COMPARISON ANALYSIS

Analog Informatics Privileged Access Comparison

Compare AIC and privileged-access platforms for rotation, sessions, elevation and secret custody, including customer-operated and air-gapped deployments.

Deployment and customer-control revision: November 20, 2026

Scope: Enterprise

Analog Informatics Corporation

View the related production resource

Copyright © 2026 Analog Informatics Corporation. All rights reserved.

Choose the exact edition, users, systems, session requirements, and deployment before requesting prices. The full AIC Enterprise Privilege Suite™ is priced by quote.

Compare Products

- AIC and CyberArk
- AIC and Delinea
- AIC and BeyondTrust
- AIC and Keeper

Keep the Package Clear

AIC Privileged Access for Microsoft CMMC is a distinct package. Its price and minimum order are on AIC CMMC Complete™ Pricing. The enterprise suite's modules, recording capacity, and other entitlements are scoped through AIC Enterprise Privilege Suite™ Pricing.

Ask both providers to price the same CUI boundary: 25 users, 25 managed systems, the required mailboxes, and the same privileged administrators. 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 A different user count or an unpublished price cannot establish which complete solution costs less.

Comparison source revision: November 20, 2026

Choose who controls the software and secrets

Compare the complete management service, not only the connector installed beside a server. A local gateway may still depend on vendor-hosted authentication or control services; a separately licensed self-managed product can have a different feature set.

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.

Copyright © 2026 Analog Informatics Corporation. All rights reserved.

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 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

Copyright © 2026 Analog Informatics Corporation. All rights reserved.

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 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.

Copyright © 2026 Analog Informatics Corporation. All rights reserved.

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.

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

Copyright © 2026 Analog Informatics Corporation. All rights reserved.