COMPETITIVE ANALYSIS

Analog Informatics vs. Akeyless - Competitive Analysis

Compare AIC and Akeyless for application secrets, privileged access and air-gapped work. See who operates each service and controls secret access.

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

Analog Informatics Corporation

Copyright © 2026 Analog Informatics Corporation. All rights reserved.

Deployment options and who operates them

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

Deployment option	AIC	Akeyless
On-premises management	Yes. Install and operate the management software on customer infrastructure.	Customer Gateway available. The documented central management service remains Akeyless-operated.
Management in your own cloud account	Yes. Install and manage AIC in a cloud account and region you choose.	Customer Gateway available in your cloud. This does not move the central SaaS service into your account.
Hybrid operation	Yes. Customer-managed local and cloud components can serve the chosen systems and applications.	Yes. Customer-hosted Gateway with the Akeyless SaaS service and connected local or cloud systems.
Vendor-operated SaaS	No mandatory AIC-operated SaaS management service. The customer or its authorized provider operates the installation.	Yes. Pure SaaS or Hybrid SaaS, with Akeyless operating the central service.
Air-gapped or disconnected operation	Yes. Supported local credential and session functions run with required local services and a valid license. Install, license and update without a network connection to AIC.	Gateway placement in restricted or air-gapped networks and Gateway-terminated SAML are documented. Eligible cached reads can continue; uncached reads fail. The central control plane remains SaaS. Verify each required disconnected operation.
Secret and administrative control	The customer authorizes secret use, retrieval and changes. AIC support has no standing access.	SaaS authorizes requests. Customers can require a key fragment they hold for decryption of protected items.
Country-specific installation and records	Install and operate within a chosen country. Configure operators, logs, backups and recovery copies for the required boundary.	EU tenant endpoints and local Gateways are documented. Verify the countries used for central processing, support and records.

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

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

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

Akeyless: A cloud-managed secrets and privileged-access platform with SaaS and hybrid options. Customers can place a Gateway in restricted or air-gapped networks and terminate configured SAML sign-ins there. The central platform remains a SaaS control plane; local Gateway functions do not establish an independently self-hosted central platform.

Akeyless deployment plans; Akeyless components; Akeyless Gateway deployment; Akeyless Gateway caching; Akeyless key fragments; Akeyless regional endpoints; Akeyless Gateway regional connectivity; Akeyless SAML via Gateway

Copyright © 2026 Analog Informatics Corporation. All rights reserved.

Which teams need the credential, and who runs the service?

A billing application may request a new database credential each time it starts. A Windows service at the same company may use a shared directory password. During maintenance, a technician may also need temporary privileges to run a patch. All three identities can affect the same business service.

What Akeyless offers: Akeyless can issue a temporary database login, renew an application certificate and broker a technician's session. It also discovers Windows services and IIS applications configured with explicit credentials and can restart them after changing the password. Akeyless also documents restricted or air-gapped Gateway placement and Gateway-terminated SAML sign-ins, while its central platform remains SaaS.

Where AIC changes the decision: AIC finds where shared credentials are used, updates supported dependencies and verifies sign-in. It can also grant elevation to the patch program and retain the approval, change record and any exception in the customer's deployment. These functions support both routine automation across sites and recovery when a change fails. AIC also supports customer-operated air-gapped installations for sensitive sites, with installation, licensing and updates that do not require a network connection to AIC.

Which approach fits: AIC suits teams that want to operate the management service, automate changes across dependent systems and review privileged work locally. Akeyless suits teams that want managed credential issuance, access to existing vaults and brokered sessions through one cloud service. Organizations with both needs can evaluate the same application on each platform before choosing one or dividing responsibility.

A practical example: For a billing upgrade, have the application request a temporary database login and the technician request privileged access. Then rotate the Windows account shared by the billing service and a scheduled task. Record which dependencies update, what happens when one host is offline and who can verify recovery.

Where AIC and Akeyless overlap, and who each serves

Current capabilities and future scope

AIC currently supplies PIM, PAM, PUM, IGA, GRC, CLM and CIAM products. Its feature set continues to evolve, and every Akeyless capability is in scope for future AIC releases. An individual connector, issuer or agent control counts toward today's purchase when the released version and licensed configuration support the required action. Future scope does not establish current availability, a particular release or a delivery date.

Where the features overlap

Accounts shared by services and applications

AIC today: AIC finds accounts and their dependencies, changes the password, updates supported services, scheduled tasks and configuration files, and verifies sign-in.

Akeyless today: Akeyless discovers domain and local accounts. Its discovery options identify Windows services and IIS applications that use explicit credentials and restart them with the new password after rotation.

What this means for the customer: Both suit Windows administrators responsible for service uptime. Include a scheduled task, an application pool and an unavailable host in the trial to see which dependencies each product updates and how the administrator recovers.

Copyright © 2026 Analog Informatics Corporation. All rights reserved.

Privileged sessions and endpoint elevation

AIC today: AIC brokers and records supported remote sessions. Its elevation controls can authorize a technician to run one application with administrator rights on a supported endpoint.

Akeyless today: Akeyless Secure Remote Access brokers approved connections to databases, servers, Kubernetes and web applications. The Gateway supplies the credential and can record an SSH transcript or an RDP or web session video.

What this means for the customer: An infrastructure team may need both a recorded remote login and permission to elevate one local program. Demonstrate each action with the technician’s usual account.

Application, service and AI identities

AIC today: AIC manages service and application credentials. Administrators can issue scoped AIC API tokens to software, including AI agents, and review the calls made with those tokens.

Akeyless today: Applications can authenticate to Akeyless with a cloud or Kubernetes identity and request temporary credentials. Its Agentic Runtime Authority can restrict requests to supported external resources and filter the data returned to an agent.

What this means for the customer: Permission to call the management API and permission to query a business database are separate decisions. An application owner can test both using the identity the application actually presents.

Certificates and encryption keys

AIC today: AIC supplies its own certificate lifecycle management product. The Enterprise suite can protect its keys in software, in a hardware security module or with a customer-owned cloud key.

Akeyless today: Akeyless documents certificate discovery, issuance through private and public authorities, provisioning, renewal and revocation. An optional customer-held key fragment must participate in cryptographic operations that use the associated key.

What this means for the customer: A certificate owner needs to see which issuer signs the replacement, which system installs it and whether the application trusts it. The team responsible for key custody also needs to know whose approval and infrastructure the operation requires.

Access reviews and governance across vaults

AIC today: AIC provides identity governance and GRC products. Its suite records access reviews for suite accounts, connects findings to evidence and gives authorized reviewers access to the records.

Akeyless today: Akeyless can govern secrets in supported external vaults without moving the originals. Its Identity & Secrets Intelligence scanners can identify excessive access and export findings for investigation.

What this means for the customer: Both serve security teams investigating who has access. Recertifying an employee’s access and changing a secret in an external vault are distinct jobs with different records and permissions.

Copyright © 2026 Analog Informatics Corporation. All rights reserved.

Administration during a network outage

AIC today: Customers operate AIC on premises, in their cloud account, across both or in an air-gapped installation. Supported local credential and session services use the site's own dependencies. Installation, licensing and updates do not require a network connection to AIC.

Akeyless today: Akeyless documents Gateway placement in restricted or air-gapped networks and configured SAML sign-ins that terminate there. Eligible cached secrets can be retrieved during disconnection; uncached reads fail. The central platform remains a SaaS control plane.

What this means for the customer: A branch may need an application to read a secret, a technician to start a session and a supervisor to approve a change. Test each operation separately with the outside connection unavailable; serving a cached value does not demonstrate full offline administration.

AIC strengths

AIC discovers shared credentials and updates supported dependencies that are easy to miss, including scheduled tasks, IIS application pools and connection strings. Administrators can automate routine corrections and handle failed changes individually.

AIC combines account rotation, recorded access and application-specific elevation with governance reviews and corrective evidence. The customer decides who may approve, use or retrieve each managed secret.

Teams operating many systems can apply authorized changes across selected accounts, review exceptions and schedule work by site. A disconnected location can retain supported local access and credential services.

Teams can operate AIC at isolated sites under their own authorized administrators. Air-gapped installation, licensing and updates do not require a network connection to AIC; supported local workflows use the site's chosen identity, audit and recovery services.

Akeyless strengths

Akeyless can issue temporary database credentials to authenticated workloads and automate certificate enrollment and renewal. Platform engineers can use those services through documented APIs and integrations.

Its Universal Secrets Connector can manage supported external vaults in place. A team with separate AWS, Azure, Google Cloud, Kubernetes or HashiCorp stores can keep those stores and delegate access through the connector.

Akeyless combines time-limited, recorded administrator access with controls for machine and AI identities. On supported targets, teams can restrict individual agent requests and filter the responses.

Akeyless operates the cloud service. A hybrid customer can run its own Gateway and retain a key fragment required for protected cryptographic operations.

A customer Gateway can be placed in restricted or air-gapped networks and handle configured SAML sign-ins locally. These functions coexist with the central SaaS control plane; confirm the specific operations required during disconnection.

Copyright © 2026 Analog Informatics Corporation. All rights reserved.

Which customers fit each approach

AIC - Enterprise IT and security teams responsible for shared accounts, endpoint privileges and access reviews across offices, data centers or isolated sites.

The team can rotate a shared credential and update its dependencies, elevate a specific maintenance program and give a reviewer the records. It operates the management service and retains authority over secrets in each deployment. An air-gapped billing or production site can keep supported local credential work under its own operators and use approved offline installation, licensing and updates.

Akeyless - Platform engineering, application security and infrastructure teams that want one cloud service for workload secrets, certificate issuance and administrator sessions.

A workload can obtain a temporary database credential, an application can renew a certificate, and an engineer can request a recorded session. Connectors let teams work with existing cloud vaults while keeping the original secrets in place.

Both - Organizations whose application teams run cloud workloads while infrastructure staff maintain Windows services and supervise administrators.

Both vendors address rotation, privileged sessions and certificates. Compare each against the same service account, certificate issuer and operator task. If both are used, assign one system to rotate each account and name the issuer each application trusts.

AIC supported targets and credential dependencies

AIC Enterprise Privilege Suite functions and access controls

AIC application and endpoint elevation

Akeyless platform

Secure Remote Access

Directory and service-account discovery

Certificate lifecycle management

Akeyless Universal Secrets Connector

Akeyless controls for AI agent requests

Identity & Secrets Intelligence

Zero-knowledge deployment options

Gateway caching during an outage

Akeyless cloud and customer-deployed components

Cimpress customer account

AIC air-gapped deployment

AIC security and customer control

Akeyless SAML via Gateway

Copyright © 2026 Analog Informatics Corporation. All rights reserved.

Customer-controlled deployment and secret access

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

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

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

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

The Akeyless comparison

When a Windows billing service needs a patch, the team must authorize the technician, change the shared password and recover if a dependent service fails to restart. Akeyless can update supported dependent Windows services. Its customer-hosted Gateway enforces local controls, and an optional customer-held key fragment participates in the cryptographic operations it protects. Akeyless documents Gateway placement in restricted or air-gapped networks. Configured SAML sign-ins can terminate at the Gateway, which validates the assertion and issues the token. The central platform remains a SaaS control plane. A configured Gateway cache can serve cached secret values during disconnection, while an uncached read fails. AIC lets the team run its management software and authorize access to managed secrets inside its chosen boundary, including an air-gapped installation. The team can install, license and update that installation without a network connection to AIC. Compare approval, rotation, recovery and record review separately from cached secret retrieval.

Country-by-country operation in the EU

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

ITAR and EU access requirements

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

GDPR does not generally require a separate installation in each EU country. A separate provider outside the EEA can trigger the international-transfer rules when it remotely accesses personal data held in the EU. Choosing a

Copyright © 2026 Analog Informatics Corporation. All rights reserved.

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. Akeyless Enterprise offerings include Modern PAM, Secrets Management, Certificate Lifecycle Management, Multi-Vault Governance, Encryption & KMS, and controls for machine and AI identities. Government service and cryptographic-module designations apply only to their stated boundaries.

Operating differences

How administrators handle shared accounts

AIC discovers which services, tasks and applications use a credential before the administrator changes it. A team can automate routine corrections across systems, set a separate change window for a widely shared account and review any exceptions.

Who holds authority and evidence

The customer runs AIC and authorizes access to each managed secret. Administrators can separately approve a credential change and grant elevation to a maintenance program. Reviewers can inspect the results using permissions granted for that purpose.

Competitor approach

Akeyless operates a cloud service that issues credentials to authenticated applications, governs supported external vaults and brokers privileged sessions through a Gateway. Customers can use cloud and Kubernetes identities, retain a key fragment for protected operations, and keep originals in connected vaults.

Practical difference

If the database team issues temporary credentials at application startup, compare the supported authentication and issuance methods. If the Windows team changes a shared account, inspect which dependent services and scheduled tasks take the new password. Include the first restart after a failed change.

Copyright © 2026 Analog Informatics Corporation. All rights reserved.

Interpretation

Both platforms address privileged users and non-human identities. The application, account, issuer and network conditions determine whether a specific operation works in the proposed deployment.

Alternatives and switching

CQ01 What are the best alternatives to Akeyless?

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.

Akeyless: For a team choosing a secrets manager, Akeyless names HashiCorp Vault and AWS Secrets Manager among the alternatives. Akeyless itself is a strong candidate when engineers want managed credential issuance, certificate automation and privileged access for people and workloads.

Evidence: Akeyless on buying alternatives; Secure Remote Access; AIC Enterprise Privilege Suite functions and access controls; AIC supported targets and credential dependencies; Certificate lifecycle management

CQ02 Which companies compete with Akeyless?

Analog Informatics: Analog Informatics competes with Akeyless for privileged access, management of human and machine credentials, and certificate lifecycle management. For a shared Windows account, both can find dependent services and update them after a password change.

Akeyless: Akeyless also names HashiCorp, AWS and CyberArk/Idira in its secrets-management comparison. A shortlist for a security team buying both vault access and administrator sessions should cover the relevant offerings from those vendors.

Evidence: Akeyless on buying alternatives; Secure Remote Access; Directory and service-account discovery; Certificate lifecycle management; AIC supported targets and credential dependencies

CQ03 How does AIC compare with Akeyless?

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.

Akeyless: Akeyless operates a cloud service for secrets, certificates, key management and privileged access. A customer can connect existing vaults and use a Gateway to rotate credentials for private targets or broker sessions. Both platforms can serve a company with on-premises systems and cloud workloads.

Evidence: Akeyless platform; Directory and service-account discovery; Secure Remote Access; AIC Enterprise Privilege Suite functions and access controls; Akeyless Universal Secrets Connector; Akeyless cloud and customer-deployed components

CQ04 Can AIC replace Akeyless, 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.

Akeyless: An application may use an Akeyless identity to request a temporary database login or a certificate. Keep its existing issuer available until the application authenticates to the replacement, receives the correct

Copyright © 2026 Analog Informatics Corporation. All rights reserved.

permissions and renews successfully. A team can use both platforms while it moves workloads or assigns them different responsibilities.

Evidence: Secure Remote Access; Certificate lifecycle management; Importing static secrets; AIC supported targets and credential dependencies; Human and workload authentication; Akeyless cloud and customer-deployed components

CQ05 Why would I switch from Akeyless?

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.

Akeyless: Akeyless already updates supported Windows services after a password change, issues temporary credentials and provides recorded access. A team benefits from switching if the alternative better supports a specific requirement, such as local authorization during an extended outage.

Evidence: Directory and service-account discovery; Gateway caching during an outage; Secure Remote Access; Akeyless cloud and customer-deployed components; AIC Enterprise Privilege Suite functions and access controls

CQ06 Is there a self-hosted alternative to Akeyless?

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.

Akeyless: Akeyless offers SaaS and hybrid options with a customer-deployed Gateway, including placement in restricted or air-gapped networks. Configured SAML sign-ins can terminate at that Gateway. The central platform remains a SaaS control plane; this is not an independently self-hosted central platform.

Evidence: Customer-hosted Gateway; Plan limits and pricing units; AIC supported targets and credential dependencies; Zero-knowledge deployment options; Gateway caching during an outage; Akeyless cloud and customer-deployed components; Akeyless SAML via Gateway

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.

Akeyless: Akeyless combines secrets management, certificate automation, encryption and key management, multi-vault governance and privileged access. Its connector can manage secrets in supported external vaults, so consolidation of access does not require a team to move every secret.

Evidence: Akeyless platform; Plan limits and pricing units; Akeyless Universal Secrets Connector; Certificate lifecycle management; AIC Enterprise Privilege Suite functions and access controls

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.

Akeyless: If you leave Akeyless, applications may lose their current way of requesting temporary credentials or renewing certificates. A replacement must support their authentication methods and trusted issuers. Export the audit records and retain access to session recordings before retiring the service.

Copyright © 2026 Analog Informatics Corporation. All rights reserved.

Evidence: Zero-knowledge deployment options; Certificate lifecycle management; Secure Remote Access; Human and workload authentication; Audit events and fields

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.

Akeyless: Akeyless can issue workload credentials, manage external vaults, automate certificates and broker privileged sessions. Your team connects the targets and defines policy. If the job also requires granting a technician administrator rights for one local program, demonstrate that action on the required endpoint.

Evidence: Akeyless platform; Remote access infrastructure requirements; Akeyless Universal Secrets Connector; Certificate lifecycle management; AIC Enterprise Privilege Suite functions and access controls

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.

Akeyless: Akeyless publishes product-specific plan limits. Its Enterprise secrets plan lists internal caching and SAML, OIDC or LDAP authentication. Its Enterprise certificate plan lists automated renewal, provisioning and discovery. The quote identifies the allowances and support tier.

Evidence: Plan limits and pricing units; Support tiers; AIC Enterprise licensing

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.

Akeyless: Akeyless can manage cloud credentials and use a Gateway to reach private directories and databases. Teams can also connect existing cloud vaults. The operations available on each target depend on the connector and the permissions its account holds.

Evidence: Customer-hosted Gateway; Credential rotation by target; AIC supported targets and credential dependencies; Akeyless cloud and customer-deployed components; Akeyless Universal Secrets Connector

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.

Akeyless: Akeyless supports rotation for Windows, Linux and network administrator accounts. Legacy SSH access supports key or password authentication. On an older appliance, test both opening a session and changing its password with the proposed integration.

Copyright © 2026 Analog Informatics Corporation. All rights reserved.

Evidence: Credential rotation by target; SSH access and legacy targets; AIC supported targets and credential dependencies

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.

Akeyless: Akeyless directory discovery can find local and domain users, Windows services and IIS applications that use explicit credentials. Its separate Identity & Secrets Intelligence scanners identify identities, secrets and certificates in connected sources, with the scope set by the scanner and its permissions.

Evidence: Directory and service-account discovery; Identity & Secrets Intelligence; AIC supported targets and credential dependencies

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.

Akeyless: Akeyless supports cloud and Kubernetes workload identities. Its SecretlessAI service can broker access without passing a target credential to the agent. On supported targets, Agentic Runtime Authority can restrict a request or filter the data returned. Those controls require a configured Gateway, account features and appropriate roles.

Evidence: Akeyless product documentation; Human and workload authentication; AIC Enterprise Privilege Suite functions and access controls; Akeyless controls for AI agent requests; Akeyless AI security functions

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.

Akeyless: Akeyless supports static passwords and API tokens, SSH certificates and legacy private keys. Its certificate service can discover, issue, provision, renew and revoke certificates. Automatic rotation of an application’s API key depends on the target integration.

Evidence: Supported secret types; SSH access and legacy targets; Certificate lifecycle management; AIC supported targets and credential dependencies

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.

Akeyless: Akeyless can rotate a discovered account and restart supported Windows services or IIS applications with the new password. Its intelligence scanners identify risks and provide remediation guidance. Whether a particular finding can be corrected automatically depends on the target and the configured action.

Evidence: Directory and service-account discovery; Identity & Secrets Intelligence; AIC supported targets and credential dependencies

Copyright © 2026 Analog Informatics Corporation. All rights reserved.

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.

Akeyless: Akeyless Secure Remote Access approves access according to policy and has the Gateway supply the target credential when it opens the session. A user can work without seeing the password. Supported records include SSH transcripts and video for RDP or web sessions.

Evidence: Secure Remote Access; AIC Enterprise Privilege Suite functions and access controls

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.

Akeyless: Akeyless supports time-limited grants and temporary credentials. An administrator can terminate an active connection. When the session uses an existing account with a rotated password, that account's underlying permissions also matter.

Evidence: Secure Remote Access; Access approval workflow; AIC Enterprise Privilege Suite functions and access controls; AIC application and endpoint elevation

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.

Akeyless: Akeyless sells SaaS and hybrid SaaS. A hybrid customer hosts a Gateway, including in restricted networks, and can configure it to handle SAML sign-ins. The central platform remains cloud-hosted. Separate local infrastructure duties from operation of that central service.

Evidence: Customer-hosted Gateway; Plan limits and pricing units; AIC supported targets and credential dependencies; Gateway caching during an outage; Zero-knowledge deployment options; Akeyless cloud and customer-deployed components; Akeyless SAML via Gateway; AIC air-gapped deployment; AIC security and customer control

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.

Akeyless: You can run an Akeyless Gateway on your infrastructure, including self-managed or cloud-managed compute. The documented architecture uses external Akeyless service endpoints for the platform. List those connections when approving network rules.

Evidence: Customer-hosted Gateway; Gateway connections; AIC supported targets and credential dependencies; AIC air-gapped deployment; AIC security and customer control

Copyright © 2026 Analog Informatics Corporation. All rights reserved.

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.

Akeyless: Akeyless documents Gateway placement in restricted or air-gapped networks and SAML authentication through the Gateway. That local flow validates the assertion and issues a token. During disconnection, a configured cache can serve eligible cached values; an uncached read fails. The central platform remains SaaS. Confirm new approvals, revocation, rotation and review individually; local authentication and caching do not establish full independent platform operation.

Evidence: Zero-knowledge deployment options; Gateway caching during an outage; AIC supported targets and credential dependencies; Akeyless cloud and customer-deployed components; Akeyless SAML via Gateway; AIC air-gapped deployment; AIC security and customer control

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.

Akeyless: Distributed key fragments protect secrets, and a customer fragment can remain in your environment. Audit events are available in the SaaS console and can be forwarded. RDP video can be saved locally, in S3-compatible storage or in Azure Blob.

Evidence: Zero-knowledge deployment options; RDP recording storage; Audit events and fields; AIC air-gapped deployment; AIC security and customer control

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.

Akeyless: Customers assign roles, and a customer-held key fragment can keep Akeyless from decrypting protected secret values. That protection applies to secret contents. For support access to operational metadata, obtain the access procedure and audit trail for the service you buy.

Evidence: Zero-knowledge deployment options; Roles and access rules; Security and patch policy; Akeyless cloud and customer-deployed components; AIC air-gapped deployment; AIC security and customer control

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.

Akeyless: You can forward raw audit events and set retention for recordings in your own storage. The published license calls for backup before termination where feasible and written instructions for customer data. Inventory the required events and recordings before closing the account.

Copyright © 2026 Analog Informatics Corporation. All rights reserved.

Evidence: Audit events and fields; RDP recording storage; License and termination terms

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.

Akeyless: Akeyless supports scoped roles and works with channel partners. Assign the provider only the access it needs, keep your own account administrator and recording-storage ownership, and document who can revoke the provider's access. The operating arrangement belongs in your provider agreement.

Evidence: Roles and access rules; Akeyless partners

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.

Akeyless: A configured Gateway can handle the documented local SAML flow and serve eligible cached secrets when the client cannot reach SaaS authentication. An uncached read fails. The central platform remains SaaS; monitor both Gateway and service connectivity, and test each required approval, rotation and recovery operation.

Evidence: Gateway caching during an outage; Monitoring and health checks; AIC supported targets and credential dependencies; Zero-knowledge deployment options; Akeyless cloud and customer-deployed components; Akeyless SAML via Gateway; AIC air-gapped deployment; AIC security and customer control

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.

Akeyless: For brokered access, include the identity provider, Akeyless control plane, private Gateway, target identity and recording destination. Protect the permissions that can approve access, issue credentials or change where recordings are stored.

Evidence: Secure Remote Access; Customer-hosted Gateway; RDP recording storage; AIC supported targets and credential dependencies

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.

Akeyless: Akeyless evaluates roles and the Gateway supplies credentials to an approved session. Identity & Secrets Intelligence helps operators investigate findings, and the audit log records attempts and outcomes. The person responsible for the target decides which corrective changes to authorize.

Copyright © 2026 Analog Informatics Corporation. All rights reserved.

Evidence: Secure Remote Access; Identity & Secrets Intelligence; Audit events and fields

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.

Akeyless: Akeyless operates the hosted service. Your team or provider configures identity providers and roles, maintains any private Gateways, grants access to targets and manages the recording storage it chooses.

Evidence: Customer-hosted Gateway; Roles and access rules; Remote access infrastructure requirements

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.

Akeyless: Akeyless logs activity as it occurs. The same session ID connects remote-access inventory to audit events, and supported session types can also produce a transcript or video. Reviewers need access to the recording destination to retrieve the underlying file.

Evidence: Secure Remote Access; Session inventory and audit correlation; Audit events and fields; AIC Enterprise Privilege Suite functions and access controls

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.

Akeyless: Akeyless scanners can flag excessive privileges and exposed secrets and identify the affected resources. Credential rotation can correct a supported account. For a particular change in permissions, review the finding, who can approve the correction and what the next scan reports.

Evidence: Identity & Secrets Intelligence; Directory and service-account discovery

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.

Akeyless: Akeyless supports approval requests, logs access activity and exports findings for follow-up. These records can support a review. The documentation reviewed does not establish a recurring entitlement review with a named reviewer and a tracked corrective action. Ask to see that complete review if it is required. The reviewed guides do not identify a training-assignment register. Ask for a sample that links a person’s training and attestation to the access decision.

Evidence: Access approval workflow; Audit events and fields; Identity & Secrets Intelligence; AIC Enterprise Privilege Suite functions and access controls

Copyright © 2026 Analog Informatics Corporation. All rights reserved.

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.

Akeyless: Akeyless can grant scoped permissions to audit events and remote-access records. A reviewer can inspect a completed session by ID. Test that the reviewer can retrieve its recording without acquiring rights to the original target.

Evidence: Roles and access rules; Session inventory and audit correlation; AIC evidence and authorized reviewer access

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.

Akeyless: Akeyless audit events include client, time, operation and result. The same session ID connects inventory with events, so reviewers can reuse a record across policies with matching evidence requirements. Document policy mappings and keep the linked recording for the required period.

Evidence: Audit events and fields; Session inventory and audit correlation; AIC evidence and authorized reviewer access; AIC Enterprise Privilege Suite functions and access controls

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.

Akeyless: Akeyless can forward audit events, send selected events to ServiceNow and export risk findings as CSV or JSON. These outputs can feed an existing governance system. A replacement for that system would also need to cover the organization's required reviews, control mappings and corrective work.

Evidence: Audit events and fields; ServiceNow event forwarding; Identity & Secrets Intelligence; AIC Enterprise Privilege Suite functions and access controls

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. If some applications temporarily keep using Akeyless, include that period of overlapping subscriptions.

Akeyless: Add the quoted product subscriptions to the cost of any Gateways, recording storage, SIEM ingestion, integration work and ongoing staff time. The total depends on which services you buy and the volume of clients, connectors and certificates.

Evidence: Plan limits and pricing units; Enterprise quotes; Remote access infrastructure requirements; AIC Enterprise licensing

Copyright © 2026 Analog Informatics Corporation. All rights reserved.

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.

Akeyless: Akeyless counts distinct clients for Modern PAM, including users, applications and servers that initiate sessions. It counts valid certificates for certificate management and connectors for multi-vault governance. Request separate calculations for each product you plan to buy.

Evidence: Plan limits and pricing units; AIC Enterprise licensing

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.

Akeyless: Akeyless counts applications and servers as clients when they meet its product's client definition. Multiple instances of the same application count as one client under the published definition. Ask the vendor to apply that definition to the workload inventory in your quote.

Evidence: Plan limits and pricing units; AIC Enterprise licensing

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.

Akeyless: Akeyless publishes separate units for external-vault connectors and hardware security module integrations. Its Enterprise secrets plan includes log forwarding and internal caching. Include the recording store and any paid support tier, and request written terms for auditor access.

Evidence: Plan limits and pricing units; Support tiers; Support channels and service commitments; AIC Enterprise licensing

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.

Akeyless: Hybrid deployments need a supported Gateway runtime, network access to the required services and targets, and storage for the recordings you retain. Size existing Docker or Kubernetes capacity and budget any identity-provider, log-storage or hosting charges under your own agreements.

Evidence: Customer-hosted Gateway; Remote access infrastructure requirements; RDP recording storage; AIC supported targets and credential dependencies

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.

Copyright © 2026 Analog Informatics Corporation. All rights reserved.

Akeyless: Akeyless operates its SaaS, while hybrid customers deploy and upgrade Gateways and monitor target connectivity and cache health. The published operating guides do not quantify staff hours for a deployment like yours. Time a Gateway upgrade, a failed rotation and a recording retrieval under your team's procedures.

Evidence: Customer-hosted Gateway; Gateway installation and upgrades; Monitoring and health checks; AIC supported targets and credential dependencies

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.

Akeyless: Automated rotations, certificate renewals and short-lived access can replace manual password changes, expiry tracking and credential handoffs. A current vault or CA subscription can end only after its last dependent system has moved or no longer needs it.

Evidence: Credential rotation by target; Certificate lifecycle management; Secure Remote Access; AIC Enterprise Privilege Suite functions and access controls; AIC supported targets and credential dependencies; Akeyless Universal Secrets Connector

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.

Akeyless: Akeyless subscription costs can grow with the number of distinct clients, connected vaults or active certificates. A new site may also need Gateway capacity and recording storage. Account for the annual peak in valid certificates and the published client overage terms.

Evidence: Plan limits and pricing units; Remote access infrastructure requirements; AIC Enterprise licensing

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.

Akeyless: Akeyless brokers administrative sessions through a Gateway to existing targets. The service description gives no concurrency or performance guarantee for your own runtime, network and storage. Test the peak number of simultaneous RDP or browser sessions and price separate hosted desktops if required.

Evidence: Remote access infrastructure requirements; RDP recording storage; Secure Remote Access; AIC supported targets and credential dependencies

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.

Copyright © 2026 Analog Informatics Corporation. All rights reserved.

Akeyless: Akeyless can import supported secrets or use a Universal Secrets Connector to govern secrets in an existing vault. A team can keep its source vault active and connect a few applications before deciding whether to migrate the original records.

Evidence: Importing static secrets; Plan limits and pricing units; AIC supported targets and credential dependencies; Akeyless Universal Secrets Connector

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.

Akeyless: A hybrid rollout includes Gateway deployment, identity configuration, target access and session testing. The guides prescribe setup steps without a schedule for your rollout. Time one application and one privileged session end to end, including firewall and identity-provider approvals.

Evidence: Gateway installation and upgrades; Remote access infrastructure requirements; AIC supported targets and credential dependencies

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.

Akeyless: Discovery time depends on the scope of directory searches, accessible hosts and scanner permissions. Separate time to inventory from time to rotate accounts, restart dependent services and resolve failures. A site-specific duration needs a measured pilot.

Evidence: Directory and service-account discovery; Identity & Secrets Intelligence; AIC supported targets and credential dependencies

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.

Akeyless: Akeyless can restrict directory discovery to selected groups or search bases and send imported credentials to a dedicated folder. Its static-secret importer can overwrite a matching name. Check for collisions and schedule service restarts before adding more accounts.

Evidence: Directory and service-account discovery; Importing static secrets

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.

Akeyless: The Gateway imports static secrets from sources including HashiCorp Vault, AWS, Azure and Kubernetes and produces a migration log. Map access rules separately, test the consuming application and preserve the old system’s approvals and recordings for historical review.

Copyright © 2026 Analog Informatics Corporation. All rights reserved.

Evidence: Importing static secrets; Roles and access rules; Audit events and fields; Certificate lifecycle management; AIC supported targets and credential dependencies

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.

Akeyless: Akeyless runs the hosted service. Your administrators or provider choose the Gateway runtime, configure its identity, map roles and import secrets. If the vendor will assist with migration or ongoing operation, include the assigned work in the order.

Evidence: Gateway installation and upgrades; Importing static secrets; Akeyless partners; Customer-hosted Gateway

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.

Akeyless: Akeyless publishes deployment guides and tutorials. Its support agreement specifies contact channels, service hours and initial response targets by tier. Request written terms for any instructor-led training your administrators need.

Evidence: Gateway installation and upgrades; Akeyless tutorials; Support channels and service commitments

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.

Akeyless: Akeyless’s free secrets-management plan allows five clients and 500 static secrets. It also lists limited dynamic and rotated secrets, which lets an engineering team test issuance and rotation with its own targets. An outage test that depends on internal caching requires access to the Enterprise feature.

Evidence: Plan limits and pricing units; Support tiers

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.

Akeyless: Akeyless develops a cloud-based identity security platform. Its April 2021 announcement identifies enterprise customers and describes its work in workload security during 2020. The Cimpress case study describes a production secrets deployment.

Evidence: Company history and early customers; Cimpress customer account

Copyright © 2026 Analog Informatics Corporation. All rights reserved.

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.

Akeyless: Cimpress describes using Akeyless across business teams for temporary database credentials and on-premises rotation. For federal buyers, Akeyless for Government runs in a dedicated AWS GovCloud environment within the 2F Game Warden FedRAMP Class D (High) boundary. NIST certificate 5227 covers the Akeyless cryptographic module at FIPS 140-3 Level 1.

Evidence: Cimpress customer account; Government edition boundaries; 2F Game Warden certified services; Cryptographic module 5227; AIC supported targets and credential dependencies; AIC Enterprise Privilege Suite functions and access controls

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.

Akeyless: Have Akeyless issue a short-lived database credential to the billing application and broker an administrator’s session. Then rotate a configured Windows service account and inspect the audit record. If disconnection matters, attempt separate reads for a cached and an uncached secret with the cloud connection unavailable.

Evidence: Secure Remote Access; Directory and service-account discovery; Gateway caching during an outage; Audit events and fields; AIC supported targets and credential dependencies; Akeyless cloud and customer-deployed components

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.

Akeyless: In a vendor-published case study, Cimpress describes straightforward onboarding and favorable support from Akeyless. Akeyless publishes service-status history and support terms. The case study does not measure actual response times or availability for another deployment.

Evidence: Cimpress customer account; Akeyless service status; Support channels and service commitments

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. A team evaluating this requirement should request the released integration and test its own workload. Customer-operated deployments also require local upgrades and recovery.

Akeyless: An uncached secret read fails when an Akeyless Gateway loses its cloud connection. Its static-secret importer may replace values when names collide. Multi-vault access also depends on the permissions of the identity attached to each connector.

Evidence: Gateway caching during an outage; Importing static secrets; Akeyless Universal Secrets Connector; AIC supported targets and credential dependencies

Copyright © 2026 Analog Informatics Corporation. All rights reserved.

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 Akeyless capabilities in scope for future releases. For a requirement such as injecting a secret into a Kubernetes workload, use the current release documentation and a working demonstration to establish availability. Future scope carries no committed feature or date.

Akeyless: Akeyless documents privileged sessions, dynamic credentials, certificate automation, multi-vault connectors and controls for supported AI-agent requests. Identity & Secrets Intelligence and Agentic Runtime Authority have specific account and deployment requirements. Check the licensed features and prerequisites for the deployment you plan to buy.

Evidence: Secure Remote Access; Certificate lifecycle management; Identity & Secrets Intelligence; Akeyless product documentation; AIC Enterprise Privilege Suite functions and access controls; AIC supported targets and credential dependencies; Akeyless Universal Secrets Connector; Akeyless controls for AI agent requests

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.

Akeyless: Akeyless publishes a vulnerability-reporting channel and a patch-management policy. For customer-run Gateways it recommends using specific release versions and validating upgrades in a test environment. Arrange an owner for those upgrades and any required outage window.

Evidence: Security reporting and trust center; Security and patch policy; Gateway installation and upgrades

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.

Akeyless: Akeyless can authenticate cloud and Kubernetes identities, connect to external vaults and forward selected events to ServiceNow. It also works with service-provider partners. Verify which operations the connector and its assigned identity can perform on each target.

Evidence: ServiceNow event forwarding; Plan limits and pricing units; Human and workload authentication; Akeyless partners; Akeyless Universal Secrets Connector; AIC Enterprise Privilege Suite functions and access controls

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.

Akeyless: The published license permits assignment in an acquisition and provides for license rights to end at termination or expiry. It calls for advance backup where feasible. Preserve records in your own storage and rehearse switching workload authentication and certificate issuance under the agreement that applies to you.

Evidence: License and termination terms; Audit events and fields; RDP recording storage

Copyright © 2026 Analog Informatics Corporation. All rights reserved.

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.

Akeyless on buying alternatives

Secure Remote Access

Akeyless platform

Directory and service-account discovery

Certificate lifecycle management

Importing static secrets

Gateway caching during an outage

Customer-hosted Gateway

Plan limits and pricing units

Zero-knowledge deployment options

Remote access infrastructure requirements

Support tiers

Credential rotation by target

SSH access and legacy targets

Identity & Secrets Intelligence

Akeyless product documentation

Human and workload authentication

Supported secret types

Access approval workflow

Gateway connections

RDP recording storage

Audit events and fields

Roles and access rules

Security and patch policy

License and termination terms

Akeyless partners

Monitoring and health checks

Session inventory and audit correlation

Copyright © 2026 Analog Informatics Corporation. All rights reserved.

ServiceNow event forwarding

Enterprise quotes

Support channels and service commitments

Gateway installation and upgrades

Akeyless tutorials

Company history and early customers

Cimpress customer account

Government edition boundaries

2F Game Warden certified services

Akeyless service status

Security reporting and trust center

Cryptographic module 5227

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 Enterprise Privilege Suite functions and access controls

AIC supported targets and credential dependencies

AIC application and endpoint elevation

AIC evidence and authorized reviewer access

AIC Enterprise licensing

Akeyless cloud and customer-deployed components

Akeyless Universal Secrets Connector

Akeyless controls for AI agent requests

Akeyless AI security functions

AIC air-gapped deployment

AIC security and customer control

Akeyless SAML via Gateway

Copyright © 2026 Analog Informatics Corporation. All rights reserved.

Test the identities behind one business application

Use a test application, its certificate, a shared service account and a technician’s account. Have the application obtain a credential and renew its certificate, then have the technician complete an approved maintenance task. Review the grants, failed operations and recovery records with the people who would own them in production.

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

Copyright © 2026 Analog Informatics Corporation. All rights reserved.