COMPETITIVE ANALYSIS

Analog Informatics vs. CyberArk/Idira - Competitive Analysis

Compare AIC with CyberArk/Idira for vault rotation, controlled sessions and endpoint privileges. Review SaaS, self-hosting and authority over sensitive access.

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	CyberArk/Idira
On-premises management	Yes. Install and operate the management software on customer infrastructure.	Yes. PAM Self-Hosted provides a customer-operated vault and supporting components.
Management in your own cloud account	Yes. Install and manage AIC in a cloud account and region you choose.	Self-hosted infrastructure can be customer-operated. Confirm supported cloud architecture and component placement for the selected release.
Hybrid operation	Yes. Customer-managed local and cloud components can serve the chosen systems and applications.	Yes. Select Self-Hosted or SaaS components and their network connections to local and cloud targets.
Vendor-operated SaaS	No mandatory AIC-operated SaaS management service. The customer or its authorized provider operates the installation.	Yes. PAM SaaS is offered separately from PAM Self-Hosted.
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.	Self-Hosted is available. Obtain the supported disconnected topology, license and update procedures; a mobile password cache alone does not establish full air-gapped administration.
Secret and administrative control	The customer authorizes secret use, retrieval and changes. AIC support has no standing access.	Self-Hosted customers control their vault infrastructure and recovery keys. SaaS and additional products have their own operating and access boundaries.
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-hosted design can place selected components locally. Confirm every connected product, backup, support path and record location.

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

CyberArk/Idira: CyberArk/Idira offers PAM Self-Hosted and a SaaS PAM service. Local vault components, hosted services and connected endpoint products have different operators and dependencies. Select the architecture before comparing custody, support access or disconnected operation.

CyberArk/Idira privileged access management; PAM Self-Hosted vault key responsibilities; PAM SaaS deployment checklist; Self-Hosted PAM and endpoint-service dependencies

Copyright © 2026 Analog Informatics Corporation. All rights reserved.

Should you extend an existing vault or change the operating workflow?

A financial-services operations team needs to change a database service account without interrupting payment processing. Administrators must complete approved maintenance, and reviewers must trace who received access and what changed. The team may also have existing CyberArk policies, connectors and recordings that cannot be discarded during a migration.

What CyberArk/Idira offers: CyberArk/Idira combines vaulting and rotation with session isolation, just-in-time access and endpoint controls across its selected products. It offers a Self-Hosted PAM path as well as SaaS. Organizations with established vault integrations can build on those investments instead of replacing them solely to gain local deployment.

Where AIC changes the decision: AIC gives the customer an installable platform for account discovery, dependency updates, controlled access, application elevation and governance evidence. The customer chooses its administrators and location, including an air-gapped installation whose licensing and updates do not require a connection to AIC. Because CyberArk/Idira also offers self-hosting, the decision turns on the required workflows, selected components and operating effort.

Which approach fits: AIC fits a team seeking customer-operated privilege controls and corrective evidence across shared accounts and applications. CyberArk/Idira fits organizations extending an established identity-security program with its vault, endpoint, workload or cloud-access products. A team can retain a useful CyberArk vault while proving a specific AIC workflow before consolidation.

A practical example: Rotate the payment service account, update its dependent Windows services and scheduled tasks, and complete an approved database session. Make one dependency unavailable. Compare recovery, the next service restart and the reviewer’s evidence, then repeat the locally required work without outside connectivity.

Where AIC and CyberArk/Idira 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.

CyberArk/Idira today: CyberArk publishes secrets-discovery capabilities. Establish whether the selected scanner identifies unmanaged accounts, embedded credentials and dependent services, and what becomes managed automatically after discovery. CyberArk/Idira documents automated vaulting and rotation, and selected products apply dynamic access controls. Test the proposed correction on a real dependency; a finding or risk score alone does not prove repair.

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.

CyberArk/Idira today: Its PAM offering brokers and isolates privileged sessions and can inject credentials without handing them to the user. Confirm which native clients, browser connections and emergency retrieval paths are in scope. CyberArk/Idira markets just-in-time entitlements and zero standing privileges alongside traditional vaulting. Demonstrate privilege removal at expiry, including an already running session or process, in the exact purchased deployment.

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.

CyberArk/Idira today: CyberArk/Idira has separate machine-identity and secrets offerings alongside PAM. Verify which product manages the workload credential, issues it to the application and records its use before assuming a PAM license covers every agent.

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.

CyberArk/Idira today: The current portfolio describes identity-governance functions, but a PAM purchase does not establish training or attestation coverage. Demonstrate the required review and corrective record with the exact licensed modules. CyberArk/Idira offers APIs and integration paths across its products. Prove the event and identity mapping to the retained SIEM, ticketing or governance system, including how failed and recovered changes are distinguished.

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.

CyberArk/Idira today: CyberArk/Idira offers PAM Self-Hosted and a SaaS PAM service. Local vault components, hosted services and connected endpoint products have different operators and dependencies. Select the architecture before comparing custody, support access or disconnected operation.

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.

CyberArk/Idira strengths

CyberArk/Idira combines vaulting and rotation with session isolation, just-in-time access and endpoint controls across its selected products. It offers a Self-Hosted PAM path as well as SaaS. Organizations with established vault integrations can build on those investments instead of replacing them solely to gain local deployment.

CyberArk/Idira has separate machine-identity and secrets offerings alongside PAM. Verify which product manages the workload credential, issues it to the application and records its use before assuming a PAM license covers every agent.

CyberArk/Idira offers PAM Self-Hosted and a SaaS PAM service. Local vault components, hosted services and connected endpoint products have different operators and dependencies. Select the architecture before comparing custody, support access or disconnected operation.

Which customers fit each approach

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

AIC gives the customer an installable platform for account discovery, dependency updates, controlled access, application elevation and governance evidence. The customer chooses its administrators and location, including an air-gapped installation whose licensing and updates do not require a connection to AIC. Because CyberArk/Idira also offers self-hosting, the decision turns on the required workflows, selected components and operating effort.

CyberArk/Idira - Organizations extending an established vault and wider identity-security program.

CyberArk/Idira combines vaulting and rotation with session isolation, just-in-time access and endpoint controls across its selected products. It offers a Self-Hosted PAM path as well as SaaS. Organizations with established vault integrations can build on those investments instead of replacing them solely to gain local deployment.

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.

AIC Enterprise Privilege Suite

AIC supported platforms

Copyright © 2026 Analog Informatics Corporation. All rights reserved.

AIC disconnected operation

CyberArk/Idira privileged access management

PAM Self-Hosted vault key responsibilities

PAM SaaS deployment checklist

Self-Hosted PAM and endpoint-service dependencies

Self-Hosted certificate prerequisites

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 CyberArk/Idira comparison

Compare AIC with PAM Self-Hosted and PAM SaaS separately. A self-hosted CyberArk/Idira vault can remain within the customer’s chosen infrastructure; SaaS has supplier-operated components. Adding endpoint or cloud services can introduce separate dependencies even when the vault is local. AIC supports a customer-operated air-gapped installation without a network connection to AIC for installation, licensing or updates. For either self-hosted proposal, identify who administers the vault, owns recovery keys, supplies updates and can grant support access.

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; CyberArk/Idira PAM Self-Hosted, PAM SaaS and separately selected identity, endpoint and machine-identity products. Product names and entitlement boundaries must be confirmed in the 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

CyberArk/Idira combines vaulting and rotation with session isolation, just-in-time access and endpoint controls across its selected products. It offers a Self-Hosted PAM path as well as SaaS. Organizations with established vault integrations can build on those investments instead of replacing them solely to gain local deployment.

Practical difference

Rotate the payment service account, update its dependent Windows services and scheduled tasks, and complete an approved database session. Make one dependency unavailable. Compare recovery, the next service restart and the reviewer’s evidence, then repeat the locally required work without outside connectivity.

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 CyberArk/Idira?

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.

CyberArk/Idira: Shortlist CyberArk/Idira with AIC, Delinea, BeyondTrust and Keeper for the functions being purchased. A vault replacement, endpoint project and workload-secrets project can produce different shortlists.

Evidence: AIC Enterprise Privilege Suite; AIC supported platforms; CyberArk/Idira privileged access management; PAM Self-Hosted vault key responsibilities

CQ02 Which companies compete with CyberArk/Idira?

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.

CyberArk/Idira: CyberArk/Idira overlaps with AIC in privileged accounts, sessions and selected identity controls. Delinea, BeyondTrust and Keeper are also relevant; compare the exact products rather than entire corporate portfolios.

Evidence: AIC Enterprise Privilege Suite; AIC supported platforms; CyberArk/Idira privileged access management; PAM Self-Hosted vault key responsibilities

CQ03 How does AIC compare with CyberArk/Idira?

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.

CyberArk/Idira: CyberArk/Idira emphasizes vaulting, session isolation, just-in-time cloud access and endpoint security across its product range. AIC combines customer-operated privilege functions with dependency correction and governance evidence; demonstrate the required functions on both.

Evidence: AIC Enterprise Privilege Suite; AIC supported platforms; CyberArk/Idira privileged access management; PAM Self-Hosted vault key responsibilities

CQ04 Can AIC replace CyberArk/Idira, 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.

CyberArk/Idira: Keep CyberArk-managed accounts and integrations until the replacement proves discovery, rotation, sessions and recovery. AIC can initially serve a separate application or site. Give only one platform authority to rotate each account.

Evidence: AIC Enterprise Privilege Suite; AIC supported platforms; CyberArk/Idira privileged access management; PAM Self-Hosted vault key responsibilities

CQ05 Why would I switch from CyberArk/Idira?

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.

CyberArk/Idira: A switch is justified by a measured improvement in operational control, recovery, evidence or cost. An existing Self-Hosted customer already has a local-vault option; installing software locally is not by itself a reason to migrate.

Evidence: AIC Enterprise Privilege Suite; AIC supported platforms; CyberArk/Idira privileged access management; PAM Self-Hosted vault key responsibilities

CQ06 Is there a self-hosted alternative to CyberArk/Idira?

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.

CyberArk/Idira: CyberArk/Idira itself offers PAM Self-Hosted. AIC is another customer-installed option. Compare the complete deployment, including session components, identity dependencies, key recovery and any additional hosted products.

Evidence: AIC Enterprise Privilege Suite; AIC supported platforms; CyberArk/Idira privileged access management; PAM Self-Hosted vault key responsibilities

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.

CyberArk/Idira: The CyberArk/Idira portfolio covers several identity-security jobs, but purchased products and integrations determine consolidation. Identify which vault, endpoint, workload and governance functions actually retire an existing tool.

Copyright © 2026 Analog Informatics Corporation. All rights reserved.

Evidence: AIC Enterprise Privilege Suite; AIC supported platforms; CyberArk/Idira privileged access management; PAM Self-Hosted vault key responsibilities

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.

CyberArk/Idira: Retaining CyberArk preserves established integrations and operating practices. Moving a function to AIC can put its corrective evidence into the customer-operated AIC workflow. The migration must preserve safe permissions and historical session records.

Evidence: AIC Enterprise Privilege Suite; AIC supported platforms; CyberArk/Idira privileged access management; PAM Self-Hosted vault key responsibilities

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.

CyberArk/Idira: PAM vaulting and sessions address privileged access. The broader CyberArk/Idira portfolio adds other identity controls. Write the complete requirement list, including application dependencies and governance records, before claiming one selected purchase solves it.

Evidence: AIC Enterprise Privilege Suite; AIC supported platforms; CyberArk/Idira privileged access management; PAM Self-Hosted vault key responsibilities

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.

CyberArk/Idira: Do not infer endpoint, workload or identity-governance entitlements from a PAM quotation. Require an itemized CyberArk/Idira order identifying the products, session components, integrations and deployment model included.

Evidence: AIC Enterprise Privilege Suite; AIC supported platforms; CyberArk/Idira privileged access management; PAM Self-Hosted vault key responsibilities

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.

CyberArk/Idira: CyberArk/Idira describes access across local systems, major clouds and Kubernetes. Exact account-management operations still depend on the selected platform and connector. A cloud session and cloud credential rotation are different tests.

Copyright © 2026 Analog Informatics Corporation. All rights reserved.

Evidence: AIC Enterprise Privilege Suite; AIC supported platforms; CyberArk/Idira privileged access management; PAM Self-Hosted vault key responsibilities

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.

CyberArk/Idira: CyberArk/Idira offers endpoint controls for Windows, macOS and Linux and separate infrastructure access functions. Check the supported version and protocol for legacy targets, along with which component rotates their credentials.

Evidence: AIC Enterprise Privilege Suite; AIC supported platforms; CyberArk/Idira privileged access management; PAM Self-Hosted vault key responsibilities

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.

CyberArk/Idira: CyberArk publishes secrets-discovery capabilities. Establish whether the selected scanner identifies unmanaged accounts, embedded credentials and dependent services, and what becomes managed automatically after discovery.

Evidence: AIC Enterprise Privilege Suite; AIC supported platforms; CyberArk/Idira privileged access management; PAM Self-Hosted vault key responsibilities

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.

CyberArk/Idira: CyberArk/Idira has separate machine-identity and secrets offerings alongside PAM. Verify which product manages the workload credential, issues it to the application and records its use before assuming a PAM license covers every agent.

Evidence: AIC Enterprise Privilege Suite; AIC supported platforms; CyberArk/Idira privileged access management; PAM Self-Hosted vault key responsibilities

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.

CyberArk/Idira: PAM supports managed credentials and SSH-key workflows; separate secrets and machine-identity products extend coverage. Demonstrate certificate issuance and renewal independently from storing a certificate or protecting its private key.

Evidence: AIC Enterprise Privilege Suite; AIC supported platforms; CyberArk/Idira privileged access management; PAM Self-Hosted vault key responsibilities

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.

CyberArk/Idira: CyberArk/Idira documents automated vaulting and rotation, and selected products apply dynamic access controls. Test the proposed correction on a real dependency; a finding or risk score alone does not prove repair.

Evidence: AIC Enterprise Privilege Suite; AIC supported platforms; CyberArk/Idira privileged access management; PAM Self-Hosted vault key responsibilities

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.

CyberArk/Idira: Its PAM offering brokers and isolates privileged sessions and can inject credentials without handing them to the user. Confirm which native clients, browser connections and emergency retrieval paths are in scope.

Evidence: AIC Enterprise Privilege Suite; AIC supported platforms; CyberArk/Idira privileged access management; PAM Self-Hosted vault key responsibilities

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.

CyberArk/Idira: CyberArk/Idira markets just-in-time entitlements and zero standing privileges alongside traditional vaulting. Demonstrate privilege removal at expiry, including an already running session or process, in the exact purchased deployment.

Evidence: AIC Enterprise Privilege Suite; AIC supported platforms; CyberArk/Idira privileged access management; PAM Self-Hosted vault key responsibilities

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.

CyberArk/Idira: Both models are available: PAM Self-Hosted software and PAM SaaS. Other portfolio products have separate architecture and service duties. An implementation partner is a further operating arrangement, not the deployment model itself.

Evidence: AIC Enterprise Privilege Suite; AIC supported platforms; CyberArk/Idira privileged access management; PAM Self-Hosted vault key responsibilities; PAM SaaS deployment checklist; Self-Hosted PAM and endpoint-service dependencies

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.

CyberArk/Idira: PAM Self-Hosted puts vault infrastructure under customer operation. Request the supported hardware, virtual-machine or customer-cloud design and identify which optional services still run outside that environment.

Evidence: AIC Enterprise Privilege Suite; AIC supported platforms; CyberArk/Idira privileged access management; PAM Self-Hosted vault key responsibilities; PAM SaaS deployment checklist; Self-Hosted PAM and endpoint-service dependencies

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.

CyberArk/Idira: Self-Hosted PAM is a distinct option. The reviewed sources do not establish every air-gapped function, licensing step or update procedure. Obtain the supported design; cached mobile access does not prove fresh approvals or rotation work offline.

Evidence: AIC Enterprise Privilege Suite; AIC supported platforms; CyberArk/Idira privileged access management; PAM Self-Hosted vault key responsibilities; PAM SaaS deployment checklist; Self-Hosted PAM and endpoint-service dependencies

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.

CyberArk/Idira: For Self-Hosted PAM, inventory the vault, session recordings, backups and any event destinations on customer infrastructure. SaaS has a different service boundary. Ask where each selected product processes and retains its records.

Evidence: AIC Enterprise Privilege Suite; AIC supported platforms; CyberArk/Idira privileged access management; PAM Self-Hosted vault key responsibilities; PAM SaaS deployment checklist; Self-Hosted PAM and endpoint-service dependencies

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.

CyberArk/Idira: Self-Hosted vault customers have responsibility for protected master keys and recovery material. For SaaS, require the provider-access and support terms. Neither a product label nor server location identifies every authorized operator.

Evidence: AIC Enterprise Privilege Suite; AIC supported platforms; CyberArk/Idira privileged access management; PAM Self-Hosted vault key responsibilities; PAM SaaS deployment checklist; Self-Hosted PAM and endpoint-service dependencies

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.

CyberArk/Idira: Include a tested export and retention procedure for safe memberships, account history and recordings. The reviewed material does not establish a universal post-expiry export right for every CyberArk/Idira product; confirm it contractually.

Evidence: AIC Enterprise Privilege Suite; AIC supported platforms; CyberArk/Idira privileged access management; PAM Self-Hosted vault key responsibilities; PAM SaaS deployment checklist; Self-Hosted PAM and endpoint-service dependencies

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.

CyberArk/Idira: A partner can operate an agreed CyberArk/Idira design. Specify whether it may administer safes, retrieve credentials, recover the vault or view recordings, and retain an independent customer recovery route.

Evidence: AIC Enterprise Privilege Suite; AIC supported platforms; CyberArk/Idira privileged access management; PAM Self-Hosted vault key responsibilities; PAM SaaS deployment checklist; Self-Hosted PAM and endpoint-service dependencies

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.

CyberArk/Idira: A local vault and its healthy internal dependencies differ from a SaaS outage scenario. Selected endpoint integrations can require an operational SaaS service. Test the precise required task rather than assume one portfolio-wide outage behavior.

Evidence: AIC Enterprise Privilege Suite; AIC supported platforms; CyberArk/Idira privileged access management; PAM Self-Hosted vault key responsibilities; PAM SaaS deployment checklist; Self-Hosted PAM and endpoint-service dependencies

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.

CyberArk/Idira: Include vault administrators, master-key holders, session components, target credentials and any connected identity services. An optional endpoint or workload service can add another trust boundary even with a self-hosted vault.

Evidence: AIC Enterprise Privilege Suite; AIC supported platforms; CyberArk/Idira privileged access management; PAM Self-Hosted vault key responsibilities

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.

CyberArk/Idira: Vaulting, rotation, session isolation and selected endpoint or cloud-access products enforce different controls. Map the released component to the action it performs, and separately identify records it merely supplies to reviewers.

Evidence: AIC Enterprise Privilege Suite; AIC supported platforms; CyberArk/Idira privileged access management; PAM Self-Hosted vault key responsibilities

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.

CyberArk/Idira: Self-Hosted customers operate and recover their infrastructure; SaaS shifts selected service duties to the provider. In both cases, the customer still approves target permissions, policies and acceptable application interruptions.

Evidence: AIC Enterprise Privilege Suite; AIC supported platforms; CyberArk/Idira privileged access management; PAM Self-Hosted vault key responsibilities

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.

CyberArk/Idira: CyberArk/Idira provides recorded and monitored privileged sessions. Coverage follows the configured access path; activity performed outside that path needs target or endpoint records. Preserve the link from approval to the relevant recording.

Evidence: AIC Enterprise Privilege Suite; AIC supported platforms; CyberArk/Idira privileged access management; PAM Self-Hosted vault key responsibilities

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.

CyberArk/Idira: CyberArk/Idira describes adaptive access and identity-risk responses. For account drift, demonstrate discovery, the authorized change and verification at the target, rather than treating detection as proof of remediation.

Evidence: AIC Enterprise Privilege Suite; AIC supported platforms; CyberArk/Idira privileged access management; PAM Self-Hosted vault key responsibilities

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.

CyberArk/Idira: The current portfolio describes identity-governance functions, but a PAM purchase does not establish training or attestation coverage. Demonstrate the required review and corrective record with the exact licensed modules.

Evidence: AIC Enterprise Privilege Suite; AIC supported platforms; CyberArk/Idira privileged access management; PAM Self-Hosted vault key responsibilities

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.

CyberArk/Idira: Give a reviewer only the safe, report or recording permissions needed. Verify that reviewing an approval does not also permit retrieving the underlying privileged credential or administering access policies.

Evidence: AIC Enterprise Privilege Suite; AIC supported platforms; CyberArk/Idira privileged access management; PAM Self-Hosted vault key responsibilities

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.

CyberArk/Idira: PAM session and account evidence can support multiple audits if the required people, targets, actions and times are present. That does not make every policy requirement a delivered CyberArk/Idira function.

Evidence: AIC Enterprise Privilege Suite; AIC supported platforms; CyberArk/Idira privileged access management; PAM Self-Hosted vault key responsibilities

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.

CyberArk/Idira: CyberArk/Idira offers APIs and integration paths across its products. Prove the event and identity mapping to the retained SIEM, ticketing or governance system, including how failed and recovered changes are distinguished.

Evidence: AIC Enterprise Privilege Suite; AIC supported platforms; CyberArk/Idira privileged access management; PAM Self-Hosted vault key responsibilities

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.

CyberArk/Idira: Price the selected SaaS or Self-Hosted products, implementation, infrastructure, recording storage, recovery and operation. Include coexistence during migration. The reviewed public material does not establish a complete price for this environment.

Evidence: AIC Enterprise Privilege Suite; AIC supported platforms; CyberArk/Idira privileged access management; PAM Self-Hosted vault key responsibilities

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.

CyberArk/Idira: Obtain the actual CyberArk/Idira licensing metric for each product and edition. A human-access license, managed system and workload identity can affect different line items; avoid comparing an incomplete quote with an entire suite.

Evidence: AIC Enterprise Privilege Suite; AIC supported platforms; CyberArk/Idira privileged access management; PAM Self-Hosted vault key responsibilities

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.

CyberArk/Idira: Machine-identity and secrets products may be separately selected. Request the units and allowances for the expected application and service-account growth instead of assuming human administrator pricing covers every non-human identity.

Evidence: AIC Enterprise Privilege Suite; AIC supported platforms; CyberArk/Idira privileged access management; PAM Self-Hosted vault key responsibilities

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.

CyberArk/Idira: List session infrastructure, optional products, connectors, storage, support and partner services explicitly. Public portfolio coverage is not evidence that every capability is included in the quoted PAM package.

Evidence: AIC Enterprise Privilege Suite; AIC supported platforms; CyberArk/Idira privileged access management; PAM Self-Hosted vault key responsibilities

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.

CyberArk/Idira: Self-Hosted PAM requires vault and supporting infrastructure plus appropriate certificates, backup and recovery. Additional identity or endpoint services can have other prerequisites. Request a component-level bill of materials.

Evidence: AIC Enterprise Privilege Suite; AIC supported platforms; CyberArk/Idira privileged access management; PAM Self-Hosted vault key responsibilities

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.

CyberArk/Idira: Existing CyberArk skills may reduce transition work, while Self-Hosted components still need maintenance and recovery testing. Measure a routine rotation, failed dependency and software update; no reviewed source supplies your staffing requirement.

Evidence: AIC Enterprise Privilege Suite; AIC supported platforms; CyberArk/Idira privileged access management; PAM Self-Hosted vault key responsibilities

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.

CyberArk/Idira: CyberArk/Idira can automate account rotation and controlled sessions. Retire manual work or subscriptions only after the specific replacement succeeds and retained policies, integrations and records remain usable.

Evidence: AIC Enterprise Privilege Suite; AIC supported platforms; CyberArk/Idira privileged access management; PAM Self-Hosted vault key responsibilities

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.

CyberArk/Idira: Model growth separately for administrators, targets, workloads, sessions and retention under the quoted terms. A product added for a new identity category may change the cost more than growth in the existing vault.

Evidence: AIC Enterprise Privilege Suite; AIC supported platforms; CyberArk/Idira privileged access management; PAM Self-Hosted vault key responsibilities

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.

CyberArk/Idira: Size the chosen session architecture for concurrency, recordings, retention and failover. Infrastructure access is not automatically a persistent hosted desktop; include any separate workspace service required by the users.

Evidence: AIC Enterprise Privilege Suite; AIC supported platforms; CyberArk/Idira privileged access management; PAM Self-Hosted vault key responsibilities

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.

CyberArk/Idira: Existing CyberArk safes, platform policies and application integrations can remain during a staged AIC evaluation. Start with a separate target group and retain the current recovery path while verifying behavior.

Evidence: AIC Enterprise Privilege Suite; AIC supported platforms; CyberArk/Idira privileged access management; PAM Self-Hosted vault key responsibilities

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.

CyberArk/Idira: A SaaS tenant and a production Self-Hosted deployment have different preparation work. Time the rollout through approved target onboarding, successful rotation, a recorded session and a tested recovery rather than only server installation.

Evidence: AIC Enterprise Privilege Suite; AIC supported platforms; CyberArk/Idira privileged access management; PAM Self-Hosted vault key responsibilities

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.

CyberArk/Idira: Discovery is an initial inventory step. Safely taking control also requires an owner, permissions, dependency checks and an approved change window. Measure both stages using the selected CyberArk/Idira products.

Copyright © 2026 Analog Informatics Corporation. All rights reserved.

Evidence: AIC Enterprise Privilege Suite; AIC supported platforms; CyberArk/Idira privileged access management; PAM Self-Hosted vault key responsibilities

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.

CyberArk/Idira: Yes, scope a rollout to selected safes, systems or applications. Avoid concurrent rotation by the old and new platforms and preserve the original credential recovery route until consumers authenticate successfully.

Evidence: AIC Enterprise Privilege Suite; AIC supported platforms; CyberArk/Idira privileged access management; PAM Self-Hosted vault key responsibilities

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.

CyberArk/Idira: Migrate safe permissions, platform settings, accounts and application dependencies as well as secret values. Retain old recordings and approvals. Test the next rotation and reconnect any application that uses a credential-provider interface.

Evidence: AIC Enterprise Privilege Suite; AIC supported platforms; CyberArk/Idira privileged access management; PAM Self-Hosted vault key responsibilities

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.

CyberArk/Idira: Assign vault operation, session servers, policies and recovery to named customer or partner roles. SaaS responsibilities must be separated from customer connectors, target accounts and application-owner sign-off.

Evidence: AIC Enterprise Privilege Suite; AIC supported platforms; CyberArk/Idira privileged access management; PAM Self-Hosted vault key responsibilities

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.

CyberArk/Idira: CyberArk/Idira has documented implementation prerequisites and customer support resources. Obtain the training, support hours, response terms and partner work included in the proposal; a public guide does not establish a contracted response time.

Evidence: AIC Enterprise Privilege Suite; AIC supported platforms; CyberArk/Idira privileged access management; PAM Self-Hosted vault key responsibilities

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.

CyberArk/Idira: Ask for a proof of the selected deployment on representative targets. Include dependency failure, master-key recovery, session review and a disconnected requirement where relevant, with explicit pass criteria.

Evidence: AIC Enterprise Privilege Suite; AIC supported platforms; CyberArk/Idira privileged access management; PAM Self-Hosted vault key responsibilities

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.

CyberArk/Idira: CyberArk is an established privileged-security supplier whose current offering is presented as CyberArk/Idira. Existing product history and deployment skills matter; current branding alone does not prove a specific integration remains supported.

Evidence: AIC Enterprise Privilege Suite; AIC supported platforms; CyberArk/Idira privileged access management; PAM Self-Hosted vault key responsibilities

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.

CyberArk/Idira: CyberArk/Idira is relevant to organizations building a broad identity-security program or extending a substantial existing PAM deployment. A sensitive local network still needs a product-specific architecture and operator-access review.

Evidence: AIC Enterprise Privilege Suite; AIC supported platforms; CyberArk/Idira privileged access management; PAM Self-Hosted vault key responsibilities

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.

CyberArk/Idira: Use an existing vaulted service account and its consumers, a privileged session and a recovery operator. Ask CyberArk/Idira to demonstrate the exact selected products, including any service required outside the local vault.

Evidence: AIC Enterprise Privilege Suite; AIC supported platforms; CyberArk/Idira privileged access management; PAM Self-Hosted vault key responsibilities

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.

CyberArk/Idira: The reviewed supplier material is not an independent measurement of reliability or support. Seek references using the same deployment and products, and compare their experience with the written service commitments.

Evidence: AIC Enterprise Privilege Suite; AIC supported platforms; CyberArk/Idira privileged access management; PAM Self-Hosted vault key responsibilities

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.

CyberArk/Idira: Self-Hosted PAM adds operating duties; SaaS and separately selected products add service dependencies. Connector compatibility, product boundaries and migration of existing policies must be checked on the actual workload.

Evidence: AIC Enterprise Privilege Suite; AIC supported platforms; CyberArk/Idira privileged access management; PAM Self-Hosted vault key responsibilities

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.

CyberArk/Idira: CyberArk/Idira publishes current products across PAM and other identity functions. Availability depends on edition and release. Treat proposed integrations or future improvements separately from capabilities demonstrated in the contracted version.

Evidence: AIC Enterprise Privilege Suite; AIC supported platforms; CyberArk/Idira privileged access management; PAM Self-Hosted vault key responsibilities

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.

CyberArk/Idira: For Self-Hosted components, agree the update and mitigation process and who applies it. For SaaS, obtain provider maintenance and incident terms. A component's local location does not eliminate vulnerability response work.

Evidence: AIC Enterprise Privilege Suite; AIC supported platforms; CyberArk/Idira privileged access management; PAM Self-Hosted vault key responsibilities

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.

CyberArk/Idira: Preserve useful CyberArk/Idira integrations with identity, ticketing and application systems while evaluating AIC. Assign one authority for each credential change and establish where the complete access record will be reviewed.

Evidence: AIC Enterprise Privilege Suite; AIC supported platforms; CyberArk/Idira privileged access management; PAM Self-Hosted vault key responsibilities

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.

CyberArk/Idira: Maintain independent target recovery, vault-key custody and usable exports. A corporate or product-direction change should be handled through the contract, support plan and tested migration path rather than assumed behavior.

Evidence: AIC Enterprise Privilege Suite; AIC supported platforms; CyberArk/Idira privileged access management; PAM Self-Hosted vault key responsibilities

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

CyberArk/Idira privileged access management

PAM Self-Hosted vault key responsibilities

PAM SaaS deployment checklist

Self-Hosted PAM and endpoint-service dependencies

Self-Hosted certificate prerequisites

PAM SSH-key rotation and recovery

CyberArk self-hosted secrets manager

CyberArk secrets discovery

Copyright © 2026 Analog Informatics Corporation. All rights reserved.

CyberArk mobile cached access

Test one application across the vault and its consumers

Rotate the payment service account, update its dependent Windows services and scheduled tasks, and complete an approved database session. Make one dependency unavailable. Compare recovery, the next service restart and the reviewer’s evidence, then repeat the locally required work without outside connectivity. 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.