COMPETITIVE ANALYSIS

Analog Informatics vs. Tailscale - Competitive Analysis

Compare AIC and Tailscale for private routes, privileged sessions and air-gapped operations. See local customer control and hosted-service dependencies.

Analysis date: November 17, 2026 | Revised: November 20, 2026

Analog Informatics Corporation

Copyright © 2026 Analog Informatics Corporation. All rights reserved.

Deployment options and who operates them

Compare where the management software runs, who operates it and which functions remain local. A local connector, an outage cache and a customer-operated air-gapped installation have different dependencies.

Deployment option	AIC	Tailscale
On-premises management	Yes. Install and operate the management software on customer infrastructure.	Clients, routers and PAM connectors run locally. Commercial coordination and PAM services remain hosted.
Management in your own cloud account	Yes. Install and manage AIC in a cloud account and region you choose.	Run clients, routers or PAM connectors in your cloud. The commercial management services remain hosted.
Hybrid operation	Yes. Customer-managed local and cloud components can serve the chosen systems and applications.	Yes. Connect local and cloud systems through the private network, using hosted coordination.
Vendor-operated SaaS	No mandatory AIC-operated SaaS management service. The customer or its authorized provider operates the installation.	Yes. Tailscale hosts network coordination and PAM services. Customers run the PAM connectors.
Air-gapped or disconnected operation	Yes. Supported local credential and session functions run with required local services and a valid license. Install, license and update without a network connection to AIC.	Existing network peers can use cached rules and valid keys while a network path remains. The PAM connector separately requires internet access to the PAM API and proxies.
Secret and administrative control	The customer authorizes secret use, retrieval and changes. AIC support has no standing access.	The PAM connector reads configured secret sources. Tailscale stores enabled recordings by default. On Premium, recordings pass through its PAM API to customer-owned Amazon S3.
Country-specific installation and records	Install and operate within a chosen country. Configure operators, logs, backups and recovery copies for the required boundary.	Tailscale does not guarantee EU data residency. Local connectors or storage do not localize all hosted-service processing.

AIC deployment choices include the product owner's November 20 confirmation of air-gapped support. Competing options follow the cited documentation. An outage cache or a surviving connection is not evidence that every administrative workflow works offline. Future AIC feature scope is separate from the released capabilities available for a purchase today.

AIC: Customer-installed security software for on-premises, customer-controlled cloud, hybrid and air-gapped deployment. The customer chooses the location and authorized operators and controls access to its managed secrets. Installation, licensing and updates can be completed without a network connection to AIC.

AIC Enterprise Privilege Suite; AIC disconnected operation; AIC security and customer control

Tailscale: Private networking with supplier-operated coordination and customer-side clients and routers. The separate PAM beta adds customer-run connectors and hosted access services. Headscale is a separate community project for self-hosted network coordination. It is not the commercial PAM service.

Tailscale architecture; Tailscale coordination outages; Tailscale PAM connectors; Tailscale PAM secrets; Tailscale customer recording storage; Tailscale EU residency position; Tailscale and Headscale

Copyright © 2026 Analog Informatics Corporation. All rights reserved.

Which platform fits a production database access request?

A contractor who works in the staging environment needs temporary access to production data. The incident lead needs to know who approved access, which queries the contractor ran and when access ended. A scheduled job uses the same database account and must still be able to sign in after its password changes.

What Tailscale offers: 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.

Where AIC changes the decision: The customer decides who can use or retrieve every secret AIC manages. AIC can discover the database account, rotate the password, update supported dependent services and report failures to the operator. In a supported disconnected installation, local administrators can continue credential and session work while the required local services are running. For a mission that requires an air-gapped installation, AIC places supported local operations and their administration inside the customer's chosen boundary. Installation, licensing and updates do not require a network connection to AIC.

Which approach fits: 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.

A practical example: In a pilot, have the manager approve one hour of database access. Test whether the current session ends and whether a new login is denied after the approval expires. Tailscale combines permissions from matching grants, so inspect every grant that allows the same access. Retrieve the query log, rotate the database account password, refresh the connector’s saved secret and run the scheduled job with the new password.

Where AIC and Tailscale overlap and who uses them

Current capabilities and future scope

As of November 18, 2026, both platforms address privileged access and audit evidence. AIC considers every Tailscale capability in scope for future releases, including private networking, device-based access policies and protocol-specific session controls. The timing and contents of those releases are open. For a purchase today, verify the required routing, protocol and recording behavior in the AIC version offered and check access to Tailscale’s PAM beta.

Where the features overlap

Access to private infrastructure

AIC today: AIC provides browser-based SSH, RDP and VNC access to supported systems through a customer-run session service. Its Jump component provides an isolated path for privileged sessions.

Tailscale today: Tailscale connects devices and workloads using encrypted WireGuard connections. Subnet routers give authorized users access to private systems that cannot run a Tailscale client.

What this means for the customer: A database team may already have a suitable network route and need to control who can administer the server. A developer connecting a build runner to the database also needs a private route.

Copyright © 2026 Analog Informatics Corporation. All rights reserved.

User privileges and device checks

AIC today: AIC can allow, challenge or deny sign-ins to its own suite based on the source address, country or threat intelligence. It also supports approved elevation and correction of unauthorized privilege changes on supported endpoints.

Tailscale today: Tailscale grants specify which users, groups or tagged workloads may connect to which services. Administrators can require a source device to meet defined security conditions where Tailscale can evaluate its posture.

What this means for the customer: A security team may need to restrict sign-ins to its administrative console, check the device connecting to a service and remove an unexpected local administrator. The point at which each policy is enforced matters.

Temporary access and session records

AIC today: AIC can broker approved sessions and grant time-limited access. Recording and session controls depend on the target and protocol.

Tailscale today: In the PAM beta, managers can approve access to a service in Slack. Depending on the protocol and configuration, investigators can replay SSH sessions, inspect database queries or review Kubernetes API requests.

What this means for the customer: An incident lead who needs evidence of a particular command or query should run that action through each proposed session broker and inspect the record.

Workload identities and credentials

AIC today: AIC inventories human and non-human accounts, rotates supported credentials and updates supported jobs and services that use them.

Tailscale today: Tailscale can restrict a build runner to selected services. A PAM connector can read an external secret locally. After rotation, an operator saves the service configuration again or restarts the connector to load the new value.

What this means for the customer: A platform team can restrict where a job connects and still need to rotate the account it uses at its destination. Identify who manages the target account and each dependent job.

AI agents and API access

AIC today: Administrators can issue scoped AIC API tokens to software, including AI agents, and review the calls made with those tokens.

Tailscale today: Tailscale’s separate Aperture gateway uses Tailscale identities to control which AI models an agent can call without distributing a provider key to each agent.

What this means for the customer: An AI platform team may need to authorize calls to a management API and calls to a model provider. Those permissions apply at different services; test each one using the agent’s actual identity.

Audit evidence and data control

AIC today: Customers control their AIC credentials and evidence. They can give auditors scoped access to reports and export credentials, logs and evidence, including after their license expires.

Copyright © 2026 Analog Informatics Corporation. All rights reserved.

Tailscale today: Tailscale records network configuration changes and PAM access decisions. With the Premium plan, customers can store new PAM recordings in their own S3 bucket. The recordings pass through the Tailscale PAM API.

What this means for the customer: Reviewers can investigate who accessed a resource using either product. A team with in-country requirements must also identify where records are processed, who may read them and how to retrieve them later.

Local and remote operations

AIC today: AIC runs in customer-operated on-premises, cloud, hybrid and air-gapped installations. Supported local credential and elevation workflows use local services. Installation, licensing and updates can be completed without a network connection to AIC.

Tailscale today: Existing Tailscale devices can retain network access under cached rules and valid keys during a coordination outage. The PAM connector separately requires internet access to the PAM API and proxies.

What this means for the customer: For an isolated mission site, demonstrate local authorization, revocation, credential changes and record review with external services unavailable. For a connected site, a private network and a customer-operated credential service can serve different requirements together.

AIC strengths

Administrators can discover previously unknown accounts, rotate their credentials and identify failed updates to the applications that use them.

An IT team can manage privilege, identity governance and compliance across AIC’s PIM, PAM, PUM, IGA, GRC, CLM and CIAM products. It can authorize corrections on many supported systems and review exceptions individually.

The customer selects the hosting location and the people who may use or retrieve its secrets. Its administrators can retain local access at a supported disconnected site and export evidence after license expiry.

AIC offers customer-operated air-gapped deployment for sensitive missions. The local team controls administrators, managed secrets and selected audit storage; installation, licensing and updates do not require a network connection to AIC.

Tailscale strengths

Tailscale connects developers, cloud workloads and remote devices through private routes. Its plans serve individuals, engineering teams and enterprises with multiple sites or cloud environments.

Network administrators can use existing identities, workload tags and supported device checks to restrict connections. A short-lived build runner can have different access from the developer who launched it.

With access to the PAM beta, a team can grant temporary access to individual services, keep its existing SSH or database clients and review protocol-specific session records.

Copyright © 2026 Analog Informatics Corporation. All rights reserved.

Which customers fit each approach

AIC - An enterprise identity, infrastructure or compliance team responsible for privileged accounts across data centers, cloud applications or isolated sites.

The same team can discover accounts, authorize corrections across many systems, recover from failed changes and provide evidence to auditors while controlling the installation and its secrets. A mission site that must continue supported local work without internet connectivity can evaluate AIC's air-gapped installation and its local identity and recovery services.

Tailscale - A developer connecting a few devices, a platform team connecting build runners, or an enterprise networking team connecting offices, clouds and remote technicians.

They can use identity-based policies to connect people and workloads to private resources. Teams admitted to the separate PAM beta can also approve access to individual services and inspect supported session activity.

Both - A distributed engineering organization whose network team already runs Tailscale and whose identity team owns administrator accounts and service passwords.

Tailscale can provide the private route while AIC manages target credentials and dependent jobs. For each production service, the teams can choose one session broker, assign responsibility for approvals and test the recovery procedure.

How Tailscale connects devices

Network pricing and plan features

Private network access for CI/CD runners

Network and application grants

Device posture conditions and exceptions

PAM beta announcement

Upstream credentials and secret sources

PAM session logs and protocol coverage

PAM recording storage in a customer S3 bucket

Network behavior during a coordination outage

PAM connector requirements

AIC conditional access and sign-in policy

AIC browser-based remote access for administrators and service providers

AIC Enterprise Privilege Suite

Aperture controls for AI users and agents

AIC air-gapped deployment

AIC security and customer control

Copyright © 2026 Analog Informatics Corporation. All rights reserved.

Customer-controlled deployment and secret access

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?

AIC is installed where you choose and managed by you. Your organization controls who may use, retrieve or change its managed secrets. Choosing cloud or hybrid infrastructure does not require you to give an outside SaaS operator control of those decisions.

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.

The Tailscale comparison

A contractor's existing private route and approval for a new privileged session are separate requirements. Tailscale can preserve communication between existing devices under cached rules and valid keys when coordination is unavailable. The PAM connector still requires internet access to the PAM API and proxies. AIC lets a mission team run supported local credential and elevation operations in its own air-gapped installation, with installation, licensing and updates that do not require a network connection to AIC. At a connected site, the team can keep Tailscale for private routing while AIC manages selected credentials. Whichever system brokers the session, name who may approve access, retrieve the secret and review the record.

Country-by-country operation in the EU

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.

ITAR and EU access requirements

For ITAR-controlled technical data, granting a foreign person a password, code or key that enables access to the unencrypted data requires the applicable authorization. An unauthorized release can violate U.S. export law even when the recipient works in the United States. The ITAR definition of U.S. person includes qualifying permanent residents and protected individuals, as well as citizens. Qualifying end-to-end encrypted storage and transmission can fall outside export treatment under 22 CFR 120.54; its conditions include keeping the means of decryption from third parties.

GDPR does not generally require a separate installation in each EU country. A separate provider outside the EEA can trigger the international-transfer rules when it remotely accesses personal data held in the EU. Choosing a local installation and local operators can support a customer's residency and access requirements; the full hosting, support and recovery arrangement determines the actual data paths.

Copyright © 2026 Analog Informatics Corporation. All rights reserved.

Compare the actual authorization service, secret custody, support permissions and operator locations in the proposed configuration. A cloud region, a company address or customer ownership of a storage bucket alone does not answer who can authorize access. Establish which personnel and legal entities may obtain access, from which countries and under which project requirements.

ITAR access information and releases

ITAR encrypted storage and transmission conditions

ITAR U.S. person definition

GDPR, including Articles 1, 28 and 44

EDPB guidance on remote access and international transfers

AIC air-gapped deployment

AIC security and customer control

Scope

This comparison covers AIC’s Enterprise Privilege Suite and related identity and governance products, Tailscale’s private network, and the Tailscale privileged access management (PAM) beta. Tailscale calls each private network a tailnet. The service that brokers a connection determines how credentials are supplied and which activity a reviewer can see.

Operating differences

After account discovery

An administrator can correct one finding or authorize changes across many supported systems. AIC records unsuccessful changes so the application owner can identify a dependent job that still needs attention.

At an isolated site

The customer runs AIC with local identity services, storage and recovery access. An engineer working outside the site needs a network connection to administer it remotely.

Competitor approach

A Tailscale administrator defines who may connect to a device or service. For privileged access, the administrator publishes a database or another resource through a PAM connector and assigns permissions. The connector authenticates to the resource, and the reviewer can inspect the activity recorded for that protocol.

Practical difference

If both products serve one database, decide who can approve the session and which system will change the database password. After changing a password in an external secret source, save the Tailscale PAM service configuration again or restart the connector so it loads the new value.

Copyright © 2026 Analog Informatics Corporation. All rights reserved.

Interpretation

An incident lead may need to see the queries an engineer ran. The database owner also needs to know whether the account password changed and whether the scheduled jobs can still sign in. Those are separate records, even when the same team reviews them.

Alternatives and switching

CQ01 What are the best alternatives to Tailscale?

Analog Informatics: AIC is an alternative for teams that need to discover privileged accounts on servers, rotate credentials or control elevation on supported endpoints. For a team replacing Tailscale's network, the alternative must also provide the private routes its people and workloads use.

Tailscale: Tailscale compares its private networking offering with Cloudflare Access, NetBird and Twingate. For privileged access, compare the Tailscale PAM beta and AIC Enterprise Privilege Suite against the same database, server and approval request.

Evidence: Network access alternatives; PAM beta announcement

CQ02 Which companies compete with Tailscale?

Analog Informatics: Analog Informatics and Tailscale compete when infrastructure and security teams need to approve privileged sessions and retain evidence of the work. A procurement team replacing a private network also needs to evaluate routing, client support and device policies.

Tailscale: Cloudflare and Twingate compete for network access. Analog Informatics competes for privileged administration where the buyer needs to approve access to production resources and account for the resulting work.

Evidence: Network access alternatives; PAM beta announcement

CQ03 How does AIC compare with Tailscale?

Analog Informatics: AIC's customer-run products govern privileged access, manage accounts between logins and collect evidence for reviewers. AIC can discover an account, rotate its credential, update supported dependent services and alert the operator if a change fails.

Tailscale: Tailscale provides a private network for users, devices and workloads. In its PAM beta, a connector in the customer's network enforces access to named resources and supplies credentials. An administrator can grant access to a specific database and review the queries a user runs through that connection.

Evidence: PAM architecture and customer-run connectors; Upstream credentials and secret sources; How Tailscale connects devices; PAM session logs and protocol coverage

CQ04 Can AIC replace Tailscale, or do I need both?

Analog Informatics: AIC can replace a session broker or credential-management tool for supported targets. If administrators, build jobs or remote sites depend on Tailscale's private network, identify how they will connect before removing it. AIC and Tailscale can also serve the same organization.

Tailscale: The two can coexist when Tailscale provides connectivity and AIC manages target credentials and service dependencies. Before removing Tailscale, identify any private network routes, application grants or PAM session policies that users still depend on.

Copyright © 2026 Analog Informatics Corporation. All rights reserved.

Evidence: PAM architecture and customer-run connectors; Upstream credentials and secret sources; Network and application grants

CQ05 Why would I switch from Tailscale?

Analog Informatics: Consider AIC if the team that approves sessions also needs to find unknown accounts, control elevation on endpoints and rotate credentials used by dependent services. If users already have a suitable path to the target, that team can add AIC while preserving the routes and clients users rely on.

Tailscale: Tailscale suits teams that want to connect private services and authorize sessions through their existing identity provider. If the purchase also requires password rotation across several services or administration during an internet outage, test how the external secret source and PAM connector behave.

Evidence: Upstream credentials and secret sources; PAM connector requirements

CQ06 Is there a self-hosted alternative to Tailscale?

Analog Informatics: AIC is a self-hosted choice for privileged administration. The customer operates its credential and session services on supported infrastructure, including disconnected sites. Private connectivity between sites still needs its own design.

Tailscale: Tailscale operates its commercial coordination service. Customers run their own PAM connectors. Headscale is an independent, community-run coordination server for Tailscale clients. Tailscale documents a separate requirement for its PAM connector to reach its API and proxies over the internet.

Evidence: Hosted coordination and Headscale; PAM connector requirements

CQ07 Can I replace several security tools with one platform?

Analog Informatics: AIC supplies PIM, PAM, PUM, IGA, GRC, CLM and CIAM products. Depending on the licenses and targets, a team can use AIC for account discovery, credential changes, endpoint elevation and evidence collection. Its Tailscale network can continue carrying traffic during the change.

Tailscale: Tailscale combines private networking with service-specific approvals and session auditing for customers admitted to its PAM beta. Teams that configure a connector to read an external secret remain responsible for that source and its rotation procedure.

Evidence: PAM beta announcement; Upstream credentials and secret sources

CQ08 What will I lose - and gain - by switching?

Analog Informatics: The customer operates AIC’s credential service, maintains its records and controls its update schedule. It also handles backups and recovery. During a switch, assign someone to preserve existing Tailscale grants, routes and access to earlier recordings.

Tailscale: Removing Tailscale can interrupt private routes, disable identity-based grants and affect access to earlier PAM recordings. A team adopting the Tailscale PAM beta can give users approved access from supported SSH and database clients while the connector supplies the target credential.

Evidence: Network and application grants; PAM session logs and protocol coverage; Upstream credentials and secret sources

Copyright © 2026 Analog Informatics Corporation. All rights reserved.

Capabilities and coverage

CQ09 Does this solution solve my whole problem, or only part of it?

Analog Informatics: A team responsible for privileged accounts can use AIC for discovery, credential changes, endpoint elevation, supported sessions and audit evidence. A team that also connects developers and build systems across networks must identify how traffic will travel between those systems.

Tailscale: Tailscale serves developers and enterprises that need a private network. The PAM beta can authorize a database connection and record its queries. Its service setup begins with a known resource. If you also need to find unknown accounts or update jobs after a password change, ask for a demonstration on your own targets.

Evidence: Supported PAM services; PAM session logs and protocol coverage; Upstream credentials and secret sources; Network pricing and plan features; PAM beta access and setup

CQ10 Which features are included, and which require another product?

Analog Informatics: AIC documents account discovery and rotation, controlled sessions and endpoint elevation on supported targets. The Enterprise pricing page and an itemized quote identify which licenses, capacity and recording options apply to the protocols and systems you use.

Tailscale: Tailscale lists network features by plan, including user seats and allowances for tagged resources. PAM requires separate beta access. Tailscale directs buyers to sales for pricing. Ask which PAM services, recording options and support terms the quote includes.

Evidence: Network pricing and plan features; PAM terms, including export and support; PAM beta access and setup

CQ11 Does it manage both on-premises and cloud assets?

Analog Informatics: AIC can manage supported on-premises and cloud systems from a customer-run installation. To discover or change accounts in a private cloud database, its service identity needs suitable database permissions as well as a network path to the database.

Tailscale: A connector with a network path to the resource can broker sessions to on-premises services or cloud resources such as Amazon RDS and Google Cloud SQL. The service definition and its access grants determine what users can do.

Evidence: PAM architecture and customer-run connectors; Supported PAM services

CQ12 Does it support Windows, Linux, network devices, and legacy systems?

Analog Informatics: AIC documents support for Windows, Linux, Unix, macOS, directories, databases, cloud identities, Cisco equipment, ESXi and management controllers. For a switch already reachable over SSH, check whether AIC supports changing its administrator credential on that specific software version.

Tailscale: Tailscale PAM documents access through Windows Remote Desktop (RDP), SSH and generic TCP. A connector may be able to reach a legacy device over TCP. Check the service type and authentication method to determine which permissions, recordings and credential options apply.

Evidence: Windows Remote Desktop access; PAM SSH access methods; TCP service access

Copyright © 2026 Analog Informatics Corporation. All rights reserved.

CQ13 Does it discover accounts and credentials I don't know about?

Analog Informatics: Yes. AIC discovers human and non-human accounts on supported connected targets, including accounts outside the list of services an administrator has chosen to publish. The operator can identify dependencies before putting a newly discovered account under rotation.

Tailscale: The PAM setup guide starts with an administrator naming a service and supplying its authentication details. It does not establish automatic discovery of unknown local accounts, credentials or dependent jobs. Ask Tailscale to show what its discovery tools find on a host with an unlisted service account.

Evidence: Supported PAM services; Upstream credentials and secret sources

CQ14 Does it manage non-human identities, service accounts, and AI-agent credentials?

Analog Informatics: AIC can discover and manage passwords, SSH keys, certificates and API keys used by people, services and workloads on supported targets. For a build job or AI agent, identify the account or key it presents to its destination and test the required changes there.

Tailscale: Tailscale supports tagged workloads and PAM service accounts for programmatic access. Its separate Aperture gateway uses Tailscale identities to control which AI models an agent can call without distributing a provider key to each agent. Determine who owns and rotates the agent's credentials for other systems.

Evidence: PAM service accounts; Upstream credentials and secret sources; Aperture controls for AI users and agents; Private network access for CI/CD runners

CQ15 Can it manage passwords, SSH keys, certificates, and API keys?

Analog Informatics: AIC supports passwords, SSH keys, certificates and API keys. For a database password, a rotation can include changing the database account's password and updating a supported scheduled job that uses it. Other credential types require operations specific to the target.

Tailscale: Tailscale manages its network and API credentials. Its PAM connector can load a database password or SSH credential locally from a supported source such as AWS Secrets Manager or Keeper. After rotation in that source, save the service configuration again or restart the connector to load the new value. Check who rotates the credential on the target itself. For devices on its private network, Tailscale can request a TLS certificate from Let's Encrypt. Renewal of certificates installed from files remains the operator's responsibility.

Evidence: Tailscale credentials and keys; PAM SSH access methods; Upstream credentials and secret sources; Tailscale HTTPS certificates

CQ16 Does it fix problems automatically, or just tell me they exist?

Analog Informatics: The initial AIC blast-radius report identifies findings on managed systems. Operators can authorize supported automatic corrections, including credential changes, and receive events for exceptions. A failed update to a dependent service therefore remains visible after the change job runs.

Tailscale: PAM can enforce access grants and limit SSH and database session durations. When a password changes in the configured secret source, an administrator can make the connector reload it. To establish whether a failed change can be repaired automatically, ask for a demonstration that includes the target account and a job that still uses its old password.

Evidence: PAM grant controls; Time limits on PAM sessions; Upstream credentials and secret sources

Copyright © 2026 Analog Informatics Corporation. All rights reserved.

CQ17 Does it provide controlled access without exposing credentials?

Analog Informatics: AIC PAM can broker an administrator's session without showing the target password. Where an emergency procedure genuinely requires a person to retrieve the credential, AIC PIM also supports approved retrieval. Identify which path your team permits for each target.

Tailscale: Yes. For supported SSH and RDP services, users authenticate with their Tailscale identity and the connector authenticates to the upstream system. An administrator can reference an external secret source so users need no copy of the target password or SSH key.

Evidence: PAM SSH access methods; Upstream credentials and secret sources; Windows Remote Desktop access; AIC browser-based remote access for administrators and service providers

CQ18 Can it remove standing privileges and expire approved access automatically?

Analog Informatics: AIC can grant approved access for a limited time. For a contractor who already has a private route to a server, verify that the target privilege expires as agreed and document how an open session responds to expiry or early revocation.

Tailscale: An approver can authorize a time-limited request in Slack. Separately, administrators can set a maximum session duration for SSH and database services only. If another matching grant gives the same access without a duration limit, that access remains unlimited. Check privileges the contractor already holds on the target itself.

Evidence: PAM beta announcement; Time limits on PAM sessions

Deployment and customer control

CQ19 Is it SaaS, self-hosted software, or a managed service?

Analog Informatics: AIC is customer-installed software for on-premises, customer-controlled cloud, hybrid and air-gapped deployment. Your organization operates the management installation or authorizes a provider to run it. At a connected site, you can continue using Tailscale for private routing.

Tailscale: 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.

Evidence: Hosted coordination and Headscale; PAM connector requirements; AIC air-gapped deployment; AIC security and customer control

CQ20 Can I run it on my own hardware or in my own cloud account?

Analog Informatics: Yes. You can run AIC on supported hardware you own or on virtual machines in your cloud account. A team in one EU country can run its own AIC installation, assign its own operators and choose the storage for local session records. Plan a recovery route that works if the normal private network path is unavailable.

Tailscale: Customers can run Tailscale clients and PAM connectors on their own infrastructure. Connector deployment options include Linux or macOS hosts, containers and cloud instances. The commercial network uses Tailscale's coordination service, and the connector needs internet access to the PAM API and proxies.

Evidence: PAM beta access and setup; PAM connector requirements; Hosted coordination and Headscale; AIC air-gapped deployment; AIC security and customer control

Copyright © 2026 Analog Informatics Corporation. All rights reserved.

CQ21 Can it operate in an air-gapped or disconnected environment?

Analog Informatics: Yes. AIC supports air-gapped installations for supported local credential and elevation workflows. Installation, licensing and updates do not require a network connection to AIC. Remote access requires a separately approved network path. Include local identity, time, audit, backup and recovery services in the design; external alerts and feeds need an approved transfer path.

Tailscale: During a coordination-service outage, existing devices can keep communicating under cached rules while their keys remain valid and a network path exists. Enrollment, policy changes and key revocation require the coordination service. The PAM connector separately requires internet access to the PAM API and proxies. Continued network traffic therefore does not establish disconnected PAM operation.

Evidence: Network behavior during a coordination outage; PAM connector requirements; AIC air-gapped deployment; AIC security and customer control

CQ22 Where are my credentials, logs, and compliance evidence stored?

Analog Informatics: You select storage for AIC-managed credentials, audit records, supported session recordings and backups. If one session runs through Tailscale and another through AIC, the two brokers can write to different locations. Record which broker holds the evidence for each database.

Tailscale: A connector can load credentials locally from a supported external store. Tailscale stores PAM recordings by default. On the Premium plan the PAM API can write recordings to your S3 bucket using a role you authorize. Access decisions and session records are also available in the administrative console.

Evidence: Upstream credentials and secret sources; PAM recording storage in a customer S3 bucket; PAM session logs and protocol coverage; AIC air-gapped deployment; AIC security and customer control

CQ23 Who can access my data - including the vendor and its support staff?

Analog Informatics: Your organization alone decides who can use or retrieve any secret managed by AIC. A contractor can receive a network route and a scoped session while an account owner retains password-retrieval rights. You also decide who may review recordings. AIC support has no standing access to your installation. Your organization chooses the administrators and provider arrangements, including the people and work locations approved for a sensitive mission.

Tailscale: Tailscale’s PAM terms authorize processing of access activity and enabled recordings. PAM roles govern console access. When you use your own S3 bucket, you grant the PAM API a cross-account role that can write recordings. Playback in the console also requires read access. Ask how support access is approved, which personnel can receive it and where that access is recorded.

Evidence: PAM terms, including export and support; PAM recording storage in a customer S3 bucket; PAM architecture and customer-run connectors; AIC air-gapped deployment; AIC security and customer control

CQ24 Can I control retention, export my records, and leave without losing evidence?

Analog Informatics: You set retention for AIC records and can export credentials, audit logs and evidence, including after license expiry. When transferring a database from one session broker to another, preserve the earlier recordings so incident reviewers can follow activity across the cutover.

Tailscale: On the Premium plan, you can set retention and permissions for recordings in your own S3 bucket. Switching recording locations leaves earlier recordings in their previous location and removes their replay from the console. Network configuration logs have a 90-day window. The PAM terms require customers to export needed records before access ends unless otherwise agreed.

Copyright © 2026 Analog Informatics Corporation. All rights reserved.

Evidence: PAM terms, including export and support; PAM recording storage in a customer S3 bucket; Configuration audit logs

CQ25 Can my MSP operate it while I retain control?

Analog Informatics: Yes. You grant and can revoke the MSP's AIC permissions while retaining authority over the secrets, the installation and its records. If the provider also manages Tailscale, keep customer-controlled recovery accounts for the tailnet and for AIC.

Tailscale: Tailscale’s channel agreement provides for MSPs to operate services for customers. Define who owns the tailnet, identity provider, connector hosts and recording bucket, and retain a customer-controlled administrator account that you can use to replace the provider.

Evidence: Channel partner and MSP arrangements; PAM architecture and customer-run connectors

CQ26 What happens if the vendor’s service is unavailable?

Analog Informatics: A customer-operated AIC installation does not require a live connection to AIC for supported local credential and session work. With a valid license and healthy local dependencies, that work can continue during an outside-service outage. Remote users also need an approved route into the site. At license expiry, licensed operation stops and export remains available.

Tailscale: During a coordination outage, existing devices can communicate if they have a working path, valid keys and cached rules permitting access. Administrators cannot add users or devices, refresh or revoke keys, or change firewall rules. Separately, the PAM connector needs internet access to the PAM API and proxies. Test both active and new PAM sessions if those services become unreachable.

Evidence: Network behavior during a coordination outage; PAM connector requirements; AIC air-gapped deployment; AIC security and customer control

Privileged controls and operational evidence

CQ27 What belongs inside the privileged-access boundary?

Analog Informatics: For a database reached through a private network, include the requesting engineer, identity provider, credential store, session broker, target account and scheduled jobs that use it. The AIC console, recovery credentials and evidence storage also sit inside the privileged-access boundary.

Tailscale: Include the identity provider, managed coordination service, policy administrators, connectors, secret sources, targets and recording storage. Tailnet Lock lets peers verify customer-controlled signatures on node keys. The PAM connector still enforces application policy and authenticates to the resource.

Evidence: PAM architecture and customer-run connectors; Upstream credentials and secret sources; PAM recording storage in a customer S3 bucket; Tailnet Lock and key verification

CQ28 Which privileged-security controls does the software enforce, assist with, or record?

Analog Informatics: AIC can enforce approved access and supported endpoint privilege controls, change target credentials and record the result. The administrator decides which accounts may be corrected automatically and who may approve an exception.

Tailscale: PAM grants can restrict SSH permissions, database actions and Kubernetes API operations on supported services. Session logs record access decisions and can capture activity specific to the protocol. Administrators select which resources and accounts come under those controls.

Copyright © 2026 Analog Informatics Corporation. All rights reserved.

Evidence: PAM grant controls; PAM session logs and protocol coverage; AIC conditional access and sign-in policy; AIC browser-based remote access for administrators and service providers

CQ29 What remains my responsibility or my MSP's responsibility?

Analog Informatics: The customer or MSP runs AIC, maintains target permissions and backups, and resolves exceptions such as an application that cannot pick up its new password. Management assigns access approvers. If another team owns private routes, it retains responsibility for reachability.

Tailscale: The customer selects, tests and maintains its access policies, protects credentials and connectors, configures recording, and maintains backup and recovery for its systems. Tailscale operates its hosted services. Name an operator from the customer or its MSP for each connector and recording destination.

Evidence: PAM terms, including export and support; Shared responsibility

CQ30 Does it continuously record privileged activity, or will we still reconstruct it for an audit?

Analog Informatics: AIC continuously collects and reports activity on supported systems, including the results of credential changes. With the appropriate recording functions, a reviewer can inspect the privileged session and the audit records for changes to the underlying account after the engineer signed out.

Tailscale: PAM records allowed and denied access attempts. Depending on the service and settings, a reviewer can replay SSH or supported browser sessions, read database queries or inspect Kubernetes API requests. Standalone Tailscale SSH uses a separate recorder. By default it permits sessions if that recorder is unavailable. An administrator can require recording so affected sessions are blocked or ended.

Evidence: PAM session logs and protocol coverage; Standalone Tailscale SSH recording

CQ31 Can it detect privilege drift and remediate problems during daily operations?

Analog Informatics: AIC can discover changes on supported targets, apply corrections authorized by policy and report exceptions. For a server exposed through a private route, the relevant drift might be an unexpected privileged account on that server even when the network grant is still correct.

Tailscale: Tailscale can use device checks to restrict connections and enforce permissions at a configured service. Its documented posture checks apply to source devices within the same private network, with exceptions for outside users of shared nodes and devices behind subnet routers. To assess local-account drift, ask Tailscale to detect and correct a change to an administrator group on a target host.

Evidence: Device posture conditions and exceptions; PAM grant controls; Upstream credentials and secret sources

CQ32 Does it track training, attestations, access approvals, access reviews and corrective actions?

Analog Informatics: AIC records privileged approvals and corrective work. The relevant review or attestation functions depend on the licensed products. Include an access decision followed by a change to the underlying account when designing the reviewer's report. AIC can also track training assignments and attestations.

Tailscale: An approver can authorize temporary access in Slack. Tailscale records configuration changes, and PAM session records identify the grants it evaluated. The reviewed guides do not establish recurring access certification or show that an account change was completed on the target. Request a sample that links a reviewer's decision to the completed change. The reviewed guides do not identify a training-assignment register. Ask for a sample that links a person's training and attestation to the access decision.

Copyright © 2026 Analog Informatics Corporation. All rights reserved.

Evidence: PAM beta announcement; PAM session logs and protocol coverage; Configuration audit logs; AIC Enterprise Privilege Suite

CQ33 Can security reviewers inspect current access records without disrupting IT?

Analog Informatics: Yes. A reviewer with the appropriate AIC permissions can inspect current reports and access records while operators continue managing accounts. The customer can grant that review access without disclosing the target password or creating an account on the target.

Tailscale: Tailscale assigns users with the Auditor role read-only access in PAM. A reviewer can inspect the user identity, source device, outcome and available session activity in the console. Check which recordings and resources the reviewer can see.

Evidence: PAM architecture and customer-run connectors; PAM session logs and protocol coverage

CQ34 Can the same access records support multiple security policies and audits?

Analog Informatics: AIC evidence can support multiple reviews when the record identifies the person, target, approval, action and time each policy requires. A reconciled service-account change may matter to the application owner and to the security auditor. Automated mapping depends on the licensed audit functions.

Tailscale: Several audits can use the same record of the user, service, authorization decision and time. The service's protocol and recording settings determine what activity is captured. Check that a sample contains the fields each audit requires and that the organization retains it for the required period.

Evidence: PAM session logs and protocol coverage; PAM recording storage in a customer S3 bucket

CQ35 Can it replace our governance tool or feed our SIEM, ticketing and governance systems?

Analog Informatics: AIC can send security events to a customer's SIEM or ticketing system and supply supported exports. If Tailscale sends a session record and AIC sends an alert about a failed rotation, use common service and account identifiers so the responder can find both records. AIC also supplies GRC software. Its licensed controls, reviews and reporting determine whether it can replace your current tool.

Tailscale: Tailscale can stream network flow and configuration logs to supported destinations. Its PAM terms also describe exports to third-party systems. Test which PAM events your SIEM receives, whether they carry the ticket identifiers you need and whether your governance system can send updates back. For full replacement, ask to see control mapping, recurring reviews and follow-up on corrective actions in the proposed product.

Evidence: Streaming network and configuration logs; PAM terms, including export and support; AIC Enterprise Privilege Suite

Cost and value

CQ36 What is the total cost - not just the advertised subscription?

Analog Informatics: Budget for the AIC Enterprise license, installation, target onboarding, infrastructure, recordings, backups, staff and any third-party licenses. Include the ongoing network subscription when the tailnet remains in service. Use the Enterprise pricing page and a written, itemized quote for license fees and allowances.

Tailscale: Budget for network seats, tagged resources, any PAM fees in the order, connector hosting, retention, and operational support. An existing secrets manager and a customer-owned S3 bucket can each add charges. Use the same workload and recording retention period when comparing quotes.

Evidence: Network pricing and plan features; PAM terms, including export and support; PAM recording storage in a customer S3 bucket

Copyright © 2026 Analog Informatics Corporation. All rights reserved.

CQ37 Is pricing based on users, administrators, identities, assets, or usage?

Analog Informatics: AIC licenses systems, applications and users under product-specific allowances. The quote also reflects selected modules, session capacity and term length. Count the systems and applications AIC will manage even if the same devices already appear on a network subscription.

Tailscale: Tailscale publishes seat-based network pricing and allowances for tagged resources. The PAM terms refer buyers to the applicable order, rate card or pricing documentation for PAM fees and usage limits. Obtain the PAM charges separately when comparing quotes.

Evidence: Network pricing and plan features; PAM terms, including export and support

CQ38 Are non-human identities charged separately?

Analog Informatics: AIC does not charge per non-human identity, account or credential. A database used by many jobs may therefore have many managed accounts without a matching per-account license charge. Its systems, applications and users still count under the selected package.

Tailscale: Tagged resources and the time short-lived workloads spend on the network can affect network charges. PAM supports service accounts for automation, but the public pricing material does not specify a PAM charge per service account or AI agent. Ask for the billing unit and allowances in the order.

Evidence: Network pricing and plan features; PAM service accounts; PAM terms, including export and support

CQ39 Which connectors, reports, storage, support or audit features cost extra?

Analog Informatics: The AIC order identifies licensed functions, recording capacity and support. Customer storage, third-party licenses and provider labor add costs. Best-effort product support is free, while a contractual response commitment requires a purchased enterprise agreement.

Tailscale: Additional tagged resources and purchased support can increase the cost of the network plan, and a customer-owned S3 bucket carries storage charges. PAM connector, recording, reporting and reviewer entitlements depend on the commercial offer. Ask which features the quote includes and how much exceeding each allowance costs.

Evidence: Network pricing and plan features; Support packages and scope; PAM recording storage in a customer S3 bucket; PAM terms, including export and support

CQ40 What infrastructure and third-party licenses will I need?

Analog Informatics: Provide the supported AIC host, network access to managed targets, storage for credentials and recordings, backups and required platform licenses. If the site must operate during an internet outage, include local identity and an independent recovery path in that design.

Tailscale: Provide a supported PAM connector host, outbound internet connectivity and a network path to each private target. Include the identity provider, existing secret source, operating systems and any customer-owned S3 recording storage in the bill of materials.

Evidence: PAM connector requirements; PAM beta access and setup; Upstream credentials and secret sources; PAM recording storage in a customer S3 bucket

Copyright © 2026 Analog Informatics Corporation. All rights reserved.

CQ41 How much staff time does it take to operate?

Analog Informatics: AIC automates routine discovery, credential changes and evidence collection. Staff still add targets, resolve failed changes and maintain the installation. To estimate staffing, time those tasks on representative accounts, including one used by several applications. Measure session approvals separately.

Tailscale: Tailscale operates the coordination service. Your staff add services, maintain connector hosts, review grants and set recording retention. The guides do not establish staffing hours for your deployment. During a pilot, record how often each task occurs and how much staff time it takes.

Evidence: Shared responsibility; PAM beta access and setup

CQ42 Which manual tasks and existing subscriptions could it eliminate?

Analog Informatics: AIC can automate account inventories, scheduled password changes, supported updates to dependent services and reporting. An organization can retire scripts or subscriptions that performed those tasks once it has verified coverage. If the private network still carries traffic between sites, include it in the ongoing budget.

Tailscale: Service-specific requests and centralized records can reduce manual key distribution, temporary access changes and log collection. Teams can keep a supported secrets manager and reference its credentials from PAM. Before retiring a VPN or bastion, check which routes, clients and emergency procedures depend on it.

Evidence: PAM beta announcement; Upstream credentials and secret sources; PAM session logs and protocol coverage

CQ43 How do costs change as the company grows?

Analog Informatics: Estimate growth in AIC licenses from the number of managed systems, applications and users. Include selected modules and the session capacity your team needs. Adding workload accounts can increase discovery and rotation work without adding a per-account charge. Retaining recordings longer increases storage and backup requirements.

Tailscale: More seats, tagged devices, time spent on the network by short-lived workloads, storage and support can change the total. PAM usage limits and fees follow the applicable commercial terms. Model concurrent sessions and retained recordings separately from the number of network users.

Evidence: Network pricing and plan features; PAM terms, including export and support; PAM recording storage in a customer S3 bucket

CQ44 What infrastructure and capacity limits apply to remote sessions or hosted workspaces?

Analog Informatics: You supply AIC’s session infrastructure and recording storage. Size the session broker for the number of simultaneous connections and the storage for the length of each recording and its retention period. An RDP target’s desktop capacity and licenses remain separate from the capacity of the session broker.

Tailscale: Tailscale PAM brokers RDP access to a Windows server that you supply. Size the Windows hosts and connectors for simultaneous users, and obtain any PAM usage limits in the order. The published service guide gives no universal desktop performance or concurrency figure.

Evidence: Windows Remote Desktop access; PAM connector requirements; PAM terms, including export and support

Copyright © 2026 Analog Informatics Corporation. All rights reserved.

Implementation and migration

CQ45 Can it work with our existing environment, or must we start over?

Analog Informatics: AIC can be introduced alongside existing private routes. Begin with discovery and the initial blast-radius report, then select accounts whose applications and service owners are known. Users can keep their established network access during that work.

Tailscale: Tailscale can add a connector beside an existing set of reachable services and publish individual targets. Users can continue to work in supported SSH, database and RDP clients. Test existing access paths before routing production administrators through PAM.

Evidence: PAM architecture and customer-run connectors; Supported PAM services

CQ46 How quickly can we deploy the Enterprise platform?

Analog Informatics: AIC can generate a new, isolated environment in minutes. Installing and integrating a production deployment also requires local infrastructure, identity integration, target permissions and onboarding. Time the first server from installation through a successful credential change and recovery from an interrupted update. A full rollout has no established duration.

Tailscale: First obtain beta access, enable PAM, deploy a connector, define a service and grant access. Tailscale does not publish a duration for a full rollout. Measure the time to connect a representative production service, including the work to obtain network approvals and configure its identity settings.

Evidence: PAM beta access and setup; PAM connector requirements

CQ47 How long does it take to discover and secure existing assets?

Analog Informatics: The duration depends on target reachability, discovery permissions and how many dependent services need a change window. Measure the time from discovery to the first verified rotation on representative Windows services and database jobs. Record any hosts that the discovery account could not inspect.

Tailscale: Tailscale documents how to register a known service with a connector. It gives no organization-wide credential discovery time or standard onboarding rate. To estimate this work, time registration, credential setup and policy validation for a group of representative services.

Evidence: PAM beta access and setup; Supported PAM services

CQ48 Can we introduce it gradually without interrupting operations?

Analog Informatics: Yes. Start with discovery on a limited group of reachable systems, then authorize selected changes. Keep current grants and emergency access in place while service owners verify that dependent jobs still run after each rotation.

Tailscale: Yes. Administrators can create one PAM service behind a connector and grant access to selected users. Pilot a separate service name and preserve the current access path until authorization, emergency use and logging have been tested.

Evidence: PAM beta access and setup; PAM grant controls

Copyright © 2026 Analog Informatics Corporation. All rights reserved.

CQ49 How do we migrate credentials, policies, and evidence?

Analog Informatics: Inventory credentials and the jobs that use them, map privileged approvals to the new session broker, and archive earlier session records. Assign an owner to any private routes you keep. Verify a credential rotation, an emergency login and a reviewer's access to records from both brokers.

Tailscale: Keep upstream credentials in a supported secret source where practical, map existing access decisions to PAM grants and pilot each service. Preserve historical approvals and recordings in a readable archive. For a later exit, the PAM terms require export before access ends unless otherwise agreed.

Evidence: Upstream credentials and secret sources; PAM grant controls; PAM terms, including export and support

CQ50 Who handles configuration, migration, and ongoing operations?

Analog Informatics: The customer or its chosen provider operates AIC and handles account migration, configuration, backups and exceptions. AIC supplies product guidance. Assign responsibility for sessions, rotation and private routing separately when teams share the same target.

Tailscale: Tailscale runs its hosted coordination and PAM services. Your organization or its provider runs the connectors, defines services and grants, selects recording storage and migrates required records. Under the PAM terms, the customer remains responsible for its access decisions and safeguards.

Evidence: PAM terms, including export and support; PAM beta access and setup; Shared responsibility

CQ51 What training, deployment guides, and support are included?

Analog Informatics: AIC includes deployment guides, cookbooks, recipes, training materials and free best-effort support. Non-enterprise email responses typically take 24-72 hours. Customers who purchase enterprise support receive a four-hour response commitment, 24 hours a day, seven days a week.

Tailscale: Tailscale publishes setup guides, a walkthrough and support options. Customers on paid business plans can buy support with contractual response times. The PAM terms describe the priority support standards for customers covered by a service-level agreement. Ask which training or deployment assistance the offer includes.

Evidence: PAM beta access and setup; Support packages and scope; PAM terms, including export and support

CQ52 Can we test it on our own systems before committing?

Analog Informatics: AIC offers a free 30-day Enterprise Privilege Suite trial. On an authorized test database, grant an engineer access and rotate the password for an account that a scheduled job uses. Take one dependent system offline and check whether the account owner can identify the failed update and recover.

Tailscale: Tailscale has a waitlist for free access to the PAM beta. After Tailscale enables your organization's participation, an administrator can publish a test resource through a connector and run a session against it.

Evidence: PAM beta access and setup; PAM beta announcement

Vendor credibility and fit

CQ53 Who is this company, and how long has it supported this kind of environment?

Analog Informatics: Analog Informatics Corporation develops the Enterprise Privilege Suite. Its founder's work on privileged identity products dates to 1993. Buyers can evaluate that experience against their own requirements for discovery, credential changes and recovery of dependent services.

Copyright © 2026 Analog Informatics Corporation. All rights reserved.

Tailscale: Tailscale says it started in 2019. It announced its dedicated PAM beta on August 27, 2026, following the Border0 integration. Its networking customers therefore have a longer operating history with the company than users of the dedicated PAM beta.

Evidence: Tailscale company history; PAM beta announcement

CQ54 Does it understand organizations like ours?

Analog Informatics: AIC fits enterprise identity, infrastructure and compliance teams responsible for accounts across on-premises and cloud systems. Teams with isolated sites can test local operations. Teams with many dependent applications can evaluate discovery, automated corrections and exception handling across their own systems.

Tailscale: Tailscale offers network plans for individuals, engineering teams and enterprises. Instacart describes using it to reach internal systems and troubleshoot production incidents. Tailscale also documents short-lived build runners and remote equipment. For a regulated deployment, ask for a PAM beta reference with comparable connectivity and evidence requirements.

Evidence: Instacart network access case study; PAM beta announcement; Network pricing and plan features; Private network access for CI/CD runners; Tailscale products and use cases

CQ55 Can it demonstrate our specific use case?

Analog Informatics: Use an authorized target that engineers can reach over your existing network. Have an engineer start a controlled session. Then ask the account owner to rotate a password used by a scheduled job while one dependent system is unavailable. Inspect the session record, the result of the change and the operator’s recovery steps.

Tailscale: With beta access, a team can publish a test service through a connector, approve an SSH or database session and inspect the resulting records. If several services use the same password, rotate it in the external secret source, reload it on the connector and verify that each service can sign in.

Evidence: PAM beta access and setup; PAM session logs and protocol coverage; Upstream credentials and secret sources

CQ56 What do customers say about reliability and support?

Analog Informatics: The available evidence includes no published AIC customer account of reliability or support quality. Use the trial to test a local recovery login during a network outage, and compare the result with your recovery requirement. Purchased support agreements specify response commitments.

Tailscale: In Tailscale’s published case study, KABAM Robotics reports reliable terminal access for engineers supporting robots in the field. Instacart describes fewer internal support requests after its network rollout. Neither case measures PAM beta reliability or Tailscale support response times.

Evidence: KABAM Robotics network access case study; Instacart network access case study; Support packages and scope

CQ57 What are its limitations?

Analog Informatics: AIC requires a supported credential operation, appropriate permissions and a path to the target. Being able to reach a legacy appliance by TCP or SSH does not establish support for rotating its administrator password or updating its consumers.

Tailscale: The PAM connector needs outbound access to the PAM API and proxies. Session evidence varies by protocol. If an external source rotates a password, save the PAM service configuration again or restart the

Copyright © 2026 Analog Informatics Corporation. All rights reserved.

connector to load the new value. Check who updates the target account and any other services using that password.

Evidence: PAM connector requirements; PAM session logs and protocol coverage; Upstream credentials and secret sources

CQ58 Which capabilities are available today, and which are roadmap items?

Analog Informatics: As of November 18, 2026, AIC supplies PIM, PAM, PUM, IGA, GRC, CLM and CIAM. Released functions include discovery, supported credential changes, controlled sessions, remediation and audit reporting. AIC considers all Tailscale features in scope for future releases. That direction carries no commitment to a particular feature, version or date. Verify private networking and protocol requirements against the version offered.

Tailscale: Tailscale offers its private network today. Its dedicated PAM product is in beta with a waitlist. Tailscale documents resource grants, native clients for supported services, approvals and protocol-specific records. Obtain written availability and support terms for any beta feature required in production.

Evidence: PAM beta announcement; PAM beta access and setup; Supported PAM services; Network pricing and plan features

CQ59 How does it handle vulnerabilities and security updates?

Analog Informatics: AIC generally responds to severe vulnerability reports within 24 hours and typically has a mitigation within 24 hours of notice. These are best-effort time frames. The customer schedules installation of the mitigation or update, including at sites that receive updates offline.

Tailscale: Tailscale publishes security bulletins with affected and fixed versions, and receives vulnerability reports through its security team. Tailscale maintains its hosted service while customers keep their clients and customer-operated components current. Check the bulletin for the affected platform.

Evidence: Security bulletins and fixed versions; Security and vulnerability reporting; Shared responsibility

CQ60 Will it work with our existing vendors and service providers?

Analog Informatics: AIC supports specified Microsoft systems, customer-selected service providers and supported event destinations. An existing private network can connect AIC to a supported target. To use a shared secret source or exchange policy data with another product, verify that the proposed integration supports the specific operation.

Tailscale: Tailscale can work with existing identity providers, supported secrets managers, SIEM destinations and MSPs. For a provider-operated connector, verify which identity the connector uses, which secrets it can read and whether your audit system receives the expected record.

Evidence: PAM grant controls; Streaming network and configuration logs; Upstream credentials and secret sources; Channel partner and MSP arrangements

CQ61 What happens to our deployment if the vendor is acquired or changes direction?

Analog Informatics: You retain your AIC installation, credentials and records. Licensed operation stops when the license expires, and data export remains available. Keep emergency target access and readable archives under customer control, including earlier session records held in another product.

Tailscale: The commercial network depends on Tailscale’s hosted coordination service. Its PAM terms require customers to export retained records before expiry or termination unless otherwise agreed. Keep independent access to critical systems, storage and the credentials needed for a transition.

Copyright © 2026 Analog Informatics Corporation. All rights reserved.

Evidence: PAM terms, including export and support; Hosted coordination and Headscale; PAM recording storage in a customer S3 bucket

Sources and evaluation

Analysis uses vendor product documentation and current AIC product-owner statements. No independent performance benchmark or customer-support measurement was performed for this comparison.

PAM beta announcement

Network access alternatives

PAM architecture and customer-run connectors

Supported PAM services

Upstream credentials and secret sources

Network and application grants

Network behavior during a coordination outage

PAM connector requirements

Hosted coordination and Headscale

PAM session logs and protocol coverage

PAM beta access and setup

PAM terms, including export and support

Network pricing and plan features

TCP service access

Windows Remote Desktop access

PAM service accounts

PAM grant controls

Time limits on PAM sessions

PAM recording storage in a customer S3 bucket

Configuration audit logs

Streaming network and configuration logs

Channel partner and MSP arrangements

Shared responsibility

Device posture conditions and exceptions

Standalone Tailscale SSH recording

Support packages and scope

Copyright © 2026 Analog Informatics Corporation. All rights reserved.

Tailscale company history

Instacart network access case study

KABAM Robotics network access case study

Security bulletins and fixed versions

Security and vulnerability reporting

Tailnet Lock and key verification

Tailscale credentials and keys

PAM SSH access methods

ITAR access information and releases

ITAR encrypted storage and transmission conditions

ITAR U.S. person definition

GDPR, including Articles 1, 28 and 44

EDPB guidance on remote access and international transfers

How Tailscale connects devices

Private network access for CI/CD runners

Tailscale products and use cases

Aperture controls for AI users and agents

AIC conditional access and sign-in policy

AIC browser-based remote access for administrators and service providers

Tailscale HTTPS certificates

AIC Enterprise Privilege Suite

AIC air-gapped deployment

AIC security and customer control

Test a one-hour production access request

Use a contractor test account, a staging service and a test database. Have the contractor request access and run a query. After access expires, verify that the incident lead can find the query and that the build job can still connect to the staging service. If an administrator also needs elevated access to the database host, test that separately.

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

Copyright © 2026 Analog Informatics Corporation. All rights reserved.