COMPARISON ANALYSIS

Analog Informatics CMMC Software Scorecard

Compare 45 CMMC and security offerings across deployment, privileged controls, evidence, costs and 61 buyer questions, including disconnected work.

Deployment and customer-control revision: November 20, 2026

Scope: CMMC

Analog Informatics Corporation

View the related production resource

Copyright © 2026 Analog Informatics Corporation. All rights reserved.

Analysis date: October 17, 2026

Find a Comparison

- Aeroplicity
- Apptega
- Ardalyst Tesseract
- AWS GovCloud
- Axio360
- BeyondTrust
- C3 Integrated Solutions
- Cocoon Data
- ComplyUp by Exostar
- ControlMap
- Cuick Trac
- CyberArk
- CyberSaint CyberStrong
- CyberSheath
- Cyturus
- Delinea
- Drata
- EgnyteGov
- Exostar
- FutureFeed
- Google Workspace and Assured Workloads
- Hyperproof
- Ignyte
- KeeperPAM
- Kieri Solutions
- Kiteworks
- Microsoft GCC High and Azure Government
- Mycroft

Copyright © 2026 Analog Informatics Corporation. All rights reserved.

- NeoSystems
- NeQter Labs
- NtelSec CUI Vault
- One Identity Safeguard
- Paramify
- PreVeil
- RegDOX
- RegScale
- Scrut
- Secureframe
- Sentinel Blue
- Sprinto
- Summit 7
- Thoropass
- Totem HRDN-IT
- Vanta
- Virtru

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.

Comparison source revision: November 20, 2026

Copyright © 2026 Analog Informatics Corporation. All rights reserved.

Choose who controls the software and secrets

Use this 45-offering matrix to distinguish operating security controls, cloud hosting, compliance programs and managed services. Customer control and disconnected operation are evaluated alongside the actual software and staffing scope.

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

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

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

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

Enterprise privilege, secrets and access options

These are Enterprise comparisons. They do not extend the CMMC package scope or assume that each product performs the same job.

Platform: AIC Enterprise Privilege Suite

Management and deployment: Customer-operated installable software: on premises, customer cloud, hybrid or air-gapped. Installation, licensing and updates can be performed without a network connection to AIC.

Strengths and suitable customers: Teams that need to operate credential changes, privilege use and supporting evidence under their own administration and deployment location.

Platform: CyberArk/Idira

Management and deployment: Both models are available: PAM Self-Hosted software and PAM SaaS. Other portfolio products have separate architecture and service duties. An implementation partner is a further operating arrangement, not the deployment model itself.

Strengths and suitable customers: CyberArk/Idira combines vaulting and rotation with session isolation, just-in-time access and endpoint controls across its selected products. It offers a Self-Hosted PAM path as well as SaaS. Organizations with established vault integrations can build on those investments instead of replacing them solely to gain local deployment. AIC fits a team seeking customer-operated privilege controls and corrective evidence across shared accounts and applications. CyberArk/Idira fits organizations extending an established identity-security program with its vault, endpoint, workload or cloud-access products. A team can retain a useful CyberArk vault while proving a specific AIC workflow before consolidation.

Copyright © 2026 Analog Informatics Corporation. All rights reserved.

Platform: Delinea

Management and deployment: Secret Server is available as On-Premises software or Cloud SaaS. Delinea manages the Cloud backend; the customer runs its distributed engines. A staffed service provider is a separate operational choice.

Strengths and suitable customers: Delinea Secret Server discovers local and domain accounts and common Windows dependencies. Its recorded-session options offer different levels of video, keystroke and process detail. Customers can select Cloud or On-Premises, and Delinea explicitly documents offline activation for air-gapped Secret Server installations. AIC fits teams seeking local authority across credential correction, privilege use and review evidence. Delinea fits organizations centered on Secret Server's vault, Windows dependency discovery and selected session-recording architecture, with a choice of customer operation or a managed backend. Evaluate each against the same service restart and failed-change recovery.

Platform: BeyondTrust

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

Strengths and suitable customers: BeyondTrust has distinct products for privileged credential management, vendor and employee remote access, and endpoint elevation. Password Safe is offered as a hosted service or customer-operated physical, virtual and private-cloud appliances, with marketplace deployment in AWS and Azure. Its broader access products are useful when third-party maintenance and endpoint policy are central requirements. AIC fits teams seeking customer-operated credential correction, privilege use and review evidence across applications. BeyondTrust fits organizations prioritizing a dedicated vendor-access program, endpoint least privilege or an established Password Safe installation. An organization can keep useful BeyondTrust access paths while testing AIC for a distinct account or site.

Platform: Keeper

Management and deployment: KeeperPAM is available as cloud-based PAM. Separately licensed Self-Managed Keeper runs an independent local tenant. A customer-run Gateway for the cloud service is not equivalent to moving the full tenant into the customer environment.

Strengths and suitable customers: Keeper connects a familiar credential vault to password rotation, privileged connections, tunnels and secrets delivery. Its documented rotation updates Windows service and scheduled-task logins. Beyond the cloud PAM offering, Self-Managed Keeper provides an independent local tenant for sensitive and air-gapped networks; it is more than a local Gateway for a cloud vault. AIC fits teams seeking customer-operated account correction, privilege use and review evidence across systems. Keeper fits teams extending their vault and secrets workflows into rotation, connections and tunnels, or selecting a separate Self-Managed Keeper tenant for a restricted network. Trial the actual tenant type; cloud and self-managed features should not be assumed identical.

Platform: Akeyless

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

Copyright © 2026 Analog Informatics Corporation. All rights reserved.

Strengths and suitable customers: Akeyless can issue a temporary database login, renew an application certificate and broker a technician's session. It also discovers Windows services and IIS applications configured with explicit credentials and can restart them after changing the password. Akeyless also documents restricted or air-gapped Gateway placement and Gateway-terminated SAML sign-ins, while its central platform remains SaaS. AIC suits teams that want to operate the management service, automate changes across dependent systems and review privileged work locally. Akeyless suits teams that want managed credential issuance, access to existing vaults and brokered sessions through one cloud service. Organizations with both needs can evaluate the same application on each platform before choosing one or dividing responsibility.

Platform: Tailscale

Management and deployment: Tailscale operates the network coordination service. The customer runs each PAM connector with access to its targets and configures the grants in Tailscale's administrative console.

Strengths and suitable customers: In the Tailscale PAM beta, a manager can approve a request for a specific database in Slack. The contractor can use a supported database client without receiving the database password, and a reviewer can inspect the query log. A separate grant setting limits the duration of SSH and database sessions. Tailscale suits a team that needs to connect engineers and build systems to private services. AIC suits an IT team responsible for privileged accounts, endpoint elevation and recovery after a failed change. A team that needs both can keep its private routes and choose which product will control each session.

Platform: Silverfort

Management and deployment: Silverfort lists on-premises, SaaS and hybrid deployment models. Managed operation is also available through providers, as illustrated by ITC Secure's work for a UK financial services company. The provider's operating responsibilities belong in the services agreement.

Strengths and suitable customers: Silverfort can challenge administrators who sign in to a legacy application through a supported directory and restrict a service account to approved source and destination systems. Its Privileged Access Security product can enable a domain administrator account for an approved window. An on-premises appliance can also enforce MFA with FIDO2 hardware tokens on an isolated network. The hospital's identity team has a reason to choose Silverfort if it needs to challenge direct directory sign-ins across older applications. The application owner has a reason to choose AIC if the team must also update service credentials, grant temporary rights and document maintenance. If both teams need those controls, test the directory policy and the maintenance procedure on the same job.

A customer connector does not by itself establish an independent management service. Keeper's separately documented Self-Managed Keeper and Delinea's offline activation are credited in their individual guides. Evaluate current modules, license validity, updates, recovery and administrator access for the actual order.

Evaluate current available functions and the selected edition. AIC's feature set is evolving, and the full competitor feature range is in scope for future releases; that scope is not a promise that a function is available today or committed for a particular release.

Compare 45 named offerings by their actual role. Some are operating security products; others are collaboration tools, GRC programs, infrastructure or professional services. This is a market shortlist, not a count of 45 independent corporations: ComplyUp is part of Exostar.

Copyright © 2026 Analog Informatics Corporation. All rights reserved.

AIC discovers and manages human and non-human 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 deploy the software in their own environment and retain control of credentials, logs and compliance evidence. Passwords, SSH keys, certificates and API keys are part of the credential-management scope.

Automated discovery, collection, remediation and reporting connect the security work to its evidence. Initial deployment produces a blast-radius report; administrators can fix one finding or all findings at their own pace, automatically or manually. Exceptions generate real-time events, including email and text notifications through available communication channels.

AIC CMMC Complete is sold in Level 1, Level 2, and Level 3 packages; see CMMC Pricing. Licensing uses systems, applications and users, not counts of human or non-human accounts. All customers receive free best-effort support; purchased enterprise agreements provide a four-hour response commitment, 24/7. See Enterprise Pricing and CMMC Pricing for current product prices.

Licensed operation stops at license expiry, but data export remains available. Temporary Internet or license-service outages are a separate continuity question, addressed in the answers below.

Operating Models and Transition Decisions

Offering: Vanta

Deployment: Cloud compliance platform

AIC Fit: Connect credential rotation, approved sessions and verified repairs to the control record.

Transition: Export control mappings, evidence history and owner assignments; prove that the replacement preserves required audit workflows.

Offering: Drata

Deployment: Cloud compliance platform

AIC Fit: Generate access, session and configuration evidence from the security controls themselves.

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

Offering: Secureframe

Deployment: Compliance platform with customer-cloud enclave provisioning

AIC Fit: Compare customer-deployed credential, session, configuration and evidence functions across the actual systems in scope.

Transition: Preserve the cloud boundary and SSP, then test supported operating systems, administrative paths and evidence exports before changing platforms.

Copyright © 2026 Analog Informatics Corporation. All rights reserved.

Offering: Thoropass

Deployment: Compliance software and audit services

AIC Fit: Combine authorized remediation, retesting and audit evidence with built-in engagement workflows.

Transition: Separate the software subscription, evidence archive and audit-service agreement; move only the functions the new operating model replaces.

Offering: Sprinto

Deployment: Cloud trust and compliance platform

AIC Fit: Operate privileged identities and sessions inside the customer's environment and preserve their control evidence.

Transition: Inventory integrations and obligation mappings before consolidating; keep the original evidence lineage available.

Offering: Scrut

Deployment: Cloud security and compliance platform

AIC Fit: Connect the finding to supported remediation, a rescan and retained control-state history.

Transition: Map asset identifiers and evidence ownership, then validate that findings remain traceable after a staged transition.

Offering: Hyperproof

Deployment: Enterprise compliance operations platform

AIC Fit: Provide credential management, recorded access and configuration evidence tied to the work.

Transition: Preserve control crosswalks, request history and evidence retention before changing the system of record.

Offering: Mycroft

Deployment: Integrated security and compliance service/platform

AIC Fit: Evaluate AIC's customer-operated software, privileged controls and integrated evidence against Mycroft's operating model.

Transition: Identify which monitoring, response and device-management responsibilities will move to internal staff or the chosen MSP.

Offering: FutureFeed

Deployment: CMMC program-management platform

Copyright © 2026 Analog Informatics Corporation. All rights reserved.

AIC Fit: Generate privileged-access and configuration records while operating the controls; connect them to built-in evidence requests.

Transition: Map SSP sections, objectives and evidence identifiers before replacing documentation workflows.

Offering: Paramify

Deployment: Compliance documentation platform

AIC Fit: Use approved, time-limited access and retained session evidence to support the implementation statements.

Transition: Export the documented boundary and implementation statements, then reconcile them with the actual deployed controls.

Offering: RegScale

Deployment: Continuous controls and compliance platform

AIC Fit: Generate operational evidence alongside credential rotation, session control and supported repairs.

Transition: Test an evidence handoff with identifiers, dates and control mappings before consolidating any workflow.

Offering: CyberSaint CyberStrong

Deployment: Cyber risk and compliance platform

AIC Fit: Control privileged credentials and sessions, then supply evidence of the corrective work.

Transition: Preserve risk models and reporting obligations while introducing the security controls that produce current evidence.

Offering: Apptega

Deployment: Compliance platform for organizations and providers

AIC Fit: Operate a repeatable customer-deployed security kit with privileged-access and configuration records.

Transition: Separate portfolio reporting from each customer's security boundary and retention requirements.

Offering: ControlMap

Deployment: Compliance workflow platform

AIC Fit: Run supported security controls and collect their evidence in the same operating workflow.

Transition: Preserve objective-level evidence and responsibility mappings; check framework requirements before moving a program.

Copyright © 2026 Analog Informatics Corporation. All rights reserved.

Offering: ComplyUp by Exostar

Deployment: Assessment and documentation platform

AIC Fit: Combine the operational controls with audit requests, evidence and document lifecycle.

Transition: Preserve policy versions, POA&Ms and assessment history before consolidating documentation.

Offering: Cyturus

Deployment: Control-based GRC platform

AIC Fit: Attach privileged-access and configuration evidence to the operational work that changes the control state.

Transition: Map control identities and risk decisions before changing collection or reporting workflows.

Offering: Ignyte

Deployment: Compliance platform and professional services

AIC Fit: Combine credential control, recorded administration, configuration findings and retained evidence.

Transition: Preserve documentation and service responsibilities; agree which security functions internal IT or the MSP will operate.

Offering: Axio360

Deployment: Cyber risk assessment platform

AIC Fit: Use privileged controls and configuration history to support the risk and assessment record.

Transition: Maintain historical assessments and risk assumptions while validating the new evidence sources.

Offering: PreVeil

Deployment: Encrypted email/files plus managed VDI option

AIC Fit: Evaluate customer-deployed software with privileged controls, configuration evidence, training records and built-in GRC.

Transition: Inventory mail, files, external sharing, application licensing and endpoint boundaries; have the customer or MSP plan the transition.

Offering: NtelSec CUI Vault

Deployment: Provider-managed Azure Government/GCC High VDI

AIC Fit: Choose customer-operated infrastructure and AIC's privileged access, configuration and evidence workflows where local control matters.

Copyright © 2026 Analog Informatics Corporation. All rights reserved.

Transition: Plan data export, user identities, application compatibility and the customer/MSP operating responsibilities before leaving a managed service.

Offering: Kiteworks

Deployment: Secure content platform with on-premises, cloud and hybrid options

AIC Fit: Evaluate integrated privileged access, secure sharing, configuration evidence and GRC within the required boundary.

Transition: Inventory automated transfers, external recipients, retention and integrations before changing collaboration tools.

Offering: Virtru

Deployment: Data-centric email and file protection

AIC Fit: Add credential and session controls, configuration checks and evidence alongside the collaboration workflow.

Transition: Map recipients, encryption dependencies and data handling before moving collaboration or adding the security layer.

Offering: Aeroplicity

Deployment: Aerospace/defense applications and cloud desktops

AIC Fit: Choose customer infrastructure for the workload and evaluate AIC's privileged controls and integrated evidence.

Transition: Inventory application data, workflows, VM utilization and integration dependencies before a staged transition.

Offering: RegDOX

Deployment: Secure repository and browser-based computing enclave

AIC Fit: Compare AIC's customer-deployed security controls and evidence with the exact RegDOX package under consideration.

Transition: Map application access, data export and endpoint restrictions before moving away from the hosted workspace.

Offering: EgnyteGov

Deployment: Secure content enclave and compliance workflows

AIC Fit: Connect privileged identity and session controls with configuration and compliance evidence.

Transition: Preserve labels, sharing permissions, file history and retention when evaluating a content migration.

Copyright © 2026 Analog Informatics Corporation. All rights reserved.

Offering: Cocoon Data

Deployment: Encrypted file-sharing service

AIC Fit: Evaluate a customer-operated platform that combines those controls with secure sharing and evidence.

Transition: Map sharing permissions, external identities and retention before changing the repository.

Offering: Exostar

Deployment: Managed GCC High enclave and secure desktop

AIC Fit: Evaluate AIC software operated by the customer or its chosen MSP instead of a provider-operated enclave.

Transition: Plan responsibility transfer, data exports, identities and application licensing before moving the enclave.

Offering: Cuick Trac

Deployment: Beryllium InfoSec managed virtual enclave

AIC Fit: Compare a customer-deployed AIC kit plus scoped MSP services against the managed enclave bundle.

Transition: Identify monitoring, incident-response and documentation duties that must be reassigned during a move.

Offering: Ardalyst Tesseract

Deployment: Cybersecurity program and managed services

AIC Fit: Offer AIC's integrated controls and evidence to a customer or partner prepared to operate the environment.

Transition: Assign ownership for monitoring, recovery, documentation and migration before replacing a managed program.

Offering: Summit 7

Deployment: Microsoft-focused managed IT, security and GRC services

AIC Fit: Supplement Microsoft environments with AIC credential, session and evidence controls or build a customer-operated alternative.

Transition: Transfer responsibilities explicitly, including support, SOC coverage and policy ownership, before changing providers.

Offering: CyberSheath

Deployment: Managed cloud enclave and security services

Copyright © 2026 Analog Informatics Corporation. All rights reserved.

AIC Fit: Evaluate AIC's customer-operated controls and evidence with a separately scoped internal or MSP service model.

Transition: Document the handover of monitoring, incident response, backups and access administration before transition.

Offering: C3 Integrated Solutions

Deployment: Managed or guided CMMC implementation

AIC Fit: Provide integrated security software for the customer's chosen operating model.

Transition: Preserve the reference architecture and responsibility map while selecting which functions to operate with AIC.

Offering: Sentinel Blue

Deployment: Integrated managed IT, security and compliance services

AIC Fit: Evaluate AIC's integrated software with customer-selected service delivery.

Transition: Scope the transfer of SOC, IT support and governance responsibilities before replacing services.

Offering: NeoSystems

Deployment: Managed security, IT and enclave services

AIC Fit: Use explicit control ownership with integrated privileged access, configuration findings and evidence.

Transition: Inventory service dependencies and assign named owners before changing the security platform or provider.

Offering: Totem HRDN-IT

Deployment: Hardened on-premises PC enclave and planning tool

AIC Fit: Evaluate AIC's broader credential, session and configuration workflows for the required deployment size.

Transition: Preserve the existing narrow CUI boundary while testing additional systems and administrative paths.

Offering: NeQter Labs

Deployment: Security and compliance tooling

AIC Fit: Evaluate integrated privileged access and supported repairs alongside control evidence.

Transition: Map existing findings, log sources and compliance records before changing tools.

Offering: Microsoft GCC High and Azure Government

Deployment: Government cloud productivity and infrastructure

Copyright © 2026 Analog Informatics Corporation. All rights reserved.

AIC Fit: Supplement Microsoft with supported credential rotation, session control, command restrictions and integrated evidence.

Transition: Map identities, applications, cloud responsibilities and operational controls before changing any tenant or workload.

Offering: AWS GovCloud

Deployment: Cloud infrastructure

AIC Fit: Run supported AIC software in the selected architecture and operate its privileged controls and evidence.

Transition: Treat a cloud move as an infrastructure project; preserve security logs, identity controls and evidence continuity.

Offering: Google Workspace and Assured Workloads

Deployment: Collaboration and cloud infrastructure

AIC Fit: Add supported privileged-access and configuration evidence where the customer needs it.

Transition: Inventory data flows, eligible services and external-system controls before moving workloads.

Offering: CyberArk

Deployment: Privileged-access security platform

AIC Fit: Compare AIC's integrated privileged controls with configuration evidence, training records and built-in GRC.

Transition: Pilot account discovery, rotation dependencies, emergency access and session retention before moving vault workloads.

Offering: Delinea

Deployment: Privileged credential and access platform

AIC Fit: Compare AIC's credential and session functions together with configuration findings and evidence workflows.

Transition: Test password-change dependencies, service accounts and recovery paths before moving managed credentials.

Offering: BeyondTrust

Deployment: Privileged access and password security

AIC Fit: Evaluate AIC's privileged workflow alongside built-in control mappings, findings and audit evidence.

Transition: Preserve recordings, approval history, account dependencies and emergency access during a staged change.

Copyright © 2026 Analog Informatics Corporation. All rights reserved.

Offering: KeeperPAM

Deployment: Cloud-based PAM or independent Self-Managed Keeper

AIC Fit: Compare Self-Managed Keeper's independent tenant with AIC's supported local credential, session and evidence functions.

Transition: Validate secret migration, rotations, gateway dependencies and session retention before transition.

Offering: One Identity Safeguard

Deployment: Privileged password and session products

AIC Fit: Compare AIC's privileged workflow with its configuration checks, evidence requests and built-in GRC.

Transition: Map passwords, protocols, recordings and reviewer access before moving any production administration.

Offering: Kieri Solutions

Deployment: Documentation, reference architecture and assessment services

AIC Fit: Use AIC to operate supported security controls and provide evidence to the customer's advisors and assessors.

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

Capabilities by Offering

Offering: Vanta

Privileged Credentials and Access: The published material reviewed for Vanta 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. The published material reviewed for Vanta 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.

Remediation: The published material reviewed for Vanta 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.

Evidence: Vanta collects evidence through integrations and runs automated tests. Coverage depends on connected systems and the required artifact; retain separately collected organizational records and inspect failed/stale checks.

Copyright © 2026 Analog Informatics Corporation. All rights reserved.

Offering: Drata

Privileged Credentials and Access: 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. 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.

Remediation: 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.

Evidence: 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.

Offering: Secureframe

Privileged Credentials and Access: The published material reviewed for Secureframe 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. The published material reviewed for Secureframe 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.

Remediation: Navigator applies supported enclave configurations automatically, validates them with tests and flags drift. Compare initial configuration with the corrective actions available after deployment.

Evidence: Configuration evidence feeds automated tests; personnel and configuration data remain synchronized. Policies and other organizational evidence still have separate owners.

Offering: Thoropass

Privileged Credentials and Access: The published material reviewed for Thoropass 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. The published material reviewed for Thoropass 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.

Remediation: The published material reviewed for Thoropass 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.

Evidence: Thoropass documents automated collection through integrations and audit workflows. Retain the professional audit engagement separately when evaluating replacement of software.

Copyright © 2026 Analog Informatics Corporation. All rights reserved.

Offering: Sprinto

Privileged Credentials and Access: The published material reviewed for Sprinto 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. The published material reviewed for Sprinto 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.

Remediation: Sprinto describes automated actions and approval routing as part of continuous compliance. Compare the supported corrective actions with the actual credential and configuration changes your systems require.

Evidence: The offering describes Continuous compliance workflows, integrations, risk management and trust-center functions. Determine which evidence is collected automatically, which requires integrations and which still needs a person. Test freshness, failed collection and historical traceability; a current dashboard is not necessarily a complete audit record.

Offering: Scrut

Privileged Credentials and Access: The published material reviewed for Scrut 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. The published material reviewed for Scrut 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.

Remediation: Scrut documents finding-to-ticket handoff and recommended corrections. Its published material does not establish automatic execution of every target-system repair.

Evidence: The offering describes Control monitoring, asset visibility, evidence workflows and CMMC-related automation. Determine which evidence is collected automatically, which requires integrations and which still needs a person. Test freshness, failed collection and historical traceability; a current dashboard is not necessarily a complete audit record.

Offering: Hyperproof

Privileged Credentials and Access: The published material reviewed for Hyperproof 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. The published material reviewed for Hyperproof 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.

Remediation: The published material reviewed for Hyperproof 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.

Evidence: The offering describes CMMC templates, evidence collection, recurring control tests, task assignment and SSP reports. Determine which evidence is collected automatically, which requires integrations and which still needs a person. Test freshness, failed collection and historical traceability; a current dashboard is not necessarily a complete audit record.

Copyright © 2026 Analog Informatics Corporation. All rights reserved.

Offering: Mycroft

Privileged Credentials and Access: The published material reviewed for Mycroft 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. The published material reviewed for Mycroft 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.

Remediation: Mycroft markets automated remediation and combines security operations with GRC. Compare execution permissions, target coverage and approval controls; do not treat it as evidence-only software.

Evidence: The offering describes GRC, security operations and device-management positioning with AI agents and expert support. Determine which evidence is collected automatically, which requires integrations and which still needs a person. Test freshness, failed collection and historical traceability; a current dashboard is not necessarily a complete audit record.

Offering: FutureFeed

Privileged Credentials and Access: The published material reviewed for FutureFeed 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. The published material reviewed for FutureFeed 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.

Remediation: The published material reviewed for FutureFeed 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.

Evidence: The offering describes Control and objective tracking, accountability, SSP documentation and evidence exports. Determine which evidence is collected automatically, which requires integrations and which still needs a person. Test freshness, failed collection and historical traceability; a current dashboard is not necessarily a complete audit record.

Offering: Paramify

Privileged Credentials and Access: The published material reviewed for Paramify 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. The published material reviewed for Paramify 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.

Remediation: The published material reviewed for Paramify 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.

Evidence: The offering describes Gap assessment, SPRS tracking, SSP and POA&M automation and partner-delivered implementation options. Determine which evidence is collected automatically, which requires

Copyright © 2026 Analog Informatics Corporation. All rights reserved.

integrations and which still needs a person. Test freshness, failed collection and historical traceability; a current dashboard is not necessarily a complete audit record.

Offering: RegScale

Privileged Credentials and Access: The published material reviewed for RegScale 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. The published material reviewed for RegScale 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.

Remediation: The published material reviewed for RegScale 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.

Evidence: The offering describes Automated evidence, CMMC documentation, cross-framework mapping and OSCAL-oriented exports. Determine which evidence is collected automatically, which requires integrations and which still needs a person. Test freshness, failed collection and historical traceability; a current dashboard is not necessarily a complete audit record.

Offering: CyberSaint CyberStrong

Privileged Credentials and Access: The published material reviewed for CyberSaint CyberStrong 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. The published material reviewed for CyberSaint CyberStrong 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.

Remediation: CyberStrong describes remediation planning and risk-based prioritization. A plan or quantified risk decision is different from executing a password change or configuration correction; evaluate that execution path separately.

Evidence: The offering describes Continuous controls monitoring, cross-framework mapping and cyber risk analysis. Determine which evidence is collected automatically, which requires integrations and which still needs a person. Test freshness, failed collection and historical traceability; a current dashboard is not necessarily a complete audit record.

Offering: Apptega

Privileged Credentials and Access: The published material reviewed for Apptega 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. The published material reviewed for Apptega 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.

Remediation: The published material reviewed for Apptega 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.

Evidence: Apptega describes framework-based GRC and compliance workflows. Evaluate evidence integrations and the treatment of sensitive artifacts for the selected service boundary.

Offering: ControlMap

Privileged Credentials and Access: The published material reviewed for ControlMap 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. The published material reviewed for ControlMap 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.

Remediation: The published material reviewed for ControlMap 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.

Evidence: ControlMap documents automated evidence workflows, including Backup Radar proof feeding mapped controls. Coverage depends on tier and connected tools; test freshness and the evidence gaps outside those integrations.

Offering: ComplyUp by Exostar

Privileged Credentials and Access: The published material reviewed for ComplyUp by Exostar 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. The published material reviewed for ComplyUp by Exostar 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.

Remediation: The published material reviewed for ComplyUp by Exostar 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.

Evidence: The offering describes Assessment workflows, POA&Ms and policy generation; part of Exostar. Determine which evidence is collected automatically, which requires integrations and which still needs a person. Test freshness, failed collection and historical traceability; a current dashboard is not necessarily a complete audit record.

Offering: Cyturus

Privileged Credentials and Access: The published material reviewed for Cyturus 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. The published material reviewed for Cyturus 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.

Remediation: The published material reviewed for Cyturus 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.

Evidence: Cyturus documents conformity engagements against a shared control set. Compare control reuse, evidence relationships and corrective-work execution separately.

Offering: Ignyte

Privileged Credentials and Access: The published material reviewed for Ignyte 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. The published material reviewed for Ignyte 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.

Remediation: The published material reviewed for Ignyte 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.

Evidence: Ignyte documents platform automation, asset inventory and documentation workflows, alongside advisory and audit offerings. Separate software scope from contracted professional services.

Offering: Axio360

Privileged Credentials and Access: The published material reviewed for Axio360 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. The published material reviewed for Axio360 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.

Remediation: The published material reviewed for Axio360 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.

Evidence: The offering describes CMMC assessment reporting with SSP and POA&M exports. Determine which evidence is collected automatically, which requires integrations and which still needs a person. Test freshness, failed collection and historical traceability; a current dashboard is not necessarily a complete audit record.

Offering: PreVeil

Privileged Credentials and Access: The published material reviewed for PreVeil 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. The published material reviewed for PreVeil 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.

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

Copyright © 2026 Analog Informatics Corporation. All rights reserved.

Evidence: The offering describes Encrypted collaboration and a managed Windows VDI offering using AWS GovCloud and bundled security tools. Determine which evidence is collected automatically, which requires integrations and which still needs a person. Test freshness, failed collection and historical traceability; a current dashboard is not necessarily a complete audit record.

Offering: NtelSec CUI Vault

Privileged Credentials and Access: The published material reviewed for NtelSec CUI Vault 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. The published material reviewed for NtelSec CUI Vault 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.

Remediation: The published material reviewed for NtelSec CUI Vault 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.

Evidence: The offering describes Managed Windows desktop enclave with identity controls, monitoring, scanning and compliance documentation; a documented Trout partnership connects authorized physical assets. Determine which evidence is collected automatically, which requires integrations and which still needs a person. Test freshness, failed collection and historical traceability; a current dashboard is not necessarily a complete audit record.

Offering: Kiteworks

Privileged Credentials and Access: The published material reviewed for Kiteworks 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. The published material reviewed for Kiteworks 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.

Remediation: The published material reviewed for Kiteworks 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.

Evidence: The offering describes Controlled content exchange with multiple deployment choices. Determine which evidence is collected automatically, which requires integrations and which still needs a person. Test freshness, failed collection and historical traceability; a current dashboard is not necessarily a complete audit record.

Offering: Virtru

Privileged Credentials and Access: The published material reviewed for Virtru 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. The published material reviewed for Virtru 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.

Remediation: The published material reviewed for Virtru 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.

Evidence: The offering describes Encryption, access controls and secure collaboration for CUI. Determine which evidence is collected automatically, which requires integrations and which still needs a person. Test freshness, failed collection and historical traceability; a current dashboard is not necessarily a complete audit record.

Offering: Aeroplicity

Privileged Credentials and Access: The published material reviewed for Aeroplicity 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. The published material reviewed for Aeroplicity 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.

Remediation: The published material reviewed for Aeroplicity 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.

Evidence: The offering describes Collaboration and business applications, training features and published VM configurations. Determine which evidence is collected automatically, which requires integrations and which still needs a person. Test freshness, failed collection and historical traceability; a current dashboard is not necessarily a complete audit record.

Offering: RegDOX

Privileged Credentials and Access: The published material reviewed for RegDOX 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. The published material reviewed for RegDOX 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.

Remediation: The published material reviewed for RegDOX 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.

Evidence: The offering describes Secure Data Room and Compliant Computing Enclave options. Determine which evidence is collected automatically, which requires integrations and which still needs a person. Test freshness, failed collection and historical traceability; a current dashboard is not necessarily a complete audit record.

Copyright © 2026 Analog Informatics Corporation. All rights reserved.

Offering: EgnyteGov

Privileged Credentials and Access: The published material reviewed for EgnyteGov 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. The published material reviewed for EgnyteGov 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.

Remediation: The published material reviewed for EgnyteGov 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.

Evidence: The offering describes CUI collaboration, content classification and Compliance Center evidence mapping. Determine which evidence is collected automatically, which requires integrations and which still needs a person. Test freshness, failed collection and historical traceability; a current dashboard is not necessarily a complete audit record.

Offering: Cocoon Data

Privileged Credentials and Access: The published material reviewed for Cocoon Data 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. The published material reviewed for Cocoon Data 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.

Remediation: The published material reviewed for Cocoon Data 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.

Evidence: The offering describes Controlled file sharing, MFA and SaaS/custom-cloud options. Determine which evidence is collected automatically, which requires integrations and which still needs a person. Test freshness, failed collection and historical traceability; a current dashboard is not necessarily a complete audit record.

Offering: Exostar

Privileged Credentials and Access: The published material reviewed for Exostar 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. The published material reviewed for Exostar 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.

Remediation: The published material reviewed for Exostar 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.

Evidence: The offering describes Managed Microsoft 365 collaboration, identity controls and optional secure desktops. Determine which evidence is collected automatically, which requires integrations and which still needs a

Copyright © 2026 Analog Informatics Corporation. All rights reserved.

person. Test freshness, failed collection and historical traceability; a current dashboard is not necessarily a complete audit record.

Offering: Cuick Trac

Privileged Credentials and Access: The published material reviewed for Cuick Trac 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. The published material reviewed for Cuick Trac 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.

Remediation: The published material reviewed for Cuick Trac 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.

Evidence: The offering describes VDI, SIEM, encrypted collaboration, MFA and compliance-support documentation. Determine which evidence is collected automatically, which requires integrations and which still needs a person. Test freshness, failed collection and historical traceability; a current dashboard is not necessarily a complete audit record.

Offering: Ardalyst Tesseract

Privileged Credentials and Access: The published material reviewed for Ardalyst Tesseract 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. The published material reviewed for Ardalyst Tesseract 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.

Remediation: The published material reviewed for Ardalyst Tesseract 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.

Evidence: The offering describes Enclave setup, government-cloud licensing, documentation, detection and response services. Determine which evidence is collected automatically, which requires integrations and which still needs a person. Test freshness, failed collection and historical traceability; a current dashboard is not necessarily a complete audit record.

Offering: Summit 7

Privileged Credentials and Access: The published material reviewed for Summit 7 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. The published material reviewed for Summit 7 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.

Remediation: The published material reviewed for Summit 7 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.

Evidence: The offering describes Guardian IT management, Vigilance security services and Commander GRC advisory. Determine which evidence is collected automatically, which requires integrations and which still needs a person. Test freshness, failed collection and historical traceability; a current dashboard is not necessarily a complete audit record.

Offering: CyberSheath

Privileged Credentials and Access: The published material reviewed for CyberSheath 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. The published material reviewed for CyberSheath 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.

Remediation: The published material reviewed for CyberSheath 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.

Evidence: The offering describes Federal Enclave with managed security operations for CUI environments. Determine which evidence is collected automatically, which requires integrations and which still needs a person. Test freshness, failed collection and historical traceability; a current dashboard is not necessarily a complete audit record.

Offering: C3 Integrated Solutions

Privileged Credentials and Access: The published material reviewed for C3 Integrated Solutions 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. The published material reviewed for C3 Integrated Solutions 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.

Remediation: The published material reviewed for C3 Integrated 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.

Evidence: The offering describes Command and Catalyst services for enclave or enterprise environments. Determine which evidence is collected automatically, which requires integrations and which still needs a person. Test freshness, failed collection and historical traceability; a current dashboard is not necessarily a complete audit record.

Copyright © 2026 Analog Informatics Corporation. All rights reserved.

Offering: Sentinel Blue

Privileged Credentials and Access: The published material reviewed for Sentinel Blue 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. The published material reviewed for Sentinel Blue 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.

Remediation: The published material reviewed for Sentinel Blue 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.

Evidence: The offering describes Shield combines infrastructure, governance, readiness advisory and SOC services. Determine which evidence is collected automatically, which requires integrations and which still needs a person. Test freshness, failed collection and historical traceability; a current dashboard is not necessarily a complete audit record.

Offering: NeoSystems

Privileged Credentials and Access: The published material reviewed for NeoSystems 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. The published material reviewed for NeoSystems 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.

Remediation: The published material reviewed for NeoSystems 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.

Evidence: The offering describes NeoSecure combines NeoSec, NeoTech and NeoEnclave services. Determine which evidence is collected automatically, which requires integrations and which still needs a person. Test freshness, failed collection and historical traceability; a current dashboard is not necessarily a complete audit record.

Offering: Totem HRDN-IT

Privileged Credentials and Access: The published material reviewed for Totem HRDN-IT 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. The published material reviewed for Totem HRDN-IT 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.

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

Copyright © 2026 Analog Informatics Corporation. All rights reserved.

Evidence: The offering describes Small-business on-premises enclave with self-managed or provider-managed options. Determine which evidence is collected automatically, which requires integrations and which still needs a person. Test freshness, failed collection and historical traceability; a current dashboard is not necessarily a complete audit record.

Offering: NeQter Labs

Privileged Credentials and Access: The published material reviewed for NeQter Labs 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. The published material reviewed for NeQter Labs 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.

Remediation: The published material reviewed for NeQter Labs 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.

Evidence: The offering describes CMMC documentation, gap tracking, SSP, POA&M and compliance reporting. Determine which evidence is collected automatically, which requires integrations and which still needs a person. Test freshness, failed collection and historical traceability; a current dashboard is not necessarily a complete audit record.

Offering: Microsoft GCC High and Azure Government

Privileged Credentials and Access: The published material reviewed for Microsoft GCC High and Azure Government 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. The published material reviewed for Microsoft GCC High and Azure Government 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.

Remediation: The published material reviewed for Microsoft GCC High and Azure Government 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.

Evidence: The offering describes Microsoft services supporting CMMC through configured services and shared responsibilities. Determine which evidence is collected automatically, which requires integrations and which still needs a person. Test freshness, failed collection and historical traceability; a current dashboard is not necessarily a complete audit record.

Offering: AWS GovCloud

Privileged Credentials and Access: The published material reviewed for AWS GovCloud 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. The published material reviewed for AWS GovCloud 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.

Remediation: The published material reviewed for AWS GovCloud 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.

Evidence: The offering describes Government-region infrastructure with customer responsibility for workload security. Determine which evidence is collected automatically, which requires integrations and which still needs a person. Test freshness, failed collection and historical traceability; a current dashboard is not necessarily a complete audit record.

Offering: Google Workspace and Assured Workloads

Privileged Credentials and Access: The published material reviewed for Google Workspace and Assured Workloads 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. The published material reviewed for Google Workspace and Assured Workloads 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.

Remediation: The published material reviewed for Google Workspace and Assured Workloads 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.

Evidence: The offering describes CMMC guidance for eligible services, Assured Controls Plus and Assured Workloads boundaries. Determine which evidence is collected automatically, which requires integrations and which still needs a person. Test freshness, failed collection and historical traceability; a current dashboard is not necessarily a complete audit record.

Offering: CyberArk

Privileged Credentials and Access: CyberArk documents self-hosted secrets management for applications/scripts and cloud secret discovery. Human/non-human coverage is a comparison dimension, not an exclusive AIC feature. The offering includes privileged session/access functions. Demonstrate a session where the user never receives the target secret, then inspect the protocol and audit record; evaluate credential checkout separately.

Remediation: The published material reviewed for CyberArk 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.

Evidence: The offering describes Privileged credentials, sessions and SaaS or self-hosted deployment. Determine which evidence is collected automatically, which requires integrations and which still needs a person. Test freshness, failed collection and historical traceability; a current dashboard is not necessarily a complete audit record.

Copyright © 2026 Analog Informatics Corporation. All rights reserved.

Offering: Delinea

Privileged Credentials and Access: Delinea documents human and non-human user classifications. Match platform identities, Secret Server licenses and target credential functions to the proposed edition. Secret Server documents proxied privileged sessions and SSH session recording. Demonstrate credential hiding and permissions for the chosen launcher/protocol rather than assume every connection mode has identical behavior.

Remediation: The published material reviewed for Delinea 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.

Evidence: The offering describes Secret Server on-premises/cloud options and remote password changing. Determine which evidence is collected automatically, which requires integrations and which still needs a person. Test freshness, failed collection and historical traceability; a current dashboard is not necessarily a complete audit record.

Offering: BeyondTrust

Privileged Credentials and Access: Password Safe describes human and non-human credential/secret management. Validate the target types and application dependencies for service accounts and AI-agent identities. The offering includes privileged session/access functions. Demonstrate a session where the user never receives the target secret, then inspect the protocol and audit record; evaluate credential checkout separately.

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

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

Offering: KeeperPAM

Privileged Credentials and Access: KeeperPAM describes service-account rotation across on-premises and cloud environments. Its cloud-native management model must be distinguished from the location of managed assets. The offering includes privileged session/access functions. Demonstrate a session where the user never receives the target secret, then inspect the protocol and audit record; evaluate credential checkout separately.

Remediation: The published material reviewed for KeeperPAM 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.

Evidence: The offering describes Passwords, secrets, connection management, remote access and discovery. Determine which evidence is collected automatically, which requires integrations and which still needs a person. Test freshness, failed collection and historical traceability; a current dashboard is not necessarily a complete audit record.

Copyright © 2026 Analog Informatics Corporation. All rights reserved.

Offering: One Identity Safeguard

Privileged Credentials and Access: The published discovery scope includes service and machine credentials. Determine which management operations and licensed components cover each non-human target; discovery alone is not full lifecycle coverage. The offering includes privileged session/access functions. Demonstrate a session where the user never receives the target secret, then inspect the protocol and audit record; evaluate credential checkout separately.

Remediation: The published material reviewed for One Identity Safeguard 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.

Evidence: The offering describes Controlled, monitored and recorded administrator sessions. Determine which evidence is collected automatically, which requires integrations and which still needs a person. Test freshness, failed collection and historical traceability; a current dashboard is not necessarily a complete audit record.

Offering: Kieri Solutions

Privileged Credentials and Access: 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. 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.

Remediation: 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.

Evidence: 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 necessarily a complete audit record.

All 61 Buyer Questions

Each answer below uses the same wording as the individual supplier analysis. Publicly unresolved details are stated explicitly and are not scored as absent features.

Supplier Sources

Vanta

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

Copyright © 2026 Analog Informatics Corporation. All rights reserved.

Drata

- Provider source 1
- Provider source 2

Secureframe

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

Thoropass

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

Sprinto

- Provider source 1
- Provider source 2

Scrut

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

Hyperproof

- Provider source 1
- Provider source 2

Mycroft

- Provider source 1
- Provider source 2

FutureFeed

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

Copyright © 2026 Analog Informatics Corporation. All rights reserved.

Paramify

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

RegScale

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

CyberSaint CyberStrong

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

Apptega

- Provider source 1
- Provider source 2

ControlMap

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

ComplyUp by Exostar

- Provider source 1
- Provider source 2

Cyturus

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

Ignyte

- Provider source 1
- Provider source 2

Copyright © 2026 Analog Informatics Corporation. All rights reserved.

Axio360

- Provider source 1

PreVeil

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

NtelSec CUI Vault

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

Kiteworks

- Provider source 1
- Provider source 2

Virtru

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

Aeroplicity

- Provider source 1

RegDOX

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

EgnyteGov

- Provider source 1
- Provider source 2

Cocoon Data

- Provider source 1

Copyright © 2026 Analog Informatics Corporation. All rights reserved.

Exostar

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

Cuick Trac

- Provider source 1
- Provider source 2

Ardalyst Tesseract

- Provider source 1
- Provider source 2

Summit 7

- Provider source 1
- Provider source 2

CyberSheath

- Provider source 1

C3 Integrated Solutions

- Provider source 1
- Provider source 2

Sentinel Blue

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

NeoSystems

- Provider source 1

Totem HRDN-IT

- Provider source 1
- Provider source 2

NeQter Labs

- Provider source 1

Copyright © 2026 Analog Informatics Corporation. All rights reserved.

- Provider source 2
- Provider source 3

Microsoft GCC High and Azure Government

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

AWS GovCloud

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

Google Workspace and Assured Workloads

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

CyberArk

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

Delinea

- Provider source 1
- Provider source 2
- Provider source 3
- Provider source 4
- Provider source 5
- Provider source 6
- Provider source 7

BeyondTrust

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

Copyright © 2026 Analog Informatics Corporation. All rights reserved.

- Provider source 4

KeeperPAM

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

One Identity Safeguard

- Provider source 1
- Provider source 2
- Provider source 3
- Provider source 4
- Provider source 5

Kieri Solutions

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

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

Copyright © 2026 Analog Informatics Corporation. All rights reserved.