COMPETITIVE ANALYSIS

Analog Informatics vs. CyberArk/Idira — Competitive Analysis

Compare CyberArk/Idira's privileged-access options with AIC's customer-run credential, session and remediation controls, secret custody and air-gapped work.

Analysis: October 17, 2026

Deployment and customer-control revision: November 20, 2026

Analog Informatics Corporation

analoginfo.com

Copyright © 2026 Analog Informatics Corporation. All rights reserved.

Analysis date: October 17, 2026. Deployment and customer-control revision: November 20, 2026.

A strong PAM deployment can still leave compliance evidence fragmented across separate tools. Compare AIC's integrated privileged controls with configuration evidence, training records and built-in GRC.

Deployment, secret control and sensitive missions

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.

How this changes the CyberArk/Idira decision

CyberArk/Idira strengths: Privileged credentials, sessions and SaaS or self-hosted deployment. The deployment comparison below distinguishes the location of protected systems from the location and operator of the management software.

Decision: Management service and operating model

AIC: Customer-installed security software on premises, in a customer cloud account, or in a hybrid environment. No mandatory AIC-operated SaaS management service.

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.

Decision: Customer hardware or cloud account

AIC: The customer chooses and operates the supported installation and its management components.

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.

Decision: Air-gapped and disconnected work

AIC: Installation, licensing and updates need no network connection to AIC. Supported local workflows use their required local services; external integrations retain their own connectivity requirements.

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.

Decision: Secret and record locations

AIC: The customer controls approved storage, logs, backups, exports and recovery copies; configure all copies for the required country or mission boundary.

Copyright © 2026 Analog Informatics Corporation. All rights reserved.

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.

Decision: Administrator and support access

AIC: The customer controls managed-secret permissions and delegated operator access. AIC support has no standing access.

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.

Which customers fit each approach

AIC: A team responsible for shared service accounts can use AIC to update supported dependencies and link an approved repair to its configuration and control evidence. That combination matters when the same team must restore a service and explain the change to a reviewer.

CyberArk/Idira: An enterprise identity team with existing CyberArk vault integrations and session policies may prefer to extend them. CyberArk/Idira offers self-hosted PAM and SaaS, and the team can select endpoint or workload identity products for needs beyond its existing vault.

Administrator identity, location and country requirements

For either platform, establish which legal entities and people may administer the proposed deployment, which secrets and records they may access, and from which countries they can work. A storage region alone does not establish operator identity, citizenship or authorization. In AIC, your organization selects its operators and controls any provider access it grants. Country-specific EU installations can be managed within each selected country; include logs, support arrangements, backups and recovery copies in that decision.

Keep the identity, time, backup and other services required for the chosen local workflow available inside the boundary. AIC does not need an Internet connection to AIC for the installation, license or update process; an integration with an external service still needs its own supported connection.

Buyer questions

What are the best alternatives to CyberArk/Idira?

AIC: AIC is a strong shortlist choice when you need customer-deployed privileged security and continuous compliance across on-premises and cloud assets. Select alternatives by the job: operating controls, managed services, content collaboration or enterprise governance. A single universal winner would hide those differences.

CyberArk/Idira: For the Privileged access portion of the purchase, shortlist Delinea, BeyondTrust, KeeperPAM, One Identity Safeguard. AIC is the customer-deployed security/control option. The best fit depends on whether you need software, operating staff, collaboration or governance; compare that job before ranking vendors.

Copyright © 2026 Analog Informatics Corporation. All rights reserved.

Which companies compete with CyberArk/Idira?

AIC: AIC competes with privileged-access platforms and overlapping security/GRC software, and with the software portion of CMMC enclave offerings. Infrastructure providers and independent assessors can also be partners in an AIC deployment; they are not interchangeable replacements.

CyberArk/Idira: Delinea, BeyondTrust, KeeperPAM, One Identity Safeguard are adjacent offerings in this comparison set. They overlap in different ways with CyberArk/Idira; they are not identical replacements. AIC overlaps where privileged controls, remediation and security evidence are the required outcome.

How does AIC compare with CyberArk/Idira?

AIC: Compare AIC's integrated privileged controls with configuration evidence, training records and built-in GRC. AIC operates supported credential, session, configuration and evidence functions in the installation your organization controls. Compare the CyberArk/Idira functions you need separately from the location of its management service and the people allowed to administer it.

CyberArk/Idira: CyberArk/Idira emphasizes Privileged credentials, sessions and SaaS or self-hosted deployment. Compare this with AIC’s customer-deployed operating controls and the required evidence flow. The specific purchasing difference is: Compare AIC's integrated privileged controls with configuration evidence, training records and built-in GRC.

Can AIC replace CyberArk/Idira, or do I need both?

AIC: Replace overlapping functions after proving the required workload and preserving records. Retain a useful external GRC program, content service, cloud platform or MSP where it still does work you need. AIC can supply operational evidence to a wider program through supported interfaces and agreed mappings.

CyberArk/Idira: CyberArk/Idira offers privileged-access controls and self-hosted options. Retain useful capabilities where they fit, and compare the selected protocols, integrations and security-to-evidence workflow before consolidating.

Why would I switch from CyberArk/Idira?

AIC: Switch when customer control, automated corrective action, privileged access or consolidation solves a demonstrated operating problem. A new logo alone is not a reason. Show the improvement on one real workflow before changing production access.

CyberArk/Idira: A strong PAM deployment can still leave compliance evidence fragmented across separate tools. A change is justified when the pilot resolves that problem and the transition preserves required functions.

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

AIC: Yes. AIC is an installable alternative when customer control of the management software, managed secrets and operating location is required. CyberArk/Idira's own deployment options are described below; do not assume it is cloud-only. AIC also supports an air-gapped installation for a sensitive mission, with installation, licensing and updates handled without a network connection to AIC.

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.

Copyright © 2026 Analog Informatics Corporation. All rights reserved.

Can I replace several security tools with one platform?

AIC: AIC can consolidate privileged credentials, access, configuration remediation and security-compliance evidence with built-in GRC. Package entitlements matter. Broader corporate governance, specialist collaboration and staffed services may remain separate purchases.

CyberArk/Idira: The published scope combines Privileged credentials, sessions and SaaS or self-hosted deployment. Whether that eliminates other tools depends on retained connectors, controls and service duties. Build a function-by-function retirement list rather than assume an entire stack is replaced.

What will I lose - and gain - by switching?

AIC: You gain a customer-operated path from identity discovery through security action to evidence. You may give up vendor-specific connectors, hosted operations or governance features if you retire them. Inventory those dependencies and retain useful functions until the replacement is proven.

CyberArk/Idira: The functions to preserve are Privileged credentials, sessions and SaaS or self-hosted deployment. The potential gain from AIC is customer-operated control and evidence in the same workflow. Pilot account discovery, rotation dependencies, emergency access and session retention before moving vault workloads.

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

AIC: AIC supplies an integrated security platform and CMMC kits. People still own risk decisions, policies, physical practices and customer-specific operation. Choose the product and scope that cover your technical work; do not equate a software package with every organizational duty.

CyberArk/Idira: This is Privileged-access security platform, so evaluate it for that role. The stated product scope does not establish that it covers every organizational duty, infrastructure dependency and application in your environment.

Which features are included, and which require another product?

AIC: Enterprise packages and CMMC levels have different inclusions. The CMMC Level 2 list includes PIM, PAM, PUM, IGA, audit, secure sharing, training/attestation and application launch; Level 1 has a narrower scope. Enterprise audit/training entitlements vary by edition. Use the current product price list for the exact order.

CyberArk/Idira: The published capability summary is Privileged credentials, sessions and SaaS or self-hosted deployment. Exact entitlements, optional modules and third-party dependencies require the selected package’s bill of materials. Preserve the distinction between product features and separately purchased professional services.

Does it manage both on-premises and cloud assets?

AIC: Yes. AIC discovers and manages credentials on connected devices, applications, systems, websites and web services across on-premises and cloud environments. Integration kits support management of most on-premises and cloud systems and infrastructure. Customers retain control of the deployed platform, credentials and evidence.

CyberArk/Idira: The published material reviewed for CyberArk/Idira does not specify the exact on-premises/cloud target inventory and operations for each target. Obtain the connector/protocol matrix and test one local and one cloud workload. Hosting location alone does not answer managed-asset coverage.

Copyright © 2026 Analog Informatics Corporation. All rights reserved.

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

AIC: AIC provides integration kits to manage most on-premises and cloud systems and infrastructure. Documented targets include Windows, Linux/Unix/macOS, AD/LDAP, databases, cloud identities, Cisco, ESXi and management controllers, with browser automation and scripts extending integration to websites, web services and other systems. Match the integration kit and supported operations to the specific device, application, version and protocol.

CyberArk/Idira: The published material reviewed for CyberArk/Idira does not specify an exhaustive Windows/Linux/network-device/legacy support matrix for the required functions. Separate endpoints that can access the service from systems whose credentials or configurations it can actually manage. Request versions, protocols and extension limits.

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

AIC: Yes. AIC discovers human and non-human accounts and credentials across connected devices, applications, systems, websites and web services, on-premises and in cloud environments. Integration kits connect discovery and credential management to the target systems. Review discovered ownership and dependencies before applying changes.

CyberArk/Idira: The published PAM offering includes credential/account functions. Establish which discovery methods find unmanaged accounts and which merely import a known list; run against a test target with an undisclosed service account.

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

AIC: Yes. AIC manages non-human identities and their credentials alongside human identities. For an AI agent, identify its actual account, API key or certificate and its target service. Managing that identity is distinct from claiming a native connector to every AI runtime.

CyberArk/Idira: CyberArk/Idira documents self-hosted secrets management for applications/scripts and cloud secret discovery. Human/non-human coverage is a comparison dimension, not an exclusive AIC feature.

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

AIC: Yes. Current capabilities include passwords, SSH keys, certificates and API keys. Verify lifecycle operations against each target - for example issuance, rotation, revocation and dependent application updates - rather than assuming every credential type uses the same mechanism.

CyberArk/Idira: The published material reviewed for CyberArk/Idira does not specify full discover/rotate/revoke/propagate coverage for passwords, SSH keys, certificates and API keys. Use a four-type credential test plan. Storing a secret is not equivalent to rotating it on the target or updating dependent services.

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

AIC: AIC automates discovery, collection, remediation and reporting. Mitigations can run automatically or be surfaced for an administrator to resolve manually. Initial deployment generates a blast-radius report; the administrator can address one finding or all findings at their own pace. Exceptions generate real-time events, including email and text notifications.

CyberArk/Idira: The published material reviewed for CyberArk/Idira does not specify which corrective actions execute directly on the customer’s target systems. Demonstrate one failed check through authorization, actual correction, verification and evidence; distinguish an assigned ticket from an executed repair.

Copyright © 2026 Analog Informatics Corporation. All rights reserved.

Does it provide controlled access without exposing credentials?

AIC: Yes. PAM supplies controlled sessions without disclosing the target credential to the user. PIM can provide approved credential access when that is the required workflow. Test the selected protocol, recording and emergency-access path.

CyberArk/Idira: The offering includes privileged session/access functions. Demonstrate a session where the user never receives the target secret, then inspect the protocol and audit record; evaluate credential checkout separately.

Can it remove standing privileges and expire approved access automatically?

AIC: Approved, limited-time access and expiry are part of the privileged-access workflow. Use named people, specified targets, purpose and duration instead of shared standing administration. Test revocation at the target and termination of an already-open session for the chosen protocol.

CyberArk/Idira: The published material reviewed for CyberArk/Idira does not specify end-to-end grant expiry, target revocation and already-open session termination for the chosen workload. Test a named, time-bounded approval and observe what actually stops at expiry. Role activation alone does not prove every target session is terminated.

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

AIC: AIC is customer-installed software. For a comparison with CyberArk/Idira, separate the software operator from the underlying infrastructure provider: you can run AIC on premises, in your own cloud account or across a hybrid environment. Your organization sets the permissions for the secrets AIC manages. AIC does not require an AIC-operated SaaS management service.

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.

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

AIC: Yes. Your organization chooses the supported hardware or cloud account, operating location and administrators. CyberArk/Idira's customer-side components and its management service must be evaluated separately; installing a connector locally does not by itself place a supplier's entire service under your control. In AIC, your team controls the installed management software and any provider access it authorizes.

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.

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

AIC: Yes. AIC supports air-gapped deployments for sensitive missions. The software can be installed, licensed and updated without a network connection to AIC. Keep the identity, time, backup and other services required for the chosen local workflow available inside the boundary. AIC does not need an Internet connection to AIC for the installation, license or update process; an integration with an external service still needs its own supported connection. Compare CyberArk/Idira's documented disconnected functions with the exact local operations your mission needs.

Copyright © 2026 Analog Informatics Corporation. All rights reserved.

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.

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

AIC: The organization running AIC chooses the approved locations for its managed secrets, session records, logs and compliance evidence. It also controls backup, export and recovery copies. A German operation can install and manage AIC in Germany, while a French operation does the same in France. Compare those locations with the CyberArk/Idira processing and storage arrangement proposed for your purchase.

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.

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

AIC: Your organization decides who may use, retrieve or change the secrets managed by AIC and who may administer the software. AIC support has no standing access; you control any support access you grant. Identify your own administrators and approved providers, their operating locations, and the access each receives. Apply the same review to CyberArk/Idira, including its support, subcontractor and emergency-access arrangements.

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.

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

AIC: Your team sets AIC retention and backup policies and can export credentials, audit records and evidence in supported usable formats. Data export remains available after the license expires, although licensed operation stops. Preserve a tested exit and recovery plan when moving functions to or from CyberArk/Idira; customer custody is useful only when the required records can actually be recovered.

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.

Can my MSP operate it while I retain control?

AIC: Yes. Your organization can authorize an MSP to operate AIC while retaining control of the installation and its managed secrets. Define the provider's named administrators, permissions, operating locations, support access and offboarding. Compare that delegated service with the specific CyberArk/Idira arrangement; hiring an operator does not require giving that operator unrestricted authority over every secret.

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.

Copyright © 2026 Analog Informatics Corporation. All rights reserved.

What happens if the vendor's service is unavailable?

AIC: A supported local AIC installation does not require a connection to AIC for installation, licensing or updates. Supported credential and session services can remain available during an Internet or AIC-service outage while the license is valid and their required local infrastructure remains available. Keep the identity, time, backup and other services required for the chosen local workflow available inside the boundary. AIC does not need an Internet connection to AIC for the installation, license or update process; an integration with an external service still needs its own supported connection. AIC licensed operation stops at license expiry, while export remains available. Test these conditions against the CyberArk/Idira workflow you intend to replace or retain.

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.

Do I need a full enclave, or will secure email and document sharing be enough?

AIC: Follow the FCI/CUI data flow. Email/files alone do not address an application, engineering workstation or machine that processes the data outside that boundary. AIC offers customer-deployed enclave and broader privileged-security functions; select the boundary around the actual work.

CyberArk/Idira: Select the environment around actual FCI/CUI workflows. Neither a cloud subscription nor a governance tool defines all assets in scope. The comparison must include systems that process the data and systems providing their protection; the final boundary follows the applicable scoping guidance.

Which CMMC requirements does the software perform, assist with, or document?

AIC: AIC's requirement-level mapping distinguishes controls the kit performs, activities it assists and evidence it records. Privileged access, credential management, automated collection and remediation operate within the selected package; management decisions and organizational procedures remain assigned to people. Use the level-specific mapping for each assessment objective.

CyberArk/Idira: The published material reviewed for CyberArk/Idira does not specify a current requirement-by-requirement allocation for the selected complete customer configuration. Obtain the shared-responsibility/control matrix with performed, assisted and customer-owned activities. Do not rank suppliers by percentages that use different denominators.

What remains my responsibility or my MSP's responsibility?

AIC: The customer and chosen MSP handle deployment configuration, FCI/CUI migration, operation, exceptions and organizational practices. Management owns risk decisions. AIC supplies software and its documented capabilities; professional assessment is a separate role.

CyberArk/Idira: The customer retains responsibility for scope, authorized users, organizational procedures and the systems outside the purchased service. Assign integration, remediation and evidence-review duties explicitly to the customer, MSP and supplier.

Does it continuously collect evidence, or will we still gather screenshots before an assessment?

AIC: Automated collection and reporting are current AIC capabilities. Keep control evidence current as the environment operates. Organizational interviews, policy decisions and physical procedures still need their own records; the goal is to stop reconstructing technical evidence before every review.

Copyright © 2026 Analog Informatics Corporation. All rights reserved.

CyberArk/Idira: The offering describes Privileged credentials, sessions and SaaS or self-hosted deployment. Determine which evidence is collected automatically, which requires integrations and which still needs a person. Test freshness, failed collection and historical traceability; a current dashboard is not necessarily a complete audit record.

Can it detect drift and remediate problems between assessments?

AIC: Yes. Continuous discovery and remediation are the operating model, with real-time exception events and automated reporting. Define the checks, permitted corrections and exception owners for the deployed scope.

CyberArk/Idira: The published material reviewed for CyberArk/Idira does not specify which corrective actions execute directly on the customer's target systems. Demonstrate one failed check through authorization, actual correction, verification and evidence; distinguish an assigned ticket from an executed repair. Establish the check cadence and the owner of exceptions between assessments.

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

AIC: AIC has training assignments, attestations and attempt records, privileged approval workflows, risk records and corrective evidence. Match package entitlements and the deployed workflow; do not substitute a training record for evidence that a person understood and followed a procedure.

CyberArk/Idira: The published material reviewed for CyberArk/Idira does not specify all four workflows - training, attestations, access approvals and corrective actions - in the selected package. Request each workflow and its retained records separately. Policy acknowledgement does not establish a full training program, and a task list does not establish access enforcement.

Can auditors review current evidence without disrupting IT?

AIC: AIC provides engagement/evidence workflows and controlled disclosure to reviewers. Prepare scoped access and current reports so IT does not repeat data collection for every request. Auditors still decide what additional evidence they need.

CyberArk/Idira: The published material reviewed for CyberArk/Idira does not specify scoped assessor access to the complete required evidence set. Run a mock evidence request. Identify who prepares records, who can disclose them and whether the reviewer can inspect them without interrupting operations.

Can it support multiple frameworks without duplicating work?

AIC: AIC has framework mappings, assessments, control history and evidence records across multiple standards. Reuse a record where its scope and time period support the relevant control; a framework's presence in a catalog is not equal automation of every requirement.

CyberArk/Idira: The published material reviewed for CyberArk/Idira does not specify multi-framework mappings and reuse of the same scoped evidence across the required standards. Ask for one record mapped across the actual frameworks and inspect any additional assessment or GRC product needed.

Can it replace our security-focused GRC tool or feed our existing GRC system?

AIC: Both approaches are possible. AIC's own GRC can serve a defined security-compliance scope, while supported exports and event interfaces feed a larger enterprise GRC program. Agree identifiers, fields, retention and ownership before claiming a particular integration is turnkey.

Copyright © 2026 Analog Informatics Corporation. All rights reserved.

CyberArk/Idira: CyberArk/Idira offers privileged-access controls and self-hosted options. Retain useful capabilities where they fit, and compare the selected protocols, integrations and security-to-evidence workflow before consolidating. An integration needs an identified API/export, matching control identifiers and an owner; a generic partnership claim is not a working data connection.

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

AIC: Total cost includes the selected AIC license, infrastructure, third-party licenses, implementation, operating labor, backups and independent assessment. Published AIC prices remain on the product pricing pages. Compare equal workloads and responsibilities rather than software price against a staffed service.

CyberArk/Idira: The published material reviewed for CyberArk/Idira does not specify a complete current price and license-meter schedule for this customer configuration. Obtain the edition, quantities, add-ons, implementation, recurring support and renewal terms in one itemized quote. Add infrastructure, operating staff, migration, retention and assessment costs that are outside that quote. Compare the same workloads and service hours.

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

AIC: AIC licenses by systems, applications and users, with product-specific package allowances. Counts of human and non-human identities, accounts or credentials do not determine license counts or pricing. Use the current product price list for the applicable meters and entitlements.

CyberArk/Idira: The published material reviewed for CyberArk/Idira does not specify a complete current price and license-meter schedule for this customer configuration. Obtain the edition, quantities, add-ons, implementation, recurring support and renewal terms in one itemized quote.

Are non-human identities charged separately?

AIC: Human and non-human account counts are not used for AIC license counts or pricing. Passwords, SSH keys, certificates and API keys do not introduce a per-identity charge. Licensed systems, applications and users still determine the selected package and capacity.

CyberArk/Idira: The published material reviewed for CyberArk/Idira does not specify a separate non-human-identity charge or an explicit exemption in the selected license. Ask how service identities, application accounts, secrets, managed targets and API usage are counted. Do not assume a people-seat price includes every machine identity.

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

AIC: Enterprise editions and CMMC packages have different allowances for functions and capacity. Free best-effort support is available to all customers; a guaranteed support SLA requires an enterprise support agreement. Infrastructure, third-party software and provider services are separate. Use the current order and price list for exact inclusions.

CyberArk/Idira: The published material reviewed for CyberArk/Idira does not specify a complete current price and license-meter schedule for this customer configuration. Obtain the edition, quantities, add-ons, implementation, recurring support and renewal terms in one itemized quote. Have the supplier identify optional connectors, reporting, storage, reviewer seats and support explicitly as included or separately charged.

Copyright © 2026 Analog Informatics Corporation. All rights reserved.

What infrastructure and third-party licenses will I need?

AIC: Supply supported compute, storage, backup, networking and the operating-system/application licenses the design uses. Customer-cloud deployments incur that provider's charges. Include resilient administration and independent recovery access, not only the minimum server specification.

CyberArk/Idira: List the server/service prerequisites, identity integration, storage, backup and third-party applications for the selected architecture. A documented product capability does not prove the customer already owns its dependencies.

How much staff time does it take to operate?

AIC: Automation reduces repeated collection, reporting and corrective work, but there is no verified universal staffing figure for an AIC deployment. Measure setup effort and recurring exception/review time in a representative pilot, including the systems automation cannot reach.

CyberArk/Idira: No independently verified staffing estimate for your CyberArk/Idira deployment is established here. Measure setup, connector maintenance, exception handling, evidence review and update work during the pilot. Managed-service labor belongs in the contract, not an assumed zero-hour estimate.

Which manual tasks and existing subscriptions could it eliminate?

AIC: Candidates include manual credential inventories, repeated rotation work, screenshot collection, evidence assembly and overlapping security/GRC subscriptions. Retire a tool only after its required workflows, records and integrations have been reproduced or deliberately retained elsewhere.

CyberArk/Idira: Potential consolidation follows the documented scope: Privileged credentials, sessions and SaaS or self-hosted deployment. Identify the exact existing task or subscription replaced and the records it preserves. Avoid double-counting savings while keeping the same staff work or another required module.

How do costs change as the company grows?

AIC: Growth changes licensed systems, applications and users, infrastructure, evidence retention and operating effort. Human and non-human account counts do not drive AIC licensing. Apply the selected package allowances to the forecast and include infrastructure and operating costs.

CyberArk/Idira: The published material reviewed for CyberArk/Idira does not specify a complete current price and license-meter schedule for this customer configuration. Obtain the edition, quantities, add-ons, implementation, recurring support and renewal terms in one itemized quote. Model growth using additional users/tenants/assets, workload capacity, retained evidence and support scope. Verify renewal and overage terms instead of assuming the initial unit rate remains constant.

For hosted VDI, what compute, storage, performance, and usage limits apply?

AIC: AIC software is not a vendor-hosted VDI seat with a universal CPU/RAM allowance. The customer selects infrastructure capacity. For a marketplace instance or secure-enclave offer, size compute, storage, concurrency, GPU needs and cloud consumption against the actual workload.

CyberArk/Idira: A hosted VDI capacity allowance is not established as part of the offering reviewed. If VDI is added through another product or provider, its compute, storage, concurrency and usage terms belong in a separate line of the comparison.

Copyright © 2026 Analog Informatics Corporation. All rights reserved.

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

AIC: Both. AIC discovers and remediates issues in existing brownfield environments and generates greenfield enclaves. Initial deployment produces a blast-radius report so the administrator can fix one finding or all findings at their own pace. Existing business applications do not all have to move into a new hosted desktop.

CyberArk/Idira: Pilot account discovery, rotation dependencies, emergency access and session retention before moving vault workloads. Distinguish integrating existing systems from moving the workload into a new boundary; they involve different change and migration effort.

How quickly can we deploy a new enclave?

AIC: AIC can generate greenfield enclaves in minutes. That describes enclave generation, not the time to migrate data, integrate every application, train staff or complete an organizational assessment. Scope those subsequent tasks explicitly.

CyberArk/Idira: The published material reviewed for CyberArk/Idira does not specify a reproducible end-to-end enclave deployment time for your architecture. Ask for measured provisioning prerequisites and distinguish instance creation from configuration, data transfer, training and operational handover. For a GRC or assessment-only purchase, enclave provisioning is a separate project.

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

AIC: No universal time is established for an entire environment. Discovery reachability, account access, dependencies, change windows and the number of exceptions affect the work. Run a measured sample and scale the plan from its findings.

CyberArk/Idira: No validated whole-environment discovery/remediation duration for CyberArk/Idira is available here. Reachability, privileges, integrations and change approval determine elapsed time. Require a representative discovery sample and a plan for exceptions rather than adopt a marketing launch-time claim.

Can we introduce it gradually without interrupting operations?

AIC: Begin with the initial blast-radius report and choose which findings to address first. Administrators can remediate one finding or all findings at their own pace, using automatic mitigation or manual action. Use change windows, dependency checks and recovery plans to bring an existing environment under control in stages.

CyberArk/Idira: Pilot account discovery, rotation dependencies, emergency access and session retention before moving vault workloads. Stage the change with acceptance tests, retained records and rollback. If the offering requires a new service boundary, include the interim data path and access dependencies in the pilot.

How do we migrate credentials, policies, and evidence?

AIC: Inventory credentials and dependencies; map policies; export and preserve historical evidence; pilot import/rotation and reviewer access; then retire old access in stages. Verify export formats and recovery before the change. CMMC data migration belongs to the customer or chosen provider.

CyberArk/Idira: Pilot account discovery, rotation dependencies, emergency access and session retention before moving vault workloads. Preserve source evidence and timestamp/owner relationships. Validate the import and credential-change behavior before deleting or terminating any original service.

Copyright © 2026 Analog Informatics Corporation. All rights reserved.

Who handles configuration, migration, and ongoing operations?

AIC: The customer or its MSP/qualified provider configures, migrates and operates the environment. AIC supplies commercial software and product guidance. Allocate monitoring, backup, update and exception duties to named owners.

CyberArk/Idira: The customer retains responsibility for scope, authorized users, organizational procedures and the systems outside the purchased service. Assign integration, remediation and evidence-review duties explicitly to the customer, MSP and supplier. The purchase must identify who executes the migration and who accepts the resulting environment.

What training, deployment guides, and support are included?

AIC: All customers receive free best-effort support without a guaranteed SLA. Non-enterprise email support typically responds within 24-72 hours. Purchased enterprise support agreements provide a four-hour response commitment, 24 hours a day, seven days a week; this is a response commitment, not a resolution deadline. Guides, cookbooks, recipes and training materials are included with the products. AIC recommends the customer's existing MSP or service provider for direct operational support.

CyberArk/Idira: The published material reviewed for CyberArk/Idira does not specify the complete included training, deployment assistance, support hours and response commitments for this package. Obtain the named support schedule and training deliverables. Distinguish a response target from a resolution commitment and product support from managed operations.

Can we test it on our own systems before committing?

AIC: AIC offers a free 30-day trial of every product. Use the trial to test discovery, controlled access, remediation, evidence exports and exception handling on representative systems. Agree authorized targets and success criteria before connecting production assets.

CyberArk/Idira: The published material reviewed for CyberArk/Idira does not specify a trial entitlement on your own systems with the required modules and duration. Request a scoped evaluation with agreed targets, license terms, success criteria and cleanup. A sales demo is not automatically permission to run a production pilot.

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

AIC: Analog Informatics Corporation develops AIC Enterprise Privilege Suite and AIC CMMC Complete. Our cybersecurity experience spans decades. A company founding date is not established in these source materials; discuss the team's relevant deployment experience and request references for your environment.

CyberArk/Idira: CyberArk/Idira is represented here by its published Privileged-access security platform offering. The reviewed evidence does not establish an independently checked duration of support for your exact environment; ask for relevant delivery history rather than infer it from brand age.

Does it understand organizations like ours?

AIC: Evaluate AIC against your actual operating problem: shared administration, non-human credentials, brownfield remediation, enclave deployment or current audit evidence. Bring the relevant architecture and constraints to the demonstration; a sector label alone is not proof of fit.

CyberArk/Idira: The relevant fit question is: A strong PAM deployment can still leave compliance evidence fragmented across separate tools. Ask the supplier for a reference architecture and customer reference matching your system mix, operating team and regulatory scope.

Copyright © 2026 Analog Informatics Corporation. All rights reserved.

Can it demonstrate our specific use case?

AIC: Use one real scenario: discover an identity, approve limited access, perform a correction, verify it, then inspect the resulting evidence and exception notification. Include one on-premises and one cloud target where both matter to the purchase.

CyberArk/Idira: Demonstrate the entire repair-to-evidence workflow, including privileged access and the control record. Require the supplier to perform the comparable workflow on its proposed edition and retain the observed result.

What do customers say about reliability and support?

AIC: No independently verified customer reliability or support measurements are supplied here. Request a customer reference with comparable scale and deployment constraints, and evaluate it alongside the support agreement.

CyberArk/Idira: This review does not contain independently verified CyberArk/Idira customer interviews or support-performance measurements. Supplier case studies can identify references, but are not a substitute for speaking with a comparable customer and reviewing the contracted service terms.

What are its limitations?

AIC: Product/package coverage, supported targets and operational dependencies define the boundary. Broad SaaS connector parity, universal bidirectional GRC integration, a full LMS and every financial-risk function have not been established. Customer control does not eliminate licensing, backup or operating obligations.

CyberArk/Idira: The documented scope is Privileged-access security platform, with edition-specific limits. Unverified target support, export completeness, outage behavior and contractual entitlements remain explicit procurement checks; resolve them in the technical evaluation and contract.

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

AIC: Automated discovery, remediation, reporting and human/non-human credential management are current capabilities. The platform record still marks certain pipeline/Kubernetes secret-delivery and RPA integrations as planned; their individual delivery status is not established by broader non-human identity support.

CyberArk/Idira: The published offering currently describes Privileged credentials, sessions and SaaS or self-hosted deployment. Any feature discussed only as roadmap or without an orderable edition should stay outside the scored current comparison until release documentation and a demonstration establish delivery.

How does it handle vulnerabilities and security updates?

AIC: Vulnerability notification considers severity, likelihood, impact and which customers may be affected. AIC generally responds within 24 hours to a severe vulnerability report and typically has a mitigation within 24 hours of notice. These are typical best-effort practices, not guaranteed mitigation deadlines; the specific issue determines the work required. Customers and their providers incorporate mitigations and updates into their controlled operating process, including offline deployments.

CyberArk/Idira: The published material reviewed for CyberArk/Idira does not specify the exact vulnerability notification, update timing and emergency patch process applicable to this deployment. Obtain the security advisory channel, support policy and maintenance responsibilities. For self-hosted components, test the customer update process; for managed services, specify supplier notification and evidence duties.

Copyright © 2026 Analog Informatics Corporation. All rights reserved.

Will it work with our existing vendors and service providers?

AIC: AIC works alongside Microsoft, existing infrastructure, MSPs and external GRC using supported integrations and exports. Agree the version, fields, permissions and operating responsibilities for each connection.

CyberArk/Idira: CyberArk/Idira offers privileged-access controls and self-hosted options. Retain useful capabilities where they fit, and compare the selected protocols, integrations and security-to-evidence workflow before consolidating. Validate the specific connector, export format or service relationship and its permissions before presenting coexistence as turnkey.

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

AIC: Your organization retains its AIC installation, managed-secret permissions and stored records if a supplier changes ownership or strategy. This is operational control, not an unlimited license: licensed operation stops when the AIC license expires, while data export remains available. Keep backups, export procedures and independent emergency access tested. Evaluate the CyberArk/Idira agreement and service dependencies separately before relying on a similar continuity outcome.

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.

Sources and Next Step

• Provider source 1

• Provider source 2

• Provider source 3

AIC evidence: current owner confirmations; supported-platforms document; current Enterprise/CMMC price lists; software license; registered audit/GRC modules. Public references: Supported Platforms, Enterprise Pricing, CMMC Pricing, Product Downloads. CMMC Level 2 scoping guidance informs the boundary questions.

Explore AIC Enterprise Privilege Suite · Explore AIC CMMC Complete · Request a Demonstration

Updated supplier deployment references

Reviewed November 20, 2026 for the deployment and operating-control answers.

• https://www.paloaltonetworks.com/idira/human/privileged-access-management

• https://knowledgebase.paloaltonetworks.com/KCSArticleDetail?id=kA1hj000000133vCAA&lang=en_US

• https://cyberark.my.site.com/s/article/CyberArk-SaaS-PAM-Pre-Implementation-Checklist

• https://community.cyberark.com/s/article/Better-Together-Configuring-LCD-with-CyberArk-PAM-and-CyberArk-EPM

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

Copyright © 2026 Analog Informatics Corporation. All rights reserved.