COMPARISON ANALYSIS

Analog Informatics CMMC Solutions Comparison

Choose CMMC software, infrastructure or services by the work required. Compare operating duties, secret control and cloud, local or air-gapped designs.

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.

AIC CMMC Complete™ is a standardized commercial software kit that customers deploy and operate. Run it on your own hardware and software, or on networking and virtual machines supplied by a commercial cloud provider. Your organization controls the environment and authorizes access for its staff, MSP, and qualified solution providers. Analog Informatics supplies the software and does not host or manage your CMMC systems.

Start with the work you need done: protect CUI collaboration, operate security controls, organize evidence, choose infrastructure, or hire ongoing administration. These approaches can complement each other.

Compare Customer-Deployed Software with SaaS Email and VDI · Where Each Approach Works Best

Confirm Hosting Costs and VDI Capacity

A per-user SaaS price does not explain the VDI capacity behind it. If a provider does not publish hosting charges or capacity limits, mark them as undisclosed and obtain a written quote. Do not assume unlimited desktops, compute, or storage.

• Are virtual desktops included, separately billed, or metered by session or usage? What is the total at your peak concurrent sessions?

• What CPU, RAM, storage, GPU, and persistent desktop sizes are available? What are the maximum sizes and upgrade costs?

• Which engineering, CAD/CAM, business applications, peripherals, and local file workflows are supported?

• What are the session-duration, idle timeout, storage, bandwidth, and data-transfer limits?

• What changes when you add named users, auditor or MSP accounts, sites, or workload capacity? AIC includes one email account per named user; extra named users are $15 per user per month.

• Who patches and monitors the environment, retains logs, handles incidents, restores backups, and supplies assessment evidence?

With AIC, you select and pay for your own infrastructure and any VDI platform. That makes the infrastructure choices visible to you; it does not make compute, storage, administration, or third-party licensing free.

AIC CMMC Complete™ Level 2

CUI email and file sharing, privileged credential vaulting, brokered sessions with command restriction, endpoint elevation, configuration compliance, training and attestation, and the Assessment Binder. The base kit includes 25 managed systems and the stated 25-person/user allowances; one email account per named user is included; extra named users are $15 per user per month. Confirm other add-on quantities in your quote. Session Recording is included only in Level 3.

Current package prices, add-ons, and purchase terms are on AIC CMMC Complete™ Pricing. Cloud or hardware, ongoing administration, and independent assessment fees are separate.

Compare by Purchase Decision

Published prices for different seat counts or service scopes are reference points, not a complete-cost ranking.

Copyright © 2026 Analog Informatics Corporation. All rights reserved.

Approach: PreVeil

Primary Scope: Encrypted CUI email and file sharing with compliance documentation.

Next Step: Compare Scope and Responsibilities

Approach: Virtru

Primary Scope: Email and file encryption integrated with existing collaboration tools.

Next Step: Compare Scope and Responsibilities

Approach: Totem

Primary Scope: Compliance software and advisory services for defense contractors.

Next Step: Compare Scope and Responsibilities

Approach: Vanta, Drata, and Secureframe

Primary Scope: Compliance automation and evidence workflows connected to other systems.

Next Step: Compare Scope and Responsibilities

Approach: One Identity

Primary Scope: Privileged access and identity governance products.

Next Step: Compare Scope and Responsibilities

Approach: Managed CMMC Services

Primary Scope: A provider operates tools and delivers ongoing compliance and administration services.

Next Step: Compare Scope and Responsibilities

Approach: Keeper

Primary Scope: Password management and privileged access through the appropriate KeeperPAM offering.

Next Step: Compare Scope and Responsibilities

Approach: Google Workspace

Primary Scope: A productivity and collaboration platform.

Next Step: Compare Scope and Responsibilities

Copyright © 2026 Analog Informatics Corporation. All rights reserved.

Approach: FutureFeed

Primary Scope: CMMC program documentation, control tracking, and assessment workflows.

Next Step: Compare Scope and Responsibilities

Approach: FedRAMP Cloud Services

Primary Scope: A cloud service with a defined authorization boundary and customer responsibility matrix.

Next Step: Compare Scope and Responsibilities

Approach: Exostar

Primary Scope: Managed Microsoft 365 collaboration and CMMC-related offerings.

Next Step: Compare Scope and Responsibilities

Approach: a DIY Microsoft 365 Environment

Primary Scope: A customer-designed combination of Microsoft licenses, security tools, processes, and evidence records.

Next Step: Compare Scope and Responsibilities

Approach: Delinea

Primary Scope: Privileged access products including Secret Server and Privilege Manager.

Next Step: Compare Scope and Responsibilities

Approach: CyberArk

Primary Scope: Privileged access and identity security products.

Next Step: Compare Scope and Responsibilities

Approach: BeyondTrust

Primary Scope: Privileged access products including Password Safe.

Next Step: Compare Scope and Responsibilities

Approach: Cuick Trac

Primary Scope: A hosted CUI enclave service.

Next Step: Compare Scope and Responsibilities

Copyright © 2026 Analog Informatics Corporation. All rights reserved.

Approach: AWS GovCloud

Primary Scope: Cloud infrastructure for eligible regulated workloads.

Next Step: Compare Scope and Responsibilities

Approach: Microsoft GCC High

Primary Scope: Microsoft productivity and collaboration services in a government cloud environment.

Next Step: Compare Scope and Responsibilities

Approach: Kiteworks

Primary Scope: Governed exchange of sensitive files and content.

Next Step: Compare Scope and Responsibilities

Build Your Purchase Checklist

Ask both providers to price the same CUI boundary: 25 users with one included email account per named user, 25 managed systems, and the same privileged administrators. Extra named users are $15 per user per month. Itemize software, hosting, setup, ongoing administration, assessment support, and existing licenses. A different user count or an unpublished price cannot establish which complete solution costs less.

Deployment, configuration, and FCI/CUI data migration are the client's responsibility, typically with an MSP or another qualified provider under the client's control. Infrastructure, third-party products, independent assessment, and separately agreed provider services are separate costs.

Open the Software Scorecard · Use the Sample RFP

Choose Your Next Step

Review the package entitlements, walk through your requirements, or ask us to scope a matched quote.

See CMMC Pricing

Request a Demo · Request a Quote · All CMMC Comparisons

Comparison source revision: November 20, 2026

Choose who controls the software and secrets

Separate security software from cloud infrastructure, collaboration services, compliance workflows and ongoing administration. Match the CUI boundary and required work to the named product, edition and people who will operate it.

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?

Copyright © 2026 Analog Informatics Corporation. All rights reserved.

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.

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

Copyright © 2026 Analog Informatics Corporation. All rights reserved.

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.

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

Copyright © 2026 Analog Informatics Corporation. All rights reserved.

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.

Choose the role and deployment of each offering

Offering: Aeroplicity

Documented operating role: Aerospace/defense applications and cloud desktops

Context for the comparison: Compare Aeroplicity's CUI collaboration offering with AIC's customer-run credential, session and remediation controls in local or air-gapped environments.

Offering: Apptega

Documented operating role: Compliance platform for organizations and providers

Context for the comparison: Compare Apptega's assessments and compliance collaboration with AIC's locally operated access, remediation and evidence for sensitive mission systems.

Copyright © 2026 Analog Informatics Corporation. All rights reserved.

Offering: Ardalyst Tesseract

Documented operating role: Cybersecurity program and managed services

Context for the comparison: Compare Ardalyst Tesseract's enclave and security services with AIC's customer-operated controls, secret custody and disconnected mission support.

Offering: AWS GovCloud

Documented operating role: Cloud infrastructure

Context for the comparison: Compare AWS GovCloud infrastructure with customer-operated AIC access controls, secret custody and local or air-gapped mission environments.

Offering: Axio360

Documented operating role: Cyber risk assessment platform

Context for the comparison: Compare Axio360's assessment and risk reporting with AIC's customer-operated access, remediation and secret controls in local or air-gapped environments.

Offering: BeyondTrust

Documented operating role: Privileged access and password security

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

Offering: C3 Integrated Solutions

Documented operating role: Managed or guided CMMC implementation

Context for the comparison: Compare C3's Command and Catalyst services with AIC's customer-run access, credential and evidence controls in local, cloud or air-gapped environments.

Offering: Cocoon Data

Documented operating role: Encrypted file-sharing service

Context for the comparison: Compare Cocoon Data's secure file collaboration with AIC's customer-operated credential and session controls, local evidence and air-gapped deployment.

Offering: ComplyUp by Exostar

Documented operating role: Assessment and documentation platform

Context for the comparison: Compare ComplyUp's assessments and policy workflows with AIC's customer-operated security controls, secret custody and air-gapped mission deployment.

Copyright © 2026 Analog Informatics Corporation. All rights reserved.

Offering: ControlMap

Documented operating role: Compliance workflow platform

Context for the comparison: Compare ControlMap's SSP, POA&M and responsibility workflows with AIC's customer-run access controls, local secret custody and disconnected operation.

Offering: Cuick Trac

Documented operating role: Beryllium InfoSec managed virtual enclave

Context for the comparison: Compare Cuick Trac's managed VDI and security services with AIC's customer-run access controls, local secret custody and air-gapped deployment.

Offering: CyberArk/Idira

Documented operating role: Privileged-access security platform

Context for the comparison: Compare CyberArk/Idira's privileged-access options with AIC's customer-run credential, session and remediation controls, secret custody and air-gapped work.

Offering: CyberSaint CyberStrong

Documented operating role: Cyber risk and compliance platform

Context for the comparison: Compare CyberSaint CyberStrong's risk and control monitoring with AIC's customer-run access controls, local evidence and air-gapped mission support.

Offering: CyberSheath

Documented operating role: Managed cloud enclave and security services

Context for the comparison: Compare CyberSheath's Federal Enclave and managed security with AIC's customer-operated controls, secret custody and air-gapped sensitive missions.

Offering: Cyturus

Documented operating role: Control-based GRC platform

Context for the comparison: Compare Cyturus's shared controls and remediation workflows with AIC's customer-operated security, secret custody and evidence from air-gapped systems.

Offering: Delinea

Documented operating role: Privileged credential and access platform

Context for the comparison: Compare Delinea Secret Server's on-premises and cloud options with AIC's customer-run controls, secret custody and air-gapped deployment.

Copyright © 2026 Analog Informatics Corporation. All rights reserved.

Offering: Drata

Documented operating role: Cloud compliance platform

Context for the comparison: Compare Drata's compliance workflows and integrations with AIC's locally operated access controls, secret management and air-gapped deployment.

Offering: EgnyteGov

Documented operating role: Secure content enclave and compliance workflows

Context for the comparison: Compare EgnyteGov's content governance and collaboration with AIC's customer-run access, credential and remediation controls for sensitive local systems.

Offering: Exostar

Documented operating role: Managed GCC High enclave and secure desktop

Context for the comparison: Compare Exostar's managed collaboration and enclave options with AIC's customer-operated controls, secret custody and air-gapped mission deployment.

Offering: FutureFeed

Documented operating role: CMMC program-management platform

Context for the comparison: Compare FutureFeed's SSP and control tracking with AIC's customer-operated access controls, secret custody and evidence from disconnected systems.

Offering: Google Workspace and Assured Workloads

Documented operating role: Collaboration and cloud infrastructure

Context for the comparison: Compare Google Workspace and Assured Workloads with AIC's customer-operated credential, session and evidence controls for sensitive local missions.

Offering: Hyperproof

Documented operating role: Enterprise compliance operations platform

Context for the comparison: Compare Hyperproof's control tasks and evidence workflows with AIC's customer-operated security controls, secret custody and air-gapped deployment.

Offering: Ignyte

Documented operating role: Compliance platform and professional services

Context for the comparison: Compare Ignyte's compliance automation and advisory services with AIC's customer-run access controls, local evidence and air-gapped mission deployment.

Copyright © 2026 Analog Informatics Corporation. All rights reserved.

Offering: KeeperPAM

Documented operating role: Cloud-based PAM or independent Self-Managed Keeper

Context for the comparison: Compare KeeperPAM and Self-Managed Keeper with AIC for customer-operated credential and session controls, secret custody and air-gapped sensitive missions.

Offering: Kieri Solutions

Documented operating role: Documentation, reference architecture and assessment services

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

Offering: Kiteworks

Documented operating role: Secure content platform with on-premises, cloud and hybrid options

Context for the comparison: Compare Kiteworks's secure content collaboration with AIC's customer-run access, credential and remediation controls for sensitive or air-gapped systems.

Offering: Microsoft GCC High and Azure Government

Documented operating role: Government cloud productivity and infrastructure

Context for the comparison: Compare Microsoft GCC High and Azure Government foundations with AIC controls in customer-run cloud, local and air-gapped mission deployments.

Offering: Mycroft

Documented operating role: Integrated security and compliance service/platform

Context for the comparison: Compare Mycroft's compliance and security operations with AIC's customer-run credential controls, local evidence and air-gapped mission deployment.

Offering: NeoSystems

Documented operating role: Managed security, IT and enclave services

Context for the comparison: Compare NeoSystems's managed enclave and compliance services with AIC's customer-run access controls, local evidence and air-gapped mission deployment.

Offering: NeQter Labs

Documented operating role: Security and compliance tooling

Context for the comparison: Compare NeQter Labs's customer-deployed compliance tools with AIC's local access, credential and remediation controls for sensitive or air-gapped work.

Copyright © 2026 Analog Informatics Corporation. All rights reserved.

Offering: NtelSec CUI Vault

Documented operating role: Provider-managed Azure Government/GCC High VDI

Context for the comparison: Compare NtelSec CUI Vault's managed enclave service with AIC's customer-operated controls, local secret custody and air-gapped mission deployment.

Offering: One Identity Safeguard

Documented operating role: Privileged password and session products

Context for the comparison: Compare One Identity Safeguard's password and session controls with AIC's customer-operated security, remediation evidence and disconnected deployment.

Offering: Paramify

Documented operating role: Compliance documentation platform

Context for the comparison: Compare Paramify's SSP and POA&M automation with AIC's customer-run credential, session and remediation controls in local or air-gapped environments.

Offering: PreVeil

Documented operating role: Encrypted email/files plus managed VDI option

Context for the comparison: Compare PreVeil's encrypted collaboration and managed VDI with AIC's customer-operated security controls, secret custody and air-gapped mission support.

Offering: RegDOX

Documented operating role: Secure repository and browser-based computing enclave

Context for the comparison: Compare RegDOX's protected document collaboration with AIC's customer-operated access controls, secret custody and evidence from disconnected systems.

Offering: RegScale

Documented operating role: Continuous controls and compliance platform

Context for the comparison: Compare RegScale's evidence automation and OSCAL workflows with AIC's customer-operated security controls, secret custody and air-gapped deployment.

Offering: Scrut

Documented operating role: Cloud security and compliance platform

Context for the comparison: Compare Scrut's asset visibility and control monitoring with AIC's locally operated access, remediation and evidence for sensitive or air-gapped work.

Copyright © 2026 Analog Informatics Corporation. All rights reserved.

Offering: Secureframe

Documented operating role: Compliance platform with customer-cloud enclave provisioning

Context for the comparison: Compare Secureframe Defense Navigator and cloud enclave provisioning with AIC's customer-run credential, session and air-gapped security controls.

Offering: Sentinel Blue

Documented operating role: Integrated managed IT, security and compliance services

Context for the comparison: Compare Sentinel Blue Shield's managed infrastructure and SOC services with AIC's customer-operated controls, secret custody and disconnected operation.

Offering: Sprinto

Documented operating role: Cloud trust and compliance platform

Context for the comparison: Compare Sprinto's compliance integrations and trust workflows with AIC's customer-operated security controls, secret custody and air-gapped deployment.

Offering: Summit 7

Documented operating role: Microsoft-focused managed IT, security and GRC services

Context for the comparison: Compare Summit 7's Guardian, Vigilance and Commander services with AIC's customer-run access controls, local evidence and air-gapped mission deployment.

Offering: Thoropass

Documented operating role: Compliance software and audit services

Context for the comparison: Compare Thoropass's compliance software and audit services with AIC's customer-operated controls, secret custody and disconnected mission support.

Offering: Totem HRDN-IT

Documented operating role: Hardened on-premises PC enclave and planning tool

Context for the comparison: Compare Totem HRDN-IT's customer-deployed approach with AIC's local access, credential and remediation controls, secret custody and air-gapped operation.

Offering: Vanta

Documented operating role: Cloud compliance platform

Context for the comparison: Compare Vanta's audit evidence automation with AIC's customer-run security controls, secret custody and air-gapped operation for sensitive missions.

Copyright © 2026 Analog Informatics Corporation. All rights reserved.

Offering: Virtru

Documented operating role: Data-centric email and file protection

Context for the comparison: Compare Virtru's data protection and collaboration with AIC's customer-operated credential, session and evidence controls for sensitive local missions.

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.

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

Copyright © 2026 Analog Informatics Corporation. All rights reserved.