret and administrative control	The customer authorizes secret use, retrieval and changes. AIC support has no standing access.	Policies govern authentication through connected identity systems. Specify administrator access and record custody for the chosen deployment.
Country-specific installation and records	Install and operate within a chosen country. Configure operators, logs, backups and recovery copies for the required boundary.	Local deployment can support country-specific operation. Establish records, support access and any external service dependencies.

AIC deployment choices include the product owner's November 20 confirmation of air-gapped support. Competing options follow the cited documentation. An outage cache or a surviving connection is not evidence that every administrative workflow works offline. Future AIC feature scope is separate from the released capabilities available for a purchase today.

AIC: Customer-installed security software for on-premises, customer-controlled cloud, hybrid and air-gapped deployment. The customer chooses the location and authorized operators and controls access to its managed secrets. Installation, licensing and updates can be completed without a network connection to AIC.

AIC Enterprise Privilege Suite; AIC disconnected operation; AIC security and customer control

Silverfort: An identity-security platform offered through on-premises, SaaS and hybrid deployments. Its documented on-premises appliance supports MFA with FIDO2 hardware tokens in air-gapped networks. Other module availability and local operating requirements depend on the selected deployment.

Silverfort deployment and module options; Silverfort local MFA; Silverfort hosting locations

Copyright © 2026 Analog Informatics Corporation. All rights reserved.

Which controls does the hospital need for its overnight job?

A hospital may still depend on a Windows application that accepts Active Directory credentials but offers no MFA prompt. The security team wants to challenge administrators and spot a service account signing in from an unfamiliar server. The application owner also needs to change that account’s password without interrupting an overnight job.

What Silverfort offers: Silverfort can challenge administrators who sign in to a legacy application through a supported directory and restrict a service account to approved source and destination systems. Its Privileged Access Security product can enable a domain administrator account for an approved window. An on-premises appliance can also enforce MFA with FIDO2 hardware tokens on an isolated network.

Where AIC changes the decision: The hospital controls who may use or retrieve each managed secret. AIC can apply MFA to the administrator’s suite sign-in, change the service password and update the scheduled task that uses it. When the administrator needs elevated rights or a recorded session, the reviewer can inspect the approval and the record of the work. Air-gapped deployment is available from both vendors. Compare AIC's local credential and elevation workflows with Silverfort's documented local MFA, rather than treating an on-premises location as a unique AIC capability.

Which approach fits: The hospital’s identity team has a reason to choose Silverfort if it needs to challenge direct directory sign-ins across older applications. The application owner has a reason to choose AIC if the team must also update service credentials, grant temporary rights and document maintenance. If both teams need those controls, test the directory policy and the maintenance procedure on the same job.

A practical example: For the hospital’s overnight job, have Silverfort block a sign-in from an unauthorized host. Have AIC rotate the service credential, update the scheduled task and show its next successful run. Before retiring either product, test the exceptions too, including a permitted maintenance login and a task host that misses the update.

Which identity and access controls fit your organization?

Current capabilities and future scope

As of November 18, 2026, AIC supplies PIM, PAM, PUM, IGA, GRC, CLM and CIAM. Every Silverfort feature is in scope for a future AIC release as its products evolve. Current coverage depends on the released product, supported target and deployment. Future scope does not establish current availability, a particular release or a delivery date.

Where the features overlap

Identity discovery and access reviews

AIC today: AIC discovers human and service accounts on supported systems. Reviewers can inspect access to suite-managed accounts, revoke an assignment and retain the decision.

Silverfort today: Silverfort’s Identity Graph & Inventory maps identities and permissions across connected providers. Access Intelligence shows which people actually used a resource.

What this means for the customer: An access reviewer deciding whether to remove a privilege needs to see the assignment, recent use and the record of the change.

Copyright © 2026 Analog Informatics Corporation. All rights reserved.

MFA and sign-in policy

AIC today: AIC can allow, challenge or deny sign-ins to its own suite using network rules, threat intelligence and factors such as passkeys.

Silverfort today: Silverfort can enforce MFA on supported direct directory sign-ins, including sign-ins to legacy file shares, command-line tools and industrial systems.

What this means for the customer: A plant engineer may enter through a broker or sign in directly to a file share. Test both routes to see which product enforces the policy on each one.

Temporary privileged access

AIC today: AIC can approve a temporary grant to a managed target, elevate an approved endpoint task and broker the maintenance session.

Silverfort today: Silverfort Privileged Access Security can enable a domain administrator account for a limited time. The ServiceNow integration checks who was approved and when the ticket expires.

What this means for the customer: An enterprise might need a brief window of directory access and permission to run a single elevated task. Specify both when retiring standing privileges.

Service accounts and AI identities

AIC today: AIC manages supported machine credentials, including passwords, SSH keys, certificates and API keys. It can rotate a service password and update the scheduled tasks that use it.

Silverfort today: Silverfort can restrict service-account authentication to approved systems, map an AI agent to its owner and apply policy to supported agent activity.

What this means for the customer: For a workload that uses a long-lived key, establish who replaces it and what stops the workload from using it outside its approved purpose.

Identity threats and automated response

AIC today: AIC reports blocked or failed suite sign-ins, detects configuration changes on managed systems and can apply an authorized correction or notify the operator.

Silverfort today: Silverfort’s posture management identifies identity exposures. Its threat detection and Authentication Firewall can challenge or deny a suspicious request through a connected identity provider.

What this means for the customer: Incident responders may need to stop the next sign-in immediately and correct a setting that would otherwise leave the system exposed.

Records of access and administrative work

AIC today: AIC retains approvals and change results. On supported protocols, a reviewer can replay a brokered session to see what the administrator did.

Silverfort today: Silverfort records the authentication attempt and the policy decision. Access Intelligence shows who used a resource and when.

What this means for the customer: A successful authentication event shows that the identity provider accepted the sign-in. If the audit calls for commands or screen activity, inspect a recording from the required protocol.

Copyright © 2026 Analog Informatics Corporation. All rights reserved.

Hybrid and isolated deployments

AIC today: Customers install and manage AIC on premises, in their cloud account, across both or at an air-gapped site. Supported local credential, session and elevation workflows use local services. Installation, licensing and updates do not require a network connection to AIC.

Silverfort today: Silverfort offers on-premises, SaaS and hybrid deployments. Its documented local appliance enforces MFA with FIDO2 hardware tokens in air-gapped networks; other module availability depends on the deployment.

What this means for the customer: A plant or hospital with isolated sites can consider both. Compare the required local sign-in protections, password changes, elevation and recovery tasks; demonstrate each selected module without an outside connection.

AIC strengths

AIC supplies PIM, PAM, PUM, IGA, GRC, CLM and CIAM. An operations team can combine credential changes, endpoint elevation and session evidence with the access reviews its auditors require.

Automated changes can update a credential and its supported dependencies. Exceptions identify work still needed when a server is unavailable during a change window.

Customers control secret access, storage and export across their own sites and cloud deployments. Local teams can operate supported credential and session services when an external connection is unavailable.

AIC can be installed and managed inside an air-gapped mission site, with customer-selected administrators, local credential workflows and retained records. Installation, licensing and updates do not require a network connection to AIC.

Silverfort strengths

Silverfort can add MFA to direct directory sign-ins for older applications, command-line tools and operational technology without changing the protected application’s code.

Identity Graph & Inventory shows relationships and permissions. Access Intelligence adds actual usage so the identity team can investigate an unused privilege or an unexpected sign-in.

Its threat response, service-account restrictions and AI agent policies let security teams intervene as a covered identity requests access. Privileged Access Security can also grant time-limited domain administrator access.

Which customers fit each approach

AIC - An industrial operator whose engineers and outside suppliers maintain equipment across sites with limited connectivity.

The operator can approve a maintenance session, keep the target password in its own vault, control privileged commands on supported SSH connections and review a recording. Local staff can rotate credentials and update dependent services on site. An air-gapped plant or hospital can keep supported credential and elevation work within its own installation, while separately evaluating Silverfort's local MFA for sign-ins.

Copyright © 2026 Analog Informatics Corporation. All rights reserved.

Silverfort - An enterprise identity team protecting employees, outside advisers and service accounts across Active Directory, cloud identity providers and older business applications.

Silverfort can show where accounts sign in, apply MFA or access restrictions on direct authentication paths, and enable domain administrator accounts only for approved work. Its customer studies describe these requirements in financial services and automotive engineering.

Both - A hospital group that needs to challenge direct sign-ins to older applications and keep scheduled clinical support jobs running through password changes.

Silverfort can restrict where each service account authenticates. AIC can change the password, update the scheduled job and retain the administrator’s maintenance record. The identity and application teams can verify both results on the same system.

AIC conditional access and threat reporting for suite sign-ins

AIC supported targets and credential updates

AIC privileged access approvals, session controls and recordings

AIC account lifecycle and access review

AIC threat response, drift detection and remediation

AIC access for industrial operators and outside suppliers

AIC disconnected operations

AIC Enterprise functions and licensing

Packages and support options

Silverfort Identity Graph & Inventory and Access Intelligence

Universal MFA and supported authentication paths

Privileged Access Security

ServiceNow ticket validation for JIT access

Identity Threat Detection and Response

Silverfort controls for non-human identities and AI agents

Silverfort support for Active Directory, legacy applications and operational technology

Local FIDO2 authentication in air-gapped networks

ASAP Holding and Protea Networks

ITC Secure and a UK financial services company

AIC security and customer control

Copyright © 2026 Analog Informatics Corporation. All rights reserved.

Customer-controlled deployment and secret access

Would you delegate control of your most sensitive systems and secrets without knowing who can administer them, where those people are located, and who is accountable for their actions?

AIC is installed where you choose and managed by you. Your organization controls who may use, retrieve or change its managed secrets. Choosing cloud or hybrid infrastructure does not require you to give an outside SaaS operator control of those decisions.

Run AIC on premises, in a cloud account you control, in a hybrid environment, or on air-gapped systems for sensitive missions. You choose where the software runs, who administers it and who may use, retrieve or change the secrets it manages. AIC has no standing access to your installation. Air-gapped deployments can be installed, licensed and updated without a network connection to AIC.

For sensitive work, the server's location is only part of the decision. Your organization chooses the people and approved providers that administer AIC, where they work and which secrets they may access. You control any support access you grant. Cloud infrastructure permissions, local identity services, audit storage, backups and recovery copies remain part of the deployment you choose.

The Silverfort comparison

An air-gapped hospital or plant may need both protected sign-ins and continued maintenance of service accounts. Silverfort already offers a local appliance with FIDO2 MFA for isolated networks, as well as SaaS and hybrid deployment. AIC also supports customer-operated air-gapped installations, including installation, licensing and updates without a network connection to AIC. Compare Silverfort's identity and MFA enforcement with the AIC credential, elevation and recovery workflows the site needs. A hospital group can operate AIC separately in each EU country and choose the authorized operators, local records and information shared with the group. Available Silverfort modules and the required local services depend on the proposed deployment.

Country-by-country operation in the EU

A German operation can install and manage AIC in Germany, while a French operation does the same in France. Each country team can retain control of its secrets and decide which records it shares with the wider organization. This supports country-specific contracts and operating requirements. If a contract or policy requires particular records to stay in the country, include any logs, backups and recovery copies that contain those records.

ITAR and EU access requirements

For ITAR-controlled technical data, granting a foreign person a password, code or key that enables access to the unencrypted data requires the applicable authorization. An unauthorized release can violate U.S. export law even when the recipient works in the United States. The ITAR definition of U.S. person includes qualifying permanent residents and protected individuals, as well as citizens. Qualifying end-to-end encrypted storage and transmission can fall outside export treatment under 22 CFR 120.54; its conditions include keeping the means of decryption from third parties.

GDPR does not generally require a separate installation in each EU country. A separate provider outside the EEA can trigger the international-transfer rules when it remotely accesses personal data held in the EU. Choosing a local installation and local operators can support a customer's residency and access requirements; the full hosting, support and recovery arrangement determines the actual data paths.

Copyright © 2026 Analog Informatics Corporation. All rights reserved.

Compare the actual authorization service, secret custody, support permissions and operator locations in the proposed configuration. A cloud region, a company address or customer ownership of a storage bucket alone does not answer who can authorize access. Establish which personnel and legal entities may obtain access, from which countries and under which project requirements.

ITAR access information and releases

ITAR encrypted storage and transmission conditions

ITAR U.S. person definition

GDPR, including Articles 1, 28 and 44

EDPB guidance on remote access and international transfers

AIC air-gapped deployment

AIC security and customer control

Scope

AIC Enterprise Privilege Suite and Silverfort Identity Security Platform. The comparison covers identity discovery, sign-in policy, privileged access, service accounts, threat response and audit evidence across on-premises, cloud and hybrid environments.

Operating differences

Keep services running through a credential change

AIC can change a password on a supported system, update the Windows services and scheduled tasks that use it, and verify sign-in. If an update fails, the operator receives an exception and can identify the affected dependency.

Limit privileged work to the approved task

AIC can grant temporary endpoint elevation or connect an administrator to a target through a session broker. The customer selects the permitted actions, the duration and the records to retain for the protocol.

Give reviewers the operational record

The change result answers whether the credential was updated. An access approval explains who authorized the work, and a recording can show the session itself. A reviewer may need all three.

Plan credential changes across many systems

A single service account can support jobs on several servers. Test a representative group during a real change window, including the recovery procedure for a server that misses its update.

Competitor approach

Silverfort uses directory and cloud identity data to map permissions and actual access. Its policies can challenge an administrator during a direct sign-in, block an authentication attempt from an unexpected service-account host or check a ServiceNow ticket before enabling a domain administrator account.

Copyright © 2026 Analog Informatics Corporation. All rights reserved.

Practical difference

A service account with an exposed password presents two immediate jobs. Silverfort can restrict the hosts that may authenticate with it. AIC can change its password, update the services that use it and report a missed update. An identity team may need both actions before allowing the service back into operation.

Interpretation

Test the route an administrator takes through a broker and the route a service takes directly through the directory. Review the sign-in decisions alongside the privileged-session recording and the result of the credential change.

Alternatives and switching

CQ01 What are the best alternatives to Silverfort?

Analog Informatics: AIC belongs on the shortlist for identity teams that need to discover accounts, govern privileged access and correct problems on managed systems. It can change a service password, update supported dependencies and record an approved maintenance session. Check where users sign in when comparing MFA coverage.

Silverfort: For a team that needs to rotate shared credentials or replay privileged sessions, AIC and vault-based PAM products such as BeyondTrust belong on the shortlist. For a team trying to challenge a risky login to a legacy application, compare how each candidate handles that application’s actual authentication protocol.

Evidence: Vaultless PAM, fail-open behavior and audit events; Privileged Access Security; AIC conditional access and threat reporting for suite sign-ins; AIC supported targets and credential updates; AIC privileged access approvals, session controls and recordings; AIC account lifecycle and access review

CQ02 Which companies compete with Silverfort?

Analog Informatics: Analog Informatics competes with Silverfort for identity discovery, access reviews, conditional access and privileged administration. Delinea and BeyondTrust are also candidates when a team needs a credential vault and recorded sessions.

Silverfort: Silverfort compares its privileged access product with offerings from CyberArk/Idira, Delinea and BeyondTrust. In organizations that already have an identity provider or a threat detection product, MFA and responses to risky sign-ins may also overlap.

Evidence: Vaultless PAM, fail-open behavior and audit events; Identity Threat Detection and Response; AIC conditional access and threat reporting for suite sign-ins; AIC account lifecycle and access review; Silverfort Identity Graph & Inventory and Access Intelligence

CQ03 How does AIC compare with Silverfort?

Analog Informatics: AIC can challenge a sign-in to its own suite, grant time-limited access, change a target credential and show a reviewer what happened during a supported session. Its products include PIM, PAM, PUM, IGA, GRC, CLM and CIAM.

Silverfort: Silverfort evaluates access through connected identity providers. It can challenge a direct sign-in to an older application, restrict which servers may authenticate with a payroll service account and identify who actually used a privileged resource.

Copyright © 2026 Analog Informatics Corporation. All rights reserved.

Evidence: Privileged Access Security; Universal MFA and supported authentication paths; Service account discovery and access policies; AIC conditional access and threat reporting for suite sign-ins; AIC privileged access approvals, session controls and recordings; Silverfort Identity Graph & Inventory and Access Intelligence; Silverfort controls for non-human identities and AI agents

CQ04 Can AIC replace Silverfort, or do I need both?

Analog Informatics: AIC can replace overlapping access controls where the released product covers the same sign-in route, identity and target. For a planned migration, test direct sign-ins to older applications as well as suite-mediated access, service-account policies and time-limited directory privileges.

Silverfort: Keeping both makes sense when Silverfort protects direct directory sign-ins and AIC manages the associated credentials, access approvals and administrative sessions. For a replacement, include sign-ins that bypass the session broker in the acceptance test.

Evidence: Domain admin JIT and coexistence with PAM; Vaultless PAM, fail-open behavior and audit events; AIC conditional access and threat reporting for suite sign-ins; Privileged Access Security

CQ05 Why would I switch from Silverfort?

Analog Informatics: A strong reason to switch is that staff still change a shared password by hand and have to find every scheduled task that uses it. AIC can discover accounts, propagate changes to supported dependencies and report exceptions for repair. Model the switch on the applications that cause the most service interruptions.

Silverfort: A reason to change is a requirement to rotate credentials, update dependent applications and retain a record of work inside a privileged session. Identify which sign-ins Silverfort currently denies because the source is unfamiliar or the approval ticket has expired, so the replacement preserves those protections.

Evidence: Vaultless PAM, fail-open behavior and audit events; ServiceNow ticket validation for JIT access

CQ06 Is there a self-hosted alternative to Silverfort?

Analog Informatics: Yes. AIC supplies software that customers can operate on supported infrastructure, including in a disconnected network. It is an option when local operators need to manage credentials, control privileged sessions and retain their records on site.

Silverfort: Silverfort itself offers an on-premises virtual appliance and documents air-gapped MFA with FIDO2 hardware tokens. For either product, specify which functions must run locally when an external connection is unavailable.

Evidence: Local FIDO2 authentication in air-gapped networks; Packages and support options; AIC disconnected operations

CQ07 Can I replace several security tools with one platform?

Analog Informatics: AIC supplies its own identity governance, credential management, privileged access and compliance products. For example, a team can replace a separate elevation tool and session recorder when its licensed configuration covers the required tasks, protocols and review records.

Silverfort: Depending on the purchased modules, Silverfort can combine identity inventory, MFA, service-account protection, threat response and just-in-time access. Before retiring a vault or session recorder, demonstrate password changes and session playback in the proposed replacement.

Evidence: Packages and support options; Identity Threat Detection and Response; AIC Enterprise functions and licensing; AIC privileged access approvals, session controls and recordings

Copyright © 2026 Analog Informatics Corporation. All rights reserved.

CQ08 What will I lose - and gain - by switching?

Analog Informatics: AIC can give application owners control of credential changes, updates to dependent services and privileged sessions on their own infrastructure. Identify every sign-in policy that must survive a switch, including rules that reject a valid service credential when it is used from an unfamiliar host.

Silverfort: An existing Silverfort installation may challenge an administrator using a command-line tool or block an attempt to authenticate with a service account on an unauthorized host. Test those direct sign-ins alongside the credential rotation and session records you expect to gain.

Evidence: Domain admin JIT and coexistence with PAM; Vaultless PAM, fail-open behavior and audit events

Capabilities and coverage

CQ09 Does this solution solve my whole problem, or only part of it?

Analog Informatics: AIC covers discovery, sign-in policy for its own suite, access governance, credential changes and administrative sessions. If every direct directory sign-in must also be checked, identify which product enforces policy on each route to your applications.

Silverfort: Silverfort can discover identities, show actual access, challenge risky sign-ins and respond to suspicious activity across supported identity providers. If the same team must rotate a database password and update dependent jobs, ask to see that sequence on its proposed configuration.

Evidence: Universal MFA and supported authentication paths; Identity Threat Detection and Response; Privileged Access Security; AIC conditional access and threat reporting for suite sign-ins; AIC account lifecycle and access review; Silverfort Identity Graph & Inventory and Access Intelligence

CQ10 Which features are included, and which require another product?

Analog Informatics: Specify which operators need credential checkout, password rotation, endpoint elevation, session recording and reviewer access. AIC supplies multiple products, and the Enterprise pricing page and written, itemized quote identify which functions and capacity are included.

Silverfort: Silverfort includes posture management and Universal MFA in Core. Plus adds non-human identity and AI agent security. Advanced adds the Authentication Firewall and identity threat detection and response (ITDR). Enterprise adds Privileged Access Security and Access Intelligence. The order form specifies the modules for the selected deployment.

Evidence: Packages and support options

CQ11 Does it manage both on-premises and cloud assets?

Analog Informatics: AIC can manage credentials on supported on-premises and cloud systems. For a cloud application that authenticates through Entra ID, identify the specific account or key that must change and the API or management interface AIC can reach.

Silverfort: Silverfort integrates with Active Directory and Microsoft Entra ID and analyzes authentication for human and machine identities across on-premises and cloud environments. For an application in either location, identify which identity provider receives its sign-ins and which Silverfort policy covers that path.

Evidence: Vaultless PAM, fail-open behavior and audit events; Service account discovery and access policies

Copyright © 2026 Analog Informatics Corporation. All rights reserved.

CQ12 Does it support Windows, Linux, network devices, and legacy systems?

Analog Informatics: Supported targets include Windows, Linux, Unix, macOS, directories, databases, cloud identities, Cisco devices and management controllers. An older appliance might use directory credentials for sign-in but require its native management interface for a password change. Check both paths on your device version.

Silverfort: Silverfort covers AD-managed Kerberos, NTLM and LDAP authentication and documents controls for local Windows logins, including MFA through a linked AD identity. For a Linux host, network device or legacy application, identify whether administrators sign in through AD, another supported provider or a local account and test that route.

Evidence: Universal MFA and supported authentication paths; Local Windows account protection

CQ13 Does it discover accounts and credentials I don’t know about?

Analog Informatics: Yes. AIC discovers human and service accounts on connected systems and applications. Compare the target inventory with observed directory sign-ins, then investigate accounts in either list that lack an owner or have an unidentified dependent service.

Silverfort: Silverfort’s Identity Graph & Inventory maps identities and their relationships. Its service-account discovery identifies accounts and the systems where they authenticate. To establish whether it can find a dormant secret embedded in a configuration file, include a representative file in the evaluation.

Evidence: Privileged Access Security; Service account discovery and access policies; Identity Security Assessment; Silverfort Identity Graph & Inventory and Access Intelligence; Silverfort controls for non-human identities and AI agents

CQ14 Does it manage non-human identities, service accounts, and AI-agent credentials?

Analog Informatics: AIC can manage service and other non-human accounts and their supported credentials. For a backup service or AI agent, trace the account, API key or certificate to the job that consumes it. Test who changes the credential and how that job picks up the replacement.

Silverfort: Silverfort discovers service accounts, identifies their usual sources and destinations, and can restrict unexpected sign-ins. AI Agent Security maps agents to owners and can enforce policies on supported tool calls. If an agent also needs new keys, test which component issues, replaces and revokes them.

Evidence: Service account discovery and access policies; AI agent security and enforcement; Silverfort controls for non-human identities and AI agents

CQ15 Can it manage passwords, SSH keys, certificates, and API keys?

Analog Informatics: AIC supports passwords, SSH keys, certificates and API keys. Before onboarding an application, identify which credential AIC can change on its target and which consumers it can update. A successful directory login alone gives no evidence that a certificate was renewed or a key replaced.

Silverfort: Silverfort documents service-account protection that can operate without changing passwords or checking credentials out of a vault. Its material does not establish lifecycle management for each SSH key, certificate or API key, so ask which component issues, rotates and revokes each required credential.

Evidence: Vaultless PAM, fail-open behavior and audit events; Service account discovery and access policies

Copyright © 2026 Analog Informatics Corporation. All rights reserved.

CQ16 Does it fix problems automatically, or just tell me they exist?

Analog Informatics: AIC can make authorized changes on supported targets. Administrators select which findings to correct automatically and which need a decision. A failed update creates an event and can notify the owner by email or text when the site has a delivery path.

Silverfort: A configured Silverfort policy can deny a risky authentication attempt, prompt a user for MFA or block the use of a service account on an unauthorized host. For a finding that requires a change to the target itself, demonstrate the integration that makes the change.

Evidence: Identity Threat Detection and Response; Service account discovery and access policies; Silverfort controls for non-human identities and AI agents

CQ17 Does it provide controlled access without exposing credentials?

Analog Informatics: An engineer can enter a supported brokered session without learning the shared credential. AIC PIM also supports approved retrieval when an operator needs the secret. Both routes give the customer a record of how access was obtained.

Silverfort: Silverfort can require MFA and restrict where an existing privileged account signs in. Its vaultless design uses the identity provider’s authentication. Where a shared target requires password injection, have the supplier identify the component that holds the secret and starts the user’s session.

Evidence: Vaultless PAM, fail-open behavior and audit events; Domain admin JIT and coexistence with PAM; AIC privileged access approvals, session controls and recordings

CQ18 Can it remove standing privileges and expire approved access automatically?

Analog Informatics: AIC supports time-limited access to managed targets and temporary endpoint elevation for approved tasks. Test when each permission expires and what happens to an active session if the approval is revoked early.

Silverfort: Silverfort can enable a privileged domain account for a limited period and disable it outside that window. Its ServiceNow integration checks the approval, the user and the access window. Test what happens to a session that is already open when the window closes.

Evidence: Domain admin JIT and coexistence with PAM; ServiceNow ticket validation for JIT access; AIC account lifecycle and access review

Deployment and customer control

CQ19 Is it SaaS, self-hosted software, or a managed service?

Analog Informatics: AIC supplies commercial software for customer-operated on-premises, cloud, hybrid and air-gapped deployment. Your team or an authorized provider operates the installation and its recording storage. You control access to its managed secrets. Staffed monitoring requires a separate arrangement.

Silverfort: Silverfort lists on-premises, SaaS and hybrid deployment models. Managed operation is also available through providers, as illustrated by ITC Secure’s work for a UK financial services company. The provider’s operating responsibilities belong in the services agreement.

Evidence: Local FIDO2 authentication in air-gapped networks; ITC Secure and a UK financial services company; AIC disconnected operations; AIC security and customer control

Copyright © 2026 Analog Informatics Corporation. All rights reserved.

CQ20 Can I run it on my own hardware or in my own cloud account?

Analog Informatics: Yes. Install AIC on supported customer hardware or virtual machines in your cloud account, with access to the directory and applications it manages. A hospital group can deploy it separately in each EU country and put each installation under the authority of its local team.

Silverfort: Silverfort documents installation as a virtual appliance on customer premises. For a customer-owned cloud account, obtain the supported hypervisor or cloud image, network design and licensing terms for that installation. Its SaaS offering represents a separate hosting choice.

Evidence: Local FIDO2 authentication in air-gapped networks; Software license agreement; AIC disconnected operations; AIC security and customer control

CQ21 Can it operate in an air-gapped or disconnected environment?

Analog Informatics: Yes. AIC supports customer-operated air-gapped installations for sensitive missions. Supported local credential, session and elevation operations depend on the site's approved local services. The software can be installed, licensed and updated without a network connection to AIC. Include local identity, time, recording, backup and recovery services in the design; external alerts and feeds need an approved transfer path.

Silverfort: Silverfort documents a full on-premises virtual appliance that enforces MFA with FIDO2 hardware tokens in air-gapped networks. It also offers SaaS and hybrid deployment. Module availability varies by environment, so establish the exact local module set and test the additional functions required by the site.

Evidence: Local FIDO2 authentication in air-gapped networks; Packages and support options; AIC disconnected operations; AIC security and customer control

CQ22 Where are my credentials, logs, and compliance evidence stored?

Analog Informatics: AIC-managed credentials, privileged-session recordings and audit records reside in your installation and the storage you select. A hospital can keep the recording of a sensitive maintenance session locally and decide which events to send to a group security team. Backups and exports need their own storage and access settings.

Silverfort: Silverfort’s vaultless design evaluates sign-ins against the existing identity infrastructure and generates identity and policy logs. Its control mapping describes centralized log storage and SIEM integration. Ask for the proposed locations of event data, backups, support copies and exported records for your selected hosting model.

Evidence: Vaultless PAM, fail-open behavior and audit events; CJIS mapping and retention of identity logs; Data processing agreement; AIC disconnected operations; AIC security and customer control

CQ23 Who can access my data - including the vendor and its support staff?

Analog Informatics: You retain sole authority over access to every secret in the AIC installation. For the overnight job, you can authorize an operator to rotate its password, name the people who may retrieve it for recovery and give a reviewer access to the maintenance record. AIC support has no standing access. Your team controls any access it grants for troubleshooting. Your organization chooses its administrators and provider arrangements, including the people and locations approved for the mission.

Silverfort: Silverfort’s published terms restrict disclosure of confidential information to personnel or contractors who need it for the agreement and are bound by confidentiality. Ask how support access to your particular installation is authorized, how long it lasts and where the resulting access entry is recorded.

Evidence: Data processing agreement; Software license agreement; AIC disconnected operations; AIC security and customer control

Copyright © 2026 Analog Informatics Corporation. All rights reserved.

CQ24 Can I control retention, export my records, and leave without losing evidence?

Analog Informatics: You set retention and can export credentials, audit logs and evidence, including after license expiry. Open an exported approval and its associated session record in your normal review process before retiring the installation. Licensed operation stops at expiry.

Silverfort: Silverfort's CJIS mapping describes at least one year of identity logs and a longer-term archive option. Events can be sent to a customer SIEM, and its data agreement provides for return or deletion of covered personal data at termination, subject to exceptions. Verify export formats and your access to historical events after the service ends.

Evidence: CJIS mapping and retention of identity logs; SOCI mapping and event export; Data processing agreement

CQ25 Can my MSP operate it while I retain control?

Analog Informatics: Yes. An MSP can perform credential changes and operate sessions under access you grant and can revoke. Keep your own approval authority, backup access and recovery account so the hospital can restore the overnight service or replace the provider.

Silverfort: Silverfort documents an MSP operating with a customer to secure service accounts and external access. Identify who owns the tenant and export destination, who can relax a policy and how you revoke the provider's access. Include the provider's authority in the signed terms.

Evidence: ITC Secure and a UK financial services company; Software license agreement

CQ26 What happens if the vendor's service is unavailable?

Analog Informatics: A customer-operated AIC installation does not need a live connection to AIC for supported local credential and session work. That work can continue with a valid license and healthy local identity, audit and recovery services. Include the site's local dependencies in an outage test. At license expiry, licensed operation stops and export remains available.

Silverfort: Silverfort says that if its service is unavailable, its domain-controller integration fails open and the directory can continue authenticating users. Its on-premises FIDO2 deployment can operate without the internet. Test loss of a local Silverfort node separately from loss of the internet, including which alerts and access records survive.

Evidence: Vaultless PAM, fail-open behavior and audit events; Local FIDO2 authentication in air-gapped networks; AIC disconnected operations; AIC security and customer control

Privileged controls and operational evidence

CQ27 What belongs inside the privileged-access boundary?

Analog Informatics: Follow the operation past sign-in. Include the approver, credential store, session broker, endpoint, target and any services that consume the changed credential. Protect access to the console, backups, recordings and emergency accounts as part of the same boundary.

Silverfort: Include the directory or cloud identity provider, the Silverfort integration, the authenticator and the resources protected by each policy. A local Windows login can require binding to an AD identity for MFA. If ServiceNow validates JIT access, the ticket service also belongs in the dependency list.

Evidence: Universal MFA and supported authentication paths; Local Windows account protection; ServiceNow ticket validation for JIT access

Copyright © 2026 Analog Informatics Corporation. All rights reserved.

CQ28 Which privileged-security controls does the software enforce, assist with, or record?

Analog Informatics: AIC can enforce sign-in policy for the suite, authorize temporary access or endpoint elevation, change a supported credential and record administrative work. The customer sets the policy. The sign-in event, approval, change result and session recording show different parts of the activity.

Silverfort: Silverfort can enforce MFA, deny a risky login, restrict account use to allowed paths and grant time-limited privileged access. It produces events showing authentication, policy decisions and enforcement. A reviewer can use those events to check whether a particular sign-in met policy.

Evidence: Privileged Access Security; Identity Threat Detection and Response; Vaultless PAM, fail-open behavior and audit events; AIC conditional access and threat reporting for suite sign-ins; AIC privileged access approvals, session controls and recordings

CQ29 What remains my responsibility or my MSP's responsibility?

Analog Informatics: Your team or MSP connects the managed targets, chooses who can approve work, migrates accounts and validates dependent services. Assign ownership of failed updates, evidence retention, backups and emergency access before enabling automatic changes.

Silverfort: Your team or service provider decides which accounts to protect, what connections a service account genuinely needs and when a proposed restriction is safe to enforce. Silverfort describes guided configuration and pilot support for testing those decisions before broader rollout.

Evidence: Implementation, training and support; Service account discovery and access policies

CQ30 Does it continuously record privileged activity, or will we still reconstruct it for an audit?

Analog Informatics: AIC collects access and activity records during normal operation. When recording is supported and enabled for the protocol, an auditor can review the session, identify the target and check the approval. Specify whether the review requires a sign-in event, a change result, a recording or all three.

Silverfort: Silverfort records privileged authentications and policy decisions as they happen and sends enriched alerts to security tools. Those events let a reviewer trace a sign-in and its result. For command history or screen playback, ask for a sample from the proposed SSH or RDP configuration, since the product description covers authentication events.

Evidence: Vaultless PAM, fail-open behavior and audit events; Identity Threat Detection and Response; AIC privileged access approvals, session controls and recordings

CQ31 Can it detect privilege drift and remediate problems during daily operations?

Analog Informatics: AIC can detect configuration changes on managed systems, record drift and apply an authorized correction where automatic repair is supported. An operator can investigate a failed repair or a service that missed a credential update.

Silverfort: Silverfort's posture management identifies identity exposures. Its service-account policies and threat response can block authentication on an unexpected path or challenge a risky sign-in. If the desired outcome is to remove an excessive permission on a target, identify the component that makes and verifies that change.

Evidence: Service account discovery and access policies; Identity Threat Detection and Response; AIC threat response, drift detection and remediation; Silverfort controls for non-human identities and AI agents; Packages and support options

Copyright © 2026 Analog Informatics Corporation. All rights reserved.

CQ32 Does it track training, attestations, access approvals, access reviews and corrective actions?

Analog Informatics: AIC records privileged approvals and corrective actions. Reviewers can check existing access to suite-managed accounts, apply a decision and retain the activity record. If a ticketing system holds part of the approval, keep its reference with the access record. AIC can also track training assignments and attestations.

Silverfort: Silverfort can check privileged access against an approved ServiceNow ticket, and Access Intelligence shows reviewers who actually used a resource. The reviewed materials do not identify where a final attestation and completed correction are recorded. Follow both through the proposed deployment. The reviewed guides do not identify a training-assignment register. Ask for a sample that links a person's training and attestation to the access decision.

Evidence: ServiceNow ticket validation for JIT access; PCI DSS mapping and access reviews; AIC account lifecycle and access review; Silverfort Identity Graph & Inventory and Access Intelligence; AIC Enterprise Privilege Suite

CQ33 Can security reviewers inspect current access records without disrupting IT?

Analog Informatics: A reviewer with the appropriate permissions can inspect current access reports while an operator works. Limit the reviewer's access to the required evidence and reserve authority to approve elevation or change credentials for the designated operators.

Silverfort: Reviewers can inspect authentication events in a security information and event management (SIEM) system while administrators work. If reviewers need direct access to the Silverfort console, demonstrate which records their role can see and whether it permits policy changes.

Evidence: SOCI mapping and event export; PCI DSS mapping and access reviews; Identity Threat Detection and Response

CQ34 Can the same access records support multiple security policies and audits?

Analog Informatics: A dated access record can support several reviews when it identifies the person, target, authorization and action each policy requires. AIC supports control mappings and evidence review. Retain the password-change result or session recording when a policy asks what changed after sign-in.

Silverfort: Yes. Silverfort's CJIS and PCI DSS mappings use identity events to support monitoring of sign-ins and account use. A reviewer can reuse the same dated events where policy requirements overlap and add separate records for approvals, exceptions or work performed after login.

Evidence: CJIS mapping and retention of identity logs; PCI DSS mapping and access reviews

CQ35 Can it replace our governance tool or feed our SIEM, ticketing and governance systems?

Analog Informatics: AIC can send events to supported SIEM and ticketing systems and export evidence for a governance system. Use a maintenance ticket and its timestamps to check that reviewers can trace the sign-in, the subsequent administrative session and the result of the change. AIC also supplies GRC software. Its licensed controls, reviews and reporting determine whether it can replace your current tool.

Silverfort: Silverfort forwards identity events to SIEM and security operations tools, supports Common Event Format and validates ServiceNow tickets for JIT access. For a governance system, test the receiving connector, event identifiers and whether an update in one system is reflected in the other. For full replacement, ask to see control mapping, recurring reviews and follow-up on corrective actions in the proposed product.

Copyright © 2026 Analog Informatics Corporation. All rights reserved.

Evidence: Identity Threat Detection and Response; ServiceNow ticket validation for JIT access; SOCI mapping and event export; AIC Enterprise Privilege Suite

Cost and value

CQ36 What is the total cost - not just the advertised subscription?

Analog Informatics: Include the Enterprise license, the cost of connecting managed systems, staff time, backups and storage for credentials and session recordings. Compare quotes using the same account counts, systems and retention period. If you keep an existing identity protection service, include its subscription.

Silverfort: The quote depends on the selected modules, covered accounts and support tier. Also budget for the proposed appliance infrastructure or service, hardware tokens where required, SIEM storage, deployment assistance and the people who will review policies and exceptions.

Evidence: Packages and support options; Software license agreement; Implementation, training and support; Local FIDO2 authentication in air-gapped networks

CQ37 Is pricing based on users, administrators, identities, assets, or usage?

Analog Informatics: AIC licenses systems, applications and users under product-specific allowances. The Enterprise quote also reflects selected modules, session capacity and term length. Human and non-human account or credential counts do not set the license count.

Silverfort: Silverfort quotes by organization size. Its published software license sets an order-form limit for monitored or protected user and service accounts. Use the signed proposal to establish how those accounts are counted across directories and deployments.

Evidence: Packages and support options; Software license agreement

CQ38 Are non-human identities charged separately?

Analog Informatics: AIC carries no separate charge based on the count of service accounts, AI-agent credentials or other identities. A new application or managed system can still affect the package. Inventory systems and applications as well as accounts when comparing quotes.

Silverfort: Silverfort's published license counts service accounts. Non-human identity protection is also a package entitlement. Public pricing gives no separate rate for each service account, AI agent or machine credential.

Evidence: Software license agreement; Packages and support options

CQ39 What costs extra: connectors, reporting, storage, support, or audit access?

Analog Informatics: The Enterprise order identifies the licensed functions, capacity, connectors and reviewer access. Include recording storage if reviewers need playback. Best-effort product support is free, while contractual response commitments and provider services are separate purchases.

Silverfort: Silverfort includes Standard support and offers higher support tiers and expert services at additional cost. Ask for an itemized quote covering connectors, longer retention, report access and reviewer accounts for the modules you select.

Evidence: Packages and support options; Implementation, training and support

Copyright © 2026 Analog Informatics Corporation. All rights reserved.

CQ40 What infrastructure and third-party licenses will I need?

Analog Informatics: Provide supported servers or virtual machines, network connections, backups, recording storage and any required platform licenses. If a separate directory MFA appliance is part of the design, include its resource and licensing requirements.

Silverfort: Local MFA requires a supported appliance, directory connectivity and compatible authenticators. Budget for FIDO2 tokens in a disconnected deployment and for your own SIEM if it will retain exported events. Ask Silverfort to size the appliances and identify any required third-party licenses for the proposed topology.

Evidence: Local FIDO2 authentication in air-gapped networks; Vaultless PAM, fail-open behavior and audit events; SOCI mapping and event export

CQ41 How much staff time does it take to operate?

Analog Informatics: AIC can automate discovery, password changes and updates to supported services. Staff still connect new targets, review exceptions and repair failed updates. Measure operator time across a representative change window, including an unreachable host.

Silverfort: Automated service-account discovery and suggested restrictions can reduce inventory work. Operators still review permitted destinations, investigate exceptions and maintain integrations. The published onboarding guide gives no staffing figure for your size, so measure those tasks during the pilot.

Evidence: Service account discovery and access policies; Implementation, training and support

CQ42 Which manual tasks and existing subscriptions could it eliminate?

Analog Informatics: AIC can automate password changes, updates to supported dependencies, approved elevation and collection of session evidence. Before retiring a directory control, demonstrate how the remaining system will block a service-account sign-in from an unauthorized host.

Silverfort: Silverfort can automate service-account discovery, flag unusual sign-ins, challenge a user or deny access, reducing manual log review and policy setup. It can overlap with an MFA or identity threat tool. Keep a vault or recorder in service until the proposed replacement demonstrates each job it performs.

Evidence: Service account discovery and access policies; Identity Threat Detection and Response; Domain admin JIT and coexistence with PAM

CQ43 How do costs change as the company grows?

Analog Informatics: Cost can rise with licensed systems, applications, users, modules and required session capacity. Adding service accounts to the same systems does not itself change the license count. Include enough storage and operator time for the extra activity and exceptions.

Silverfort: Growth can exceed the count of covered user and service accounts on the order or require additional modules and support services. Request a second quote at your expected account count and include the extra ingestion and retention capacity in your SIEM.

Evidence: Software license agreement; Packages and support options

CQ44 What infrastructure and capacity limits apply to remote sessions or hosted workspaces?

Analog Informatics: AIC runs privileged sessions on customer-supplied infrastructure. Estimate peak simultaneous sessions and the storage needed for recordings over the required retention period. If you also intend to offer hosted desktops, include their separate capacity and licensing requirements.

Copyright © 2026 Analog Informatics Corporation. All rights reserved.

Silverfort: Silverfort validates authentication for remote access, including supported RDP and SSH paths. The cited offering gives no hosted desktop allowance or session-recording capacity figures. Size concurrent sessions and recording storage with the remote access or recording product in the proposed design.

Evidence: Vaultless PAM, fail-open behavior and audit events; Universal MFA and supported authentication paths

Implementation and migration

CQ45 Can it work with our existing environment, or must we start over?

Analog Informatics: Yes. AIC can discover accounts and manage selected credentials in an existing environment. Keep directory protections active while onboarding an application and check that automatic password changes, service restarts and emergency logins still work together.

Silverfort: Yes. Silverfort can add MFA to existing directory-based authentication without rewriting the target applications. PAS can run alongside a PAM system, including for administrators already enrolled in that system and accounts still outside it.

Evidence: Universal MFA and supported authentication paths; Domain admin JIT and coexistence with PAM

CQ46 How quickly can we deploy the Enterprise platform?

Analog Informatics: AIC can discover and remediate existing systems after installation. The time to approve production use depends on identity integration, target permissions, service dependencies and local change windows. Measure the first deployment with a representative group of applications before estimating the wider rollout.

Silverfort: Silverfort describes a typical vaultless PAM deployment in days to a few weeks. Its onboarding includes architecture design, configuration, testing and a pilot. Set a schedule against your own directory and application coverage, including time to test emergency access.

Evidence: Vaultless PAM, fail-open behavior and audit events; Implementation, training and support

CQ47 How long does it take to discover and secure existing assets?

Analog Informatics: Measure discovery and protection separately. Inventory may reveal a service account immediately even if its scheduled job runs only monthly. Change its credential in an approved window and verify that the job runs with the replacement before counting it as secured.

Silverfort: Silverfort advertises a one-week identity assessment that identifies exposed admin accounts, service accounts and other risks. Putting a restriction into production takes additional review, especially for a service account that uses a destination only during month-end work.

Evidence: Identity Security Assessment; Service account discovery and access policies

CQ48 Can we introduce it gradually without interrupting operations?

Analog Informatics: Yes. Start with discovery, approve changes to a small set of accounts and verify each application before broadening automation. Include a service with a known owner and recovery path while the current sign-in rules remain in place.

Silverfort: Silverfort can discover a service account and propose a policy before an administrator activates it. Test the restrictions with one account, including infrequent jobs, before applying the policy to a larger group.

Copyright © 2026 Analog Informatics Corporation. All rights reserved.

Evidence: Service account discovery and access policies; Implementation, training and support

CQ49 How do we migrate credentials, policies, and evidence?

Analog Informatics: Export historical approvals and recordings, map directory policy to the access route it protects and inventory the consumers of each credential. Move a representative account first, verify its dependent jobs and keep the original audit records accessible to the reviewer.

Silverfort: Silverfort can be added alongside an existing PAM service while the original vault and access records remain available. Map the old policies to Silverfort rules, verify event exports in your SIEM and preserve historical approval and session records before retiring their current storage.

Evidence: Domain admin JIT and coexistence with PAM; Data processing agreement; SOCI mapping and event export

CQ50 Who handles configuration, migration, and ongoing operations?

Analog Informatics: The customer or its provider configures and operates the installation. Ask the directory team to identify sign-in rules that must survive the transition and application owners to verify their services after each change. AIC supplies the product and guidance.

Silverfort: Silverfort describes expert-led onboarding that covers design, configuration, testing and pilot support. Customers or a contracted provider can handle daily operations. Assign directory changes, policy approvals and historical data migration explicitly in the services agreement.

Evidence: Implementation, training and support; ITC Secure and a UK financial services company

CQ51 What training, deployment guides, and support are included?

Analog Informatics: Guides, cookbooks, recipes and training materials are included with free best-effort support. A purchased enterprise agreement commits to a response within four hours, around the clock. Resolution depends on the issue, including whether the affected system is accessible.

Silverfort: Silverfort provides technical documentation, Academy training and a free certification program. Its support packages differ in coverage and service levels, with Standard included in the published pricing. Check which onboarding and pilot services are included with your proposal.

Evidence: Implementation, training and support; Packages and support options

CQ52 Can we test it on our own systems before committing?

Analog Informatics: AIC offers a free 30-day Enterprise Privilege Suite trial. Choose a target with a real service dependency, authorize a password change and inspect the result on both systems. Include a reviewer with limited permissions and test emergency access.

Silverfort: Silverfort offers a free identity assessment scoped with the customer, and its onboarding materials describe pilot support. The assessment focuses on identity exposure. Arrange an enforcement pilot if you need to exercise blocking, JIT and disconnected MFA on your equipment before purchase.

Evidence: Identity Security Assessment; Implementation, training and support

Copyright © 2026 Analog Informatics Corporation. All rights reserved.

Vendor credibility and fit

CQ53 Who is this company, and how long has it supported this kind of environment?

Analog Informatics: Analog Informatics Corporation develops Enterprise Privilege Suite. Its founder's work on privileged-identity products dates to 1993. For your specific application or directory, use the current supported-target record and a trial to assess operational fit.

Silverfort: Silverfort is an identity security company founded in 2016. Its product materials document privileged-account discovery, runtime access restrictions and JIT for domain administrators. Ask for a reference using the same identity providers and deployment model if support history for those systems matters.

Evidence: Company history; Domain admin JIT and coexistence with PAM

CQ54 Does it understand organizations like ours?

Analog Informatics: AIC addresses requirements that industrial operators and their suppliers share, including locally approved maintenance, restricted commands, customer control of credentials and records of work on supported systems. A plant can test these requirements on a representative engineering workstation.

Silverfort: Silverfort describes how automotive engineering group ASAP Holding protected legacy file access and how a financial services company worked with ITC Secure to protect service accounts and outside advisers' sign-ins. Choose a reference with similar applications, identity providers and access routes.

Evidence: ASAP Holding and Protea Networks; ITC Secure and a UK financial services company; AIC access for industrial operators and outside suppliers

CQ55 Can it demonstrate our specific use case?

Analog Informatics: Have an operator obtain temporary elevation for one task on a test endpoint and perform maintenance through a recorded session. After approval expires, try to start a new session. Give the reviewer the approval and recording from the test.

Silverfort: In an enforcement pilot, approve a maintenance ticket, enable the domain administrator account for that window and try the same sign-in after the window expires. For an isolated site, demonstrate local FIDO2 authentication with the external connection removed.

Evidence: Identity Security Assessment; ServiceNow ticket validation for JIT access; Local FIDO2 authentication in air-gapped networks; AIC privileged access approvals, session controls and recordings

CQ56 What do customers say about reliability and support?

Analog Informatics: The comparison materials include no published AIC customer account of reliability or support. In the trial, measure recovery after an unavailable target and ask which support response applies to that scenario under the proposed agreement.

Silverfort: In a case study published by Silverfort, Optix describes help from its customer success team during onboarding and ongoing operations. The account reflects one customer's experience. Check Silverfort's service status history for outages and the proposed agreement for response commitments.

Evidence: Optix customer account of onboarding and support; Service availability; Implementation, training and support

Copyright © 2026 Analog Informatics Corporation. All rights reserved.

CQ57 What are its limitations?

Analog Informatics: AIC needs a supported interface, permissions and connectivity to the target it will change. Local sign-in, directory authentication, endpoint elevation and session recording can each follow different paths. Verify the exact operation before promising coverage to an application owner.

Silverfort: Silverfort's vaultless PAM design depends on observing the relevant authentication request. Its domain-controller integration allows authentication to continue if the Silverfort service becomes unavailable. Silverfort documents local air-gapped MFA. For other local modules, credential rotation or session playback, obtain deployment-specific documentation or a demonstration.

Evidence: Vaultless PAM, fail-open behavior and audit events; Packages and support options; Local FIDO2 authentication in air-gapped networks

CQ58 Which capabilities are available today, and which are roadmap items?

Analog Informatics: As of November 18, 2026, AIC supplies PIM, PAM, PUM, IGA, GRC, CLM and CIAM. Every Silverfort feature is in scope for future AIC development. This direction carries no commitment to a particular feature or release date. For a purchase today, identify the released function and supported target for each requirement.

Silverfort: Silverfort lists identity inventory, access intelligence, posture management, Universal MFA, non-human identity and AI agent security, the Authentication Firewall, ITDR and Privileged Access Security with just-in-time access. Its order form determines which modules are available in the selected deployment.

Evidence: Packages and support options; Privileged Access Security; Universal MFA and supported authentication paths; Service account discovery and access policies; Identity Threat Detection and Response; Silverfort Identity Graph & Inventory and Access Intelligence

CQ59 How does it handle vulnerabilities and security updates?

Analog Informatics: AIC generally responds to severe vulnerability reports within 24 hours and typically has a mitigation within 24 hours of notice, on a best-effort basis. Customers control update timing. For an isolated site, exercise the approved transfer and installation process using its own change window.

Silverfort: Silverfort directs customers to its Trust Center, technical documentation, support channels and product updates. The reviewed materials do not specify an appliance patch deadline or how an isolated site receives and verifies a particular fix. Obtain the advisory procedure and demonstrate an offline update before rollout.

Evidence: Implementation, training and support; Local FIDO2 authentication in air-gapped networks

CQ60 Will it work with our existing vendors and service providers?

Analog Informatics: AIC can work with existing directories, supported Microsoft systems, MSPs, SIEM platforms and ticketing systems. Check whether a provider can administer the intended targets and trace one maintenance event across products with the available permissions and record identifiers.

Silverfort: Silverfort documents integrations with Active Directory, Entra ID and ServiceNow, and publishes a customer case involving an independent managed security provider. For another provider, map its admin rights, incident escalation and access to the customer's logs.

Evidence: Vaultless PAM, fail-open behavior and audit events; ServiceNow ticket validation for JIT access; ITC Secure and a UK financial services company

Copyright © 2026 Analog Informatics Corporation. All rights reserved.

CQ61 What happens to our deployment if the vendor is acquired or changes direction?

Analog Informatics: You retain the installed environment, credentials and evidence. Exports remain available after license expiry, although licensed operation stops. Keep tested copies of required records and a working independently controlled emergency login before changing suppliers.

Silverfort: Silverfort's published license permits transfer in certain acquisitions and requires software use to end at contract expiration or termination. It describes reasonable offboarding assistance on request. Negotiate any continuity rights you need and test access to independently retained event data before the contract ends.

Evidence: Software license agreement; Data processing agreement

Sources and evaluation

Analysis uses vendor product documentation and current AIC product-owner statements. No independent performance benchmark or customer-support measurement was performed for this comparison.

Privileged Access Security

Domain admin JIT and coexistence with PAM

Vaultless PAM, fail-open behavior and audit events

Universal MFA and supported authentication paths

Service account discovery and access policies

Identity Threat Detection and Response

AI agent security and enforcement

ServiceNow ticket validation for JIT access

Local FIDO2 authentication in air-gapped networks

Packages and support options

Software license agreement

Data processing agreement

Implementation, training and support

Identity Security Assessment

Company history

CJIS mapping and retention of identity logs

PCI DSS mapping and access reviews

SOCI mapping and event export

ASAP Holding and Protea Networks

Optix customer account of onboarding and support

ITC Secure and a UK financial services company

Copyright © 2026 Analog Informatics Corporation. All rights reserved.

Service availability

Local Windows account protection

AIC supported targets and credential updates

AIC Enterprise functions and licensing

AIC disconnected operations

ITAR access information and releases

ITAR encrypted storage and transmission conditions

ITAR U.S. person definition

GDPR, including Articles 1, 28 and 44

EDPB guidance on remote access and international transfers

AIC conditional access and threat reporting for suite sign-ins

AIC privileged access approvals, session controls and recordings

AIC account lifecycle and access review

AIC threat response, drift detection and remediation

AIC access for industrial operators and outside suppliers

Silverfort Identity Security Platform

Silverfort Identity Graph & Inventory and Access Intelligence

Silverfort controls for non-human identities and AI agents

Silverfort support for Active Directory, legacy applications and operational technology

AIC Enterprise Privilege Suite

AIC security and customer control

Test one emergency maintenance window

Use an approved incident ticket and the sign-in routes your on-call team uses. Check MFA on a direct directory sign-in and on a sign-in to the AIC suite. Grant temporary access, record a supported maintenance session and verify that a new request is denied after the approved window closes.

For more information about Analog Informatics Corporation, please go to analoginfo.com.

Copyright © 2026 Analog Informatics Corporation. All rights reserved.