KuppingerCole ANALYSTS

# Secure Remote Access for OT/ICS

Warwick Ashford

October 9, 2025

LEADERSHIP COMPASS 2025

This KuppingerCole Leadership Compass examines Secure Remote Access (SRA) solutions for Operational Technology (OT) and Industrial Control Systems (ICS). It evaluates products that support secure remote connectivity while addressing access control, monitoring, and compliance needs, including protocol isolation, legacy system support, and secure third-party access across a wide range of industrial environments.

# Contents



# Executive Summary

Secure remote connectivity has become a foundational requirement for industrial operations. The convergence of Information Technology (IT) and OT systems, growing regulatory pressure, and the need for real-time diagnostics and support have made SRA an operational necessity in OT and ICS environments. These environments include energy production, manufacturing, transportation, water utilities, and other infrastructure sectors where availability, safety, and operational continuity are essential.

OT environments are often structured using the Purdue model, with secure remote access typically applied at Level 3 for operations and site-level IT, Level 3.5 for the demilitarized zone, and occasionally at Level 2 for control systems. While tasks such as diagnostics, configuration changes, software updates, and troubleshooting may ultimately impact systems at the process and device control layers, direct access is rarely granted to Level 2 and Level 1, where Programmable Logic Controllers (PLCs), Remote Terminal Units (RTUs), and other field devices operate. Access is usually facilitated by jump hosts or session gateways placed at Level 3 or 3.5 where it can be governed and monitored more effectively. Many of the systems at lower levels were never designed for network exposure and they need tightly controlled paths to limit risk.

What sets SRA for OT and ICS apart from general-purpose remote access solutions is the need to accommodate legacy hardware, proprietary protocols, and control system architectures that lack native security controls such as authentication, encryption, or audit logging. Introducing remote access into these environments introduces cyber risk unless access is managed through purpose-built controls. SRA addresses this challenge by delivering secure, policy-enforced, monitored access to field-level systems, including PLCs, Human-Machine Interfaces (HMIs), and Supervisory Control and Data Acquisition (SCADA) systems.

Remote access is often requested by external contractors, system integrators, or Original Equipment Manufacturers (OEMs) who operate outside the organization’s IT environment. In these cases, SRA functions as both access point and policy enforcement layer to control who can connect, under what conditions, and for how long. Unlike Virtual Private Networks (VPNs) or generic remote desktop tools that tend to provide broad access across network segments, SRA platforms apply fine-grained controls. These include access limited in duration and restricted to specific protocols for a single HMI or engineering workstation, with session recording, file transfer restrictions, and real-time policy enforcement based on risk, all intended to minimize exposure and reduce the chance of lateral movement if credentials are misused.

In this report, we distinguish between Policy-Based Access Control (PBAC) and Attribute-Based Access Control (ABAC) in the context of SRA. PBAC refers to the use of administrator-defined policies to govern access under specific conditions, such as session type, device posture, or network location. It provides medium-grained control suitable for OT and ICS environments, where access must often be constrained to particular systems or time windows. ABAC, by contrast, applies a more fine-grained model in which access decisions are made dynamically based on a combination of user, resource, action, and

environmental attributes. While many SRA platforms support PBAC for contextual enforcement, few extend to full ABAC capabilities.

Key reasons for adopting SRA in OT and ICS environments include the need to secure third-party access for equipment vendors and support contractors, reduce the time and cost of field service through remote diagnostics, and improve responsiveness to unexpected incidents. Organizations are also under pressure to comply with regulations such as International Electrotechnical Commission 62443 (IEC 62443), the North American Electric Reliability Corporation's Critical Infrastructure Protection (NERC CIP), and the European Union's Network and Information Systems Directive version 2 (NIS2). These require strict authentication of remote users, comprehensive logging of access activity, and enforcement of least privilege access policies. Traditional IT-focused tools often lack the required capabilities. Depending on sector and geography, organizations may also need to meet other SRA-related frameworks that place further requirements on encryption standards, access governance, and auditability.

Use cases range from scheduled maintenance and software updates to emergency support and predictive diagnostics. In each case, access must be scoped to specific assets and actions with controls to terminate sessions, enforce Multifactor Authentication (MFA), and prevent lateral movement across the network. Session-level enforcement, protocol isolation, encrypted tunnels, and real-time monitoring are essential to avoid introducing new vulnerabilities when connecting to systems that were designed to operate in isolation.

Another requirement is the ability to function within the limits of industrial environments. Maintenance windows are often short, and unplanned downtime is rarely tolerated. SRA platforms must provide high availability, failover support, and minimal deployment disruption. They must also interoperate with existing tools such as Security Information and Event Management (SIEM), Security Orchestration, Automation, and Response (SOAR), and credential vaults.

This Leadership Compass evaluates vendors in this specialized market segment. It focuses on how well their solutions deliver secure remote access to OT and ICS assets, support regulatory compliance, and enable secure collaboration with third parties. It also considers their ability to integrate with cybersecurity infrastructure, accommodate legacy systems, and scale across distributed environments with varying operational needs.

For information about the Leadership Compass process, see our KuppingerCole Leadership Compass Methodology.

## Key Findings

- The SRA market for OT and ICS is shifting from niche deployments to a foundational element of industrial cybersecurity.
- Growth is driven by IT and OT network convergence, regulatory mandates, and the operational need for secure, policy-controlled, real-time connectivity to critical assets.

- Solutions combine protocol isolation, legacy system compatibility, and compliance-ready monitoring for sectors including energy, manufacturing, transportation, and water utilities.
- Vendors are expanding capabilities with Zero Trust access models, behavioral analytics, and high-availability features for environments with strict uptime requirements and limited downtime windows.
- Portfolio expansion includes integration of SRA into broader security platforms and development alongside asset visibility and risk management solutions.
- The standard capability set now includes anomaly detection, credential injection, and integration with SIEM and SOAR tools.
- Protocol isolation gateways are increasingly used to secure access to outdated or unpatchable systems without directly exposing them to external networks.
- Deployment models range from on-premises appliances to cloud-managed gateways, with flexibility needed to meet varying industrial, operational, and connectivity constraints.

## Market Analysis

The SRA for OT and ICS market is rapidly maturing, moving from niche deployments to a core pillar of industrial cybersecurity.

Driven by converging IT/OT networks, regulatory mandates, and the operational imperative for real-time support, demand for solutions that combine secure connectivity with protocol isolation, legacy system compatibility, and compliance-ready monitoring is growing across sectors such as energy, manufacturing, and transportation. Vendors are responding with platforms that go beyond basic remote access, embedding Zero Trust controls, behavioral analytics, and high-availability features tailored to uptime-sensitive industrial environments.

The market is active, with major players expanding through acquisitions and portfolio diversification. Palo Alto Networks has integrated secure remote access into its broader Strata platform, while established OT security vendors like Claroty and Armis have built out their SRA offerings alongside asset visibility and risk management tools. Specialist providers such Xona Systems are differentiating through usability-focused secure access gateways.

The baseline feature set is expanding to include real-time anomaly detection, credential injection, and integration with SIEM/SOAR, placing pressure on vendors with more limited OT heritage. As capabilities converge, competitive advantage increasingly depends on deployment flexibility, integration breadth, and the ability to operate in resource-constrained, high-availability industrial settings.

## Delivery Models

SRA solutions for OT and ICS are available in a range of delivery models to match the constraints of different industrial environments. Many deployments are on-premises to ensure control and reduce latency, particularly in air-gapped or latency-sensitive networks. Others are delivered as virtual appliances or private cloud deployments, offering centralized management for distributed facilities. Cloud-based management with edge-deployed

gateways is increasingly common for global enterprises that require centralized governance while preserving local autonomy. Flexible delivery models are important in environments where connectivity, resource constraints, and operational requirements vary widely.

## Required Capabilities

SRA solutions for OT and ICS should provide a core set of capabilities to enable secure, compliant, and operationally practical remote access to industrial systems. While there is a shared foundation of key and advanced features, the specific requirements can differ by industry sector based on varying security expectations, deployment models, integration needs, system compatibility, and regulatory obligations.

### Key Capabilities

- Strong user authentication (MFA and role verification)
- Authorization mechanisms with granular access policies
- End-to-end encrypted remote sessions
- Role-Based Access Control (RBAC) with least privilege enforcement
- Real-time monitoring and logging of all remote sessions
- Support for legacy OT and ICS protocols
- Secure remote access to field devices and control systems
- Secure third-party access with unique identities and session controls
- Integrated threat detection for access-based anomalies
- Automated response actions based on session risk
- High availability and failover for uninterrupted operations
- Support for regulatory reporting and compliance auditing
- Compatibility with embedded systems and vendor-specific environments

### Innovative Capabilities

Advanced solutions differentiate themselves by including features that go beyond standard access controls:

- Just-in-Time (JIT) authentication with time-bound access
- Context-aware authentication based on device, location, or time
- Trusted device posture checks before granting access
- Session-based credential injection using a secure vault
- Protocol isolation gateways with encrypted proxying
- Support for Perfect Forward Secrecy (PFS) in session encryption
- Real-time enforcement of separation of duties
- Granular API-level access management
- Heuristic or Artificial Intelligence (AI)-driven anomaly detection for threat visibility
- Honeypots or decoys for detecting unauthorized activity
- Integration with SOAR platforms for automated incident response
- Remote device lockdown in case of compromise

- Stateful failover and session persistence during outages
- Encrypted communications during failover or edge reconnection
- Automated testing and validation of failover access policies

SRA platforms for OT and ICS must be flexible, easy to deploy, and able to operate within environments that have little tolerance for downtime or change. Interoperability with other security infrastructure is essential, especially for organizations moving toward centralized security operations. As the market evolves, solutions will continue to emphasize real-time monitoring, automated detection, and alignment with Zero Trust and regulatory frameworks.

**Trends and Evolution**

The SRA market for OT and ICS is evolving in response to heightened security risks, operational digitization, and regulatory scrutiny. Attackers are increasingly targeting critical infrastructure (including energy, water, and manufacturing sectors), often exploiting remote access channels. As a result, demand is growing for access solutions that provide both granular control and operational transparency.

One major trend is the shift from static, VPN-based access models to dynamic, policy-driven approaches based on Zero Trust principles. Organizations are replacing legacy tools with platforms enforcing identity verification, least-privilege access, and continuous session monitoring. These platforms reduce the attack surface by limiting session scope and duration and validating each connection before granting access.

Protocol isolation continues to gain traction, particularly in environments with outdated or unpatchable equipment. Rather than relying on OT endpoint security, access traffic is routed through gateways enforcing encryption, authorization, and traffic filtering. This allows secure access to systems never designed for connectivity.

Another development is the growing use of behavioral analytics and anomaly detection in remote sessions. By learning normal access patterns, SRA solutions can alert operators to deviations such as access outside approved hours, atypical commands, or attempts to reach unauthorized systems, thereby enabling early detection of compromised credentials or insider misuse.

Regulatory compliance is a major force shaping SRA’s evolution, with more frameworks mandating stringent controls over remote access, including authentication, session monitoring, and logging. SRA platforms increasingly offer built-in reporting, governance dashboards, and compliance templates to help operators meet these obligations and other industry- or region-specific requirements.

Vendors are adding failover, high availability, and session persistence to meet industrial uptime demands. As more critical processes depend on remote connectivity, maintaining access during outages becomes essential.

Interoperability is also a priority, with many organizations integrating SRA platforms with IT security tools such as credential vaults, identity providers, SIEM, and SOAR systems. This unifies IT/OT operations, reduces duplication, and enables end-to-end threat visibility.

Finally, deployment flexibility is key. Many sites need on-premises deployments, while others benefit from centralized management across multiple facilities. Vendors offering physical appliances, virtual machines, edge installations, and cloud-connected platforms are best positioned to support diverse industrial needs.

SRA for OT and ICS is no longer just an operational convenience. It is a strategic requirement underpinning resilience, safety, and secure modernization across industrial sectors.

# Leadership

When selecting a vendor for a product or service, the decision should not be based solely on the information provided in a KuppingerCole Leadership Compass. While the Leadership Compass offers a valuable comparison based on standardized criteria and helps identify vendors for further consideration, a thorough selection process requires a detailed analysis and a Proof of Concept (PoC), or pilot phase tailored to the specific needs of the customer.

Based on our rating, we created various Leadership ratings. The Overall Leadership rating provides a combined view of the ratings for:

- Product Leadership
- Innovation Leadership
- Market Leadership

## Overall Leadership

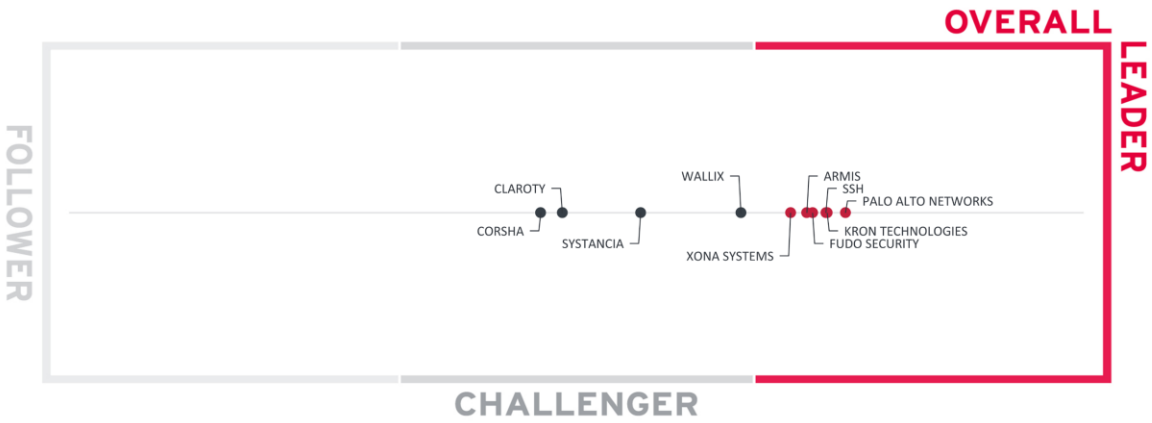



Figure 1: Overall Leadership in the SRA for OT/ICS market

The Overall Leadership chart is linear, with Followers appearing on the left side, Challengers in the center, and Leaders on the right. The rating provides a consolidated view of all-around functionality, market presence, and financial security.

However, these vendors may differ significantly in terms of product features, innovation, and market leadership. Therefore, we recommend considering our other leadership categories in the sections covering each vendor and their products to get a comprehensive understanding of the players in this market and which of your use cases they support best.

Palo Alto Networks leads the field, with Kron Technologies, SSH Communications Security, Fudo Security, Armis, and Xona Systems following in the Overall Leadership ranking. These vendors combine strong market presence, feature-rich products, and ongoing innovation tailored to the demands of SRA for OT and ICS. Their platforms address the need for controlled connectivity, legacy system compatibility, and compliance-ready monitoring, while

also advancing Zero Trust access, behavioral analytics, and high-availability features for uptime-sensitive environments.

In the Challenger section we find WALLIX, Systancia, Claroty, and Corsha, all offering solid solutions that meet many of the required capabilities but with room for further development or market expansion. Their positioning reflects either a narrower scope in OT and ICS-specific features, smaller market share, or less breadth in integrations compared with the leaders.

Overall Leaders are (in alphabetical order):

- Armis
- Fudo Security
- Kron Technologies
- Palo Alto Networks
- SSH Communications Security
- Xona Systems

## Product Leadership

Product leadership is the first specific category examined below. This view is mainly based on the presence and completeness of required features as defined in the required capabilities section above. The vertical axis shows the product strength plotted against the combined/overall strength on the horizontal axis. The Product Leadership chart is rectangular and divided into thirds. Product Leaders occupy the top section. Challengers are in the center. Followers are in the lower section.

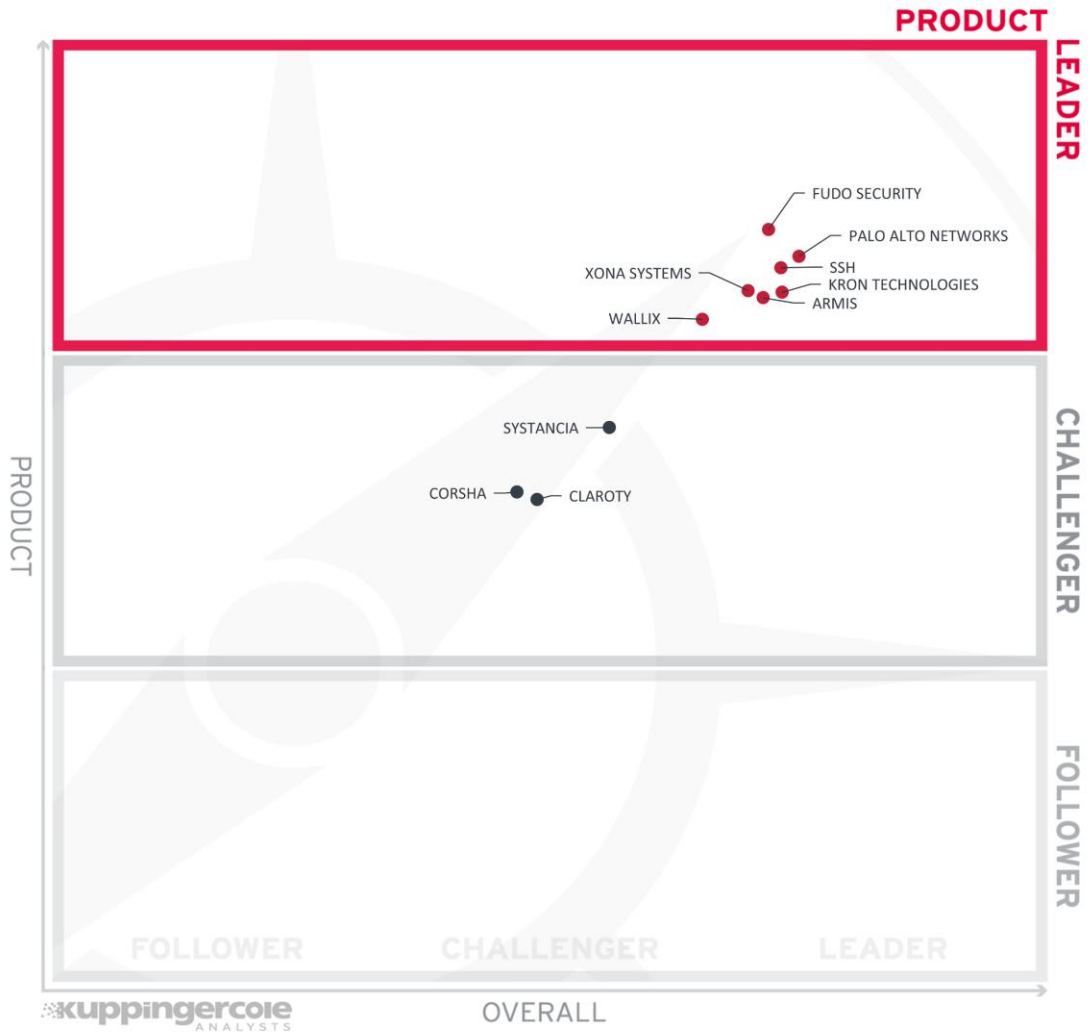



Figure 2: Product Leadership in the SRA for IT/ICS market

Fudo Security leads the Product Leadership ranking, followed by Palo Alto Networks and SSH Communications Security. Xona Systems, Kron Technologies, and Armis form a tight group just behind, reflecting a close alignment in feature depth, usability, integration breadth, and deployment flexibility for SRA in OT/ICS environments. These leaders deliver solutions that address the full range of core SRA requirements, including granular access control, session monitoring, and secure connectivity for both modern and legacy systems. WALLIX

sits between this group and the leadership threshold, showing notable progress but still some distance from the highest scoring vendors.

In the Challenger section, Systancia, Corsha, and Claroty provide credible capabilities but fall short of the breadth and maturity of the leaders. These vendors are competitive in specific areas such as identity-based access, secure connectivity, or monitoring, but they do not yet deliver the full depth of functionality and interoperability required to be considered leaders in this evaluation. With focused development and stronger alignment to OT-specific requirements, these challengers have the potential to strengthen their positioning in future editions.

Product Leaders (in alphabetical order):

- Armis
- Fudo Security
- Kron Technologies
- Palo Alto Networks
- SSH Communications Security
- WALLIX
- Xona Systems

## Innovation Leadership

Next, we examine innovation in the marketplace. Innovation is, from our perspective, a key capability in all IT market segments. Customers require innovation to meet evolving and even emerging business requirements. Innovation is not about delivering a constant flow of new releases. Rather, innovative companies take a customer-oriented upgrade approach, delivering customer-requested and other cutting-edge features, while maintaining compatibility with previous versions.

This view is mainly based on the evaluation of innovative features, services, and/or technical approaches as defined in the Required Capabilities section. The vertical axis shows the degree of innovation plotted against the combined/overall strength on the horizontal axis. The Innovation Leadership Chart is rectangular and divided into thirds. Innovation Leaders occupy the top section. Challengers are in the center. Followers are in the lower section.

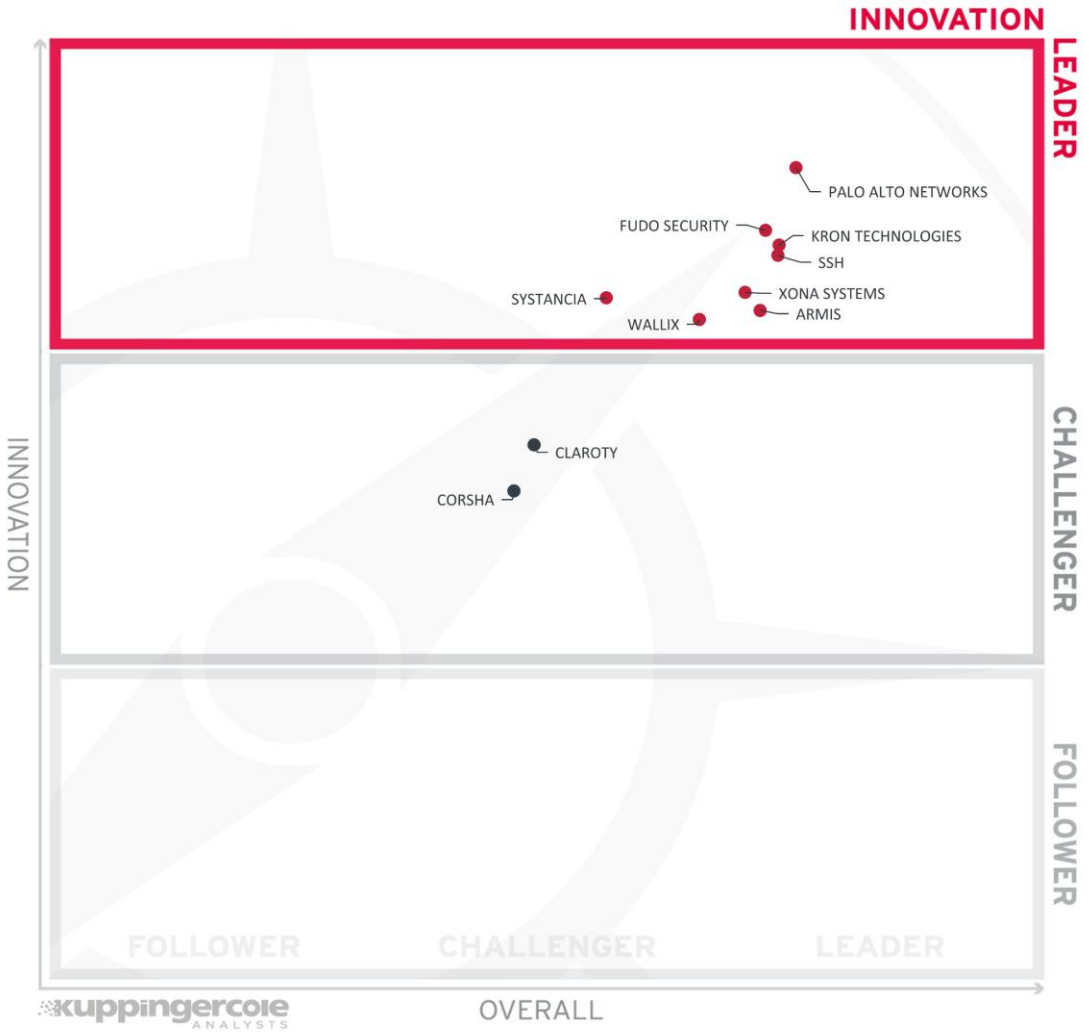



Figure 3: Innovation Leadership in the SRA for OT/ICS market

Innovation Leaders are those vendors that deliver cutting-edge products, not only in response to customers' requests but also because they are driving technical changes in the market by anticipating what will be needed in the months and years ahead. There is a correlation between the Overall, Product, and Innovation Leaders, which demonstrates that leadership requires feature-rich products that are looking over the horizon to bring advancements to help their customers.

The Leaders are Palo Alto Networks, Fudo Security, SSH Communications Security, Kron Technologies, Xona Systems, Systancia, Armis and WALLIX. The competition among these vendors is exceptionally tight, with very little separating their innovation scores. These leaders distinguish themselves through advancements such as adaptive Zero Trust architectures for OT, integration of advanced behavioral analytics, AI-driven anomaly detection, and expanded interoperability with legacy and proprietary ICS protocols.

The Challenger group for Innovation Leadership consists of Claroty and Corsha. These vendors demonstrate strong innovation in certain areas, such as specialized ICS protocol support, targeted risk analytics, or niche secure access methodologies, but have not yet achieved the breadth or depth of innovation seen in the leadership tier.

Innovation Leaders (in alphabetical order):

- Armis
- Fudo Security
- Kron Technologies
- Palo Alto Networks
- SSH Communications Security
- Systancia
- WALLIX
- Xona Systems

## Market Leadership

Finally, we analyze Market Leadership. This is an amalgamation of the number of employees and customers, the geographic distribution of customers, the size of deployments, support services, partner profiles, and the financial health of the participating companies. Market Leadership, from our point of view, requires global reach.

In this chart, the vertical axis shows the market strength plotted against the combined/overall strength on the horizontal axis. The Market Leadership Chart is rectangular and divided into thirds. Market Leaders occupy the top section. Challengers are in the center. Followers are in the lower section.

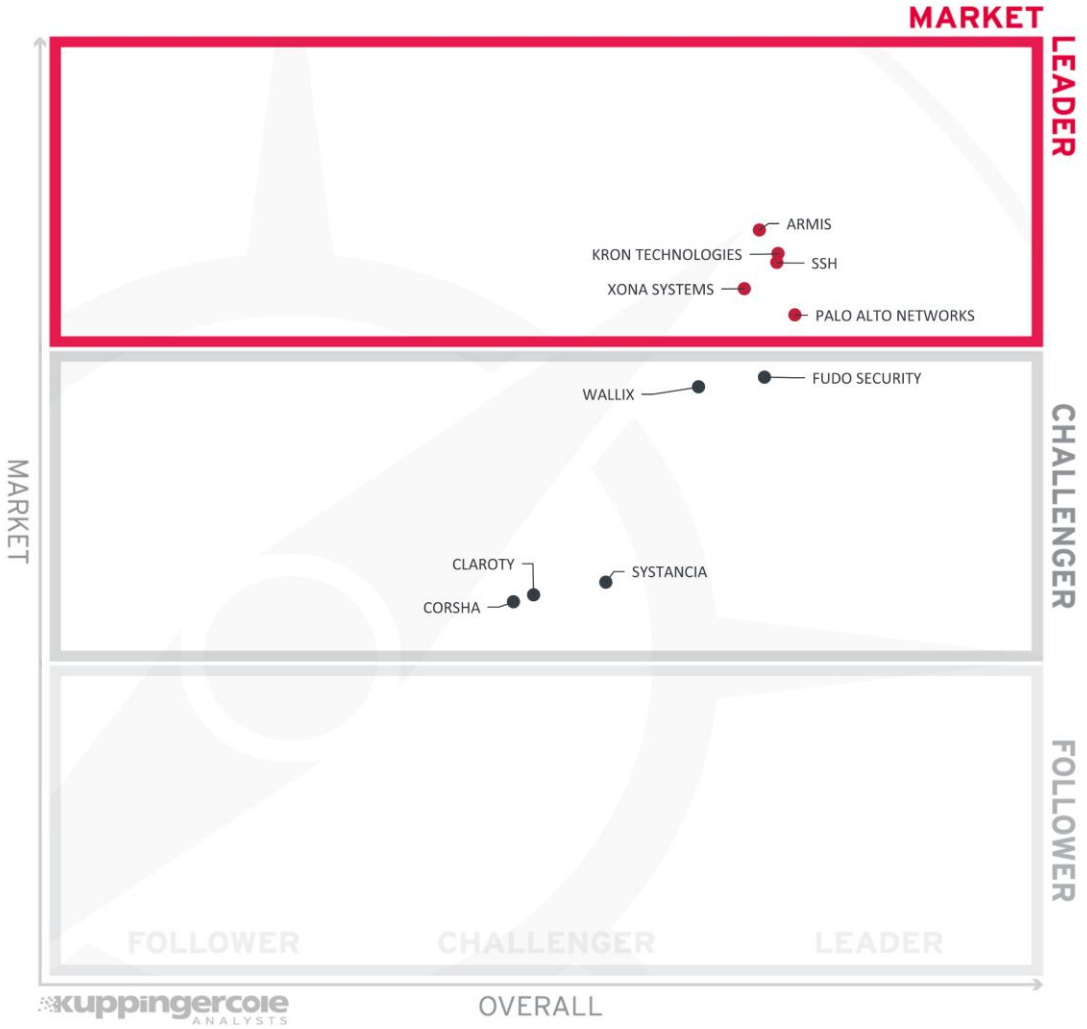



Figure 4: Market Leaders in the SRA for OT/ICS Market

Armis leads the market among the vendors evaluated in this report, followed by Kron Technologies, SSH Communications Security, Xona Systems, and Palo Alto Networks. Spacing between these leaders is generally even, with Kron Technologies positioned very

close to SSH. These vendors have achieved strong market positions through a combination of broad customer adoption, large-scale deployments, global reach, and mature partner ecosystems. Their solutions are capable of meeting the needs of organizations across a wide range of OT and ICS use cases, supporting diverse industrial environments and enabling secure connections at scale.

The Challenger segment includes Fudo Security and WALLIX, which are closely grouped together, followed by Systancia, Claroty, and Corsha. These vendors demonstrate solid market presence, with growing customer bases and regional strength, but still trail the leaders in terms of global reach, breadth of deployment, or partner network maturity. With further expansion and scaling efforts, several of these challengers could move into the leadership category.

Market Leaders (in alphabetical order):

- Armis
- Kron Technologies
- Palo Alto Networks
- SSH Communications Security
- Xona Systems

# Product/Vendor evaluation

This section contains a quick rating for every product/service included in this KuppingerCole Leadership Compass document. For many of the products there are additional KuppingerCole Product Reports and Executive Views available, providing more detailed information.

## Spider Graphs

In addition to the ratings for our standard categories such as Product Leadership and Innovation Leadership, we add a spider chart for every vendor we rate, looking at specific capabilities for the market segment researched in the respective Leadership Compass. For this market segment, we look at the following categories:

**Auth** – This rating measures the strength and flexibility of authentication and authorization capabilities for remote access into OT and ICS environments. It considers support for MFA, adaptive risk-based access, role-based authorization, and integration with identity providers. It also evaluates whether solutions can enforce continuous authentication during active sessions to prevent credential misuse.

**End-to-End Encryption** – This metric assesses the degree to which solutions provide comprehensive encryption for all data in transit, including legacy protocols that lack native security. It covers the use of strong cryptographic standards, as well as the ability to wrap insecure OT communications in secure tunnels without impacting latency-sensitive operations.

**Access Controls** – This category evaluates the granularity and flexibility of access control mechanisms, including least privilege enforcement, time-bound permissions, command-level restrictions, and JIT access provisioning. It also considers the ability to adapt access policies dynamically based on device health, user role, and operational context.

**Monitoring** – This rating reflects the extent and depth of monitoring capabilities for remote access sessions in OT/ICS. It includes real-time session recording, keystroke logging, and anomaly detection through behavioral analytics. It also assesses the ability to integrate with other tools for centralized oversight.

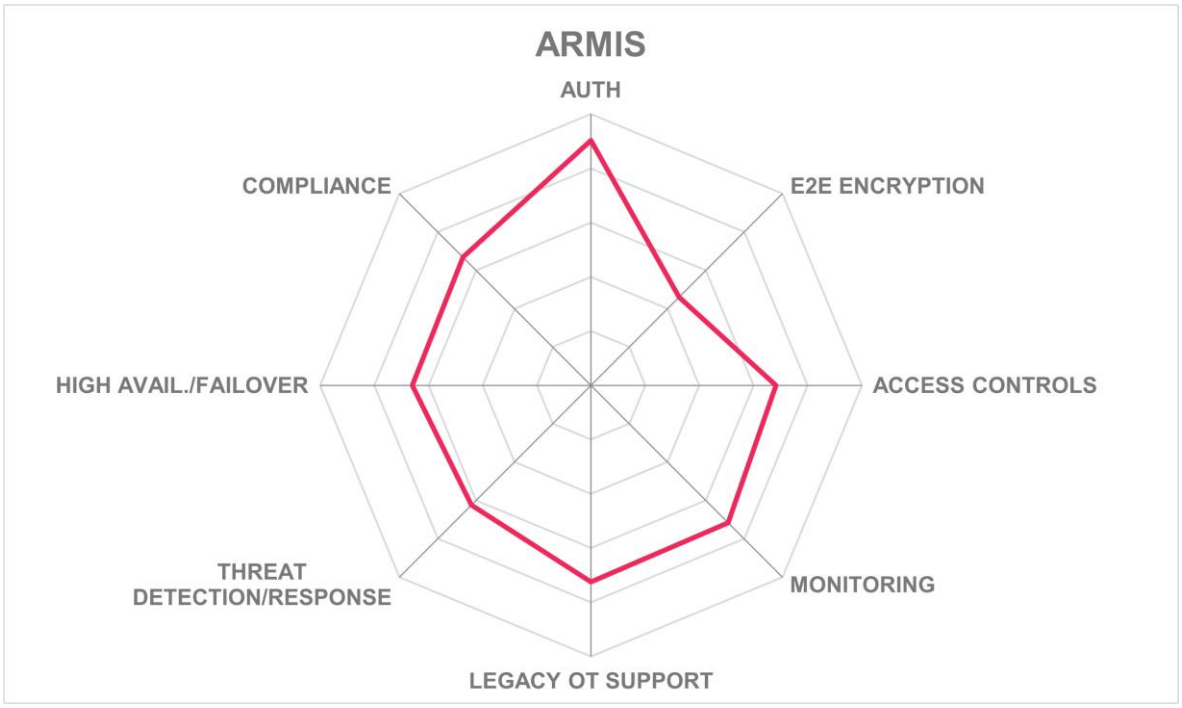
**Legacy OT Support** – This metric measures the solution’s capability to securely manage remote access to older or proprietary OT protocols. It considers protocol translation, secure tunneling, and monitoring for serial-based connections, as well as integration with a range of industrial assets.

**Threat Detection/Response** – This category evaluates the ability to detect and respond to suspicious activities in remote OT access, including unauthorized configuration changes, potential data exfiltration, and malware propagation. It looks at integration with threat intelligence feeds, SOAR platforms, and automated incident response playbooks tailored to industrial control systems.

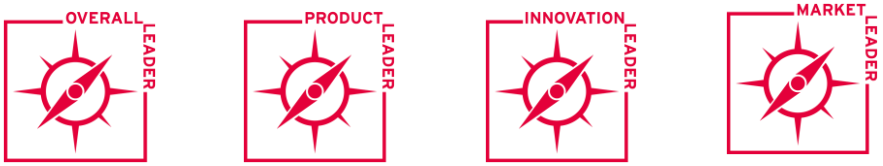
**High Availability/Failover** – This rating measures the resilience of the SRA solution in maintaining secure connectivity during planned maintenance or unexpected failures. It considers support automated failover between on-premises and cloud-based components, encrypted data replication, and seamless session continuity without re-authentication disruptions.

**Compliance** – This metric assesses the solution's compliance with key standards and ability to produce detailed, audit-ready logs and reports aligned with OT and industrial regulatory requirements. It includes out-of-the-box support for frameworks such as IEC 62443, as well as the ability to customize evidence generation for sector-specific regulations like NERC CIP.

## Armis – Centrix™ SRA




Leader in




Armis is a private cybersecurity company founded in 2016 and headquartered in Palo Alto, California, with research and development based in Israel. Originally focused on IoT security, the company now offers a broader cyber exposure management platform aimed at enterprise-scale environments. In March 2025, Armis acquired OTORIO, adding deeper OT expertise and enabling support for air-gapped and sequestered environments. Armis Centrix™ SRA, derived from the OTORIO Titan platform, is available as a standalone product or integrated into the Armis Centrix platform. The solution supports a range of deployment options, including cloud, on-premises, and hybrid configurations. Licensing is subscription-based, using tiered pricing by asset band or per site.

Armis Centrix SRA provides secure, agentless, browser-based remote access for OT, ICS and all other environments. It includes protocol isolation, granular access controls, approval workflows, and full video session recording. The solution integrates with identity providers, credential vaults, and session brokers, and enforces Zero Trust principles across distributed OT/IT environments. While Armis Centrix SRA can be deployed on its own, integration with the full suite of Armis Centrix solutions significantly enhances its value by enriching access

policies with contextual risk data and enabling centralized visibility, orchestration, and remediation workflows.

Key strengths of Armis Centrix SRA include JIT access, just-enough-access (JEA), time-bound temporary access, its alignment with the Purdue model, agentless operation, and support for OT environments without requiring VPNs or jump servers. Its design enables precise governance down to the protocol and port level, and it is architected to support multi-site and multi-tenant environments. The solution benefits from OTORIO's security engineering, delivering a hardened architecture suitable for critical infrastructure. Areas for improvement include real-time encryption visibility, support for secure tunneling of industrial protocols such as Modbus, and automated credential rotation.

The solution supports a wide range of authentication and authorization mechanisms, including MFA, certificate-based authentication, Single Sign-On (SSO), and integration with Microsoft Entra ID and Okta. It enforces access policies using real-time risk assessments and ABAC, with support for mutual Transport Layer Security (mTLS) to validate user and device identity. Device posture and contextual risk factors are incorporated into access control decisions to ensure only trusted devices establish connections.

All remote communications are encrypted using TLS 1.3 with PFS, including ephemeral key exchanges and application-level encryption of industrial protocols. Session data and control commands are encrypted in transit, and communication between SRA components is secured via Hypertext Transfer Protocol Secure (HTTPS). While the solution does not integrate directly with customer-managed Hardware Security Modules (HSMs), encryption keys are generated and protected within a FIPS 140-2 certified HSM through its use of Amazon Web Services Key Management Service (AWS KMS). Real-time visibility of encryption status is not currently available.

Access control is granular and highly configurable. The system enables access governance at the level of individual users, assets, and protocols, and enforces dynamic policies based on role, risk level, geography, or device trust. Access to specific ports or services can be constrained per policy. The platform includes geofencing, scheduled access, third-party access approval workflows, and automatic permission expiration. Multitenant support allows vendors to access only their designated systems within segregated network zones.

Armis Centrix SRA includes full session monitoring, real-time supervision via over-the-shoulder viewing, and forensic-level audit logs with timestamped session metadata. Sessions are video recorded with mouse and keyboard input captured for compliance and investigation. The solution monitors file transfers and configuration changes. While it cannot baseline user behavior or apply AI/ML for anomaly detection, these capabilities are available when used with the full Armis Centrix suite. Logs are not cryptographically signed but are securely recorded.

Support for legacy OT environments is enabled through an agentless architecture using session brokers, protocol mediation, and browser-based access gateways. No software installation is required on OT endpoints. Armis Centrix SRA supports protocol isolation and secure access enforcement even for unmanaged or outdated OT assets. The system can operate in air-gapped environments using on-premises components and unidirectional gateways.

The solution can detect anomalies in device behavior, unauthorized login attempts, lateral movement, and misuse of privileged accounts. It can also detect session hijacking. Deep

packet inspection and protocol-level analysis support detection of threats across OT networks. Integration with the Vulnerability Prioritization and Remediation (VIPR) Pro component of the Armis Centrix platform adds incident response workflows, including threat containment playbooks, although Armis Centrix SRA alone does not support automated remediation or session termination. Risk-aware policy enforcement is improved when combined with Armis Centrix and its telemetry and analytics.

High availability is supported through geographically redundant (active-passive) disaster recovery sites and automated failback. Sessions persist during failover without requiring reauthentication. Configuration data and policies are synchronized across sites. However, active-active clustering is not supported, and automated failover testing is unavailable. Dashboards provide real-time status visibility, but not availability metrics.

The solution is certified for compliance with major standards including the International Organization for Standardization 27001 (ISO 27001), System and Organization Controls 2 Type 2 (SOC 2 Type 2), Federal Information Processing Standards 140-2 (FIPS 140-2), UK Cyber Essentials, IEC 62443, and the German Cloud Computing Compliance Controls Catalogue (C5). It supports the European Union's General Data Protection Regulation (EU GDPR) and NIS2 requirements for incident reporting and includes audit-ready reporting for encryption, access logs, and asset interactions. Device access in IoT and OT environments is logged to support industry-specific regulatory requirements.

Armis Centrix SRA is particularly suited to large manufacturing and critical infrastructure operators with complex OT/ICS environments. Key sectors include automotive, energy, pulp and paper, and smart infrastructure. The solution is also used by Managed Service Providers (MSPs) to deliver secure remote access as a service. It supports multiple languages in support services and the user interface, but documentation is available only in English and German. While Armis Centrix SRA can be used as a standalone product, its capabilities are significantly extended when deployed with Armis Centrix, enabling deeper risk visibility, advanced analytics, and orchestrated response.

### Strengths

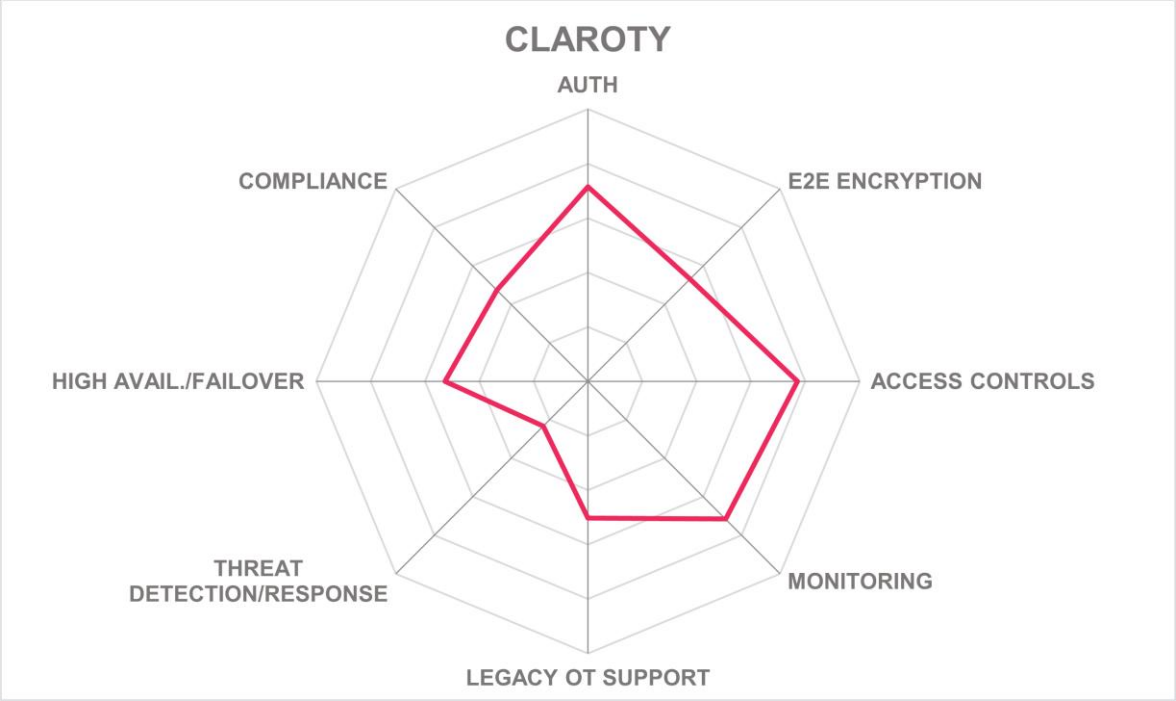
- Agentless design (simplifies deployment and integration)
- No VPN or jump server required
- Fully supports Zero Trust architecture
- JIT, JEA, and time-bound temporary access
- Granular, Purdue-aligned access controls available
- Integrated with the Armis Centrix platform
- Strong session auditing and recording features
- Works effectively in legacy OT environments
- Certificate-based authentication supported for all users
- Compliant with major cybersecurity standards
- Supports browser-based access

### Challenges

- No support for active-active clustering
- Encryption visibility lacks real-time status

- Incident response automation via integration
- No support for micro-segmentation

## Claroty – xDome Secure Access




Claroty is a private cybersecurity company founded in 2015 and headquartered in New York City in the US. The company specializes in securing Cyber-Physical Systems (CPS) including OT and ICS across industrial, healthcare, and commercial environments. xDome Secure Access is Claroty's SRA solution for OT and ICS. The product is available as an on-premises software installation or as SaaS. Claroty serves organizations in more than 50 countries and offers flexible pricing models based on access points or managed devices.

Claroty xDome Secure Access combines Zero Trust Network Access (ZTNA) with Privileged Access Management (PAM) for OT environments. It enforces least-privilege access, supports agentless and agent-based access, enables detailed session monitoring, and includes a built-in password vault. Third-party vendor access is managed through a dedicated dashboard, with automatic access revocation and fine-grained control over entitlements. The platform supports multiple protocols, including proprietary industrial protocols, and enables administrators to supervise sessions in real time. All activity is recorded, logged, and stored for auditing purposes.

What distinguishes Claroty xDome Secure Access is its two-tiered architecture, which separates the access manager (deployed on premises or in the cloud) from the access point (deployed on premises), aligning with Purdue model principles. The product is designed specifically for CPS needs such as intermittent connectivity, granular device-level access,

and administrative oversight of vendor activity. Weaknesses include limited use of AI or Machine Learning (ML), no anomaly detection capabilities, and no support for automated incident response. While xDome Secure Access and Claroty xDome currently operate as separate products, full integration is planned to unify enforcement (xDome Secure Access) with visibility and risk management (xDome) into a single platform.

xDome Secure Access supports strong authentication for internal and external users, including software tokens, OTPs, and authenticator apps. Certificate-based user authentication is supported, but not for devices. Delegated administration can be controlled through ABAC and PBAC. Policies can use contextual factors like time and network location but do not yet incorporate real-time risk scoring. The solution integrates with identity providers using OIDC and supports device authentication.

The solution protects data in transit using TLS 1.3 and Internet Protocol security (IPsec) VPN, but not WireGuard. There is support for mTLS for Application Programming Interface (API) traffic. End-to-end encryption is enforced via secure tunneling for industrial protocols like Modbus and Distributed Network Protocol version 3 (DNP3), with encryption applied at the application layer. However, the solution does not use PFS, does not support HSMs or enterprise PKI, and cannot generate alerts for encryption failures.

Claroty supports granular access control down to specific control parameters, PLC commands, and sensor data points. RBAC and PBAC policies can be defined and tailored to comply with industry-specific regulations. Role reviews and automatic credential rotation are supported. Third-party access is centrally managed and monitored, and multitenant access is available through the cloud-based console. However, geofencing is not supported, and anomaly detection specific to role misuse is lacking.

xDome Secure Access offers detailed logging, session recording, and audit trails, including keystroke and mouse activity. Admins can monitor active sessions in real time and terminate them if required. All session data is searchable and exportable. File transfer activities are logged, and files can be distributed to multiple endpoints from within the platform. However, the platform does not use AI or ML to detect anomalies or generate behavior baselines, and logs are not digitally signed to ensure integrity.

The solution supports all main OT/ICS protocols and enables agentless access to legacy devices using Virtual Network Computing (VNC), Secure Shell (SSH), Remote Desktop Protocol (RDP), and web protocols. There is also support for serial console interfaces such as VT100 and RS232. Claroty uses session brokers for agentless access but does not support access control for legacy OT or IoT devices lacking built-in security features. Context-aware access and dynamic policy adjustments are not available for legacy environments.

The product does not support automated incident response or threat containment actions. It can detect unauthorized access attempts and supports session recordings for forensics, but cannot detect session hijacking, behavioral anomalies, or misuse of privileged accounts. Anomaly detection specifically for Internet of Things (IoT) devices is not included. Claroty does not yet offer predefined playbooks or automated workflows for threat response.

High availability is supported through automated failover between geographically distributed deployments, with a typical failover time of 20 to 60 seconds according to Claroty. However, active-active clustering is not available, and the system does not maintain sessions during failover. Users do not need to reauthenticate after failover, but automated failback and real-time dashboards for availability metrics are not supported.

Claroty xDome Secure Access complies with ISO 27001, SOC 2, Payment Card Industry Data Security Standard (PCI DSS), National Institute of Standards and Technology Special Publication 800-57 (NIST 800-57), IEC 62443, and the Cybersecurity Maturity Model Certification (CMMC) developed by the US Department of Defense (DoD). Support is provided for 72-hour incident reporting under GDPR and NIS2. However, the solution does not generate automated compliance reports and lacks certifications such as ISO 15408 and FIPS 197. Although the audit logs support compliance processes, report generation for audit-readiness is not yet available.

The solution is best suited for large enterprises with complex CPS environments across industrial, energy, utilities, and healthcare sectors. Most current customers are enterprise organizations with significant remote access needs, large vendor ecosystems, and requirements for granular control and oversight. Support services are available in English, and documentation is provided in six languages including German, French, and Japanese. Organizations that require secure, scalable vendor access with high administrative oversight in sensitive OT environments should evaluate this solution further.

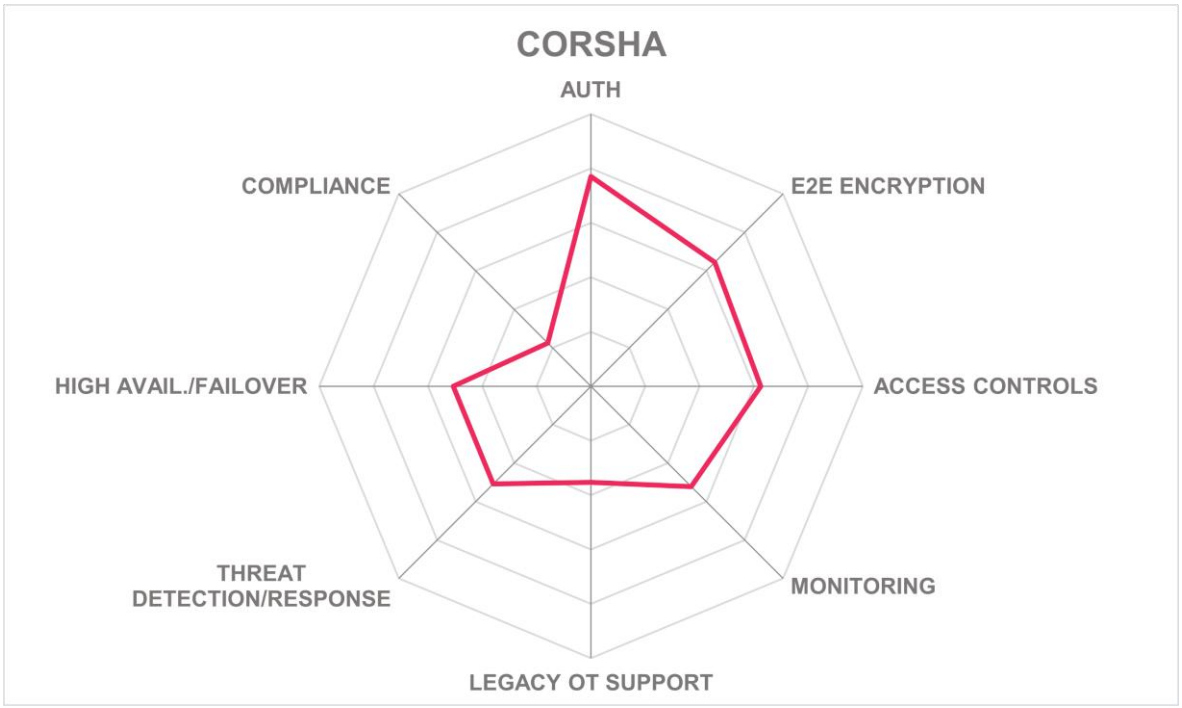
**Strengths**

- Purpose-built for CPS environments
- Supports both cloud and on-premises deployment
- Granular device-level access control
- Combines ZTNA and PAM capabilities
- Agentless access to OT systems
- Full session activity recording
- Centrally manages third-party vendor access
- Enables real-time session monitoring and termination
- Aligns with Purdue model segmentation principles

**Challenges**

- Lacks support for automated incident response
- Use of AI and machine learning limited
- Cannot detect behavioral anomalies
- Lacks digitally signed log integrity
- Does not generate compliance-ready reports

## Corsha – mIDP (Machine Identity Provider)




Corsha is a private US-based cybersecurity company founded in 2018 and headquartered in Tysons, Virginia. The company's core focus is secure machine identity and access in industrial environments, with SRA as a capability of its Machine Identity Provider (mIDP) platform. Corsha's first customers came from the US DoD, and the company continues to focus on both government and commercial sectors. The platform is licensed annually on a tiered per-identity basis and can be deployed as SaaS or as a fully on-premises system, including in air-gapped environments.

Corsha mIDP offers a unified platform that integrates machine identity, microsegmentation, scheduled access, and SRA. The solution supports both software and hardware-based gatekeeper appliances deployed at strategic points in the network, such as Level 3.5 in the Purdue model. It provides real-time visibility of traffic, manages hybrid identities from sources like Microsoft Entra ID, Claroty, and Dragos, and enforces policies across OT and IT environments. Key features include the use of cryptographic mechanisms to bind device identity, session recording, secure remote access via browser-based connections, and enforcement of fine-grained policies based on identity, time, and geography.

Corsha focuses on securing machine-to-machine communication and managing identity lifecycles without relying on static credentials. It uses a patented Time-based One-Time Password (TOTP) mechanism for machine authentication and can detect reused credentials or secrets in real time. The platform combines SRA with microsegmentation under a single management interface with agentless access to legacy systems. However, it offers limited automation for incident response.

Corsha supports a broad range of authentication methods, including smart cards, TOTP, and certificate-based authentication. It integrates with existing identity providers such as Microsoft Entra ID and Amazon Cognito to enable identity federation without requiring duplicate user management. Policies can be enforced using PBAC and ABAC. The Corsha Gatekeeper enables mutual device authentication through client certificates and enforces connection policies based on trusted machine identity attributes and real-time context.

All remote connections are secured with mTLS, with TLS 1.3 required across all communications. The platform supports selective encryption at the asset and user group level and includes centralized key management via cert-manager. Although Corsha does not use HSMs, its centralized system provides strong control of certificate lifecycles. All encrypted communications, including secure tunneling for OT protocols, are logged and visible to administrators, and session recordings provide forensic support for post-event analysis.

Corsha enforces Zero Trust access controls with support for continuous authentication and microsegmentation. Granular role-based permissions can be applied to individual OT assets, systems, and industrial protocols. Dynamic access can be adjusted in real time based on contextual attributes such as location and schedule. Gatekeepers support geofencing, policy-based access per microsegment, and automatic revocation of third-party access based on contract timelines or inactivity. A vendor management dashboard simplifies oversight of third-party sessions and permissions.

Monitoring is provided through live session logs, detailed audit trails, and full video session recordings, including keystrokes and mouse movements. Corsha is now moving to use AI and machine learning to establish behavioral baselines or flag anomalies in user behavior and currently correlates session data with third-party threat intelligence. All access attempts and policy violations are logged in real time. The Corsha Gatekeeper provides detailed network-level observability, including packet-level visibility and encrypted traffic status.

Corsha supports Ethernet-based industrial protocols including Modbus, Open Platform Communications Unified Architecture (OPC UA), DNP3, and Ethernet/Internet Protocol (IP). Policies can be applied at the device level, including for devices identified through integration with monitoring tools like Claroty. Support is not available for serial console interfaces or Process Field Bus (PROFIBUS).

Threat detection is handled through network-level observability and identity-based analytics. The Corsha Gatekeeper identifies reused secrets, reused machine identities, and anomalies in IP and Media Access Control (MAC) address mappings, and can flag suspicious activity such as unusual login times or lateral movement. Although Corsha does not support

automated response workflows, it includes predefined containment playbooks and session controls that allow administrators to terminate access manually or programmatically through integration with external security orchestration tools.

Corsha supports high availability through active-active clustering and geographic redundancy. Disaster recovery deployments are supported, with synchronized policies and configuration data across sites. However, active sessions are not preserved during failover events, and users must reauthenticate if interrupted. Failover typically completes within a few seconds, but the solution does not include automated failback, failover testing, or real-time dashboards for availability monitoring.

Corsha is certified to NIST SP 800-53 and operates with a US DoD Authority-to-Operate (ATO). While it does not provide automated compliance reports, it offers detailed access logs, session recordings, and traffic analysis data that can support audits for frameworks such as Cloud Security Alliance Security, Trust, Assurance, and Risk (CSA STAR) and Cyber Essentials. The Corsha platform logs user and device activity and captures traffic crossing the OT/IT boundary, enabling visibility and traceability across remote and machine-based sessions.

Corsha serves mostly large enterprises in North America, with plans to expand into Europe, initially focusing on the manufacturing sector. Its mIDP platform supports secure automation, policy-based access, and machine-to-machine identity in environments ranging from industrial automation to defense. Corsha is particularly relevant for organizations seeking a tightly integrated solution for SRA and microsegmentation in OT networks, especially those requiring Common Access Card (CAC)-based authentication, support for hybrid deployments, and visibility into machine traffic. Documentation and support are currently available only in English.

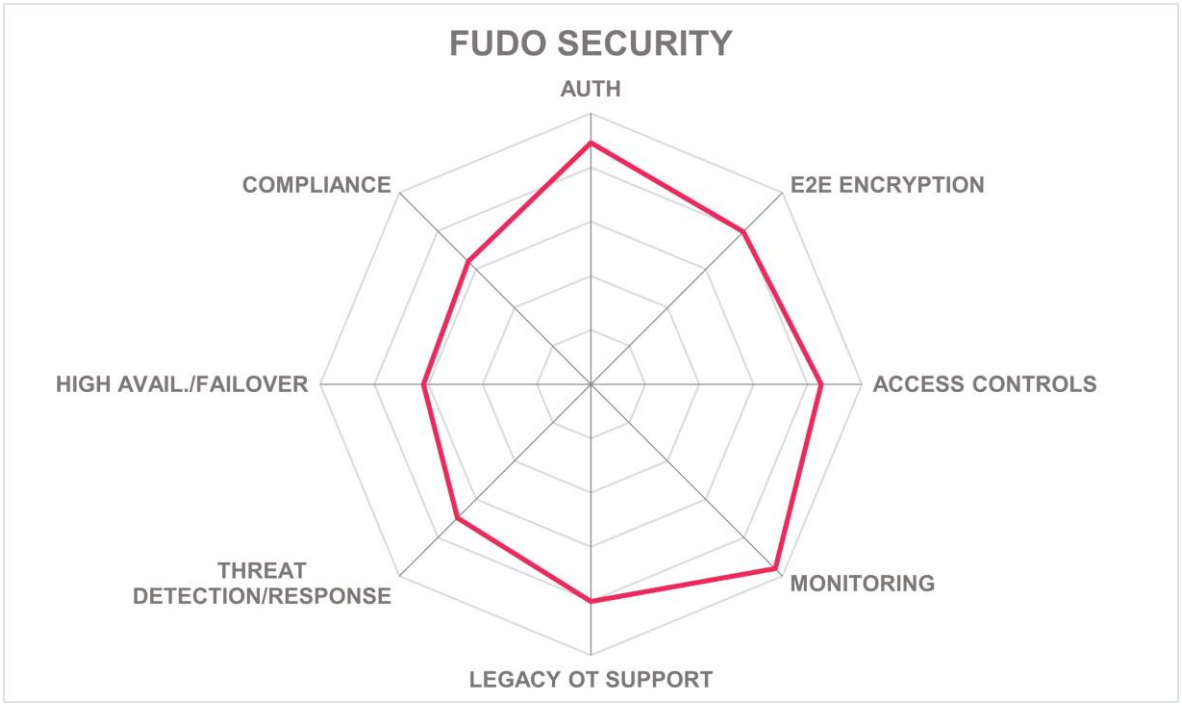
**Strengths**

- Strong machine identity lifecycle management platform
- SRA and microsegmentation in a single platform
- Real-time traffic visibility across OT environments
- Supports TLS 1.3 with mutual authentication
- Wide range of authentication options
- Supports RBAC with geo-fencing policies
- Detailed session logging with video recordings
- Integration with major identity and OT tools
- Flexible deployment including air-gapped environments
- Supports critical OT protocols like Modbus, Ethernet/IP, OPCUA, and DNP3

**Challenges**

- Limited automated incident response capabilities
- Lacks AI-driven behavior anomaly detection
- Does not preserve active sessions during failover
- No automated compliance report generation

## Fudo Security – Enterprise




Leader in







Fudo Security is a private cybersecurity company founded in 2004, with headquarters in Warsaw, Poland, and Newark, California in the US. The company focuses on secure remote access and intelligent privileged access management for medium and large enterprises. Fudo Enterprise is its main product, available via perpetual license or subscription, with licensing based on users, servers, or sessions. Deployment options include on-premises appliances, virtual machines, private and public clouds, and managed service providers. Fudo serves over 500 customers, primarily in EMEA, with expansion plans for the US and Asia-Pacific (APAC). Fudo Security claims full deployment typically takes less than 24 hours.

Fudo Enterprise includes four main modules: a Zero Trust Access Gateway, an AI-driven Privileged Session Manager, a Secret Manager password vault, and an Efficiency Analyzer. The platform uses agentless architecture for fast deployment and minimal operational disruption. It supports over ten remote access protocols, enabling video-level session monitoring without relying on screenshots. Fudo's AI capabilities are used for biometric behavior analysis, SSH session summaries, and risk-based access decisions. The platform includes dynamic port tunneling, granular RBAC, secure SSH tunneling, and automated

credential rotation. It is also designed to support clustered and high-availability environments.

The platform's strengths lie in its advanced session monitoring, AI-powered behavioral anomaly detection, and support for agentless access to even the most constrained OT environments. Its AI, trained on biometric patterns, can detect compromised accounts in real time. The Efficiency Analyzer provides operational insights beyond security, and the tunneling engine supports multiple OT protocols without VPN or port mapping. Fudo is especially strong in flexible deployment and licensing.

Fudo Enterprise supports a wide range of authentication and authorization methods including certificate-based authentication for users and devices, MFA, and device authentication. PBAC is implemented with support for contextual risk factors such as user behavior and device status. The platform supports OIDC and a limited set of policy attributes, including session metadata and network context. Delegated admin rights can be managed through configurable role definitions, but there is no support for ABAC.

Fudo Enterprise protects remote connections using TLS 1.2 and 1.3 with forward secrecy. It encrypts data at the application layer, selectively at the user or device level, and supports centralized on-premises key management. While mTLS is not supported, the solution does support certificate-based authentication for IoT and embedded OT devices and integrates with all major PKI providers. Real-time encryption status and alerts for encryption failures are available, but the solution does not support encrypted search or HSMs.

Access controls in Fudo Enterprise are designed around Zero Trust principles. The solution applies granular role-based permissions across applications, systems, and OT assets using a system of safes and groups. It supports automated credential rotation and network segmentation. Third-party access is managed via a vendor management dashboard and supports automatic revocation based on project status or inactivity. Access permissions can be dynamically adjusted based on real-time threat intelligence, vendor risk ratings, or AI-based risk scoring. Role definitions can be reviewed regularly, though there is no native optimization using analytics. The platform provides full session video monitoring, capturing mouse movements, keystrokes, and screen content in real time. Fudo correlates session activity with internal threat intelligence and supports anomaly detection through AI/ML algorithms trained on user behavior. Sessions are logged with timestamps and can be digitally signed for forensic investigations. Fudo integrates with SIEM platforms using Simple Network Management Protocol version 3 (SNMPv3) traps and can generate reports for audits and compliance documentation. Session content can be flagged, paused, terminated, or shared in real time by administrators.

Fudo Enterprise supports legacy OT environments by enabling secure access without software agents. It uses network-level proxies and jump servers for agentless communication and supports native protocols including Modbus Transmission Control Protocol (TCP) and teletype network (Telnet) for serial console access. The solution can apply access control and session policies for OT devices lacking built-in security and supports tunneling of any TCP-based protocol. It also provides SSH tunneling for secure use

of older protocols, and session monitoring is available even for legacy VNC and web interfaces rendered over HTTPS.

The solution detects threats by analyzing behavioral patterns and identifying privilege abuse or unusual access behavior. It does not support deep inspection of OT protocol payloads but can automatically terminate risky sessions and quarantine endpoints. AI-based scoring can trigger response workflows based on session content, user behavior, or device posture. Response actions include reauthentication, session blocking, and alerting. The solution supports customizable automated responses by severity but lacks predefined response playbooks for specific threat scenarios.

Fudo Enterprise supports active-active clustering and georedundant disaster recovery. Policies, session data, and configurations are synchronized across sites. Real-time dashboards provide visibility into availability and failover events. Although the platform does not maintain session persistence through failover, it does support automated failback. Failover testing is not automated, but configuration options allow customers to manage synchronization and replication directions across distributed clusters to optimize performance and redundancy.

Fudo Security complies with ISO 27001 and is in the process of implementing the necessary controls and undergoing preparations for SOC 2 Type 2 attestation. The solution is aligned with NIST 800-57 and FIPS 197 but not certified under either. It supports 72-hour breach reporting under the GDPR and NIS2. The platform can generate encryption status reports and security audit logs. Although not certified for IEC 62443, the solution supports audit logging for OT environments, including device access, which helps customers meet regulatory obligations in critical infrastructure sectors.

Fudo Security supports organizations in EMEA, with growing presence in APAC and North America. It serves mostly medium-sized businesses and mid-market enterprises in energy, telecom, and industrial sectors. Fudo Enterprise is well-suited for organizations requiring fast deployment, granular session control, agentless OT support, and strong third-party access governance. It supports seven languages for support and provides documentation in English, German, French, and Polish. Multitenant support, flexible licensing, and strong integration capabilities make it attractive for managed service providers and multinational enterprises alike.

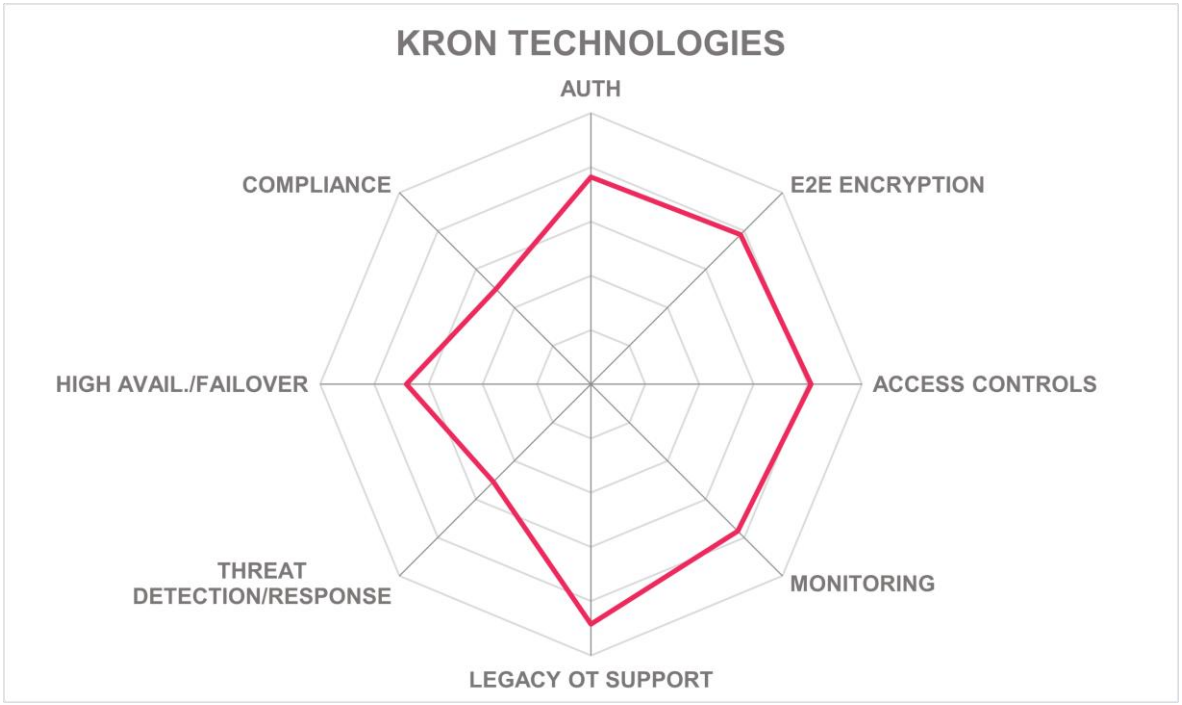
### Strengths

- Agentless architecture for fast, low-friction deployments
- Advanced session monitoring captures video, keystrokes, and mouse input
- AI-powered behavioral detection identifies compromised accounts in real time
- Dynamic tunneling supports OT protocols without VPN
- Biometric analysis enhances real-time threat detection
- Full RBAC with granular permission mapping
- SSH session summaries include threat-related insights
- Supports Zero Trust architecture across all access workflows
- Automated credential rotation

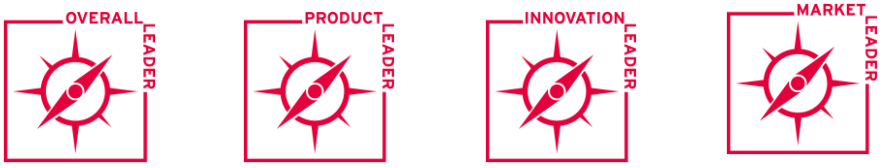
### Challenges

- Lacks predefined threat containment playbooks
- ABAC control not supported
- Session persistence lost during failover events
- Not certified for IEC 62443 compliance

# Kron Technologies – PAM




Leader in




Kron Technologies is a publicly listed cybersecurity company founded in 2007 and headquartered in Turkey, with R&D centers in Istanbul, Ankara, and Izmir. Kron PAM is deployed in over 30 countries, primarily across EMEA, and is offered via on-premises, public or private cloud, and managed service models. The solution is licensed primarily per user, with annual, three-year, and five-year subscriptions available. The standard Kron PAM license includes password vault, session manager, and multifactor authentication. SRA and User Behavior Analytics (UBA) are available as additional licensed modules.

Kron PAM supports a wide range of protocols including SSH, RDP, VNC, HTTPS, Structured Query Language (SQL), and legacy OT protocols such as Modbus and DNP3 via proxy-based tunneling. The platform enables agentless remote access with time-bound, role-based controls and secure credential injection. All sessions are logged, recorded, and made available for forensic review. Other modules include task automation, privileged account lifecycle management, and multitenant support. Administrators can monitor and control sessions in real time, apply policy-based approvals, and trigger alerts or session terminations if suspicious activity is detected.

Kron PAM's modular deployment, multitenancy, and agentless architecture enable use in both centralized enterprise deployments as well as MSP and Managed Security Service Provider (MSSP) environments. Notable features include adaptive keystroke-based MFA, session recording with searchable playback, and integration with OT protocols via encrypted tunneling. The in-house developed desktop client and browser proxy enhance user experience across IT and OT environments. However, the product does not yet include predefined response playbooks, automated role optimization, or native session integrity checks, and lacks certification under OT-specific frameworks such as IEC 62443.

The solution supports most major authentication methods, including Fast Identity Online 2 (FIDO2), One-Time Passwords (OTPs), and hardware tokens, with support for Remote Authentication Dial-In User Service (RADIUS) integration and SAML. Adaptive MFA can be triggered based on anomalous behavior, including typing patterns. The system allows fine-grained access policy enforcement using PBAC but does not support ABAC or certificate-based authentication for users, devices, or mutual verification.

Remote sessions are encrypted using TLS 1.3, WireGuard, or SSH tunneling, with support for PFS. Encryption can be applied selectively to specific assets or user groups, with enforcement and visibility managed from the dashboard. Encryption keys are stored in the environment where Kron PAM is installed (which can be on premises or in the cloud) or in HSMs, with support for Microsoft Active Directory Certificate Services (AD CS). Session-level encryption failures can trigger alerts, and forensic audit logs are available for post-incident review.

Access is governed by fine-grained policies tied to roles, time, IP range, and geography. Geofencing is supported. JIT access and post-session credential rotation are available. Role-based permissions can be customized for compliance with industry standards. The platform includes a third-party access dashboard with automated access revocation and multitenant controls. Access can be modified dynamically based on risk level or threat intelligence, but vendor risk scores are not currently integrated.

Monitoring capabilities include session video recording, keystroke and mouse tracking, and anomaly detection using machine learning. Sessions can be reviewed by keyword, timestamp, or behavior. File transfers and changes to sensitive configurations are also logged. While the platform cannot digitally sign logs or correlate activity with threat intelligence feeds, it can forward logs to external SIEM or Extended Detection and Response (XDR) systems for further analysis.

Legacy OT systems are supported through agentless access via proxies, jump servers, and tunneling. The platform can secure access to legacy protocols such as Telnet and VT100 and can enforce policy controls even for endpoints lacking native security. No protocol changes or agents are required on target devices. However, context-aware and risk-based policies for legacy systems are not supported, and unidirectional gateways are not used for air-gapped environments.

Threat detection is driven by machine learning-based User and Entity Behavior Analytics (UEBA), which can identify anomalies such as login irregularities, privilege abuse, and risky

access attempts. High-risk activities can trigger forced reauthentication or session termination. However, the platform does not support detection of lateral movement, session hijacking, or unauthorized access attempts, and does not include built-in containment playbooks or automated remediation workflows.

High availability is delivered through active-active clustering and geographic redundancy. Failover can occur within 10 to 15 seconds depending on architecture, but users must reauthenticate and reestablish sessions after failover events. Session state is not preserved. Policies and configurations are synchronized between redundant sites. Automated failback is supported, along with real-time dashboards for availability status, but non-disruptive failover testing is not available.

Kron PAM supports compliance with ISO 27001 and helps customers meet requirements of frameworks such as IEC 62443 and NERC CIP through policy enforcement, logging, and built-in reporting templates. Reports include encryption configurations, session logs, and access events. While Kron PAM is not certified under these frameworks, it can support GDPR and NIS2 incident reporting timelines and provides audit-ready exports in Portable Document Format (PDF) and Comma-Separated Values (CSV). Logs are maintained for OT, IT, and IoT environments routed through its gateway.

Kron PAM is used primarily by mid-market and enterprise organizations in EMEA, with increasing presence in APAC and North America. Energy and manufacturing sectors are the largest adopters of the SRA module, especially where third-party access must be secured without VPNs. Customers with outsourced IT or OT support will benefit from the solution's time-based and application-specific session controls. The Kron PAM interface supports six languages. Support is limited to four languages, but documentation can be localized using Kron's document management portal. The solution's multitenant capabilities and agentless deployment suit managed service scenarios and segmented environments.

### Strengths

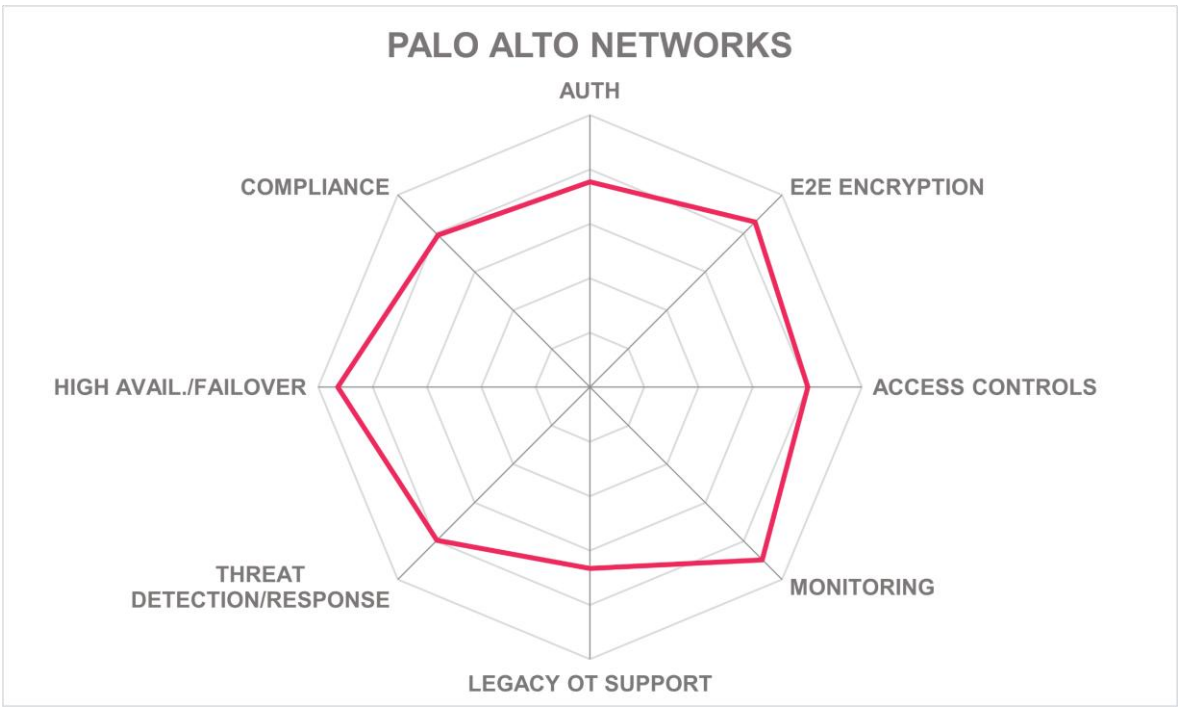
- Supports wide range of OT and legacy protocols
- Enables agentless remote access via encrypted tunneling
- Offers adaptive MFA triggered by behavioral anomalies
- Provides fine-grained access control and geofencing
- Includes ML-based behavior analytics
- Compatible with all major authentication protocols
- Supports modular and multitenant deployment
- Enables policy-based approvals and session termination
- Offers flexible encryption with dashboard visibility
- Integrates with SIEM and XDR platforms

### Challenges

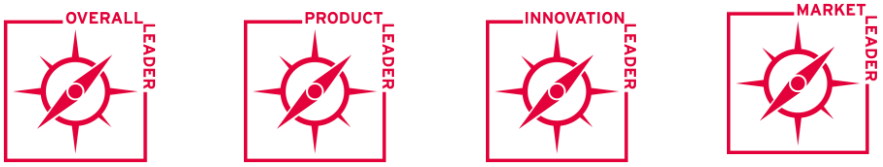
- Lacks predefined incident response playbooks
- No detection of lateral movement or session hijacking
- Not certified under key OT compliance frameworks

- Session state not preserved during failover
- No support for ABAC or certificate-based user authentication
- Log forwarding to external SIEM/XDR supported but no digital signing or threat feed correlation

## Palo Alto Networks – Strata Platform




Leader in




Palo Alto Networks, founded in 2005 and headquartered in Santa Clara, California in the US, is a global public cybersecurity company with a significant presence across North America, EMEA, APAC, and LATAM. The company has long served the OT space, primarily through its appliance-based Next-Generation Firewall (NGFW) deployments. Its SRA capabilities are offered through two main approaches: NGFW appliances for on-premises deployment, and Prisma Access, its Secure Access Service Edge (SASE) cloud service. Pricing for NGFW deployments is hardware-based with a percentage licensing model for security services, while Prisma Access follows a per-user, per-year subscription model.

The SRA capabilities of Palo Alto Networks are anchored in its Strata Platform, which includes NGFWs, Prisma Access, and Strata Cloud Manager (SCM) for unified policy and device management. The platform supports both client-based and clientless access using GlobalProtect VPN or the Prisma Access Browser for Privileged Remote Access (PRA). Key capabilities include ZTNA, deep application-level policy enforcement for OT protocols, integration with threat intelligence and detection tools like WildFire for sandboxing, and support for SSH, RDP, and VNC protocols without requiring jump servers. Prisma Access

Browser also adds visibility and control for unmanaged endpoints and third-party access scenarios.

A key differentiator is the integrated nature of the SRA platform, which extends uniform policy enforcement and deep OT-specific inspection across appliance and cloud-based deployments. The integration of application-layer OT protocol visibility and control (including support for over 1,200 App-IDs), combined with advanced session control, JIT access workflows, and on-screen watermarking, provides strong alignment with OT security needs. Prisma Access Browser further expands this with host posture validation, clipboard control, and live session supervision. Improvements could include support for serial console protocols, more automation in third-party access revocation, and expanded protocol coverage to include legacy serial interfaces like PROFIBUS.

The solution supports all main identity standards including OIDC, and all common authentication methods for internal and external users. The Cloud Identity Engine integrates with customer IdPs, enabling support for MFA, certificate-based authentication for both users and devices, and real-time risk assessments for policy enforcement. The system also uses device authentication to restrict access to trusted endpoints and supports both ABAC and PBAC for delegated administration.

All remote connections are encrypted end-to-end, with full data encryption using modern protocols such as TLS 1.3 and IPSEC VPN. PFS ensures that past sessions remain secure if any session key is compromised. Prisma Access supports mTLS authentication and uses centralized key management with integration into HSMs. The solution supports secure tunneling of encrypted industrial protocols such as Modbus and DNP3 and provides real-time visibility into encryption status and audit trails for incident investigation.

Access controls in the solution are highly granular. Policies can be applied to specific systems, assets, OT protocols, and even functional commands within industrial control environments. OT App-IDs allow command-level policy enforcement. Prisma Access Browser extends access control with policy-based restrictions on data handling, clipboard use, and session recording. Role-based permissions can be customized per asset or user group, and dynamic risk-based adjustments are possible based on endpoint posture, behavior, and vendor risk profile. However, automatic credential revocation is not supported after contract termination or user inactivity.

Real-time monitoring is provided through centralized logging and AI-driven anomaly detection. The solution can correlate session logs with threat intelligence and detect deviations from baseline user behavior. Activities such as file uploads, session hijacking, and unauthorized access attempts are logged and can trigger automated incident response workflows via integration with Cortex XSOAR. Although log entries are not cryptographically signed for tamper detection, forensic visibility is strong, with session recordings and live supervision available through Prisma Access Browser.

Legacy OT support includes agentless access to systems that cannot run software clients, with access provided via proxies, jump boxes, and session brokers. Policies can be applied even to unmanaged IoT/OT devices. While the solution cannot support serial console

protocols such as VT100 or Telnet, it does support access to air-gapped environments using local service edge brokers. Risk-based access policies can be applied to legacy systems based on contextual awareness and endpoint characteristics.

Threat detection includes deep packet inspection of OT network traffic to identify protocol manipulation and malicious commands. The platform can detect lateral movement, session hijacking, and anomalous use of privileged accounts. Real-time threat intelligence integration supports context-aware detection, and behavioral anomalies such as login time deviations or suspicious access patterns can trigger automated response. Threat response playbooks are customizable and supported via Cortex XSOAR, allowing automated session termination, quarantine actions, and alerting based on severity.

High availability is achieved through active-active and active-passive failover options in both appliance and cloud deployments. Prisma Access offers built-in disaster recovery and geographical redundancy. Access policies and configurations are synchronized across sites, and failover can occur with minimal session disruption and no need for reauthentication. The system supports automated failback and provides dashboards and alerts for failover status. Automated failover testing ensures that continuity plans can be validated without impacting operations.

The solution is certified for a broad set of regulatory frameworks, including FIPS 140-2, ISO 27001, NIST 800-57, PCI DSS, and IEC 62443. It supports GDPR and NIS2 requirements, including 72-hour incident reporting, and can log device access in IoT environments for compliance. SOC 2 Type 2 attestation is in place for key trust principles. Audit-ready reports can be automatically generated, including those focused on encryption and access logging. Data protection and audit visibility are supported across all SRA methods.

Palo Alto Networks supports a broad global customer base with a strong presence in North America and growing deployments across EMEA, APAC, and Latin America (LATAM). The solution is especially well-suited for industrial organizations seeking secure access across distributed OT environments, including utilities, manufacturing, and critical infrastructure. Typical use cases include remote vendor access, privilege remote access, access to engineering workstations, and secured inter-site connectivity. Prisma Access Browser reduces the need for virtual desktops and simplifies third-party access control. Support services are currently available in only English, Chinese, and Japanese, but documentation is available in a wide range of languages.

**Strengths**

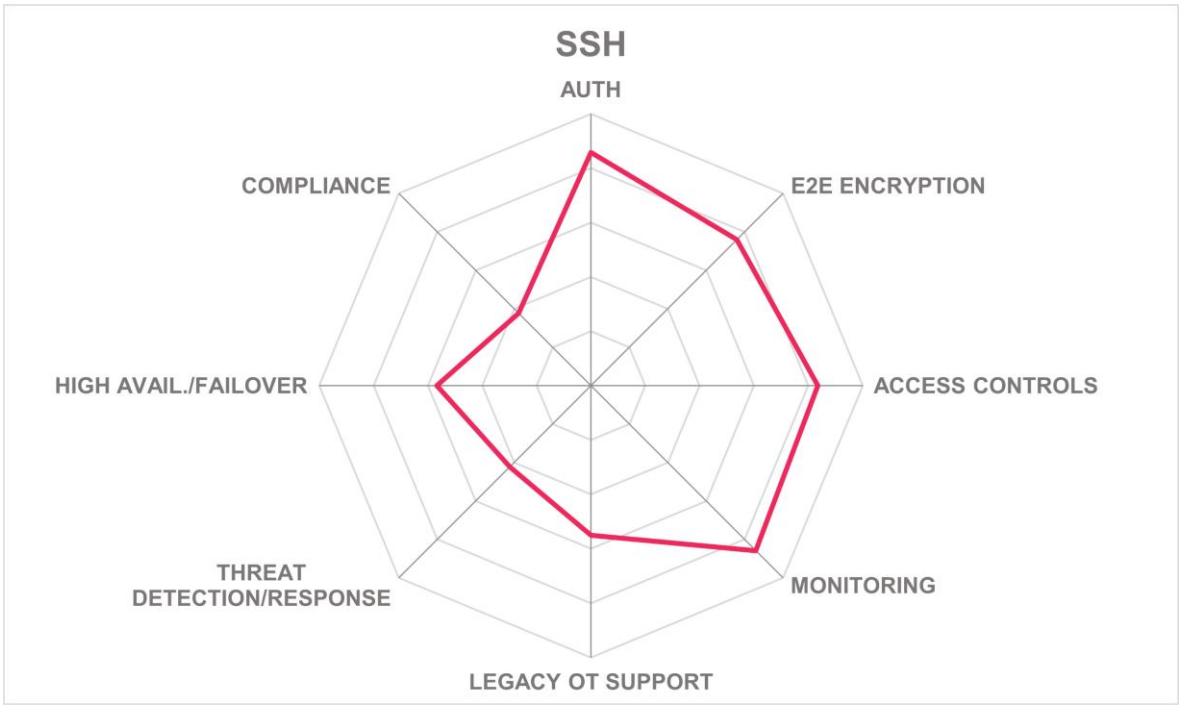
- Deep OT protocol visibility with over 1,200 App-IDs
- Unified platform for appliance and cloud-based deployments
- Deep packet inspection of OT network traffic
- Strong session control with JIT access workflows
- End-to-end encryption using TLS 1.3 and IPSEC VPN
- Integrated threat detection with real-time intelligence correlation
- Granular access controls down to protocol command level
- Live supervision and session recording for remote users
- High availability with failover and disaster recovery options

- Strong support for unmanaged and third-party devices
- Broad compliance certification for industrial environments

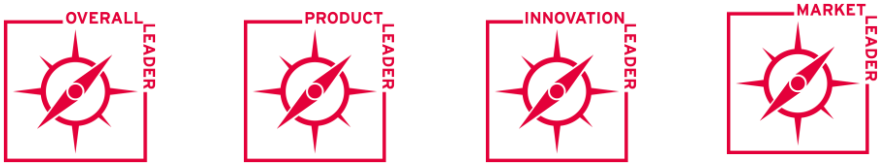
**Challenges**

- No support for legacy serial protocols like PROFIBUS
- Lacks automatic revocation of third-party access rights
- Log integrity not verified with digital signatures
- Support services in only three languages
- Serial console access such as VT100 not supported

## SSH Communications Security – PrivX OT




Leader in




SSH Communications Security is a publicly listed cybersecurity vendor founded in 1995 and headquartered in Helsinki, Finland, with additional offices in New York and Singapore. The company has a strong global presence with a customer base spanning EMEA, North America, APAC, and LATAM. SSH offers a flexible subscription-based pricing model with support included and full access to future updates. Pricing for PrivX IT/OT is based on the number of users and targets, whereas the OT Edition is based on the number of production units to accommodate large industrial deployments. PrivX can be deployed on premises, in the cloud, in Kubernetes, and in air-gapped environments.

PrivX OT is a PAM platform that is purpose-built to secure remote access for OT environments while supporting full IT/OT convergence. The solution provides secure, passwordless, and keyless access to critical infrastructure, with JIT and JEA controls, microsegmentation, session recording, and asset discovery. It supports all major protocols including SSH, RDP, VNC, and HTTPS. PrivX OT includes Representational State Transfer (REST) APIs, session monitoring, network target routing, and jump hosts. Access control

policies, approval workflows, and PAM functionalities are embedded to simplify secure remote access across complex OT networks.

PrivX OT stands out for its combination of modern microservice architecture, ease of use through browser-based access, and flexible deployment that includes Kubernetes and air-gapped environments. Customers benefit from extensive automation, rapid provisioning, and passwordless access using ephemeral certificates. Unique selling points include support for quantum-safe tunneling for remote access and dynamic JIT site-to-site connections, a vendor management dashboard, and integrations with Honeywell Forge for OT asset discovery and insights. Areas where further development is needed include built-in support for privilege escalation detection, real-time encryption status dashboards, and advanced compliance reporting automation.

PrivX OT supports modern and passwordless authentication methods including passkeys, FIDO2, biometric authentication, and device trust evaluation. It integrates with identity and governance systems such as Microsoft Entra ID, LDAP, and OIDC-based providers. Fine-grained policy enforcement is enabled through ABAC and PBAC. The solution supports device posture checks and enforces role-based access mapped from external identity sources, with real-time policy enforcement for user and device trust levels.

PrivX OT ensures all remote connections are encrypted using forward secrecy and short-lived certificates. It supports mTLS authentication, centralized key management, and integration with HSMs. TLS 1.3 and Network Level Authentication (NLA) are used for protecting data in transit. The solution supports certificate-based authentication for both users and IoT devices. Although it does not provide real-time encryption status dashboards, PrivX OT generates alerts for encryption failures and forensic-level audit logs for incident investigations.

Access control within PrivX OT is based on Zero Trust principles, using continuous verification and dynamic policy enforcement based on user roles, risk levels, and device trust. The system enables granular access to individual applications, devices, and services, supports session-specific credential injection, and provides automatic credential rotation. It includes controls for third-party access management, including automatic revocation based on contract status or inactivity. Microsegmentation, network isolation via the PrivX Extender and Router components, and production unit–level licensing further enhance access granularity and scalability.

PrivX OT includes live session monitoring, session video recording, file transfer tracking, and correlation with external threat intelligence systems via SIEM integration. The platform uses syslog and Common Event Format (CEF) for exporting logs. While full behavioral anomaly detection based on AI/ML is on the roadmap, the current release supports basic anomaly detection and forensic audit capabilities. All access and activity within the platform are logged with role-based filtering and access history, although digital signature support for log integrity is not yet available.

PrivX OT provides secure agentless access to legacy OT systems using reverse proxy architecture, session brokers, and jump servers. It supports protocols such as Modbus, OPC

UA, and DNP3, but not PROFIBUS or serial-based systems like VT100. The solution can be used in air-gapped environments through on-premises service edges and unidirectional gateways, although it lacks fine-grained control for insecure IoT endpoints. No support is available for policy enforcement based on legacy device-specific parameters.

PrivX OT includes behavioral analytics to detect suspicious login behavior, lateral movement, and abnormal device activity. Detection of session hijacking, protocol misuse, and malicious command injection is supported when PrivX OT is used together with the separately licensed PrivX OT Insights module. The platform does not support threat containment playbooks or automated incident response workflows, though these can be triggered via third-party APIs. PrivX OT can terminate sessions, block compromised accounts, and generate alerts based on behavior anomalies, but does not support fine-grained automated threat responses based on severity or attack type.

High availability is supported through active-active clustering and geographically distributed disaster recovery. Access policies, sessions, and configuration settings are synchronized across sites. Although failover requires session re-establishment, users remain authenticated and can reconnect without logging in again. Typical failover time is around 30 seconds. Automated failback is supported, but PrivX OT lacks automated failover testing and real-time availability dashboards. The solution is designed to operate reliably in critical OT environments but does not maintain live session continuity during failover.

PrivX OT supports regulatory compliance through certifications including FIPS 140-3, ISO 27001, and the EU Cybersecurity Act. It also supports GDPR and NIS2 incident reporting within 72 hours and logs IoT device access for compliance tracking. However, it does not offer SOC 2 attestation, audit-ready compliance reports, or encryption reporting for audits. PrivX OT can send logs and compliance data to external platforms but does not automate compliance report generation or provide built-in dashboards for audit visibility.

PrivX OT is well-suited to large organizations in critical infrastructure, manufacturing, energy, and defense sectors with geographically distributed OT environments. It supports multilingual service interactions, although product documentation is available only in English. Key customer groups include enterprise and mid-market organizations seeking secure remote access across both OT and IT environments. The solution supports multiple deployment models and is designed for organizations requiring high scalability, advanced security controls, and compatibility with legacy OT systems without the need for endpoint agents.

**Strengths**

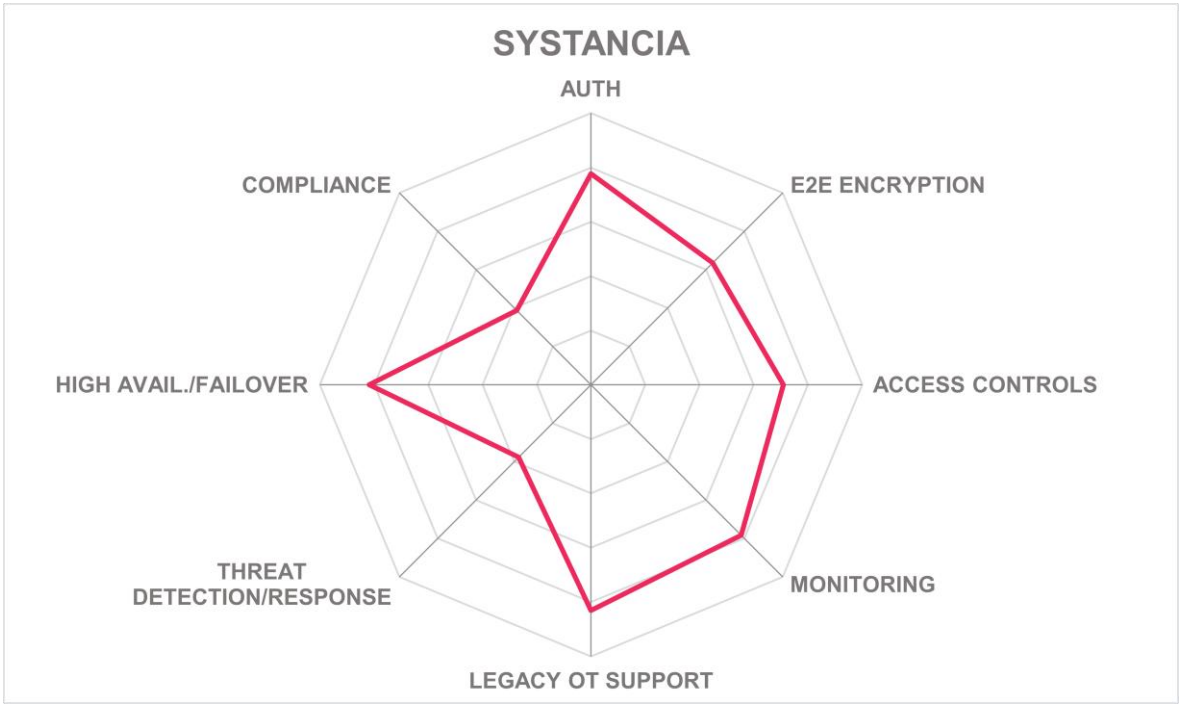
- Supports passwordless and keyless access
- Flexible deployment options including Kubernetes and air-gapped environments
- Strong integration with IAM and IGA systems
- Zero Trust access with dynamic policy enforcement
- Supports quantum-safe tunneling protocols
- Granular access control and microsegmentation
- Agentless access to legacy OT systems
- Session recording and forensic audit capabilities

- Easy integration with SIEM via syslog and CEF
- Role-based access mapped from external identity sources

**Challenges**

- No real-time encryption status dashboards
- Lacks automated compliance reporting features
- No support for PROFIBUS or serial-based systems
- Threat containment playbooks not included
- Session continuity not maintained during failover
- Limited built-in support for privilege escalation detection

## Systancia – cyberelements




Leader in


Systancia is a private French cybersecurity company founded in 1998, with its headquarters in Sausheim, France. The focuses on secure access technologies through its cyberelements SaaS platform. Systancia targets mid-sized and upper mid-market organizations, particularly in regulated sectors. The solution is available in SaaS and on-premises deployment models, with SaaS priced per concurrent user. On-premises pricing depends on the module: ZTNA and critical access management are priced per concurrent user, IGA by identity, and SSO by named user.

Customers span across EMEA, with growing presence in Northern Europe and the Middle East, and sales are driven primarily through channel partners.

The cyberelements platform consolidates ZTNA, critical access management, IGA, and SSO into a single offering. The platform provides secure remote access for employees and third parties to both IT and OT systems. Key capabilities include rapid deployment in under five minutes, adaptive access controls based on user and device posture, clientless access via protocol break, secure tunneling of encrypted OT protocols, multitenant support, real-time

session monitoring with video recording, and session credential injection. It supports agentless and software-client access modes and includes integration with identity providers, SIEM tools, and XDR systems.

cyberelements stands out for its rapid instantiation, stateless architecture, and concurrent-user pricing model. The architecture features protocol break and URL rewriting to block inbound exposure, volatile port allocation, and full session recording. The platform provides zero standing connections, JIT account provisioning, and extensive integration capabilities. The solution includes advanced session security without requiring endpoint agents, and its multitenant access controls suit MSPs. However, improvements are needed in automated incident response, anomaly detection for IoT devices, and formal compliance reporting. Certification coverage also remains limited compared with peers.

The solution supports multiple authentication options including password-based, certificate-based, smartcard, and device-contextual authentication, but not fingerprint or facial biometrics. It supports MFA methods and integrates with third-party identity providers through SAML 2.0 and OIDC. PBAC and ABAC are supported, including policies informed by real-time risk scores and device posture. Device trust checks include antivirus presence. Mutual authentication between devices and users is not supported.

cyberelements supports encrypted tunnels for protocols like Modbus and DNP3 and protects data in transit using TLS 1.3. End-to-end encryption is enforced, and encryption keys are customer-managed either on premises or via the Cloud Service Provider. The solution uses centralized key management but does not integrate with HSMs or PKI systems. PFS is not supported, but search operations on encrypted data are enabled without decryption. Real-time visibility of encryption status is included, and alerts can be triggered for failures.

Access control is granular at the level of individual OT systems, applications, and industrial protocols, and can be customized for compliance needs. Access policies can be enforced dynamically based on context, such as role, risk level, or geo-location. Role-based access is supported but not continuously optimized through analytics. Automatic credential rotation and vendor access revocation are available. The platform includes a vendor dashboard for managing third-party access and offers multitenant access management through a centralized console. However, integrations with vendor risk scoring and dynamic access tuning based on third-party threat intelligence are pending.

The platform includes AI-based user behavior analytics for anomaly detection and alerts on deviations from baseline profiles. It supports video recording of sessions, including screen and input activity, and logs file transfers and configuration changes. It integrates with SIEM platforms via open-source rocket-fast system for log processing (rsyslog) for event correlation. Session logs are not cryptographically signed. Session logs, threat feeds, and contextual metadata can be correlated to detect suspicious activity. However, the solution lacks built-in integrity verification of log files and does not generate compliance-ready audit reports.

cyberelements supports secure remote access to legacy OT systems using agentless jump servers, Hypertext Markup Language version 5 (HTML5)-based clientless access, and

network-level protocol break. It provides session control over devices using serial interfaces such as VT100 and RS232. Context-aware access policies can be applied even in legacy environments. Protocol-agnostic tunneling supports heterogeneous industrial environments. Network segmentation is enforced through distributed gateway deployment across Purdue model levels. For air-gapped environments, local gateways and unidirectional data diodes provide connectivity without inbound ports.

Behavior-based threat detection identifies anomalies such as privilege escalation, unusual remote device activity, lateral movement, and suspicious access locations. Session hijacking is prevented using real-time session validation. While the platform can terminate compromised sessions and alert administrators, it lacks predefined containment playbooks. Automated response actions are limited in customization, and the system does not support automated remediation workflows or mandatory re-authentication for sensitive actions. Integration with external XDR solutions is recommended for advanced response automation.

High availability is achieved through active-active clustering, failover support, and disaster recovery site deployment. Sessions persist across failover events without requiring users to reauthenticate, with a typical failover time of 30 seconds according to Systancia. Policy synchronization and session continuity are maintained across redundant nodes. Automated failback is supported to restore access to the primary system. However, there are no real-time dashboards for failover status, and the platform does not support scheduled failover testing.

cyberelements is not certified for compliance with relevant NIST and FIPS standards or IEC 62443. It is undergoing Agence nationale de la sécurité des systèmes d'information First-Level Security Certification (ANSSI CSPN) and has plans for European Union Cybersecurity Certification Scheme (EUCS). The platform supports incident reporting under Europe’s GDPR and NIS2 directives and includes logs for audits but lacks automated compliance reporting and mapping of controls to standards.

The solution supports organizations in regulated sectors including public administration, logistics, energy, food and beverage, water, and biomedical manufacturing. It is suited to mid-sized companies and departments of large enterprises operating under financial or regulatory pressure. It is also suitable for MSPs that deliver remote access to distributed OT environments. Language support is provided in English, French, and German, with documentation in English and French. Common use cases include third-party access, critical access, regulatory compliance, and remote work.

**Strengths**

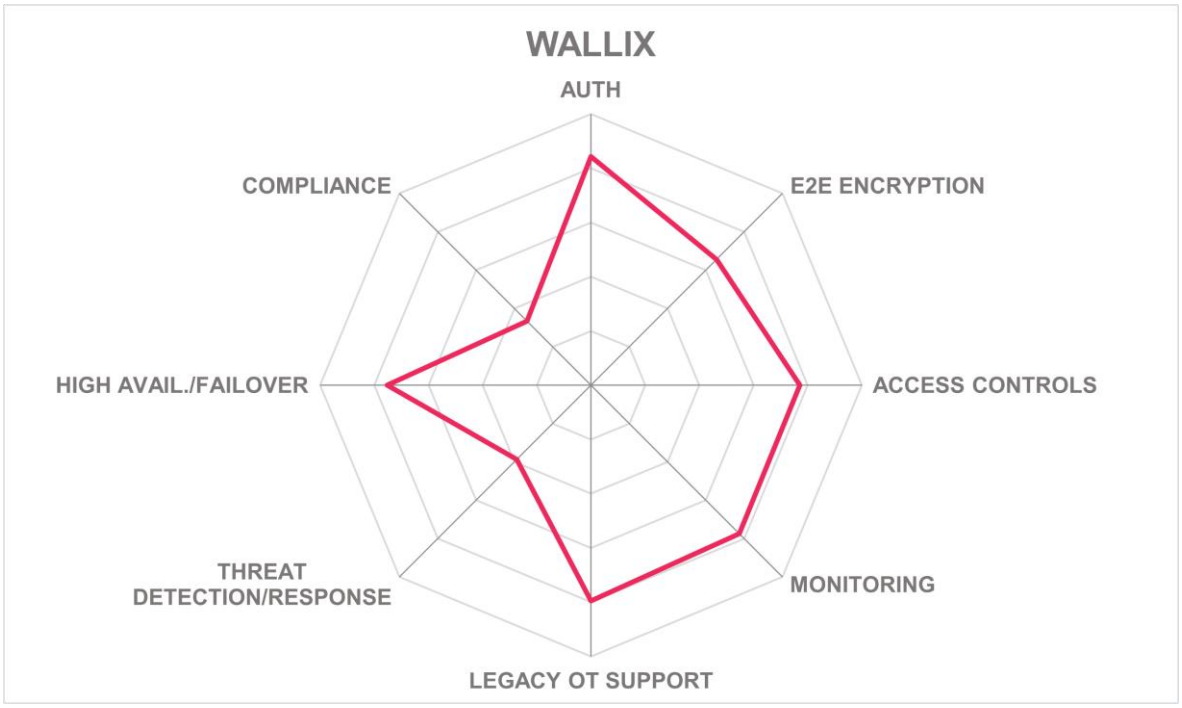
- Solution supports rapid SaaS deployment
- Concurrent-user pricing simplifies SaaS cost planning
- Supports both IT and OT remote access
- Zero Trust architecture with JIT connections
- Secure clientless browser access
- Advanced session recording with credential injection
- Multitenant architecture suits MSP environments
- Agentless access to legacy OT systems

- Secure encrypted tunneling for OT protocols
- Contextual access policies with device posture checks

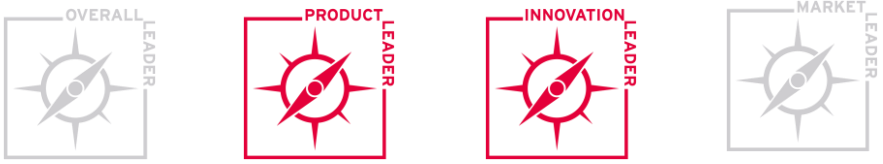
**Challenges**

- No automated compliance reporting features
- Limited support for biometrics and mutual authentication
- Certification coverage is incomplete and ongoing
- Automated response customization currently limited
- Lacks mutual authentication for devices and users

## WALLIX – IDaaS, PAM, One Remote Access, One PAM.




Leader in




WALLIX is a publicly listed French cybersecurity vendor founded in 2003. The company has its headquarters in Paris and operates globally through eight offices and a network of more than 300 partners, with most customers located in EMEA. WALLIX offers a flexible pricing model that supports multiple licensing metrics including named and concurrent users, number of managed resources, or machines. Customers can choose between perpetual and subscription models. The modular pricing structure allows organizations to tailor their purchases to specific needs and scale as their usage increases, backed by quantity-based discounts and “pay-as-you-grow” options.

WALLIX delivers secure remote access capabilities for OT environments under its OT.Security brand via a combination of interoperable products, including WALLIX PAM Bastion, Access Manager, and the cloud-based WALLIX One Remote Access and PAM platforms. The solution stack is purpose-built for industrial use cases, providing centralized access control, privileged session management, credential vaulting, and industrial protocol support through universal tunneling. All core functions are built on an agentless, Debian-

hardened, distributed platform designed to minimize operational disruption and streamline deployment in OT environments.

A key strength of the solution is its native protocol isolation capability, which replaces traditional VPN-based access with a secure gateway using HTTPS as the entry point and a secondary connection to the target asset. This enables session control, approval workflows, file scanning, credential injection, and full video recording. Universal tunneling allows direct access to PLCs and HMIs using encrypted industrial protocols, with no need for agents. Weaknesses include the lack of AI-powered anomaly detection, but this is on the roadmap.

The solution supports a range of authentication methods, including integration with identity providers using SAML and OIDC. MFA is available for both internal and external users, including token- and certificate-based methods. Administrative access is controlled via RBAC and delegated privilege management, with support for device authentication through Trusted Platform Module (TPM) binding. While real-time risk-based policies are not supported, there is support for native biometric authentication and the platform has recently added support for FIDO2 and SSH authentication.

End-to-end encryption is a design principle across all WALLIX remote sessions. TLS 1.3 and SSH protocols secure data in transit, and encryption keys are centrally managed within the platform. The solution supports mTLS for API connections. PFS is supported to ensure key compromise does not affect past sessions. The system integrates with standard PKI providers such as DigiCert and GlobalSign and supports certificate-based authentication for OT and IoT devices. It supports selective encryption for specific users or assets, but integration with HSMs is not yet supported.

WALLIX provides fine-grained access controls across users, devices, applications, and specific OT data points. Access permissions can be defined per target group using business logic and mapped to role-based policies. Third-party access is centrally managed through a dedicated dashboard, with features like automatic revocation, access expiration, approval workflows, and REST API-based integration with vendor risk tools. However, real-time automated risk scoring and adaptive access adjustments are not currently supported.

The solution includes comprehensive monitoring and auditing capabilities, including full video session recording with mouse and keyboard activity, session metadata, and searchable logs. Files uploaded or downloaded are scanned via antivirus and data loss prevention tools using Internet Content Adaptation Protocol (ICAP). Session logs can be forwarded to SIEM systems, but the solution does not support native anomaly detection. It supports digital signing of logs and forensic-level encryption audit trails. AI-based behavior analysis is on the roadmap.

WALLIX supports secure access to legacy OT systems using agentless methods such as jump servers and session brokers. It supports a wide range of protocols including VNC, Telnet, Modbus, OPC UA, Ethernet/IP and DNP3, but not PROFIBUS. The platform accommodates serial console interfaces like RS-232 and VT100 and can enforce contextual access policies for legacy devices. No software agents are required on endpoints, which helps reduce deployment friction in constrained environments.

The platform detects and responds to common threat behaviors such as privilege escalation, lateral movement, unusual login patterns, and unapproved file transfers. Responses include session termination and security team alerts. The solution can detect session hijacking and privilege abuse, does not yet detect novel attack techniques. It lacks deep inspection of industrial traffic and predefined response playbooks, but these areas are part of a longer-term roadmap that includes dynamic access governance and behavioral risk scoring.

High availability is supported through active-active clustering, disaster recovery site synchronization, and real-time configuration replication. According to WALLIX, the cloud-based WALLIX One platform uses Kubernetes with redundant pods to ensure 99.9% uptime. While user authentication is preserved during failover, remote access sessions must be re-established. Automated failback is supported on premises and in the cloud. Availability dashboards are included, but there is no automated failover testing or real-time failover status visibility.

WALLIX supports compliance with ISO 27001 and GDPR. It has BSI certification with reciprocal ANSSI certification. While the WALLIX PAM system uses the Advanced Encryption Standard (AES) aligned with FIPS 197 and integrated cryptographic libraries aligned with FIPS 140-3, it is not self-certified for FIPS 140-3. Compliance with IEC 62443 is in progress. The platform does not support automated compliance reports, incident reporting for NIS2, or logging for IoT device access. However, it maps well to regulatory frameworks such as MITRE ATT&CK® for ICS and NIST standards.

The solution is used primarily by medium-sized and large organizations in EMEA, with customers in manufacturing, utilities, transportation, critical infrastructure, and healthcare. Use cases include secure third-party maintenance access, protocol isolation for sensitive assets, delegated administration, and audit-grade visibility. Support is available in six languages, though documentation is limited to English and French. The solution is designed to be accessible to OT personnel with minimal IT background.

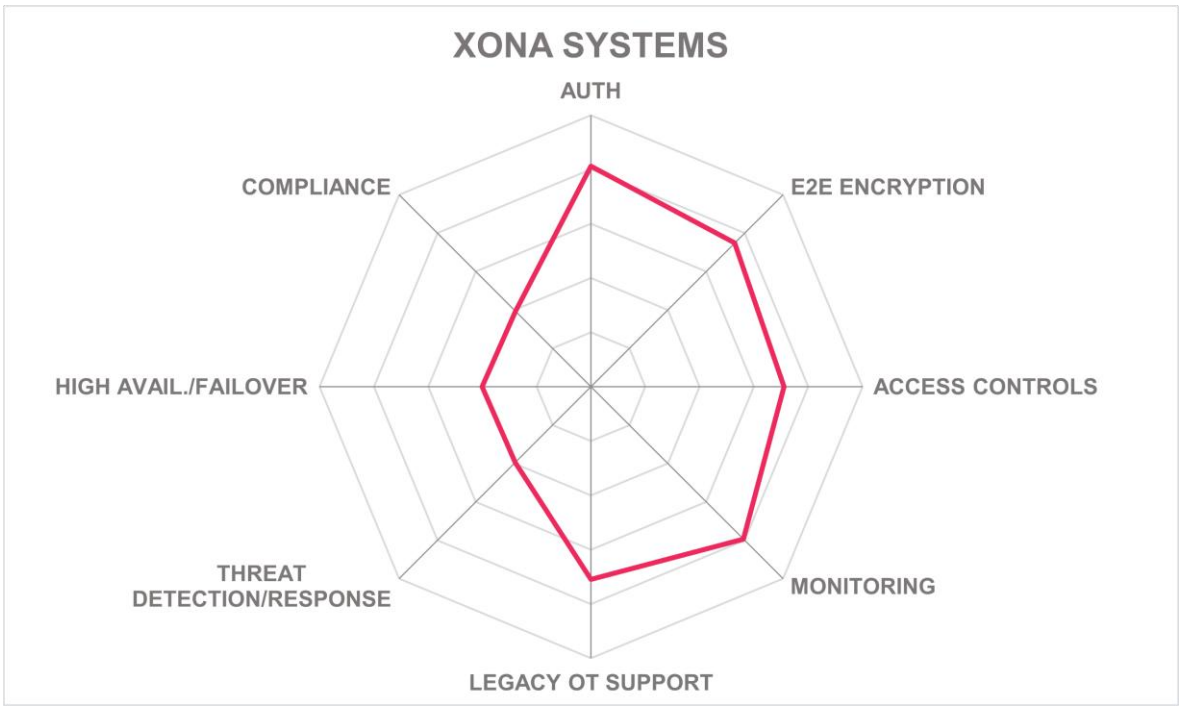
### Strengths

- Agentless platform minimizes operational disruption in OT environments
- Protocol isolation removes need for traditional VPN access
- Supports wide range of industrial and legacy protocols
- Offers flexible, scalable, and modular pricing model
- Universal tunneling enables encrypted PLC and HMI access
- Full video session recording with searchable metadata
- Centralized third-party access management with approval workflows
- Supports both on-premises and cloud-based deployment
- Device authentication using TPM
- Session logs exportable to external SIEM platforms

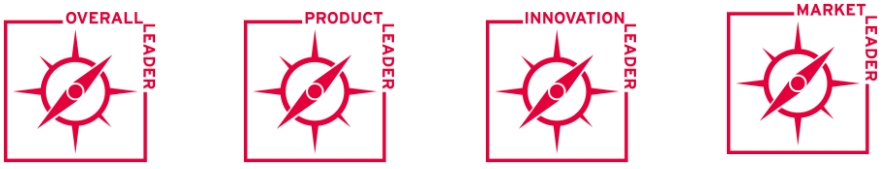
### Challenges

- Lacks native anomaly detection and behavioral analytics
- Cannot preserve remote session state during failover
- Not certified under key OT security frameworks

## Xona Systems – Platform




Leader in




Xona Systems is a private company founded in 2017 and headquartered in Hanover, Maryland in the US. The company's flagship offering, the Xona Platform, is purpose-built to provide secure remote access for critical infrastructure in OT, ICS, and CPS. Xona supports flexible deployment models including hardened physical appliances, virtual gateways, and private cloud deployments. Xona can also operate in disconnected or air-gapped environments. The software is licensed annually, primarily per gateway and per asset, with optional hardware add-ons. Xona maintains a global presence with customers in over 40 countries and strong adoption in North America, EMEA, and Southeast Asia.

Xona delivers secure access by acting as a proxy layer between remote users and OT assets, supporting interactive protocols such as RDP, SSH, VNC, and WebGL-graphical based applications through session isolation. Sessions are rendered via browser using Portable Network Graphics (PNG) images, removing direct protocol exposure while

improving responsiveness, even over low-bandwidth links. The solution supports MFA, time-based access, and session approval workflows. Every session is video-recorded and logged. The Centralizer provides centralized policy control, auditing, configuration management, and access visibility across distributed gateways, with support for active-passive high availability.

A strong feature of the Xona Platform is its browser-based protocol isolation approach. This eliminates direct endpoint-to-asset communication and requires no agents or plug-ins. This architecture supports secure access without modifying legacy assets and performs well in bandwidth-constrained environments. Xona's design prioritizes ease of use and deployment, with Xona claiming that most gateways operational in under 30 minutes. Although it lacks native device trust validation or risk-adaptive access, Xona offsets this by enabling integrations with identity providers, behavioral analytics platforms, and OT visibility tools. Active-active clustering and deeper context-aware access enforcement are two areas for future development.

Xona supports federated authentication using SAML 2.0 and integrates with identity providers such as Okta, Ping Identity, and Microsoft Entra ID. MFA is supported through TOTP apps and hardware tokens including YubiKey. Biometric authentication can be leveraged indirectly via upstream identity providers. Certificate-based user authentication is supported, and mTLS authentication for sessions and APIs is planned. Device-based trust validation and Open Authorization 2.0 (OAuth 2.0) or OIDC are not natively supported but can be added through upstream integrations.

Xona applies TLS 1.2 and TLS 1.3 encryption across all user sessions and system communications. Remote access connections are end-to-end encrypted using TLS, while internal communications between gateways and the Centralizer are protected using the WireGuard protocol. PFS is enforced to safeguard session confidentiality. Encryption keys are either managed locally or stored in external HSMs. While Xona lacks native centralized key management, users can store credentials in encrypted local vaults and rotate them using external tools. Xona integrates with external key management systems to support enterprise-grade encryption requirements.

Access control is implemented through RBAC, time-based policies, and optional JIT approvals. Sessions are strictly mediated through protocol isolation, preventing lateral movement and device-to-device communication. Access rights can be enforced at the level of individual systems, devices, and applications. Vendor access is centrally managed and automatically revoked after contract expiry or inactivity. While dynamic access control and real-time risk scoring are not supported natively, Xona integrates with upstream tools to enable risk-informed enforcement workflows.

Xona provides comprehensive session logging of all user actions, file transfers, and protocol usage, with video recordings for complete visibility. These logs can be cryptographically signed to ensure integrity and exported to external SIEM systems for correlation and compliance. The platform does not include native behavioral baselining or anomaly detection but integrates with tools like Nozomi Networks and Forescout to provide ML-driven monitoring. Real-time access visibility and alerting are managed through the Centralizer or external monitoring platforms.

The platform supports legacy OT systems by operating without agents and by tunneling unencrypted protocols such as Modbus, OPC UA, and DNP3 within encrypted sessions. Xona also enables secure access to serial interfaces using integrations with terminal servers and is compatible with air-gapped environments using on-premises gateways. While it does not enforce context-aware policies for legacy assets, Xona ensures access control, session isolation, and full auditing for all user interactions, even with devices lacking native security features.

Xona's threat detection and response capabilities rely on integration with third-party security platforms. While it does not perform anomaly detection, session telemetry and logs can be consumed by SIEM or SOAR platforms. These systems can trigger actions such as session termination or policy updates in response to detected threats. The platform supports admin- or API-triggered responses, but it does not natively assign threat severity ratings or automate remediation workflows.

Xona supports high availability through active-passive failover configurations. Active-active clustering is under development. In the event of a failure, a standby gateway takes over within approximately 120 seconds. Sessions are not preserved across failover to ensure strict access control, but user reauthentication is fairly streamlined. Failback is manual, and automated failover testing is not currently supported. While the Centralizer monitors system health and availability, alerting for failover events must be handled through external tools. Real-time monitoring dashboards are provided, but session state synchronization is not available across sites.

Xona is independently attested for SOC 2 Type 2 compliance and supports customer compliance with key industry regulations, including IEC 62443, NERC CIP, and Transportation Security Administration (TSA) security directives. The platform uses cryptographic algorithms that are FIPS 140-2 compliant, implementing AES for securing data in transit, but the platform itself is not FIPS-certified. Xona does not generate audit-ready compliance reports but provides exportable logs and recordings for reporting via external platforms. ISO 27001 certification is planned.

Xona is well suited to critical infrastructure operators seeking secure remote access to OT and ICS environments without the overhead of managing endpoint agents. The solution is particularly relevant for mid-market and enterprise organizations in energy, water, manufacturing, oil and gas, maritime, and transportation sectors. While support is primarily in English, limited Spanish-language support is available, and additional localization is handled through partners. Xona is available globally through a partner-driven model and is now also offered as a managed service in select regions.

**Strengths**

- Fast deployment
- No agent or plug-in required for access
- Strong session isolation using protocol rendering
- Native support for centralized session recording and logging
- Easy integration with major OT visibility platforms
- Designed for use by non-technical field operators

- Hardware and virtual gateway deployment flexibility
- Full support for SAML-based federated authentication
- Centralized management of multi-site access policies

**Challenges**

- No native support for adaptive access controls
- Active-active clustering not currently supported
- Lacks built-in automated threat response workflows
- No support for OAuth or OIDC
- Cannot maintain session continuity during failover events

# Vendors to Watch

Besides the vendors covered in detail in this document, we observe some other companies in the market that readers should be aware of. These vendors did not participate in the rating for various reasons but nevertheless offer a significant contribution to the market space.

## Admin By Request

Admin By Request was founded in 2015 and is headquartered in Silkeborg, Denmark. It provides endpoint privilege management capabilities designed to reduce attack surfaces without adding friction for users. Its Secure Remote Access functionality enables external contractors and internal users to request and gain temporary, audited access to privileged environments.

**Why worth watching:** Admin By Request is worth watching for organizations looking to extend least privilege principles into OT environments while maintaining operational efficiency and auditability.

## BeyondTrust

BeyondTrust is an established but growing private US-based cybersecurity vendor founded in 2003 and headquartered in Johns Creek, Georgia, with a specialization in privileged access management. Its AI-supported privileged remote access solution enables secure connections for internal and third-party users to critical systems without exposing credentials or requiring direct access to the network.

Why worth watching: BeyondTrust is worth watching for innovations such as its True Privilege Graph, which enhances visibility into identity risks and privilege escalation paths across IT and OT. BeyondTrust offers flexible deployment models for OT operators that need tight controls and strong monitoring capabilities for remote access to privileged systems without introducing unnecessary complexity or risk.

## CybergymIEC

CybergymIEC is headquartered in Hadera, Israel and was founded in 2013. Originally focused on cyber training and simulations for critical infrastructure, it has expanded into operational security offerings. Sophic Access is its secure remote access solution designed specifically for industrial operators, with granular session control and embedded training features.

**Why worth watching:** CybergymIEC is worth watching for blending remote access control with operator training and simulation to reduce both human and technical risks in OT environments.

## Cyolo

Cyolo is a private cybersecurity company founded in 2020 and headquartered in Tel Aviv, Israel. The company focuses on securing remote privileged access in OT and ICS environments. Its core offering, Cyolo Pro, is a software-based platform designed for IT and OT convergence and built around a distributed, Zero Trust architecture.

**Why worth watching:** Cyolo sets itself apart with a distributed architecture combined with centralized management, support for cloud-connected, cloud-averse, and offline deployments, and an identity-centric approach to secure access. Cyolo does not store encryption keys or access policies in the cloud, preserving customer control and reducing the risk of compromise from vendor-side breaches.

## Forescout

Forescout Technologies is a global cybersecurity vendor founded in 2000 and headquartered in San Jose, California. With a long-established presence in asset visibility and control, Forescout's 4D Platform™ delivers continuous discovery, classification, and risk assessment across managed and unmanaged assets in IT, OT, IoT, and medical environments. Through its recent integration with Xona, Forescout adds secure remote access capabilities to its existing OT security offering, allowing for dynamic, policy-enforced access to critical systems. The combination of continuous device visibility with real-time, identity-aware access controls supports a more contextual and risk-informed security posture for industrial environments.

**Why worth watching:** Forescout is worth watching for end-user organizations seeking secure remote access solutions that leverage live contextual data to drive access decisions across OT and ICS environments.

## Fortinet

Fortinet is a public cybersecurity company founded in 2000 and headquartered in Sunnyvale, California in the US. FortiSRA is Fortinet's dedicated remote access solution designed for industrial networks, leveraging its security appliances and threat intelligence platform.

**Why worth watching:** Fortinet is worth watching for its integration of secure remote access with existing industrial firewalls and centralized management, reducing the need for additional components.

## Honeywell

Honeywell is a long-standing industrial technology vendor headquartered in Charlotte, North Carolina in the US. Its Remote Secure Access and Secure Media Exchange offerings focus on secure vendor access and controlled media transfers in regulated and safety-critical environments.

**Why worth watching:** Honeywell is worth watching for its industrial pedigree and ability to integrate secure access with broader safety and reliability objectives.

## Microsoft

Microsoft, headquartered in Redmond, Washington in the US, is a global technology company with a cybersecurity portfolio spanning cloud and industrial environments. Microsoft Defender for IoT brings asset discovery, vulnerability management, and network monitoring into OT environments through agentless sensors.

**Why worth watching:** For organizations already invested in the Microsoft ecosystem and looking to extend unified visibility and control into remote OT sites, Microsoft is worth watching.

## Nozomi Networks

Nozomi Networks, founded in 2013 and headquartered in San Francisco, California in the US, provides OT and IoT security platforms focused on real-time monitoring, asset intelligence, and threat detection.

**Why worth watching:** Nozomi Networks is worth watching for its depth in asset awareness and behavioral analytics that can be used to fine-tune and restrict remote access paths in industrial environments.

## Omron

Omron Corporation is a Japanese multinational company founded in 1933, with its headquarters in Kyoto, Japan. The RT1-Series Secure Remote Access solution enables encrypted VPN-based access to PLCs and HMIs through a managed gateway approach.

**Why worth watching:** Omron is worth watching for engineering-driven OT environments seeking vendor-native remote access solutions with minimal integration overhead.

## OTIFYD

OTIFYD is a cybersecurity company headquartered in Houston, Texas in the US, focusing exclusively on secure access and monitoring for OT networks. Its solution enables encrypted and policy-enforced access for internal engineers and third-party service providers, with audit logging and real-time controls.

**Why worth watching:** OTIFYD is worth watching for industrial operators that need a focused, lean solution for secure third-party remote access in environments with limited IT oversight.

## Phoenix Contact

Phoenix Contact, headquartered in Blomberg, Germany, was founded in 1923. Its mGuard Secure Remote Service is a VPN-based platform purpose-built for secure maintenance access to industrial equipment, with device hardening and integrated firewall capabilities.

**Why worth watching:** Phoenix Contact is worth watching for its embedded access control model tailored to OEMs and operators with distributed field assets.

## Rockwell Automation

Rockwell Automation, founded in 1903 and based in Milwaukee, Wisconsin in the US, is a major player in industrial automation. Factory Talk Remote Access is Rockwell's centralized tool for managing secure connections to remote equipment, focusing on maintenance workflows and technician enablement.

**Why worth watching:** Rockwell Automation is worth watching for asset owners that rely on Rockwell control systems and want native remote support without additional integration complexity.

## Secomea

Secomea is a Danish company founded in 2008 and headquartered in Herlev, Denmark. Its SiteManager solution combines secure tunneling, granular policy enforcement, and audit logging to support industrial equipment vendors and operators with minimal on-site IT.

**Why worth watching:** Secomea is worth watching for industrial OEMs and service providers seeking a purpose-built platform to enable and control access to customer equipment in the field.

## Siemens

Founded in 1847 and headquartered in Munich, Germany, Siemens is a global industrial technology company with a long-standing presence in sectors such as automation, electrification, and digitalization. Within its Digital Industries division, Siemens offers a range of software and infrastructure solutions tailored for industrial environments. Its SRA portfolio includes SINEMA Remote Connect, RUGGEDCOM CROSSBOW and SINEC Security Monitor. Each of these products is designed to address specific OT and ICS access and monitoring challenges. These offerings support varied deployment requirements, from centralized VPN connectivity to role-based device access and on-premises security visibility, reflecting Siemens's wide customer base in regulated and infrastructure-heavy industries.

**Why worth watching:** Siemens brings a multifaceted and integrated approach to SRA for OT and ICS with a practical focus on scalability, centralized control, and operational continuity across VPN connectivity, role-based device access, and passive security monitoring.

## Silverfort

Silverfort was founded in 2016 and is based in Tel Aviv, Israel. It provides agentless authentication and policy enforcement across OT and IT systems, enabling secure access without installing software on endpoints.

**Why worth watching:** Silverfort is worth watching for its ability to extend authentication controls to legacy systems and industrial protocols that typically lack built-in security.

## TXOne Networks

TXOne Networks was established in 2019 and is headquartered in Taipei, Taiwan. The TXOne StellarProtect solution provides endpoint protection tailored to industrial environments, including offline assets and legacy Windows systems.

**Why worth watching:** TXOne Networks is worth watching for its pragmatic focus on OT-specific constraints and for enabling secure local and remote access through protected endpoints.

## Waterfall Security Solutions

Waterfall Security Solutions is a private cybersecurity vendor founded in 2007 and headquartered in Israel, with world-wide support hubs in five locations. The company's new product, Hardware-Enforced Remote Access (HERA), builds on its longstanding expertise in unidirectional gateway technology for OT and ICS, and is designed to reduce the overall attack surface.

**Why worth watching:** HERA is built for heavy industry and critical infrastructure, providing hardware-enforced secure remote access, session recording, real-time monitoring by administrators, and granular access restrictions. Because of the physically segregated nature of the solution, no firewalls or VPNs are necessary. TPM binding prevents the use of stolen credentials on unauthorized devices.

## Xage Security

Xage Security, founded in 2016 and based in Palo Alto, California in the US, offers a mesh-based access control fabric designed for operational technology and cyber-physical systems. Its platform enforces granular access and multi-factor authentication across distributed assets.

**Why worth watching:** Xage Security is worth watching for its identity-centric approach to controlling remote access in decentralized industrial environments.

# Related Research

Leadership Compass: Policy Based Access Management
Leadership Compass: Access Management
Leadership Compass: Zero Trust Network Access
Leadership Compass: Privileged Access Management
Market Compass: Cybersecurity for Industrial Control Systems
Advisory Note: Secure Remote Access in OT and ICS: Enabling Resilience and Control
Whitepaper: Zero Trust Network Access for OT Environments
Whitepaper: Global Remote Access for the Modern Organization

# Copyright



KuppingerCole Analysts supports IT professionals with exceptional expertise to define IT strategies and make relevant decisions. As a leading analyst firm, KuppingerCole offers firsthand, vendor-neutral information. Our services enable you to make decisions crucial to your business with confidence and security.

Founded in 2004, KuppingerCole is a global, independent analyst organization headquartered in Europe. We specialize in providing vendor-neutral advice, expertise, thought leadership, and practical relevance in Cybersecurity, Digital Identity & IAM (Identity and Access Management), Cloud Risk and Security, and Artificial Intelligence, as well as technologies enabling Digital Transformation. We assist companies, corporate users, integrators, and software manufacturers to address both tactical and strategic challenges by making better decisions for their business success. Balancing immediate implementation with long-term viability is central to our philosophy.

For further information, please contact clients@kuppingercole.com..