COMPETITIVE ANALYSIS

Analog Informatics vs. Kieri Solutions — Competitive Analysis

Compare Kieri's advisory and assessment role with AIC's customer-run security software, secret custody and air-gapped deployment for sensitive missions.

Analysis: October 17, 2026

Deployment and customer-control revision: November 20, 2026

Analog Informatics Corporation

analoginfo.com

Copyright © 2026 Analog Informatics Corporation. All rights reserved.

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

A reference architecture and an assessment need an operating security platform underneath them. Use AIC to operate supported security controls and provide evidence to the customer's advisors and assessors.

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 Kieri Solutions decision

Kieri Solutions strengths: CMMC documentation, GCC High reference architecture, readiness and formal assessment offerings. 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.

Kieri Solutions: This is a documentation, advisory or assessment engagement, rather than a SaaS tenant or a self-hosted security platform. Deployment choices belong to the customer implementation that uses the reference architecture; the engagement defines the supplier's service duties.

Decision: Customer hardware or cloud account

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

Kieri Solutions: A hardware-deployment label is not applicable to the documents, advisory work or assessment engagement. Evaluate the infrastructure implementing the reference architecture and who operates that infrastructure. The advisor's service is a separate responsibility.

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.

Kieri Solutions: Air-gap requirements apply to the customer's implemented systems and the permitted evidence-sharing path. Agree how an advisor or assessor can review the necessary records without violating that boundary. The professional engagement should not be classified as a disconnected software platform.

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.

Kieri Solutions: Agree where the customer and Kieri will keep architecture documents, assessment records and shared evidence under the engagement. Include approved repositories, transfer methods, retention and return or deletion duties. These are engagement controls, rather than a SaaS tenant's storage configuration.

Decision: Administrator and support access

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

Kieri Solutions: Define the advisor's or assessor's approved evidence access under the engagement. Separate review access from operational administrator authority, identify authorized recipients and locations, and establish the permitted evidence-sharing process for the customer boundary.

Which customers fit each approach

AIC: A contractor preparing for an assessment can run AIC to control privileged work and give its advisor evidence from actual operations. Its own administrators retain responsibility for performing repairs and authorizing access to managed secrets.

Kieri Solutions: A program lead who needs CMMC documentation, a GCC High reference architecture, readiness assistance or a formal assessment can evaluate the appropriate Kieri offering. The roles of the advisor, independent assessor and system operator remain distinct.

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 Kieri Solutions?

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.

Kieri Solutions: For the Assessment and advisory portion of the purchase, shortlist a scoped CMMC advisor, an independent assessor, a reference-architecture provider. 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 Kieri Solutions?

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.

Kieri Solutions: a scoped CMMC advisor, an independent assessor, a reference-architecture provider are adjacent offerings in this comparison set. They overlap in different ways with Kieri Solutions; they are not identical replacements. AIC overlaps where privileged controls, remediation and security evidence are the required outcome.

How does AIC compare with Kieri Solutions?

AIC: Use AIC to operate supported security controls and provide evidence to the customer's advisors and assessors. AIC operates supported credential, session, configuration and evidence functions in the installation your organization controls. Compare the Kieri Solutions functions you need separately from the location of its management service and the people allowed to administer it.

Kieri Solutions: Kieri Solutions emphasizes CMMC documentation, GCC High reference architecture, readiness and formal assessment offerings. Compare this with AIC’s customer-deployed operating controls and the required evidence flow. The specific purchasing difference is: Use AIC to operate supported security controls and provide evidence to the customer's advisors and assessors.

Can AIC replace Kieri Solutions, 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.

Kieri Solutions: Kieri's assessment service is complementary, not an auditor that AIC software replaces.

Why would I switch from Kieri Solutions?

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.

Kieri Solutions: A reference architecture and an assessment need an operating security platform underneath them. A change is justified when the pilot resolves that problem and the transition preserves required functions.

Is there a self-hosted alternative to Kieri Solutions?

AIC: AIC is customer-installed security software. Kieri's documentation, advisory and assessment services perform a different job: operating AIC does not replace a required independent assessment or professional engagement. Evaluate AIC as the technical operating platform underneath the agreed architecture and evidence requirements.

Kieri Solutions: Kieri supplies documentation, reference architecture, readiness and assessment services. Customer-installed AIC can operate security controls beneath that work, but buying software and engaging an advisor or assessor serve different needs. Evaluate the infrastructure implementing the reference architecture separately.

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.

Kieri Solutions: The published scope combines CMMC documentation, GCC High reference architecture, readiness and formal assessment offerings. 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.

Kieri Solutions: The functions to preserve are CMMC documentation, GCC High reference architecture, readiness and formal assessment offerings. The potential gain from AIC is customer-operated control and evidence in the same workflow. When changing tooling, preserve the architecture, evidence and engagement requirements agreed with the advisor or assessor.

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.

Kieri Solutions: This is Documentation, reference architecture and assessment services, so evaluate it for that role. It does not replace an operating security platform merely by supplying professional assessment or architecture work.

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.

Kieri Solutions: The published capability summary is CMMC documentation, GCC High reference architecture, readiness and formal assessment offerings. 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.

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

Copyright © 2026 Analog Informatics Corporation. All rights reserved.

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

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

Kieri Solutions: The published material reviewed for Kieri Solutions 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.

Kieri Solutions: This is an assessment/reference-architecture engagement, not a credential-management product. The selected operating software must supply this control; Kieri's engagement scope determines how its implementation and evidence are evaluated.

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.

Kieri Solutions: This is an assessment/reference-architecture engagement, not a credential-management product. The selected operating software must supply this control; Kieri's engagement scope determines how its implementation and evidence are evaluated.

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.

Kieri Solutions: This is an assessment/reference-architecture engagement, not a credential-management product. The selected operating software must supply this control; Kieri's engagement scope determines how its implementation and evidence are evaluated.

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.

Kieri Solutions: The published material reviewed for Kieri Solutions does not specify which corrective actions execute directly on the customer's target systems. Demonstrate one failed check through authorization, actual

Copyright © 2026 Analog Informatics Corporation. All rights reserved.

correction, verification and evidence; distinguish an assigned ticket from an executed repair.

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.

Kieri Solutions: This is an assessment/reference-architecture engagement, not a credential-management product. The selected operating software must supply this control; Kieri’s engagement scope determines how its implementation and evidence are evaluated.

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.

Kieri Solutions: This is an assessment/reference-architecture engagement, not a credential-management product. The selected operating software must supply this control; Kieri’s engagement scope determines how its implementation and evidence are evaluated.

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

AIC: AIC is software the customer installs and operates on premises, in a customer cloud account or in a hybrid environment. Kieri's documentation and professional services are a separate engagement. Choose the implementation infrastructure and operator independently from the advisor's or assessor's scope.

Kieri Solutions: This is a documentation, advisory or assessment engagement, rather than a SaaS tenant or a self-hosted security platform. Deployment choices belong to the customer implementation that uses the reference architecture; the engagement defines the supplier's service duties.

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

AIC: Yes. Your organization chooses AIC's supported hardware or cloud account, operating location and administrators. For a Kieri engagement, evaluate the infrastructure implementing the reference architecture separately from the documents and professional services being supplied.

Kieri Solutions: A hardware-deployment label is not applicable to the documents, advisory work or assessment engagement. Evaluate the infrastructure implementing the reference architecture and who operates that infrastructure. The advisor's service is a separate responsibility.

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

AIC: Yes. AIC supports air-gapped deployments and 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. If Kieri is advising or assessing the environment, agree a permitted evidence-review and transfer process without granting operational administrator authority merely for review.

Kieri Solutions: Air-gap requirements apply to the customer's implemented systems and the permitted evidence-sharing path. Agree how an advisor or assessor can review the necessary records without violating that

Copyright © 2026 Analog Informatics Corporation. All rights reserved.

boundary. The professional engagement should not be classified as a disconnected software platform.

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 Kieri Solutions processing and storage arrangement proposed for your purchase.

Kieri Solutions: Agree where the customer and Kieri will keep architecture documents, assessment records and shared evidence under the engagement. Include approved repositories, transfer methods, retention and return or deletion duties. These are engagement controls, rather than a SaaS tenant's storage configuration.

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 Kieri Solutions, including its support, subcontractor and emergency-access arrangements.

Kieri Solutions: Define the advisor's or assessor's approved evidence access under the engagement. Separate review access from operational administrator authority, identify authorized recipients and locations, and establish the permitted evidence-sharing process for the customer boundary.

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 Kieri Solutions; customer custody is useful only when the required records can actually be recovered.

Kieri Solutions: The published material reviewed for Kieri Solutions does not specify complete export coverage, formats, retained history and post-termination access for this package. Request a sample export of attachments, approvals, timestamps and control relationships; compare it with the exit clause before cancelling.

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 Kieri Solutions arrangement; hiring an operator does not require giving that operator unrestricted authority over every secret.

Kieri Solutions: The published material reviewed for Kieri Solutions does not specify the intended MSP’s administrative rights, customer tenancy rights and exit access under this contract. Assign roles in writing and test customer access to evidence without depending on one MSP employee. Managed/co-managed programs may have different boundaries.

Copyright © 2026 Analog Informatics Corporation. All rights reserved.

What happens if the vendor’s service is unavailable?

AIC: A supported local AIC installation can continue its supported credential and session work during an Internet or AIC-service outage while its license and required local infrastructure remain 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. Distinguish that technical availability from availability of Kieri's advisors or assessors under the separate engagement.

Kieri Solutions: For service continuity, distinguish operation of the customer's implemented systems from availability of the advisor or assessor. Preserve customer copies of required documents and records and agree support and handover responsibilities; a SaaS platform-outage model does not describe this engagement.

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.

Kieri Solutions: 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.

Kieri Solutions: The published material reviewed for Kieri Solutions 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.

Kieri Solutions: Kieri supplies reference architecture and professional services. These are different from an operating security product; identify implementation and assessment engagement boundaries separately.

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.

Kieri Solutions: The offering describes CMMC documentation, GCC High reference architecture, readiness and formal assessment offerings. 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

Copyright © 2026 Analog Informatics Corporation. All rights reserved.

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.

Kieri Solutions: The published material reviewed for Kieri Solutions 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.

Kieri Solutions: The published material reviewed for Kieri Solutions 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.

Kieri Solutions: The GRC/audit role supports organizing review material, but exact auditor permissions and disclosure controls must be demonstrated. Test limited reviewer access, export and evidence freshness without granting operational administrator rights.

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.

Kieri Solutions: The published material reviewed for Kieri Solutions 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.

Kieri Solutions: Kieri's assessment service is complementary, not an auditor that AIC software replaces. An integration needs an identified API/export, matching control identifiers and an owner; a generic partnership claim is not a working data connection.

Copyright © 2026 Analog Informatics Corporation. All rights reserved.

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.

Kieri Solutions: The published material reviewed for Kieri Solutions 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.

Kieri Solutions: The published material reviewed for Kieri Solutions 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.

Kieri Solutions: A software identity-count meter is not applicable to the professional engagement itself. Obtain the engagement fee and separately price the operating software specified in the architecture.

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.

Kieri Solutions: The published material reviewed for Kieri Solutions 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.

Kieri Solutions: 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.

Copyright © 2026 Analog Informatics Corporation. All rights reserved.

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.

Kieri Solutions: No independently verified staffing estimate for your Kieri Solutions 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.

Kieri Solutions: Potential consolidation follows the documented scope: CMMC documentation, GCC High reference architecture, readiness and formal assessment offerings. 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.

Kieri Solutions: The published material reviewed for Kieri Solutions 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.

Kieri Solutions: 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.

Kieri Solutions: When changing tooling, preserve the architecture, evidence and engagement requirements agreed with the advisor or assessor. Distinguish integrating existing systems from moving the workload into a new boundary; they involve different change and migration effort.

Copyright © 2026 Analog Informatics Corporation. All rights reserved.

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.

Kieri Solutions: The engagement can supply architecture or assessment work; enclave provisioning time belongs to the selected infrastructure and implementation plan. Agree the deliverables and schedule separately from software installation.

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.

Kieri Solutions: No validated whole-environment discovery/remediation duration for Kieri Solutions 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.

Kieri Solutions: When changing tooling, preserve the architecture, evidence and engagement requirements agreed with the advisor or assessor. 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.

Kieri Solutions: When changing tooling, preserve the architecture, evidence and engagement requirements agreed with the advisor or assessor. 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.

Kieri Solutions: Kieri supplies reference architecture and professional services. These are different from an operating security product; identify implementation and assessment engagement boundaries separately. The purchase must identify who executes the migration and who accepts the resulting environment.

Copyright © 2026 Analog Informatics Corporation. All rights reserved.

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.

Kieri Solutions: The published material reviewed for Kieri Solutions 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.

Kieri Solutions: The published material reviewed for Kieri Solutions 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.

Kieri Solutions: Kieri Solutions is represented here by its published Documentation, reference architecture and assessment services 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.

Kieri Solutions: The relevant fit question is: A reference architecture and an assessment need an operating security platform underneath them. 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.

Kieri Solutions: Demonstrate the records the assessor needs while keeping operational authority with the customer. Require the supplier to perform the comparable workflow on its proposed edition and retain the observed result.

Copyright © 2026 Analog Informatics Corporation. All rights reserved.

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.

Kieri Solutions: This review does not contain independently verified Kieri Solutions 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.

Kieri Solutions: The documented scope is Documentation, reference architecture and assessment services, 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.

Kieri Solutions: The published offering currently describes CMMC documentation, GCC High reference architecture, readiness and formal assessment offerings. 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.

Kieri Solutions: The published material reviewed for Kieri Solutions 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.

Kieri Solutions: Kieri's assessment service is complementary, not an auditor that AIC software replaces. Validate the specific connector, export format or service relationship and its permissions before presenting coexistence as turnkey.

Copyright © 2026 Analog Informatics Corporation. All rights reserved.

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 Kieri Solutions agreement and service dependencies separately before relying on a similar continuity outcome.

Kieri Solutions: Retain the documentation and engagement records the contract permits the customer to keep. Review continuity, intellectual-property rights and any required service handover if the supplier changes ownership or direction. The customer implementation and the professional engagement have different continuity responsibilities.

Sources and Next Step

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

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

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

Updated supplier deployment references

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

- https://www.kieri.com/

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

Copyright © 2026 Analog Informatics Corporation. All rights reserved.