COMPETITIVE ANALYSIS

Analog Informatics vs. BeyondTrust — Competitive Analysis

Compare BeyondTrust Password Safe and remote-access controls with AIC's local credential, session and remediation evidence in sensitive environments.

Analysis: October 17, 2026

Deployment and customer-control revision: November 20, 2026

Analog Informatics Corporation

analoginfo.com

Copyright © 2026 Analog Informatics Corporation. All rights reserved.

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

Remote-access records must connect to the purpose, approval and outcome of the work. Evaluate AIC's privileged workflow alongside built-in control mappings, findings and audit evidence.

Deployment, secret control and sensitive missions

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

How this changes the BeyondTrust decision

BeyondTrust strengths: Privileged Remote Access and Password Safe for controlled sessions and credentials. The deployment comparison below distinguishes the location of protected systems from the location and operator of the management software.

Decision: Management service and operating model

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

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.

Decision: Customer hardware or cloud account

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

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.

Decision: Air-gapped and disconnected work

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

BeyondTrust: BeyondTrust offers customer-operated appliances. The BeyondInsight and Password Safe U-Series updater documents an Air-Gapped Mode using locally imported offline update packages. Confirm the selected products' licensing, identity and workflow dependencies separately; this update mechanism does not establish that every BeyondTrust function operates fully offline.

Decision: Secret and record locations

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

Copyright © 2026 Analog Informatics Corporation. All rights reserved.

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.

Decision: Administrator and support access

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

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.

Which customers fit each approach

AIC: A security team that must explain why a privileged repair took place can use AIC to connect a controlled session with the configuration finding and evidence of the result. This fits organizations that keep approval and record custody with their own operators.

BeyondTrust: A supplier-access team can use BeyondTrust Privileged Remote Access for controlled third-party sessions. An organization with Password Safe can also build on its existing credential and session controls, choosing the appliance or hosted model that suits its administration team.

Administrator identity, location and country requirements

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

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

Buyer questions

What are the best alternatives to BeyondTrust?

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

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

Copyright © 2026 Analog Informatics Corporation. All rights reserved.

Which companies compete with BeyondTrust?

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

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

How does AIC compare with BeyondTrust?

AIC: Evaluate AIC's privileged workflow alongside built-in control mappings, findings and audit evidence. AIC operates supported credential, session, configuration and evidence functions in the installation your organization controls. Compare the BeyondTrust functions you need separately from the location of its management service and the people allowed to administer it.

BeyondTrust: BeyondTrust emphasizes Privileged Remote Access and Password Safe for controlled sessions and credentials. Compare this with AIC’s customer-deployed operating controls and the required evidence flow. The specific purchasing difference is: Evaluate AIC's privileged workflow alongside built-in control mappings, findings and audit evidence.

Can AIC replace BeyondTrust, or do I need both?

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

BeyondTrust: BeyondTrust provides credential and session controls through its product portfolio. Evaluate the combined products required for the use case.

Why would I switch from BeyondTrust?

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

BeyondTrust: Remote-access records must connect to the purpose, approval and outcome of the work. A change is justified when the pilot resolves that problem and the transition preserves required functions.

Is there a self-hosted alternative to BeyondTrust?

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

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.

Copyright © 2026 Analog Informatics Corporation. All rights reserved.

Can I replace several security tools with one platform?

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

BeyondTrust: The published scope combines Privileged Remote Access and Password Safe for controlled sessions and credentials. Whether that eliminates other tools depends on retained connectors, controls and service duties. Build a function-by-function retirement list rather than assume an entire stack is replaced.

What will I lose - and gain - by switching?

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

BeyondTrust: The functions to preserve are Privileged Remote Access and Password Safe for controlled sessions and credentials. The potential gain from AIC is customer-operated control and evidence in the same workflow. Preserve recordings, approval history, account dependencies and emergency access during a staged change.

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

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

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

Which features are included, and which require another product?

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

BeyondTrust: The published capability summary is Privileged Remote Access and Password Safe for controlled sessions and credentials. Exact entitlements, optional modules and third-party dependencies require the selected package’s bill of materials. Preserve the distinction between product features and separately purchased professional services.

Does it manage both on-premises and cloud assets?

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

BeyondTrust: Password Safe documents on-premises and cloud resources. Compare its managed-target scope separately from on-premises, IaaS or cloud management deployment; neither dimension is unique to AIC.

Copyright © 2026 Analog Informatics Corporation. All rights reserved.

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

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

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

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

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

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

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

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

BeyondTrust: Password Safe describes human and non-human credential/secret management. Validate the target types and application dependencies for service accounts and AI-agent identities.

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

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

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

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

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

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

Copyright © 2026 Analog Informatics Corporation. All rights reserved.

Does it provide controlled access without exposing credentials?

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

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

Can it remove standing privileges and expire approved access automatically?

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

BeyondTrust: BeyondTrust’s cloud deployment guidance describes requested session duration and a force-termination policy option. Test that policy on the intended protocol and configuration; timed access is a documented capability.

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

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

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.

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

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

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.

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

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

BeyondTrust: BeyondTrust offers customer-operated appliances. The BeyondInsight and Password Safe U-Series updater documents an Air-Gapped Mode using locally imported offline update packages. Confirm the

Copyright © 2026 Analog Informatics Corporation. All rights reserved.

selected products' licensing, identity and workflow dependencies separately; this update mechanism does not establish that every BeyondTrust function operates fully offline.

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

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

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.

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

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

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.

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

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

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.

Can my MSP operate it while I retain control?

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

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.

Copyright © 2026 Analog Informatics Corporation. All rights reserved.

What happens if the vendor's service is unavailable?

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

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.

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

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

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

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

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

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

What remains my responsibility or my MSP's responsibility?

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

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

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

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

Copyright © 2026 Analog Informatics Corporation. All rights reserved.

BeyondTrust: The offering describes Privileged Remote Access and Password Safe for controlled sessions and credentials. Determine which evidence is collected automatically, which requires integrations and which still needs a person. Test freshness, failed collection and historical traceability; a current dashboard is not necessarily a complete audit record.

Can it detect drift and remediate problems between assessments?

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

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

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

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

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

Can auditors review current evidence without disrupting IT?

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

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

Can it support multiple frameworks without duplicating work?

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

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

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

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

Copyright © 2026 Analog Informatics Corporation. All rights reserved.

BeyondTrust: BeyondTrust provides credential and session controls through its product portfolio. Evaluate the combined products required for the use case. An integration needs an identified API/export, matching control identifiers and an owner; a generic partnership claim is not a working data connection.

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

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

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

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

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

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

Are non-human identities charged separately?

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

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

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

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

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

What infrastructure and third-party licenses will I need?

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

Copyright © 2026 Analog Informatics Corporation. All rights reserved.

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

How much staff time does it take to operate?

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

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

Which manual tasks and existing subscriptions could it eliminate?

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

BeyondTrust: Potential consolidation follows the documented scope: Privileged Remote Access and Password Safe for controlled sessions and credentials. Identify the exact existing task or subscription replaced and the records it preserves. Avoid double-counting savings while keeping the same staff work or another required module.

How do costs change as the company grows?

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

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

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

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

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

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

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

Copyright © 2026 Analog Informatics Corporation. All rights reserved.

BeyondTrust: Preserve recordings, approval history, account dependencies and emergency access during a staged change. Distinguish integrating existing systems from moving the workload into a new boundary; they involve different change and migration effort.

How quickly can we deploy a new enclave?

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

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

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

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

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

Can we introduce it gradually without interrupting operations?

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

BeyondTrust: Preserve recordings, approval history, account dependencies and emergency access during a staged change. Stage the change with acceptance tests, retained records and rollback. If the offering requires a new service boundary, include the interim data path and access dependencies in the pilot.

How do we migrate credentials, policies, and evidence?

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

BeyondTrust: Preserve recordings, approval history, account dependencies and emergency access during a staged change. Preserve source evidence and timestamp/owner relationships. Validate the import and credential-change behavior before deleting or terminating any original service.

Who handles configuration, migration, and ongoing operations?

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

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

Copyright © 2026 Analog Informatics Corporation. All rights reserved.

the customer, MSP and supplier. The purchase must identify who executes the migration and who accepts the resulting environment.

What training, deployment guides, and support are included?

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

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

Can we test it on our own systems before committing?

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

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

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

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

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

Does it understand organizations like ours?

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

BeyondTrust: The relevant fit question is: Remote-access records must connect to the purpose, approval and outcome of the work. Ask the supplier for a reference architecture and customer reference matching your system mix, operating team and regulatory scope.

Can it demonstrate our specific use case?

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

Copyright © 2026 Analog Informatics Corporation. All rights reserved.

BeyondTrust: Trace the authorized purpose of a session to its repair and verification evidence. Require the supplier to perform the comparable workflow on its proposed edition and retain the observed result.

What do customers say about reliability and support?

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

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

What are its limitations?

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

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

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

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

BeyondTrust: The published offering currently describes Privileged Remote Access and Password Safe for controlled sessions and credentials. Any feature discussed only as roadmap or without an orderable edition should stay outside the scored current comparison until release documentation and a demonstration establish delivery.

How does it handle vulnerabilities and security updates?

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

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

Will it work with our existing vendors and service providers?

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

BeyondTrust: BeyondTrust provides credential and session controls through its product portfolio. Evaluate the combined products required for the use case. Validate the specific connector, export format or service relationship

Copyright © 2026 Analog Informatics Corporation. All rights reserved.

and its permissions before presenting coexistence as turnkey.

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

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

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.

Sources and Next Step

- Provider source 1
- Provider source 2
- Provider source 3
- Provider source 4

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

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

Updated supplier deployment references

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

- https://www.beyondtrust.com/products/password-safe/features/deployment
- https://www.beyondtrust.com/products/password-safe
- https://www.beyondtrust.com/products/privileged-remote-access
- https://www.beyondtrust.com/products/endpoint-privilege-management
- https://docs.beyondtrust.com/bips/v26.2/docs/mobile-app-ps-offline-mode
- https://docs.beyondtrust.com/bips/v25.3/docs/bt-updater-enterprise

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

Copyright © 2026 Analog Informatics Corporation. All rights reserved.