COMPETITIVE ANALYSIS

Analog Informatics vs. BeyondTrust - Competitive Analysis

Compare AIC and BeyondTrust for credential rotation, vendor sessions and endpoint elevation. See SaaS and appliance options, operator duties and local control.

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

Analog Informatics Corporation

Copyright © 2026 Analog Informatics Corporation. All rights reserved.

Deployment options and who operates them

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

Deployment option	AIC	BeyondTrust
On-premises management	Yes. Install and operate the management software on customer infrastructure.	Yes. Password Safe is available as physical or virtual customer-operated appliances.
Management in your own cloud account	Yes. Install and manage AIC in a cloud account and region you choose.	Yes. Password Safe appliances can be deployed through AWS and Azure marketplaces or in private-cloud infrastructure.
Hybrid operation	Yes. Customer-managed local and cloud components can serve the chosen systems and applications.	Yes. Local and cloud targets can be managed in the selected architecture; identify each product and connector.
Vendor-operated SaaS	No mandatory AIC-operated SaaS management service. The customer or its authorized provider operates the installation.	Yes. Password Safe Cloud is provider-hosted in Azure with managed platform updates.
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.	U-Series BT Updater Enterprise supports air-gapped mode and imported offline update packages. Confirm licensing and each required product workflow separately; mobile credential caching is narrower.
Secret and administrative control	The customer authorizes secret use, retrieval and changes. AIC support has no standing access.	The customer administers a local appliance and its permissions. The SaaS backend is operated by BeyondTrust; document support access and record custody for each product.
Country-specific installation and records	Install and operate within a chosen country. Configure operators, logs, backups and recovery copies for the required boundary.	Customer-operated appliances can be placed in chosen infrastructure. Confirm recordings, backups, support paths and separately hosted modules before asserting a country boundary.

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

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

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

BeyondTrust: BeyondTrust Password Safe offers hosted SaaS and customer-operated physical, virtual, private-cloud and IaaS appliances. Remote-access and endpoint products must be scoped separately. Hosted platform updates and customer appliance maintenance have different operators. U-Series BT Updater Enterprise supports imported offline update packages; this procedure does not by itself establish offline licensing or every product workflow.

Password Safe deployment models; BeyondTrust U-Series offline update packages

Copyright © 2026 Analog Informatics Corporation. All rights reserved.

Who controls the supplier’s session and the privilege behind it?

A hospital needs to admit an equipment supplier to a specific system, monitor the maintenance, rotate the shared account afterward and prove which access was used. Its endpoint team also needs to let a technician run an approved tool without permanent administrator rights.

What BeyondTrust offers: BeyondTrust has distinct products for privileged credential management, vendor and employee remote access, and endpoint elevation. Password Safe is offered as a hosted service or customer-operated physical, virtual and private-cloud appliances, with marketplace deployment in AWS and Azure. Its broader access products are useful when third-party maintenance and endpoint policy are central requirements.

Where AIC changes the decision: AIC connects discovery and supported dependency updates to controlled sessions, application elevation and governance evidence under customer operation. It also supports air-gapped installation, licensing and updates without a connection to AIC. BeyondTrust already offers local appliances; compare the selected module set, administration and end-to-end maintenance evidence rather than treating local deployment as unique to AIC.

Which approach fits: AIC fits teams seeking customer-operated credential correction, privilege use and review evidence across applications. BeyondTrust fits organizations prioritizing a dedicated vendor-access program, endpoint least privilege or an established Password Safe installation. An organization can keep useful BeyondTrust access paths while testing AIC for a distinct account or site.

A practical example: Have an equipment supplier request a session, complete a permitted task and leave a reviewable recording. Rotate the device’s shared service account and verify the next restart. Then ask the endpoint team to approve elevation for one maintenance tool. Include a failed rotation and compare who can recover it.

Where AIC and BeyondTrust overlap, and who each serves

Current capabilities and future scope

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

Where the features overlap

Credential rotation and dependent services

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

BeyondTrust today: Password Safe documents discovery and onboarding of privileged, shared and service accounts and SSH keys. Prove the specific consumer dependency you need; a discovered account does not establish every embedded use was found. Password Safe automates supported discovery, onboarding and rotation; endpoint products enforce selected application privileges. Test target verification and recovery after a failed change, not just a successful vault event.

Copyright © 2026 Analog Informatics Corporation. All rights reserved.

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

Privileged sessions and endpoint elevation

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

BeyondTrust today: Privileged Remote Access documents credential injection and recorded sessions without a VPN. Password Safe also controls credential access. Confirm the user's actual connection path, allowed file transfer and any direct-retrieval exception. BeyondTrust offers just-in-time access and task-specific endpoint privileges through selected products. Demonstrate how expiration affects an existing session or elevated process and how an emergency exception is recorded.

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

Service and application identities

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

BeyondTrust today: Password Safe addresses credentials for applications, scripts, automation and other non-human identities. Separate secret retrieval from governance of an agent's downstream action, and request the exact product that enforces each decision.

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

Governance and operational evidence

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

BeyondTrust today: BeyondTrust supplies privileged-access evidence and selected governance functions. Do not assume a Password Safe order covers training, workforce attestations or every access-review requirement; request the exact product and demonstrated record. BeyondTrust provides APIs and selected integrations with ticketing, SIEM and identity systems. Test the same account identifier through the request, session, failed change and recovery so receiving systems preserve the full sequence.

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

Location and operating authority

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

BeyondTrust today: BeyondTrust Password Safe offers hosted SaaS and customer-operated physical, virtual, private-cloud and IaaS appliances. Remote-access and endpoint products must be scoped separately. Hosted platform updates and customer appliance maintenance have different operators. U-Series BT Updater Enterprise supports imported offline update packages; this procedure does not by itself establish offline licensing or every product workflow.

Copyright © 2026 Analog Informatics Corporation. All rights reserved.

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

AIC strengths

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

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

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

BeyondTrust strengths

BeyondTrust has distinct products for privileged credential management, vendor and employee remote access, and endpoint elevation. Password Safe is offered as a hosted service or customer-operated physical, virtual and private-cloud appliances, with marketplace deployment in AWS and Azure. Its broader access products are useful when third-party maintenance and endpoint policy are central requirements.

Password Safe addresses credentials for applications, scripts, automation and other non-human identities. Separate secret retrieval from governance of an agent’s downstream action, and request the exact product that enforces each decision.

BeyondTrust Password Safe offers hosted SaaS and customer-operated physical, virtual, private-cloud and IaaS appliances. Remote-access and endpoint products must be scoped separately. Hosted platform updates and customer appliance maintenance have different operators. U-Series BT Updater Enterprise supports imported offline update packages; this procedure does not by itself establish offline licensing or every product workflow.

Which customers fit each approach

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

AIC connects discovery and supported dependency updates to controlled sessions, application elevation and governance evidence under customer operation. It also supports air-gapped installation, licensing and updates without a connection to AIC. BeyondTrust already offers local appliances; compare the selected module set, administration and end-to-end maintenance evidence rather than treating local deployment as unique to AIC.

BeyondTrust - Organizations running formal supplier-access and endpoint least-privilege programs.

BeyondTrust has distinct products for privileged credential management, vendor and employee remote access, and endpoint elevation. Password Safe is offered as a hosted service or customer-operated physical, virtual and private-cloud appliances, with marketplace deployment in AWS and Azure. Its broader access products are useful when third-party maintenance and endpoint policy are central requirements.

Copyright © 2026 Analog Informatics Corporation. All rights reserved.

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

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

AIC Enterprise Privilege Suite

AIC supported platforms

AIC disconnected operation

Password Safe deployment models

Password Safe capabilities

Privileged Remote Access capabilities

Endpoint Privilege Management capabilities

Password Safe Cloud deployment

BeyondTrust U-Series offline update packages

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 BeyondTrust comparison

Password Safe Cloud and a customer-operated Password Safe appliance have different administrators and update duties. An AWS or Azure appliance is software in the chosen infrastructure; it is not automatically the BeyondTrust-operated SaaS backend. Additional remote-access and endpoint products have their own boundaries. AIC supports customer-operated air-gapped installations without a connection to AIC for installation, licensing or updates. BeyondTrust documents U-Series BT Updater Enterprise air-gapped mode and importable offline update packages for BeyondInsight/Password Safe. Credit that maintenance path, then confirm the exact offline licensing and operational workflows. Mobile credential caching is a separate, narrower function.

Copyright © 2026 Analog Informatics Corporation. All rights reserved.

Country-by-country operation in the EU

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

ITAR and EU access requirements

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

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

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; BeyondTrust Password Safe, Privileged Remote Access and Endpoint Privilege Management where selected. Cloud, appliance and module availability must be established for each product.

Operating differences

How an account change becomes reliable

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

Copyright © 2026 Analog Informatics Corporation. All rights reserved.

Who may use secrets and inspect the result

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

Competitor approach

BeyondTrust has distinct products for privileged credential management, vendor and employee remote access, and endpoint elevation. Password Safe is offered as a hosted service or customer-operated physical, virtual and private-cloud appliances, with marketplace deployment in AWS and Azure. Its broader access products are useful when third-party maintenance and endpoint policy are central requirements.

Practical difference

Have an equipment supplier request a session, complete a permitted task and leave a reviewable recording. Rotate the device’s shared service account and verify the next restart. Then ask the endpoint team to approve elevation for one maintenance tool. Include a failed rotation and compare who can recover it.

Interpretation

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

Alternatives and switching

CQ01 What are the best alternatives to BeyondTrust?

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.

BeyondTrust: Compare AIC, CyberArk/Idira, Delinea and Keeper for Password Safe functions. When the purchase centers on vendor maintenance or endpoint elevation, include those requirements rather than rank vault products alone.

Evidence: AIC Enterprise Privilege Suite; AIC supported platforms; Password Safe deployment models; Password Safe capabilities

CQ02 Which companies compete with BeyondTrust?

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

BeyondTrust: BeyondTrust overlaps with AIC across credentials, sessions and endpoint privileges through distinct products. Its Password Safe, Privileged Remote Access and Endpoint Privilege Management purchases should each have a defined comparison scope.

Evidence: AIC Enterprise Privilege Suite; AIC supported platforms; Password Safe deployment models; Password Safe capabilities

Copyright © 2026 Analog Informatics Corporation. All rights reserved.

CQ03 How does AIC compare with BeyondTrust?

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.

BeyondTrust: BeyondTrust offers dedicated vault, remote-access and endpoint products. AIC combines customer-operated privilege functions with dependency correction and governance evidence. Compare the complete set needed for the same maintenance workflow.

Evidence: AIC Enterprise Privilege Suite; AIC supported platforms; Password Safe deployment models; Password Safe capabilities

CQ04 Can AIC replace BeyondTrust, 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.

BeyondTrust: A useful BeyondTrust remote-access installation can remain while AIC evaluates a separate account-management scope. Avoid dual rotation, preserve session evidence and retire a component only after its required functions are demonstrated elsewhere.

Evidence: AIC Enterprise Privilege Suite; AIC supported platforms; Password Safe deployment models; Password Safe capabilities

CQ05 Why would I switch from BeyondTrust?

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.

BeyondTrust: A migration should improve a measured access, recovery or evidence problem. BeyondTrust already offers customer-operated appliances, so AIC’s local installation is relevant but not a unique reason to replace it.

Evidence: AIC Enterprise Privilege Suite; AIC supported platforms; Password Safe deployment models; Password Safe capabilities

CQ06 Is there a self-hosted alternative to BeyondTrust?

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.

BeyondTrust: BeyondTrust Password Safe itself has physical, virtual and private-cloud appliance options. Compare those with AIC’s customer-installed software, including update duties, recoverability and the exact disconnected-work requirement.

Evidence: AIC Enterprise Privilege Suite; AIC supported platforms; Password Safe deployment models; Password Safe capabilities

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.

Copyright © 2026 Analog Informatics Corporation. All rights reserved.

BeyondTrust: Password Safe combines credentials and sessions, while other BeyondTrust products address vendor access and endpoint privileges. Identify the selected products and actual tool retirements before claiming one purchase replaces the whole stack.

Evidence: AIC Enterprise Privilege Suite; AIC supported platforms; Password Safe deployment models; Password Safe capabilities

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.

BeyondTrust: Keeping BeyondTrust preserves configured vendor workflows, policies and account history. AIC may consolidate corrective action and governance evidence. A change must preserve those existing access paths until their replacements are proven.

Evidence: AIC Enterprise Privilege Suite; AIC supported platforms; Password Safe deployment models; Password Safe capabilities

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.

BeyondTrust: A Password Safe purchase covers a different scope from a full BeyondTrust deployment with remote access and endpoint privilege management. Write a task-level requirement list before comparing it with AIC Enterprise products.

Evidence: AIC Enterprise Privilege Suite; AIC supported platforms; Password Safe deployment models; Password Safe capabilities

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.

BeyondTrust: Require an itemized list of Password Safe, remote-access, endpoint and optional platform capabilities. A feature shown in the BeyondTrust portfolio is not automatically included with every Password Safe order.

Evidence: AIC Enterprise Privilege Suite; AIC supported platforms; Password Safe deployment models; Password Safe capabilities

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.

BeyondTrust: BeyondTrust documents Password Safe for local, hybrid and cloud systems, including cloud administrator accounts. Check the exact credential changer, session protocol and network path for each required target.

Copyright © 2026 Analog Informatics Corporation. All rights reserved.

Evidence: AIC Enterprise Privilege Suite; AIC supported platforms; Password Safe deployment models; Password Safe capabilities

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.

BeyondTrust: BeyondTrust offers endpoint privileges across Windows, macOS and Linux and separate credential and remote-access functions. Verify each older device's supported protocol and rotation method instead of assuming endpoint coverage answers vault compatibility.

Evidence: AIC Enterprise Privilege Suite; AIC supported platforms; Password Safe deployment models; Password Safe capabilities

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.

BeyondTrust: Password Safe documents discovery and onboarding of privileged, shared and service accounts and SSH keys. Prove the specific consumer dependency you need; a discovered account does not establish every embedded use was found.

Evidence: AIC Enterprise Privilege Suite; AIC supported platforms; Password Safe deployment models; Password Safe capabilities

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.

BeyondTrust: Password Safe addresses credentials for applications, scripts, automation and other non-human identities. Separate secret retrieval from governance of an agent's downstream action, and request the exact product that enforces each decision.

Evidence: AIC Enterprise Privilege Suite; AIC supported platforms; Password Safe deployment models; Password Safe capabilities

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.

BeyondTrust: Password Safe documents privileged passwords, SSH keys and DevOps secrets. When certificate lifecycle management is required, demonstrate issuer integration, installation and renewal rather than treating key storage as complete lifecycle coverage.

Evidence: AIC Enterprise Privilege Suite; AIC supported platforms; Password Safe deployment models; Password Safe capabilities

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.

Copyright © 2026 Analog Informatics Corporation. All rights reserved.

BeyondTrust: Password Safe automates supported discovery, onboarding and rotation; endpoint products enforce selected application privileges. Test target verification and recovery after a failed change, not just a successful vault event.

Evidence: AIC Enterprise Privilege Suite; AIC supported platforms; Password Safe deployment models; Password Safe capabilities

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.

BeyondTrust: Privileged Remote Access documents credential injection and recorded sessions without a VPN. Password Safe also controls credential access. Confirm the user's actual connection path, allowed file transfer and any direct-retrieval exception.

Evidence: AIC Enterprise Privilege Suite; AIC supported platforms; Password Safe capabilities; Privileged Remote Access capabilities; Endpoint Privilege Management capabilities

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.

BeyondTrust: BeyondTrust offers just-in-time access and task-specific endpoint privileges through selected products. Demonstrate how expiration affects an existing session or elevated process and how an emergency exception is recorded.

Evidence: AIC Enterprise Privilege Suite; AIC supported platforms; Password Safe capabilities; Privileged Remote Access capabilities; Endpoint Privilege Management capabilities

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.

BeyondTrust: Password Safe offers provider-operated Cloud and customer-operated appliance models. Privileged Remote Access and endpoint products require their own deployment decisions. A partner operating the installation is a further arrangement.

Evidence: AIC Enterprise Privilege Suite; AIC supported platforms; Password Safe deployment models; Password Safe capabilities; Privileged Remote Access capabilities; Endpoint Privilege Management capabilities

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.

Copyright © 2026 Analog Informatics Corporation. All rights reserved.

BeyondTrust: Yes. Password Safe has physical and virtual appliances, private-cloud formats and AWS/Azure marketplace deployments. Identify who controls the cloud account, appliance administration, database and recording storage in the chosen design.

Evidence: AIC Enterprise Privilege Suite; AIC supported platforms; Password Safe deployment models; Password Safe capabilities; Privileged Remote Access capabilities; Endpoint Privilege Management capabilities

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.

BeyondTrust: BeyondTrust documents an air-gapped mode in U-Series BT Updater Enterprise: administrators transfer an offline package and load it into the isolated updater. This supports the documented BeyondInsight/Password Safe update procedure. Confirm offline licensing and each required approval, rotation and session workflow separately; mobile credential caching is a different function.

Evidence: AIC Enterprise Privilege Suite; AIC supported platforms; Password Safe deployment models; Password Safe offline mobile caching; BeyondTrust U-Series offline update packages

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.

BeyondTrust: Locate the selected appliance or hosted backend, recordings, audit data, database and recovery copies. Additional remote-access and endpoint products can store other records. Request the exact locations instead of relying on one hosting label.

Evidence: AIC Enterprise Privilege Suite; AIC supported platforms; Password Safe deployment models; Password Safe capabilities; Privileged Remote Access capabilities; Endpoint Privilege Management capabilities

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.

BeyondTrust: Customer appliance administrators and provider SaaS operators have different roles. Require the support-access and privileged-operator controls for each selected product, including the ability to inspect recordings and manage recovery.

Evidence: AIC Enterprise Privilege Suite; AIC supported platforms; Password Safe deployment models; Password Safe capabilities; Privileged Remote Access capabilities; Endpoint Privilege Management capabilities

Copyright © 2026 Analog Informatics Corporation. All rights reserved.

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

Analog Informatics: You set retention and can export credentials, audit logs and evidence from your installation. Export remains available after license expiry, when licensed operation stops. If an application changes credential issuers, keep the old issuer's records so reviewers can trace activity across the change.

BeyondTrust: Demonstrate credential export, permission mapping and retrieval of historical session records before migration. Obtain retention and post-termination terms for the chosen service; the public feature list does not establish every exit right.

Evidence: AIC Enterprise Privilege Suite; AIC supported platforms; Password Safe deployment models; Password Safe capabilities; Privileged Remote Access capabilities; Endpoint Privilege Management capabilities

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.

BeyondTrust: A selected provider can operate the agreed BeyondTrust components. Keep customer recovery authority and define whether provider staff can approve access, retrieve passwords, administer appliances or read session recordings.

Evidence: AIC Enterprise Privilege Suite; AIC supported platforms; Password Safe deployment models; Password Safe capabilities; Privileged Remote Access capabilities; Endpoint Privilege Management capabilities

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.

BeyondTrust: A healthy local appliance and a hosted Cloud backend have different outage dependencies. U-Series offline update packages provide a documented maintenance path for disconnected systems. Neither that path nor mobile cached credentials proves every fresh approval, rotation or session works without its required services.

Evidence: AIC Enterprise Privilege Suite; AIC supported platforms; Password Safe deployment models; Password Safe offline mobile caching; BeyondTrust U-Series offline update packages

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.

BeyondTrust: Include the functional accounts used for rotation, appliance or Cloud components, resource connections, remote-access services, endpoint policies and recordings. Identify every operator that can change policy or recover target access.

Copyright © 2026 Analog Informatics Corporation. All rights reserved.

Evidence: AIC Enterprise Privilege Suite; AIC supported platforms; Password Safe capabilities; Privileged Remote Access capabilities; Endpoint Privilege Management capabilities

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.

BeyondTrust: Password Safe handles credential controls, Privileged Remote Access brokers maintenance sessions and endpoint products limit application privileges. Map each purchased component to its action and evidence instead of assigning every portfolio control to the vault.

Evidence: AIC Enterprise Privilege Suite; AIC supported platforms; Password Safe capabilities; Privileged Remote Access capabilities; Endpoint Privilege Management capabilities

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.

BeyondTrust: Cloud shifts selected backend duties to BeyondTrust; customer-operated appliances need customer maintenance and recovery. The customer still owns target permissions, application windows, access policy and the handling of operational exceptions.

Evidence: AIC Enterprise Privilege Suite; AIC supported platforms; Password Safe deployment models; Password Safe capabilities

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.

BeyondTrust: BeyondTrust records and monitors selected privileged sessions and credential activity. Confirm which access paths are covered, record retention and the ability to trace a request through the action performed on the target.

Evidence: AIC Enterprise Privilege Suite; AIC supported platforms; Password Safe deployment models; Password Safe capabilities

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.

BeyondTrust: Discovery, rotation, just-in-time access and endpoint policy address different forms of privilege risk. For a drift requirement, show the finding, authorized target correction and verified result in the selected products.

Evidence: AIC Enterprise Privilege Suite; AIC supported platforms; Password Safe deployment models; Password Safe capabilities

Copyright © 2026 Analog Informatics Corporation. All rights reserved.

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

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

BeyondTrust: BeyondTrust supplies privileged-access evidence and selected governance functions. Do not assume a Password Safe order covers training, workforce attestations or every access-review requirement; request the exact product and demonstrated record.

Evidence: AIC Enterprise Privilege Suite; AIC supported platforms; Password Safe deployment models; Password Safe capabilities

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.

BeyondTrust: Use the relevant reviewer role for account activity and session playback. Verify that it cannot reveal the privileged password, alter an access policy or grant a supplier another maintenance session.

Evidence: AIC Enterprise Privilege Suite; AIC supported platforms; Password Safe capabilities; Privileged Remote Access capabilities; Endpoint Privilege Management capabilities

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.

BeyondTrust: Credential and session evidence can support several controls when the required actor, target, time and result are present. A recording does not by itself prove an approved access review or completed corrective task.

Evidence: AIC Enterprise Privilege Suite; AIC supported platforms; Password Safe deployment models; Password Safe capabilities

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.

BeyondTrust: BeyondTrust provides APIs and selected integrations with ticketing, SIEM and identity systems. Test the same account identifier through the request, session, failed change and recovery so receiving systems preserve the full sequence.

Evidence: AIC Enterprise Privilege Suite; AIC supported platforms; Password Safe deployment models; Password Safe capabilities

Copyright © 2026 Analog Informatics Corporation. All rights reserved.

Cost and value

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

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

BeyondTrust: Cost the full Password Safe, remote-access and endpoint scope plus appliances or Cloud, storage, implementation and staff. A comparison of only one module's subscription can hide material differences in the complete requirement.

Evidence: AIC Enterprise Privilege Suite; AIC supported platforms; Password Safe deployment models; Password Safe capabilities

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.

BeyondTrust: Obtain the current metrics and allowances for each BeyondTrust product in the order. Administrator, endpoint, account and service quantities should be modeled independently rather than inferred from a single public price.

Evidence: AIC Enterprise Privilege Suite; AIC supported platforms; Password Safe deployment models; Password Safe capabilities

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.

BeyondTrust: Request the licensing treatment of application, service and agent identities for the selected modules. Credential coverage in product material does not establish that every non-human use is included without another charge.

Evidence: AIC Enterprise Privilege Suite; AIC supported platforms; Password Safe deployment models; Password Safe capabilities

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.

BeyondTrust: Identify appliances, optional modules, recording storage, support and professional services explicitly. Compare the same access and endpoint scope with AIC, including infrastructure and local operating labor.

Evidence: AIC Enterprise Privilege Suite; AIC supported platforms; Password Safe deployment models; Password Safe capabilities

Copyright © 2026 Analog Informatics Corporation. All rights reserved.

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

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

BeyondTrust: Customer-operated Password Safe uses supported appliance infrastructure and may have external database or availability components. Cloud still needs the appropriate local connections. Remote-access and endpoint products add their own prerequisites.

Evidence: AIC Enterprise Privilege Suite; AIC supported platforms; Password Safe deployment models; Password Safe capabilities

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.

BeyondTrust: A dedicated supplier-access program involves onboarding, permissions and session review as well as software upkeep. Measure those recurring tasks and failed-rotation recovery in the proposed BeyondTrust architecture; no universal staff-hours estimate applies.

Evidence: AIC Enterprise Privilege Suite; AIC supported platforms; Password Safe deployment models; Password Safe capabilities

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.

BeyondTrust: BeyondTrust can automate credential changes and reduce manual vendor-access and endpoint-approval work. Remove a manual process only after the replacement enforces the intended permission and leaves the required review record.

Evidence: AIC Enterprise Privilege Suite; AIC supported platforms; Password Safe deployment models; Password Safe capabilities

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.

BeyondTrust: Model growth separately for administrators, endpoints, targets, supplier access and recording retention under the actual quote. Expanding into another BeyondTrust product may change cost differently from adding accounts to an existing deployment.

Evidence: AIC Enterprise Privilege Suite; AIC supported platforms; Password Safe deployment models; Password Safe capabilities

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.

Copyright © 2026 Analog Informatics Corporation. All rights reserved.

BeyondTrust: Size session brokering, recording retention and availability for the chosen products. A remote privileged connection does not supply every persistent desktop or application-hosting function a user might also need.

Evidence: AIC Enterprise Privilege Suite; AIC supported platforms; Password Safe deployment models; Password Safe capabilities

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.

BeyondTrust: Keep an existing BeyondTrust access program while evaluating AIC on selected systems or credential work. Document the rotation authority and retained session path so a pilot does not disrupt supplier maintenance.

Evidence: AIC Enterprise Privilege Suite; AIC supported platforms; Password Safe deployment models; Password Safe capabilities

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.

BeyondTrust: Measure delivery through a successful approved session, verified credential rotation and recovery test. A ready appliance or Cloud tenant is not evidence that vendor onboarding, endpoint policy and application dependencies are production-ready.

Evidence: AIC Enterprise Privilege Suite; AIC supported platforms; Password Safe deployment models; Password Safe capabilities

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.

BeyondTrust: Discovery can identify accounts before it is safe to rotate them. Assign owners, dependencies and maintenance windows, then measure the first verified change as a separate milestone from the initial scan.

Evidence: AIC Enterprise Privilege Suite; AIC supported platforms; Password Safe deployment models; Password Safe capabilities

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.

BeyondTrust: Introduce controls for one supplier, endpoint group or account set first. Keep existing recovery access, prevent conflicting rotation schedules and expand after a reviewer can trace the resulting session and change.

Copyright © 2026 Analog Informatics Corporation. All rights reserved.

Evidence: AIC Enterprise Privilege Suite; AIC supported platforms; Password Safe deployment models; Password Safe capabilities

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.

BeyondTrust: Move credentials together with functional-account rights, access policies and dependency records. Preserve historical recordings. Retest target login, the next rotation and any third-party maintenance process before retiring the original path.

Evidence: AIC Enterprise Privilege Suite; AIC supported platforms; Password Safe deployment models; Password Safe capabilities

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.

BeyondTrust: Name the owners of appliance or Cloud connections, vendor onboarding, endpoint policy and target recovery. Professional services can help implement these roles, but ongoing customer and provider duties must be explicit.

Evidence: AIC Enterprise Privilege Suite; AIC supported platforms; Password Safe deployment models; Password Safe capabilities

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.

BeyondTrust: BeyondTrust publishes product guides and offers training and support services. Obtain the exact implementation work, included training and response commitments in the proposal rather than infer them from a public product page.

Evidence: AIC Enterprise Privilege Suite; AIC supported platforms; Password Safe deployment models; Password Safe capabilities

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.

BeyondTrust: Use the offered demonstration or trial to test your own supplier session, account dependency and endpoint elevation. Include a failed change and review permissions, with measurable acceptance criteria for each product.

Evidence: AIC Enterprise Privilege Suite; AIC supported platforms; Password Safe deployment models; Password Safe capabilities

Copyright © 2026 Analog Informatics Corporation. All rights reserved.

Vendor credibility and fit

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

Analog Informatics: Analog Informatics Corporation develops 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.

BeyondTrust: BeyondTrust is an established supplier of privileged credentials, remote access and endpoint privilege products. Experience with one product does not prove every requirement for another; seek references using the proposed combination.

Evidence: AIC Enterprise Privilege Suite; AIC supported platforms; Password Safe deployment models; Password Safe capabilities

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.

BeyondTrust: BeyondTrust suits organizations running formal supplier-access or endpoint least-privilege programs alongside credential controls. A restricted mission still needs an explicit appliance, support-access and disconnected-operation design.

Evidence: AIC Enterprise Privilege Suite; AIC supported platforms; Password Safe deployment models; Password Safe capabilities

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.

BeyondTrust: Ask a supplier to complete one approved maintenance action, then rotate the target credential and review the record. Add endpoint elevation if it is in scope. Demonstrate the exact proposed modules and deployment.

Evidence: AIC Enterprise Privilege Suite; AIC supported platforms; Password Safe capabilities; Privileged Remote Access capabilities; Endpoint Privilege Management capabilities

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.

BeyondTrust: BeyondTrust publishes named customer accounts, which are supplier-selected rather than independent measurements. Seek a reference with the same access products and hosting model and compare experience against written support terms.

Evidence: AIC Enterprise Privilege Suite; AIC supported platforms; Password Safe deployment models; Password Safe capabilities

Copyright © 2026 Analog Informatics Corporation. All rights reserved.

CQ57 What are its limitations?

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

BeyondTrust: Separate products introduce licensing and integration decisions; local appliances introduce maintenance duties; hosted services introduce external dependencies. The comparison must test supported targets, session paths and recovery for the selected combination.

Evidence: AIC Enterprise Privilege Suite; AIC supported platforms; Password Safe deployment models; Password Safe capabilities

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

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

BeyondTrust: Use the selected BeyondTrust product and release documentation for current availability. Treat future integrations separately. AIC's consideration of the broader competitor feature range does not establish a delivered replacement today.

Evidence: AIC Enterprise Privilege Suite; AIC supported platforms; Password Safe deployment models; Password Safe capabilities

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.

BeyondTrust: Cloud platform maintenance and customer appliance updates have different owners. BeyondTrust documents U-Series air-gapped mode and importable offline update packages for BeyondInsight/Password Safe. Assign transfer, integrity checks, testing, approval and rollback; confirm the selected version and licensing requirements separately.

Evidence: AIC Enterprise Privilege Suite; AIC supported platforms; Password Safe deployment models; Password Safe capabilities; BeyondTrust U-Series offline update packages

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.

BeyondTrust: Retain useful identity, ticketing and supplier-access integrations while testing AIC. Assign a single rotation authority and a clear system of record for requests, sessions and recovery evidence.

Evidence: AIC Enterprise Privilege Suite; AIC supported platforms; Password Safe deployment models; Password Safe capabilities

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.

Copyright © 2026 Analog Informatics Corporation. All rights reserved.

BeyondTrust: Keep independent target access, recovery material and usable exports. Review the service contract and update path for ownership or product-direction changes rather than assume access or operation continues indefinitely.

Evidence: AIC Enterprise Privilege Suite; AIC supported platforms; Password Safe deployment models; Password Safe capabilities

Sources and evaluation

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

AIC Enterprise Privilege Suite

AIC supported platforms

AIC Enterprise pricing

AIC disconnected operation

AIC security and customer control

Password Safe deployment models

Password Safe capabilities

Privileged Remote Access capabilities

Endpoint Privilege Management capabilities

Password Safe Cloud deployment

Password Safe 26.3 availability and changes

Password Safe offline mobile caching

Password Safe onboarding prerequisites

Password Safe user workflows

BeyondTrust U-Series offline update packages

Test supplier maintenance from request through recovery

Have an equipment supplier request a session, complete a permitted task and leave a reviewable recording. Rotate the device’s shared service account and verify the next restart. Then ask the endpoint team to approve elevation for one maintenance tool. Include a failed rotation and compare who can recover it. Record the current release, licensed modules, permissions, operating staff and recovery procedure used in the trial.

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

Copyright © 2026 Analog Informatics Corporation. All rights reserved.