COMPETITIVE ANALYSIS

# Analog Informatics vs. Keeper - Competitive Analysis

Compare AIC and Keeper for vault sharing, service-account rotation and privileged sessions. Review cloud PAM and Self-Managed Keeper for air-gapped work.

Analysis date: October 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 | Keeper |
|---|---|---|
| On-premises management | Yes. Install and operate the management software on customer infrastructure. | Yes. Self-Managed Keeper supplies a local vault, administration and routing service. A cloud Gateway alone is a different design. |
| Management in your own cloud account | Yes. Install and manage AIC in a cloud account and region you choose. | Yes. Self-Managed Keeper can run on a supported private-cloud Linux host or virtual machine. Confirm private network and system prerequisites. |
| Hybrid operation | Yes. Customer-managed local and cloud components can serve the chosen systems and applications. | Yes. Cloud and local targets can be served by Gateways. Cloud and self-managed tenants remain independent with separate users and data. |
| Vendor-operated SaaS | No mandatory AIC-operated SaaS management service. The customer or its authorized provider operates the installation. | Yes. KeeperPAM is available with a cloud access-control plane and customer-operated Gateways. |
| 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. Self-Managed Keeper documents independent local credential and privileged-session operation for air-gapped networks. Confirm licensed module support and local dependencies. |
| Secret and administrative control | The customer authorizes secret use, retrieval and changes. AIC support has no standing access. | Keeper describes zero-knowledge credential protection. In Self-Managed Keeper the customer operates the tenant; cloud provider operation and local secret administration are different roles. |
| Country-specific installation and records | Install and operate within a chosen country. Configure operators, logs, backups and recovery copies for the required boundary. | A self-managed tenant can retain its service, data and recordings locally. Include internal DNS, certificates, backups, support arrangements and any chosen external integration. |

AIC’s local and air-gapped scope follows current product-owner confirmation. The competing options follow the cited documentation. Select the actual product, edition and architecture: a locally installed connector, cached secret and independent local management service have different dependencies. Test external integrations separately.

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

Keeper: Keeper offers cloud-based PAM and separately licensed Self-Managed Keeper. The latter runs Docker containers on customer-operated Linux infrastructure, supports air-gapped environments and operates as a tenant independent of Keeper Cloud. A local cloud Gateway alone is not that self-managed service.

KeeperPAM product scope; Self-Managed Keeper deployment and air-gap operation; Self-Managed Keeper licensing; Self-Managed Keeper system requirements


Copyright © 2026 Analog Informatics Corporation. All rights reserved.

## Should the vault workflow stay in the cloud or move to a local tenant?

A software company uses Keeper to share administrator credentials and now needs to rotate a Windows service account, record a database session and remove hardcoded application secrets. A separate restricted site needs its own locally operated management service.

**What Keeper offers:** Keeper connects a familiar credential vault to password rotation, privileged connections, tunnels and secrets delivery. Its documented rotation updates Windows service and scheduled-task logins. Beyond the cloud PAM offering, Self-Managed Keeper provides an independent local tenant for sensitive and air-gapped networks; it is more than a local Gateway for a cloud vault.

**Where AIC changes the decision:** AIC combines dependency discovery and supported corrections, application elevation, controlled sessions and governance evidence under customer operation. It supports air-gapped installation, licensing and updates without a connection to AIC. Keeper also offers self-management, so evaluate the complete current feature set, deployment prerequisites and recovery workflow rather than frame the decision as local software versus unavoidable SaaS.

**Which approach fits:** AIC fits teams seeking customer-operated account correction, privilege use and review evidence across systems. Keeper fits teams extending their vault and secrets workflows into rotation, connections and tunnels, or selecting a separate Self-Managed Keeper tenant for a restricted network. Trial the actual tenant type; cloud and self-managed features should not be assumed identical.

**A practical example:** Rotate the Windows account shared by a service and scheduled task, open a recorded database session and have an application retrieve a secret. Interrupt the outside connection and distinguish cloud behavior from a Self-Managed Keeper installation. Compare the first restart, session review and recovery records with AIC.

## Where AIC and Keeper overlap, and who each serves

### Current capabilities and future scope

This comparison describes currently documented products and selected deployment options. AIC’s feature set is evolving, and the full competitor feature range is in scope for future releases. That scope is not a statement that every function is delivered today, included in the order or committed for a particular date.

## Where the features overlap

### Credential rotation and dependent services

**AIC today:** AIC discovers shared credentials and supported dependencies, updates services and scheduled tasks and verifies sign-in.

**Keeper today:** KeeperPAM lists resource discovery and account management. Test an unlisted service and its consumers to establish what is detected and onboarded, and which dependencies must be configured before the first rotation. Keeper automates supported rotations and can update Windows services and scheduled tasks, with post-rotation actions. Test a failed consumer and verify recovery rather than treat the rotation schedule as proof that the application works.


Copyright © 2026 Analog Informatics Corporation. All rights reserved.

**What this means for the customer:** Test the next consumer restart and a deliberately unavailable target. A changed vault value does not prove the business service recovered.

### Privileged sessions and endpoint elevation

**AIC today:** AIC brokers and records supported sessions and can grant application-specific elevation on supported endpoints.

**Keeper today:** Keeper connections can use vault-managed credentials without exposing them to the end user, with recorded sessions. Verify retrieval rights separately from connection rights and test the actual database, remote desktop or tunnel path. Keeper provides time-limited connections and tunnels and a separate endpoint privilege product. Demonstrate expiry for the required path, including a running session or elevated process, under the chosen tenant and license.

**What this means for the customer:** Demonstrate a recorded remote session and elevation of one local maintenance program separately.

### Service and application identities

**AIC today:** AIC manages service and application credentials and supplies scoped API tokens for authorized software, including AI agents.

**Keeper today:** Keeper Secrets Manager supplies secrets to applications and scripts, while PAM manages selected service and user accounts. Request the exact identity and permissions used by an AI agent; credential delivery alone does not constrain every downstream action.

**What this means for the customer:** Distinguish delivery of a secret, authority to change the target and permission to perform a downstream application action.

### Governance and operational evidence

**AIC today:** AIC provides identity governance and GRC products, suite-account reviews and evidence of supported corrective actions.

**Keeper today:** Keeper provides access and activity records, but the reviewed sources do not establish a complete training and attestation program for every tenant. Demonstrate the required access review and corrective evidence under the purchased products. Keeper supplies APIs, automation and reporting integrations. Test event mapping to retained SIEM, ticketing or governance tools, including whether the receiving record distinguishes a failed dependency from its eventual recovery.

**What this means for the customer:** Trace one access approval through the action and review. Specify the licensed governance functions rather than infer them from audit logging.

### Location and operating authority

**AIC today:** AIC is customer-operated on premises, in customer cloud, hybrid or air-gapped. No standing AIC support access is required.

**Keeper today:** Keeper offers cloud-based PAM and separately licensed Self-Managed Keeper. The latter runs Docker containers on customer-operated Linux infrastructure, supports air-gapped environments and operates as a tenant independent of Keeper Cloud. A local cloud Gateway alone is not that self-managed service.

**What this means for the customer:** Choose the real architecture before comparing local administration, third-party access, updates and outage behavior.


Copyright © 2026 Analog Informatics Corporation. All rights reserved.

## AIC strengths

Customer authority over managed secrets, software location, authorized operators, record retention and support access.

Dependency-aware credential work connects supported changes, failure handling and verification with privileged access and governance evidence.

Customer-operated air-gapped installation, licensing and updates without a network connection to AIC, with required local services designed for the mission.

## Keeper strengths

Keeper connects a familiar credential vault to password rotation, privileged connections, tunnels and secrets delivery. Its documented rotation updates Windows service and scheduled-task logins. Beyond the cloud PAM offering, Self-Managed Keeper provides an independent local tenant for sensitive and air-gapped networks; it is more than a local Gateway for a cloud vault.

Keeper Secrets Manager supplies secrets to applications and scripts, while PAM manages selected service and user accounts. Request the exact identity and permissions used by an AI agent; credential delivery alone does not constrain every downstream action.

Keeper offers cloud-based PAM and separately licensed Self-Managed Keeper. The latter runs Docker containers on customer-operated Linux infrastructure, supports air-gapped environments and operates as a tenant independent of Keeper Cloud. A local cloud Gateway alone is not that self-managed service.

## Which customers fit each approach

### AIC - Teams that want to operate privilege controls and corrective evidence under their own authority.

AIC combines dependency discovery and supported corrections, application elevation, controlled sessions and governance evidence under customer operation. It supports air-gapped installation, licensing and updates without a connection to AIC. Keeper also offers self-management, so evaluate the complete current feature set, deployment prerequisites and recovery workflow rather than frame the decision as local software versus unavoidable SaaS.

### Keeper - Teams extending Keeper vault and secrets workflows or selecting its independent self-managed tenant.

Keeper connects a familiar credential vault to password rotation, privileged connections, tunnels and secrets delivery. Its documented rotation updates Windows service and scheduled-task logins. Beyond the cloud PAM offering, Self-Managed Keeper provides an independent local tenant for sensitive and air-gapped networks; it is more than a local Gateway for a cloud vault.

### Both - Organizations that need a staged migration or useful complementary functions.

Keep the useful current controls while proving the replacement on a distinct account or site. Name one rotation authority for each credential and retain a complete review and recovery path.


Copyright © 2026 Analog Informatics Corporation. All rights reserved.

AIC Enterprise Privilege Suite

AIC supported platforms

AIC disconnected operation

KeeperPAM product scope

Self-Managed Keeper deployment and air-gap operation

Self-Managed Keeper licensing

Self-Managed Keeper system requirements

Keeper password rotation and dependencies

# 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 Keeper comparison

KeeperPAM’s cloud model uses a hosted control plane with a customer-run Gateway. Self-Managed Keeper is a separate local tenant with its own users, data, signed license and customer infrastructure; it can operate without the cloud tenant. Keeper’s documentation credits zero-knowledge credential protection, so hosted operation should not be described as unrestricted provider access to plaintext secrets. AIC is customer-operated and has no standing AIC support access. For both local proposals, establish host administration, updates, recovery keys and which people may grant access or inspect recordings.

### 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.


Copyright © 2026 Analog Informatics Corporation. All rights reserved.

### 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.

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 related AIC products where licensed; KeeperPAM, Keeper Secrets Manager and separately licensed Self-Managed Keeper where selected. Cloud and self-managed availability, integrations and update procedures must be checked for the proposed order.

## Operating differences

### How an account change becomes reliable

AIC identifies supported account dependencies, applies an authorized credential change and verifies the result. A team can automate routine corrections and send failed changes to an operator for recovery.

### Who may use secrets and inspect the result

The customer chooses AIC administrators and can grant session use, direct retrieval and record review separately. It chooses support access, record locations and recovery arrangements.


Copyright © 2026 Analog Informatics Corporation. All rights reserved.

### Competitor approach

Keeper connects a familiar credential vault to password rotation, privileged connections, tunnels and secrets delivery. Its documented rotation updates Windows service and scheduled-task logins. Beyond the cloud PAM offering, Self-Managed Keeper provides an independent local tenant for sensitive and air-gapped networks; it is more than a local Gateway for a cloud vault.

### Practical difference

Rotate the Windows account shared by a service and scheduled task, open a recorded database session and have an application retrieve a secret. Interrupt the outside connection and distinguish cloud behavior from a Self-Managed Keeper installation. Compare the first restart, session review and recovery records with AIC.

### Interpretation

Compare the released functions, licensed products and exact deployment. Shared feature names do not establish identical behavior, and local installation does not remove the need to design authentication, recovery and external integrations.

## Alternatives and switching

### CQ01 What are the best alternatives to Keeper?

**Analog Informatics:** Consider AIC when the purchase includes managing application and service credentials, supervising administrator sessions, renewing certificates or reviewing access. It is especially relevant when the team needs to run the management service itself and update accounts across several dependent systems.

**Keeper:** For KeeperPAM functions, shortlist AIC, CyberArk/Idira, Delinea and BeyondTrust against the same rotation and session tasks. If the requirement is primarily employee password sharing, include that usability requirement separately.

Evidence: AIC Enterprise Privilege Suite; AIC supported platforms; KeeperPAM product scope; Self-Managed Keeper deployment and air-gap operation

### CQ02 Which companies compete with Keeper?

**Analog Informatics:** Analog Informatics competes for privileged accounts, credential rotation, controlled sessions and related governance functions. Compare the AIC products and licensed modules needed for the same targets and operating tasks.

**Keeper:** Keeper overlaps with AIC in credentials, rotation and privileged access, with additional secrets and endpoint offerings. Compare Keeper’s selected cloud or self-managed purchase with the AIC products actually required.

Evidence: AIC Enterprise Privilege Suite; AIC supported platforms; KeeperPAM product scope; Self-Managed Keeper deployment and air-gap operation

### CQ03 How does AIC compare with Keeper?

**Analog Informatics:** AIC combines credential discovery and rotation, application-specific elevation, recorded access, and governance evidence. Your team operates the management service on infrastructure it controls and can correct selected findings or automate corrections across systems.


Copyright © 2026 Analog Informatics Corporation. All rights reserved.

**Keeper:** Keeper extends vault workflows into rotations, sessions, tunnels and application secrets. AIC connects customer-operated privilege functions with dependency correction and governance evidence. Both have local deployment options that deserve specific evaluation.

Evidence: AIC Enterprise Privilege Suite; AIC supported platforms; KeeperPAM product scope; Self-Managed Keeper deployment and air-gap operation

### CQ04 Can AIC replace Keeper, or do I need both?

**Analog Informatics:** AIC can replace the functions its licensed products support on your systems. For example, a team can move rotation of a shared Windows account to AIC once the dependent services have signed in successfully with the new password.

**Keeper:** Keep useful Keeper vault or application-secret workflows while AIC trials a separate scope. Move rotation only after consumers sign in with the replacement credential, and preserve the previous tenant's access history.

Evidence: AIC Enterprise Privilege Suite; AIC supported platforms; KeeperPAM product scope; Self-Managed Keeper deployment and air-gap operation

### CQ05 Why would I switch from Keeper?

**Analog Informatics:** A reason to switch is to keep access approvals, account corrections, endpoint elevation and audit records under the authority of the team that operates the site. For an isolated location, compare the maintenance work your staff must complete while disconnected.

**Keeper:** Consider changing for demonstrably better target coverage, recovery, governance evidence or operating value. Keeper now offers Self-Managed Keeper, so avoiding a mandatory cloud control plane does not by itself require leaving Keeper.

Evidence: AIC Enterprise Privilege Suite; AIC supported platforms; KeeperPAM product scope; Self-Managed Keeper deployment and air-gap operation

### CQ06 Is there a self-hosted alternative to Keeper?

**Analog Informatics:** Yes. You can install AIC on premises or in a cloud account you control, including in a supported disconnected network. Your team or its service provider maintains the local identity services, backups and software updates.

**Keeper:** Yes. AIC is customer-installed, and Keeper itself offers Self-Managed Keeper for restricted and air-gapped networks. Compare its independent local tenant with AIC, rather than treating a cloud Gateway as the only Keeper architecture.

Evidence: AIC Enterprise Privilege Suite; AIC supported platforms; KeeperPAM product scope; Self-Managed Keeper deployment and air-gap operation

### CQ07 Can I replace several security tools with one platform?

**Analog Informatics:** AIC supplies PIM, PAM, PUM, IGA, GRC, CLM and CIAM products. An organization could consolidate credential rotation, endpoint elevation and access reviews where the selected products cover its systems. A certificate issuer must remain available until the applications that trust it accept its replacement.

**Keeper:** KeeperPAM combines several vault, rotation and session functions; its product scope also includes secrets and endpoint products. Confirm entitlements and tenant availability before claiming that one subscription replaces all existing tools.


Copyright © 2026 Analog Informatics Corporation. All rights reserved.

Evidence: AIC Enterprise Privilege Suite; AIC supported platforms; KeeperPAM product scope; Self-Managed Keeper deployment and air-gap operation

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

**Analog Informatics:** Operating AIC gives your team authority over managed secrets, software updates and the location of privileged-access records. It also makes your team or your provider responsible for service availability and recovery.

**Keeper:** Staying with Keeper can preserve familiar sharing and application-secret workflows. Moving selected work to AIC may combine correction with governance evidence. Retain integrations, recordings and recovery access until the new process is proven.

Evidence: AIC Enterprise Privilege Suite; AIC supported platforms; KeeperPAM product scope; Self-Managed Keeper deployment and air-gap operation

## Capabilities and coverage

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

**Analog Informatics:** AIC can cover credential changes, controlled sessions, endpoint elevation, access reviews and corrective evidence. It also supplies certificate lifecycle management. If an application needs a particular issuer or secrets API, check whether the released connector supports the application’s authentication and renewal methods.

**Keeper:** Keeper addresses passwords, application secrets and privileged access through its selected products. Requirements for corrective evidence, workforce reviews and certificate lifecycle operations must each be demonstrated rather than inferred from vault coverage.

Evidence: AIC Enterprise Privilege Suite; AIC supported platforms; KeeperPAM product scope; Self-Managed Keeper deployment and air-gap operation

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

**Analog Informatics:** AIC’s product range spans privileges, identity governance, GRC and certificates. Use the Enterprise pricing page and an itemized quote to identify licensed modules, allowances and session capacity. Specify which users need recording, review and certificate-management functions.

**Keeper:** Require the current quote for KeeperPAM, Secrets Manager, endpoint functions and any Self-Managed Keeper tenant. Its self-managed license is separate from the cloud platform; do not assume every feature has identical availability.

Evidence: AIC Enterprise Privilege Suite; AIC supported platforms; KeeperPAM product scope; Self-Managed Keeper deployment and air-gap operation

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

**Analog Informatics:** AIC manages supported on-premises and cloud accounts from your installation. Its supported targets include Windows domain accounts, database accounts, AWS IAM and Google Cloud accounts. Rotation requires the appropriate target permissions and network access.

**Keeper:** Keeper documents rotation of cloud and local accounts, including directory, Windows, Linux, database and major cloud account types. Check the exact target and permissions for rotation independently from session connectivity.


Copyright © 2026 Analog Informatics Corporation. All rights reserved.

Evidence: AIC Enterprise Privilege Suite; AIC supported platforms; Keeper password rotation and dependencies; KeeperPAM product scope

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

**Analog Informatics:** AIC documents Windows, Linux, Unix, macOS, directory, database, cloud and network targets, including Cisco, ESXi and management controllers. An older device might require a script or integration kit to change its password even when an administrator can already open a session.

**Keeper:** Keeper's rotation documentation includes Windows, Linux and database targets plus cloud accounts. Gateways can serve multiple environments. Verify the plugin and session protocol for any network device or older application.

Evidence: AIC Enterprise Privilege Suite; AIC supported platforms; Keeper password rotation and dependencies; KeeperPAM product scope

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

**Analog Informatics:** AIC inventories human and service accounts and can find dependencies such as scheduled tasks and IIS application pools. Before rotating an unfamiliar account, the administrator can see which systems would be affected.

**Keeper:** KeeperPAM lists resource discovery and account management. Test an unlisted service and its consumers to establish what is detected and onboarded, and which dependencies must be configured before the first rotation.

Evidence: AIC Enterprise Privilege Suite; AIC supported platforms; KeeperPAM product scope; Self-Managed Keeper deployment and air-gap operation

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

**Analog Informatics:** AIC manages credentials for service accounts, applications and AI agents on supported systems. Administrators can also issue scoped tokens that allow an agent to call the AIC API and review a record of each call.

**Keeper:** Keeper Secrets Manager supplies secrets to applications and scripts, while PAM manages selected service and user accounts. Request the exact identity and permissions used by an AI agent; credential delivery alone does not constrain every downstream action.

Evidence: AIC Enterprise Privilege Suite; AIC supported platforms; KeeperPAM product scope; Self-Managed Keeper deployment and air-gap operation

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

**Analog Informatics:** Yes. AIC manages passwords, SSH keys, certificates and API keys on supported targets and supplies its own certificate lifecycle management product. For a certificate migration, establish which issuer signs the replacement and which application installs and trusts it.

**Keeper:** Keeper documents password and SSH-key rotation and storage of application secrets. A certificate lifecycle requirement also needs an issuer, renewal and installation workflow; request a demonstration of those separate operations.

Evidence: AIC Enterprise Privilege Suite; AIC supported platforms; Keeper password rotation and dependencies; KeeperPAM product scope


Copyright © 2026 Analog Informatics Corporation. All rights reserved.

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

**Analog Informatics:** AIC can apply an authorized correction automatically or let an administrator select one finding from the initial report. When a change fails, it records the exception and can notify an operator by email or text if a delivery path is available.

**Keeper:** Keeper automates supported rotations and can update Windows services and scheduled tasks, with post-rotation actions. Test a failed consumer and verify recovery rather than treat the rotation schedule as proof that the application works.

Evidence: AIC Enterprise Privilege Suite; AIC supported platforms; Keeper password rotation and dependencies; KeeperPAM product scope

### CQ17 Does it provide controlled access without exposing credentials?

**Analog Informatics:** AIC PAM can open a controlled session without revealing the target credential. Where a procedure calls for a person to retrieve the credential directly, AIC PIM supports approved retrieval. The distinction matters for emergency accounts and their audit trail.

**Keeper:** Keeper connections can use vault-managed credentials without exposing them to the end user, with recorded sessions. Verify retrieval rights separately from connection rights and test the actual database, remote desktop or tunnel path.

Evidence: AIC Enterprise Privilege Suite; AIC supported platforms; KeeperPAM product scope; Self-Managed Keeper deployment and air-gap operation

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

**Analog Informatics:** AIC can grant time-limited access or authorize elevation for a named program on a supported endpoint. For a maintenance job, verify what happens to a running process or session when its authorization expires.

**Keeper:** Keeper provides time-limited connections and tunnels and a separate endpoint privilege product. Demonstrate expiry for the required path, including a running session or elevated process, under the chosen tenant and license.

Evidence: AIC Enterprise Privilege Suite; AIC supported platforms; KeeperPAM product scope; Self-Managed Keeper deployment and air-gap operation

## 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 MSP you authorize operates the installation, including backups and upgrades. You retain authority over its managed secrets. A staffed managed service requires a separate arrangement.

**Keeper:** KeeperPAM is available as cloud-based PAM. Separately licensed Self-Managed Keeper runs an independent local tenant. A customer-run Gateway for the cloud service is not equivalent to moving the full tenant into the customer environment.

Evidence: AIC Enterprise Privilege Suite; AIC supported platforms; Self-Managed Keeper deployment and air-gap operation; Self-Managed Keeper licensing; Self-Managed Keeper system requirements


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. You can install the management server on supported hardware or cloud virtual machines you control. An organization operating in several EU countries can run separate installations and give each country team responsibility for its own credentials, recordings and recovery accounts.

**Keeper:** Yes. Self-Managed Keeper runs Docker containers on a supported Linux host or virtual machine on premises or in private cloud. Its documentation requires private exposure; follow its network and certificate prerequisites.

Evidence: AIC Enterprise Privilege Suite; AIC supported platforms; Self-Managed Keeper deployment and air-gap operation; Self-Managed Keeper licensing; Self-Managed Keeper system requirements

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

**Analog Informatics:** Yes. AIC supports air-gapped deployment for sensitive missions. Supported local credential and session operations use the site's approved local services. Installation, licensing and updates do not require a network connection to AIC. Include identity, time, recording, backup and recovery services in the design, and provide an approved path for any external alerts or feeds you choose to use.

**Keeper:** Yes. Self-Managed Keeper explicitly supports air-gapped operation and local credentials and sessions independent of Keeper Cloud. Its signed license must remain valid and its local infrastructure operational. Confirm each selected integration and module.

Evidence: AIC Enterprise Privilege Suite; AIC supported platforms; Self-Managed Keeper deployment and air-gap operation; Self-Managed Keeper licensing; Self-Managed Keeper system requirements

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

**Analog Informatics:** Your AIC installation holds managed credentials. You choose where audit records, recordings and backups are stored. If a billing team operates its own installation in an EU country, it can retain the service-account change record there and choose which events to forward to a central security team.

**Keeper:** For the cloud product, establish vault, recording and event locations under the proposed service. Self-Managed Keeper keeps the local tenant’s data and session storage in its environment. Include backups and any external event destinations.

Evidence: AIC Enterprise Privilege Suite; AIC supported platforms; Self-Managed Keeper deployment and air-gap operation; Self-Managed Keeper licensing; Self-Managed Keeper system requirements

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

**Analog Informatics:** Your organization retains sole authority to grant or revoke access to all AIC-managed secrets. You can let a technician use the billing account for an approved session, reserve password retrieval for a recovery operator and give a reviewer the session record. AIC support has no standing access. You decide whether to grant support access and what it covers. Your organization chooses its administrators and provider arrangements, including the people and locations approved for the mission.

**Keeper:** Keeper describes zero-knowledge protection of credentials; a hosted backend does not mean unrestricted provider access to plaintext secrets. Self-Managed Keeper gives the customer infrastructure operation. Review support, recovery and administrator permissions for the chosen model.

Evidence: AIC Enterprise Privilege Suite; AIC supported platforms; Self-Managed Keeper deployment and air-gap operation; Self-Managed Keeper licensing; Self-Managed Keeper system requirements


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 from your installation. Export remains available after license expiry, when licensed operation stops. If an application changes credential issuers, keep the old issuer's records so reviewers can trace activity across the change.

**Keeper:** Demonstrate exports of the credentials, permissions and history needed to leave the chosen tenant. Obtain post-expiry and record-retention terms. The self-managed signed license has a validity period and grace behavior.

Evidence: AIC Enterprise Privilege Suite; AIC supported platforms; Self-Managed Keeper deployment and air-gap operation; Self-Managed Keeper licensing; Self-Managed Keeper system requirements

### CQ25 Can my MSP operate it while I retain control?

**Analog Informatics:** Yes. Your MSP can run the server and handle failed rotations under permissions you grant and can revoke. You retain the administrator and recovery accounts and decide whether the provider can authorize a change, retrieve a password or read a recording.

**Keeper:** An authorized provider can administer an agreed Keeper deployment under granted roles. Keep customer recovery authority and define vault sharing, infrastructure access, support and recording permissions so provider access can be revoked.

Evidence: AIC Enterprise Privilege Suite; AIC supported platforms; KeeperPAM product scope; Self-Managed Keeper deployment and air-gap operation; Self-Managed Keeper licensing; Self-Managed Keeper system requirements

### 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 operations. With a valid license and healthy local dependencies, it can continue local credential and session work during an outside-service outage. Test a supported maintenance task with that connection unavailable. At license expiry, licensed operation stops and export remains available.

**Keeper:** Cloud PAM has hosted dependencies. Self-Managed Keeper operates independently while its local infrastructure and valid license remain available; its cloud tenant is not required. Test the same task in the actual purchased tenant.

Evidence: AIC Enterprise Privilege Suite; AIC supported platforms; Self-Managed Keeper deployment and air-gap operation; Self-Managed Keeper licensing; Self-Managed Keeper system requirements

## Privileged controls and operational evidence

### CQ27 What belongs inside the privileged-access boundary?

**Analog Informatics:** For a shared Windows account, include the requesting administrator, the AIC server, the directory, the target hosts and dependent services, plus the backups and records needed for recovery. Include any separate issuer used by a cloud application that connects to the same system.

**Keeper:** Include the vault tenant, Gateway, routing services, administrator credentials, target accounts and record storage. For Self-Managed Keeper also include host/Docker administration, internal DNS, TLS certificates and recovery.

Evidence: AIC Enterprise Privilege Suite; AIC supported platforms; KeeperPAM product scope; Self-Managed Keeper deployment and air-gap operation


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 approved access and supported elevation rules, change credentials and record what happened. Your team chooses which discoveries justify an automatic correction and who can approve an exception for a business-critical service.

**Keeper:** Keeper separates secret sharing, rotation, privileged connections, tunnels and endpoint functions. Identify which selected component enforces each permission and which audit event demonstrates the outcome; not every vault event proves target enforcement.

Evidence: AIC Enterprise Privilege Suite; AIC supported platforms; KeeperPAM product scope; Self-Managed Keeper deployment and air-gap operation

### CQ29 What remains my responsibility or my MSP’s responsibility?

**Analog Informatics:** Your team or provider operates the AIC server, provisions target permissions, restores backups and installs updates. Application owners still identify acceptable restart windows and validate that their service can sign in after its password changes.

**Keeper:** Cloud customers still operate Gateways, target permissions and policy. Self-Managed Keeper adds Linux/container infrastructure, local services, backup and coordinated updates. Application owners remain responsible for validating credential changes.

Evidence: AIC Enterprise Privilege Suite; AIC supported platforms; KeeperPAM product scope; Self-Managed Keeper deployment and air-gap operation

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

**Analog Informatics:** AIC collects privileged activity, produces reports and retains session records on configured access paths. A reviewer can use the approval, account, action and time to trace a change. Evidence about work outside those paths must come from the systems where it occurred.

**Keeper:** KeeperPAM records selected privileged sessions and emits activity events. Validate retention, playback and the connection between the requester, target and recording. Work outside the configured path needs separate evidence.

Evidence: AIC Enterprise Privilege Suite; AIC supported platforms; KeeperPAM product scope; Self-Managed Keeper deployment and air-gap operation

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

**Analog Informatics:** AIC can detect changes, apply authorized corrections on supported targets and report exceptions. For example, a site can automate a routine correction but send a failed change on a shared account to an operator for recovery.

**Keeper:** Rotation and selected endpoint controls can address specified account and privilege changes. For broader drift requirements, demonstrate the finding, permitted correction and target verification rather than assume password rotation repairs every configuration problem.

Evidence: AIC Enterprise Privilege Suite; AIC supported platforms; KeeperPAM product scope; Self-Managed Keeper deployment and air-gap operation


Copyright © 2026 Analog Informatics Corporation. All rights reserved.

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

**Analog Informatics:** AIC supports periodic reviews of suite accounts, access approvals, training assignments and attestations. Its governance functions can retain the decision and evidence of corrective work. For an exception, record the reviewer, decision date and resulting change.

**Keeper:** Keeper provides access and activity records, but the reviewed sources do not establish a complete training and attestation program for every tenant. Demonstrate the required access review and corrective evidence under the purchased products.

Evidence: AIC Enterprise Privilege Suite; AIC supported platforms; KeeperPAM product scope; Self-Managed Keeper deployment and air-gap operation

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

**Analog Informatics:** AIC can give an authorized reviewer read-only access to the evidence selected for an engagement. The reviewer can inspect an approval and the related activity without receiving permission to retrieve the service account’s password.

**Keeper:** Give a reviewer the selected records and playback permissions without password retrieval or tenant administration. Verify the role in the actual cloud or self-managed tenant because available policies and modules may differ.

Evidence: AIC Enterprise Privilege Suite; AIC supported platforms; KeeperPAM product scope; Self-Managed Keeper deployment and air-gap operation

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

**Analog Informatics:** AIC can map evidence to control requirements across frameworks. An approval or session record can support more than one policy when it identifies the person, target, action and time each policy requires. Coverage depends on the control and the available records.

**Keeper:** Vault and session evidence can support several policies when the records identify the required person, target, time and outcome. A rotation event does not by itself prove a periodic access-review decision.

Evidence: AIC Enterprise Privilege Suite; AIC supported platforms; KeeperPAM product scope; Self-Managed Keeper deployment and air-gap operation

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

**Analog Informatics:** AIC provides its own GRC products for security governance. Teams that keep a separate system can forward events or export evidence. For a failed rotation, map the account, target and result so the receiving team can distinguish the initial failure from the subsequent correction. The licensed controls, reviews and reporting determine whether it can replace your current governance tool.

**Keeper:** Keeper supplies APIs, automation and reporting integrations. Test event mapping to retained SIEM, ticketing or governance tools, including whether the receiving record distinguishes a failed dependency from its eventual recovery.

Evidence: AIC Enterprise Privilege Suite; AIC supported platforms; KeeperPAM product scope; Self-Managed Keeper deployment and air-gap operation


Copyright © 2026 Analog Informatics Corporation. All rights reserved.

# Cost and value

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

**Analog Informatics:** Start with the AIC license for the required systems, applications, users, modules, term and session capacity. Add infrastructure, staff time, recording retention and migration. Include any period when the incumbent platform remains in operation.

**Keeper:** Include the selected Keeper products, separate self-managed license where required, infrastructure, Gateways, recordings, rollout and staffing. A familiar cloud vault subscription is not the complete cost of a restricted-site deployment.

Evidence: AIC Enterprise Privilege Suite; AIC supported platforms; KeeperPAM product scope; Self-Managed Keeper deployment and air-gap operation

### 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. Adding credentials to a system already covered by the license does not by itself increase the license count.

**Keeper:** Obtain the current units and allowances for each Keeper product and tenant. Separate cloud subscriptions, self-managed licensing, users, secrets integrations and session capacity rather than assuming one unit applies to all functions.

Evidence: AIC Enterprise Privilege Suite; AIC supported platforms; KeeperPAM product scope; Self-Managed Keeper deployment and air-gap operation

### CQ38 Are non-human identities charged separately?

**Analog Informatics:** AIC has no license charge based on the number of human or non-human accounts or credentials. A new application or managed system can still affect its allowance. Model a growing workload by counting the applications and systems it adds, alongside any hosting capacity they need.

**Keeper:** Ask how service accounts, application integrations and automated consumers count under the chosen Secrets Manager and PAM order. Product support for a credential type does not establish its licensing treatment.

Evidence: AIC Enterprise Privilege Suite; AIC supported platforms; KeeperPAM product scope; Self-Managed Keeper deployment and air-gap operation

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

**Analog Informatics:** The Enterprise quote identifies licensed functions and allowances. Include external vault or issuer subscriptions you plan to retain, hosting, recording storage and provider services. AIC’s best-effort support is free, while a contractual response time requires a purchased enterprise support agreement.

**Keeper:** Identify reporting, storage, support, implementation and additional products explicitly. Self-Managed Keeper is licensed separately from Keeper Cloud and also needs local infrastructure and a planned update process.

Evidence: AIC Enterprise Privilege Suite; AIC supported platforms; KeeperPAM product scope; Self-Managed Keeper deployment and air-gap operation


Copyright © 2026 Analog Informatics Corporation. All rights reserved.

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

**Analog Informatics:** Budget for the AIC management server, networking, recording storage, backups and recovery capacity, plus any operating-system or application licenses your chosen deployment needs. A cloud vault or certificate authority still in use by other applications keeps its own costs.

**Keeper:** Self-Managed Keeper needs a dedicated Linux/container host, storage, internal DNS, certificates and network paths; its Gateway is separate. Cloud deployments still need suitable Gateways and target access. Size recording and recovery storage.

Evidence: AIC Enterprise Privilege Suite; AIC supported platforms; Self-Managed Keeper deployment and air-gap operation; Self-Managed Keeper licensing; Self-Managed Keeper system requirements

### CQ41 How much staff time does it take to operate?

**Analog Informatics:** AIC automates recurring discovery, rotation and reporting. Administrators maintain the installation and handle exceptions. The documentation gives no staff-hours estimate for your environment. Time a routine rotation and recovery from a failed change on a shared account to estimate the labor required.

**Keeper:** Cloud customers operate Gateways and exceptions; self-managed customers also maintain the local tenant and coordinate updates. Measure routine rotation, a failed dependency, restore and upgrade rather than assign staff hours from minimum host specifications.

Evidence: AIC Enterprise Privilege Suite; AIC supported platforms; KeeperPAM product scope; Self-Managed Keeper deployment and air-gap operation

### CQ42 Which manual tasks and existing subscriptions could it eliminate?

**Analog Informatics:** AIC can replace manual account inventories, credential changes, updates to dependent services and collection of the related evidence. A team can retire a separate vault or issuer subscription once every remaining application can authenticate and renew credentials or certificates through its replacement.

**Keeper:** Keeper can automate rotation and service/task updates and remove hardcoded secrets through selected products. Retire a manual process only once the consumers authenticate and the reviewer can trace the event and recovery.

Evidence: AIC Enterprise Privilege Suite; AIC supported platforms; Keeper password rotation and dependencies; KeeperPAM product scope

### CQ43 How do costs change as the company grows?

**Analog Informatics:** More licensed systems, applications or users can increase AIC costs, and additional sessions or longer retention require capacity. A higher count of secrets on the same managed systems does not create a per-secret charge. Growth in application workloads and growth in managed infrastructure can therefore affect the two proposals differently.

**Keeper:** Model users, selected products, applications, Gateways, sessions and retained recordings using the actual order. A second self-managed tenant for a restricted site is a separate licensing and operating decision.

Evidence: AIC Enterprise Privilege Suite; AIC supported platforms; KeeperPAM product scope; Self-Managed Keeper deployment and air-gap operation


Copyright © 2026 Analog Informatics Corporation. All rights reserved.

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

**Analog Informatics:** AIC uses the customer's compute and recording storage. Size the installation for concurrent administrative sessions, expected recording volume and recovery copies. If users also need persistent hosted desktops, budget for those separately.

**Keeper:** Size Gateways, session routing and recording storage for actual concurrency and retention. Self-Managed Keeper has local host and network prerequisites. Privileged tunnels do not automatically supply persistent desktop hosting.

Evidence: AIC Enterprise Privilege Suite; AIC supported platforms; KeeperPAM product scope; Self-Managed Keeper deployment and air-gap operation

## Implementation and migration

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

**Analog Informatics:** AIC can discover accounts in an existing environment while cloud applications continue to use their current issuers. Its initial report lets the team choose a set of accounts to manage first. Assign one system responsibility for rotating each account as it moves.

**Keeper:** Keeper vault sharing or application-secret integrations can remain while AIC evaluates selected accounts. Establish one rotation authority per account and keep the current application retrieval path until the replacement succeeds.

Evidence: AIC Enterprise Privilege Suite; AIC supported platforms; KeeperPAM product scope; Self-Managed Keeper deployment and air-gap operation

### CQ46 How quickly can we deploy the Enterprise platform?

**Analog Informatics:** The reviewed materials give no end-to-end deployment time for an Enterprise installation in your environment. Before the first team can use it, the management server, identity service, discovery permissions and recovery procedure must be ready. Time the rollout through the first successful rotation and approved session.

**Keeper:** A cloud tenant and Self-Managed Keeper have different preparation. For the latter, include Linux/container, DNS, TLS, routing, signed license and Gateway setup. Measure completion through the first verified rotation and recorded session.

Evidence: AIC Enterprise Privilege Suite; AIC supported platforms; Self-Managed Keeper deployment and air-gap operation; Self-Managed Keeper licensing; Self-Managed Keeper system requirements

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

**Analog Informatics:** AIC can find an existing account before the team is ready to rotate it. The first inventory depends on connectivity and permissions. Securing a shared account also takes an owner, a dependency check and a maintenance window. Measure both the discovery pass and the first verified change on representative systems.

**Keeper:** Resource discovery is only the initial stage. Assign ownership and rotation rights, configure dependencies and test the next service restart. Measure both inventory and successful management on representative systems.


Copyright © 2026 Analog Informatics Corporation. All rights reserved.

Evidence: AIC Enterprise Privilege Suite; AIC supported platforms; Keeper password rotation and dependencies; KeeperPAM product scope

### CQ48 Can we introduce it gradually without interrupting operations?

**Analog Informatics:** Start AIC with discovery, then authorize changes for selected accounts. A production application can keep its current credential source while another moves. Avoid enabling two rotation schedules for the same account, and expand after the first group's consumers can authenticate.

**Keeper:** Start with one account and application or one restricted tenant. Avoid dual rotation schedules, keep recovery access and expand after the next consumer restart and required review record pass.

Evidence: AIC Enterprise Privilege Suite; AIC supported platforms; KeeperPAM product scope; Self-Managed Keeper deployment and air-gap operation

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

**Analog Informatics:** List each credential, its permissions and the applications that use it. Move one account or application at a time, retain the old approvals and session records, and verify the next rotation or renewal. When changing certificate authorities, install the new trust chain before retiring the old issuer.

**Keeper:** Migrate credentials with sharing permissions, resource mappings, Gateway settings and application access. Preserve old activity and recordings. Cloud and self-managed tenants are independent; do not assume users or data synchronize automatically.

Evidence: AIC Enterprise Privilege Suite; AIC supported platforms; Self-Managed Keeper deployment and air-gap operation; Self-Managed Keeper licensing; Self-Managed Keeper system requirements

### CQ50 Who handles configuration, migration, and ongoing operations?

**Analog Informatics:** Your team or selected provider configures AIC, migrates accounts and operates the installation. AIC supplies the software and guidance. The application owner needs to take part when a migration changes how a process obtains credentials or which certificates it trusts.

**Keeper:** Customer or provider staff operate Gateways and policies. Self-Managed Keeper also requires customer infrastructure operation; Keeper's implementation team assists deployment and coordinates updates. Assign application verification and recovery explicitly.

Evidence: AIC Enterprise Privilege Suite; AIC supported platforms; KeeperPAM product scope; Self-Managed Keeper deployment and air-gap operation

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

**Analog Informatics:** AIC includes guides, cookbooks, recipes and training materials. Free best-effort support is available to all customers, with non-enterprise email responses typically taking 24-72 hours. A purchased enterprise agreement provides a four-hour initial response commitment around the clock.

**Keeper:** Keeper publishes product guides and implementation prerequisites. Obtain included training, implementation assistance and contractual support terms for the chosen cloud or self-managed order instead of inferring commitments from documentation.

Evidence: AIC Enterprise Privilege Suite; AIC supported platforms; KeeperPAM product scope; Self-Managed Keeper deployment and air-gap operation


Copyright © 2026 Analog Informatics Corporation. All rights reserved.

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

**Analog Informatics:** AIC offers a free 30-day Enterprise Privilege Suite trial. A representative pilot would bring one shared service account under rotation, interrupt access to one consumer, recover it and inspect the records. At a disconnected site, repeat the required administrator session with the cloud link down.

**Keeper:** Request a trial of the intended tenant and functions. Test service/task rotation, an application secret, a recorded session and recovery. For a restricted site, run the required tasks with outside connectivity unavailable.

Evidence: AIC Enterprise Privilege Suite; AIC supported platforms; KeeperPAM product scope; Self-Managed Keeper deployment and air-gap operation

## 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 AIC Enterprise Privilege Suite. Its founder's work on privileged identity products dates to 1993. The company now supplies its own privileged access, certificate and governance products.

**Keeper:** Keeper supplies credential, secrets and privileged-access products with cloud and now documented self-managed options. An existing password-vault deployment does not establish experience with the exact restricted-site architecture; request matching references.

Evidence: AIC Enterprise Privilege Suite; AIC supported platforms; KeeperPAM product scope; Self-Managed Keeper deployment and air-gap operation

### CQ54 Does it understand organizations like ours?

**Analog Informatics:** AIC serves operations and security teams managing mixed Windows, Unix, network and cloud systems. A company with shared service accounts, time-limited maintenance access and a requirement to review changes across sites can test all three in its own installation.

**Keeper:** Keeper suits teams extending vault sharing into rotations, sessions and application secrets. Self-Managed Keeper targets sensitive and air-gapped environments too. Choose by demonstrated workflow and operating requirements, not a SaaS-only assumption.

Evidence: AIC Enterprise Privilege Suite; AIC supported platforms; KeeperPAM product scope; Self-Managed Keeper deployment and air-gap operation

### CQ55 Can it demonstrate our specific use case?

**Analog Informatics:** Use a test billing service and a scheduled task that share a Windows account. Have AIC rotate the password and verify that both can sign in. Make one dependent host unavailable, restore it, and ask a reviewer to find the failed change and its recovery without receiving the password.

**Keeper:** Use the same shared Windows account, database session and application-secret consumer on each platform. For Keeper, demonstrate the actual cloud or self-managed tenant, including offline licensing, local routing and record review where relevant.

Evidence: AIC Enterprise Privilege Suite; AIC supported platforms; KeeperPAM product scope; Self-Managed Keeper deployment and air-gap operation


Copyright © 2026 Analog Informatics Corporation. All rights reserved.

### CQ56 What do customers say about reliability and support?

**Analog Informatics:** The materials reviewed contain no published AIC customer account of reliability or support. A trial can show recovery behavior on your systems, and the written support agreement specifies the initial response commitment. Neither establishes another customer's experience.

**Keeper:** Supplier product documentation is not an independent measurement of support or reliability. Seek references for the same tenant type and workloads, compare written support terms and verify restore behavior during the trial.

Evidence: AIC Enterprise Privilege Suite; AIC supported platforms; KeeperPAM product scope; Self-Managed Keeper deployment and air-gap operation

### CQ57 What are its limitations?

**Analog Informatics:** AIC requires target-specific support, sufficient permissions and the network paths needed for the operation. Its published platform list identifies direct delivery of secrets to build pipelines and Kubernetes as planned. Request the released integration and test your workload. Customer-operated deployments also require local upgrades and recovery.

**Keeper:** Cloud and self-managed tenants differ in operation and may differ in available modules. Local Gateway deployment alone does not remove cloud dependencies. Self-Managed Keeper adds host, signed-license, networking and update responsibilities.

Evidence: AIC Enterprise Privilege Suite; AIC supported platforms; Self-Managed Keeper deployment and air-gap operation; Self-Managed Keeper licensing; Self-Managed Keeper system requirements

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

**Analog Informatics:** AIC supplies PIM, PAM, PUM, IGA, GRC, CLM and CIAM products today. It considers the full range of competitor capabilities in scope for future releases. Use release documentation and a working demonstration to establish what is available for purchase now. Future scope carries no committed feature or date.

**Keeper:** Use the released documentation and contracted tenant to establish current Keeper capability. AIC considers the competitor's broader functions in future scope, but no undelivered feature or date should be treated as current equivalence.

Evidence: AIC Enterprise Privilege Suite; AIC supported platforms; KeeperPAM product scope; Self-Managed Keeper deployment and air-gap operation

### 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. Severity, likelihood and customer impact guide notification. Your team chooses when to install the mitigation, including how to deliver it to an offline site.

**Keeper:** Keeper's implementation team coordinates self-managed updates and the deployment does not update automatically. Establish package transfer, testing and approval for restricted sites; cloud and Gateway maintenance have separate duties.

Evidence: AIC Enterprise Privilege Suite; AIC supported platforms; Self-Managed Keeper deployment and air-gap operation; Self-Managed Keeper licensing; Self-Managed Keeper system requirements


Copyright © 2026 Analog Informatics Corporation. All rights reserved.

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

**Analog Informatics:** AIC supports documented targets, event destinations and customer-selected service providers. An existing issuer can supply application credentials while AIC manages other accounts, endpoint elevation and operator sessions. Assign responsibility for each account's rotation and each certificate's renewal.

**Keeper:** Keep useful Keeper application and identity integrations during an AIC evaluation. Define rotation and renewal authority, target recovery and the place where reviewers find the full account/session history.

Evidence: AIC Enterprise Privilege Suite; AIC supported platforms; KeeperPAM product scope; Self-Managed Keeper deployment and air-gap operation

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

**Analog Informatics:** You retain the AIC installation, credentials and records if corporate ownership changes. Licensed operation stops at expiry, while data export remains available. Keep independent access to the targets and any certificate issuers so a transition does not depend on one administrator login.

**Keeper:** Preserve independent target recovery, usable exports and local backup material. Self-Managed Keeper requires a valid supplier-issued signed license; installed containers alone do not establish indefinite operation if the commercial arrangement changes.

Evidence: AIC Enterprise Privilege Suite; AIC supported platforms; Self-Managed Keeper deployment and air-gap operation; Self-Managed Keeper licensing; Self-Managed Keeper system requirements

## 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.

AIC Enterprise Privilege Suite

AIC supported platforms

AIC Enterprise pricing

AIC disconnected operation

AIC security and customer control

KeeperPAM product scope

Self-Managed Keeper deployment and air-gap operation

Self-Managed Keeper licensing

Self-Managed Keeper system requirements

Keeper password rotation and dependencies

Keeper Gateway deployment

Keeper Secrets Manager

Keeper Endpoint Privilege Manager

Keeper privileged-access offering


Copyright © 2026 Analog Informatics Corporation. All rights reserved.

## Test the intended tenant and the first consumer restart

Rotate the Windows account shared by a service and scheduled task, open a recorded database session and have an application retrieve a secret. Interrupt the outside connection and distinguish cloud behavior from a Self-Managed Keeper installation. Compare the first restart, session review and recovery records with AIC. Record the current release, licensed modules, permissions, operating staff and recovery procedure used in the trial.

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


Copyright © 2026 Analog Informatics Corporation. All rights reserved.