COMPETITIVE ANALYSIS

Analog Informatics vs. Drata — Competitive Analysis

Teams answer the same control question in several systems while administrators work in another.

Published October 17, 2026; wording revised October 31, 2026

Analog Informatics Corporation

analoginfo.com

Copyright © 2026 Analog Informatics Corporation. All rights reserved.

Operate the Controls. Build the Audit Evidence.

An audit needs evidence that security controls operate in practice. Privilege management, privileged identity management, privileged user management, and session recording connect who received access, what they were permitted to do, and what actually happened.

AIC brings these enterprise security capabilities together with built-in training and attestation. These systems feed the audit package directly: approved access, credential activity, recorded sessions, remediation results, training records, and attestations become evidence of the controls your organization operates.

The integration is the advantage. Your team operates the controls and produces their evidence in the same platform. Where a separate audit package relies on external security tools, the evidence must arrive through maintained integrations, exports, or manual collection. Compare the actual workflow: which controls does the platform operate itself, which records does it collect automatically, and what must your staff copy or reconcile?

Keep an external GRC system where it serves broader obligations. AIC can feed that system while retaining the operational controls and their evidence in your environment.

Teams answer the same control question in several systems while administrators work in another. Generate access, session and configuration evidence from the security controls themselves.

AIC is customer-deployed software for on-premises and cloud assets, with customer control of credentials and compliance evidence. The supplier comparison below separates hosting, asset coverage and operational responsibility.

Alternatives and switching

What are the best alternatives to Drata?

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.

Drata: For the GRC and audit software portion of the purchase, shortlist Vanta, Secureframe, Thoropass, Sprinto. 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.

Which companies compete with Drata?

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.

Drata: Vanta, Secureframe, Thoropass, Sprinto are adjacent offerings in this comparison set. They overlap in different ways with Drata; they are not identical replacements. AIC overlaps where privileged controls, remediation and security evidence are the required outcome.

How does AIC compare with Drata?

AIC: AIC combines discovery and management of human and non-human identities with controlled access, automated collection, remediation and reporting. Passwords, SSH keys, certificates and API keys are in scope. Customers retain control of the deployed environment, credentials and evidence.

Copyright © 2026 Analog Informatics Corporation. All rights reserved.

Drata: Drata emphasizes CMMC controls, continuous evidence and defined ownership across compliance programs. Compare this with AIC's customer-deployed operating controls and the required evidence flow. The specific purchasing difference is: Generate access, session and configuration evidence from the security controls themselves.

Can AIC replace Drata, 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.

Drata: Keep enterprise-wide compliance programs in Drata where they serve broader obligations; supply operational evidence through an agreed interface.

Why would I switch from Drata?

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.

Drata: Teams answer the same control question in several systems while administrators work in another. A change is justified when the pilot resolves that problem and the transition preserves required functions.

Is there a self-hosted alternative to Drata?

AIC: Yes. AIC is commercial software deployed in your environment, on-premises or in your own cloud account. Its documented hosting options include disconnected deployments. Other vendors may also offer self-hosting; compare the actual edition.

Drata: AIC is a self-hosted option for the overlapping security work. The offering reviewed is Cloud compliance platform. Select the specific product and edition before assigning hosting responsibilities; managed assets and the management platform can be in different places. A self-hosted edition of this exact offering has not been established in the material reviewed; request a written deployment architecture if that is mandatory.

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.

Drata: The published scope combines CMMC controls, continuous evidence and defined ownership across compliance programs. 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.

Drata: The functions to preserve are CMMC controls, continuous evidence and defined ownership across compliance programs. The potential gain from AIC is customer-operated control and evidence in the same workflow. Map shared controls and evidence retention first, then pilot one scope before changing the compliance

Copyright © 2026 Analog Informatics Corporation. All rights reserved.

system of record.

Capabilities and coverage

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.

Drata: This is Cloud compliance platform, so evaluate it for that role. The stated product scope does not establish that it covers every organizational duty, infrastructure dependency and application in your environment.

Which features are included, and which require another product?

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

Drata: The published capability summary is CMMC controls, continuous evidence and defined ownership across compliance programs. 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.

Drata: The published material reviewed for Drata 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.

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.

Drata: The published material reviewed for Drata 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.

Copyright © 2026 Analog Informatics Corporation. All rights reserved.

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.

Drata: The published material reviewed for Drata does not specify discovery of previously unknown privileged credentials, rather than asset inventory or integration-fed evidence. Ask for a discovery run that produces a new account, its owner and target dependency, not only a compliance dashboard.

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.

Drata: The published material reviewed for Drata does not specify the complete lifecycle of service accounts and AI-agent identities. Identify the underlying identity, target application, discovery method and rotation/revocation operation, then test that chain.

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.

Drata: The published material reviewed for Drata 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.

Drata: Drata describes control testing, linked evidence, ownership and POA&M oversight. Those workflows do not establish which changes it executes on your specific hosts; require an actual failing-control repair demonstration.

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.

Drata: The published material reviewed for Drata does not specify credential-hidden privileged sessions to the customer’s target systems. Demonstrate the administrative connection, not only single sign-on to a collaboration or GRC portal. Identify any additional PAM product required.

Copyright © 2026 Analog Informatics Corporation. All rights reserved.

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.

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

Deployment and customer control

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

AIC: AIC supplies customer-deployed commercial software. The customer or its selected provider operates it. Do not price that as though AIC were also supplying a staffed managed security operation.

Drata: The offering reviewed is Cloud compliance platform. Select the specific product and edition before assigning hosting responsibilities; managed assets and the management platform can be in different places.

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

AIC: Yes. Deploy on customer hardware or supported VMs in the customer's cloud account. The platform documentation distinguishes server hosting from credential-management targets; cloud hosting remains subject to the selected infrastructure and contract requirements.

Drata: The published material reviewed for Drata does not specify a customer-hardware or customer-account deployment of the entire named offering. Ask which components remain vendor-hosted and which may run in your account; a local connector does not make the whole service self-hosted.

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

AIC: The supported-platforms document lists the full product for air-gapped networks without Internet connectivity. Design offline updates, time services, licensing and recovery for that deployment. Email/text alerts require their respective communication paths; an isolated network cannot deliver them externally without a permitted route.

Drata: The published material reviewed for Drata does not specify fully disconnected operation, including license validation, authentication and updates. Require an offline test rather than infer air-gap support from self-hosting or a local agent. Document which functions stop when external connectivity is removed.

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

AIC: Credentials and compliance evidence reside in the customer-deployed environment and its chosen storage/backup architecture. Include replicated logs, exports and backups in the data map. Customer deployment does not automatically determine every external notification or integration destination.

Drata: The offering reviewed is Cloud compliance platform. Select the specific product and edition before assigning hosting responsibilities; managed assets and the management platform can be in different places. The reviewed architecture does not fully resolve storage/replication locations for credentials, evidence, logs and backups. Obtain the data-flow and hosting schedule for the exact edition, including subprocessors and optional integrations.

Copyright © 2026 Analog Informatics Corporation. All rights reserved.

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

AIC: Access is assigned to customer-authorized roles and delegated operators. Establish named administrators, scoped reviewer access and approval for support sessions. The support-access method depends on the deployment; configure and record it rather than granting standing administrative access by default.

Drata: The published material reviewed for Drata does not specify the exact supplier-support access, key custody and privileged access approval controls for the proposed tenant. Request the access model and contractual commitments, including support elevation, audit records and subprocessors. SaaS does not by itself mean the customer has no data control.

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

AIC: Customers can export credentials, audit logs and compliance evidence in usable formats. Documented evidence outputs include binder PDF and OSCAL. Data can still be exported from an installation after its license expires, although licensed operation stops. Include the required export formats, backups and retention settings in the exit plan.

Drata: The published material reviewed for Drata 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. The customer can select an MSP or qualified provider to operate the software while retaining control of the environment. Give the operator scoped access and retain customer oversight of approvals, records and recovery.

Drata: The published material reviewed for Drata 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.

What happens if the vendor’s service is unavailable?

AIC: Credential and session services can remain available during Internet or license-service outages in a supported customer-deployed configuration. Local infrastructure and identity dependencies must remain available; external email/text delivery needs a working communication path. A temporary connectivity outage is different from license expiry: operation stops when the license expires, while data export remains available.

Drata: The published material reviewed for Drata does not specify the exact behavior of every component during a service or connectivity outage. Obtain availability/recovery commitments and test authentication, existing sessions, evidence access and emergency administration. An uptime percentage alone does not describe operational continuity.

CMMC and continuous compliance

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.

Copyright © 2026 Analog Informatics Corporation. All rights reserved.

Drata: 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.

Drata: Drata's CMMC description includes shared controls, evidence, owners and POA&M oversight. That is compliance-program support; obtain the customer's actual control/responsibility matrix to distinguish documentation from operating controls.

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.

Drata: 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.

Drata: Drata describes continuous evidence and control monitoring. Connector coverage and control ownership determine what is collected automatically; organizational procedures and unconnected systems still need evidence owners.

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.

Drata: Drata describes control testing, linked evidence, ownership and POA&M oversight. Those workflows do not establish which changes it executes on your specific hosts; require an actual failing-control repair demonstration. 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.

Drata: The published material reviewed for Drata 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

Copyright © 2026 Analog Informatics Corporation. All rights reserved.

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.

Drata: 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.

Drata: The offering's framework/control workflows may support reuse. Verify the actual frameworks, editions and crosswalks you need; reusing one control record is not the same as treating different standards as identical.

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.

Drata: Keep enterprise-wide compliance programs in Drata where they serve broader obligations; supply operational evidence through an agreed interface. An integration needs an identified API/export, matching control identifiers and an owner; a generic partnership claim is not a working data connection.

Cost and value

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.

Drata: The published material reviewed for Drata 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.

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

Copyright © 2026 Analog Informatics Corporation. All rights reserved.

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.

Drata: The published material reviewed for Drata 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.

Drata: The published material reviewed for Drata 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.

Drata: 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.

Drata: No independently verified staffing estimate for your Drata 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.

Drata: Potential consolidation follows the documented scope: CMMC controls, continuous evidence and defined ownership across compliance programs. 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.

Copyright © 2026 Analog Informatics Corporation. All rights reserved.

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.

Drata: The published material reviewed for Drata 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.

Drata: 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.

Implementation and migration

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.

Drata: Map shared controls and evidence retention first, then pilot one scope before changing the compliance system of record. 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.

Drata: The published material reviewed for Drata 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.

Copyright © 2026 Analog Informatics Corporation. All rights reserved.

Drata: No validated deployment-wide discovery/remediation duration for Drata 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.

Drata: Map shared controls and evidence retention first, then pilot one scope before changing the compliance system of record. 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.

Drata: Map shared controls and evidence retention first, then pilot one scope before changing the compliance system of record. 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.

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

What training, deployment guides, and support are included?

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

Drata: The published material reviewed for Drata 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.

Copyright © 2026 Analog Informatics Corporation. All rights reserved.

Drata: The published material reviewed for Drata 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.

Vendor credibility and fit

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.

Drata: Drata is represented here by its published Cloud compliance platform offering. The reviewed evidence does not establish an independently checked duration of support for your exact environment; ask for relevant delivery history rather than infer it from brand age.

Does it understand organizations like ours?

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

Drata: The relevant fit question is: Teams answer the same control question in several systems while administrators work in another. 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.

Drata: Trace an access approval through session activity, revocation and the resulting 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.

Drata: This review does not contain independently verified Drata 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.

Copyright © 2026 Analog Informatics Corporation. All rights reserved.

Drata: The documented scope is Cloud compliance platform, with edition-specific limits. Unverified target support, export completeness, outage behavior and contractual entitlements remain explicit procurement checks; resolve them in the technical evaluation and contract.

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

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

Drata: The published offering currently describes CMMC controls, continuous evidence and defined ownership across compliance programs. 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.

Drata: The published material reviewed for Drata 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.

Drata: Keep enterprise-wide compliance programs in Drata where they serve broader obligations; supply operational evidence through an agreed interface. Validate the specific connector, export format or service relationship and its permissions before presenting coexistence as turnkey.

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

AIC: Customers retain control of their deployed environment, credentials and evidence. AIC software stops operating when its license expires, but data can still be exported from the expired installation. Customer deployment does not mean perpetual licensed operation. Maintain tested backups and independent emergency access, and include exports in the exit plan.

Drata: An acquisition or strategy change does not by itself determine your rights. The reviewed Drata material does not establish a perpetual right to use all components or a complete exit guarantee. Retain the current agreement, renewal/termination provisions, exports and a tested continuity plan.

Sources and Next Step

- Provider source 1
- Provider source 2

Copyright © 2026 Analog Informatics Corporation. All rights reserved.

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

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

Copyright © 2026 Analog Informatics Corporation. All rights reserved.