Cyolo

Datasheet

Enable Privileged Remote Access with Cyolo PRO

Discover how Cyolo PRO is redefining Secure Remote Access (SRA) by extending privileged access controls to the world of OT.

Traditional SRA solutions, including virtual private networks (VPNs), virtual desktop infrastructure (VDIs), jump boxes/jump servers, and others, are not meeting the needs of the increasingly connected modern industrial enterprise. These tools are frequently complicated to use, offer little or no visibility following the initial connection, and leave organizations exposed to serious safety and security risks by granting full network access with no supervisory controls.

CYOLO'S CORE INNOVATION

Cyolo PRO (Privileged Remote Operations) is an advanced secure remote access solution designed to meet the distinctive needs of operational technology (OT) and industrial controls systems (ICS).
Cyolo PRO is built on a unique decentralized architecture that simplifies remote access while simultaneously strengthening security, improving operational agility, and enhancing user experience.

STRENGTHEN SECURITY

- **Connect Verified Identities to Applications, Not Users to Networks:** Rather than relying on outdated network-based access controls, Cyolo PRO connects verified identities directly to the applications they are authorized to access, in accordance with the principle of least privilege. Cyolo PRO authenticates identities and authorizes access at the application level, extending VPN-less, zero-trust connectivity that mitigates the risk of unauthorized access and restricts the potential for lateral movement within or across networks.

- **Ongoing Access and Oversight Controls:** Gain full visibility and oversight for the entirety of all connections. Following the initial identity verification, Cyolo PRO performs continuous authorization for the duration of the session. Additional controls include but are not limited to just-in-time access (JIT), supervised access for real-time monitoring, and session recording. Supervisors can also limit which actions can be performed while connected and can terminate a session if suspicious or unusual activity is detected. All activity is fully logged and audited for compliance and incident response purposes.

- **Data Remains in the Customers' Trusted Boundaries:** Cyolo PRO is built on a decentralized architecture that allows customers to maintain full control over their data at all times, improving security and preventing dependence on the vendor. Even customers who use the optional cloud component to route access requests still keep all data, secrets, and keys secure within their trusted boundary.

IMPROVE OPERATIONAL AGILITY

- **Optimize Uptime and Reduce Latency:** Cyolo PRO ensures fast connections regardless of geographic location, optimizing performance and responsiveness. By routing traffic without decryption through globally distributed cloud-based points of presence (PoPs), Cyolo PRO provides fast, secure connections and eliminates the need for remote employees and third-party vendors to travel to physical sites.

- **Fast Deployment and Infrastructure-Agnostic Architecture:** Cyolo PRO is infrastructure-agnostic and can fit any environment. This flexibility enables fast, easy deployment without the need to upgrade or rip and replace existing systems, giving it the lowest cost of change.

ENHANCE USER EXPERIENCE

- **Agentless Remote Access:** Simplify third-party vendor and contractor access by securing access with SSH tunneling without requiring them to download agents onto their device.

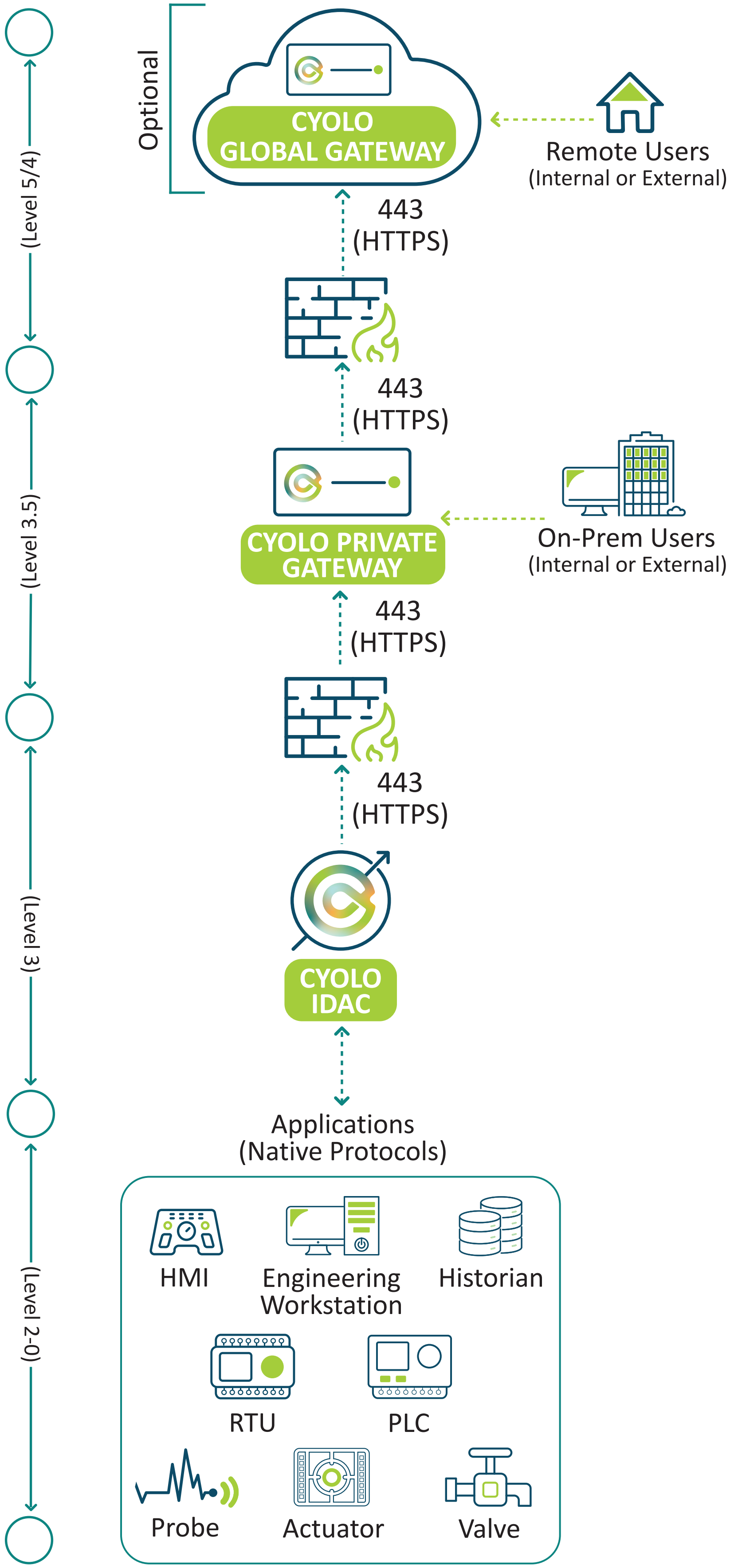
- **Vault and Password Injection:** Shorten login processes, reduce complexity, and safeguard secrets by storing them in the Cyolo PRO on-prem vault. Inject shared passwords directly into the application without exposing them to users.

CYOLO PRO ARCHITECTURE

Distributed security and decentralized architecture enable flexible management and control.

The unique combination of on-prem Identity Access Controller (IDAC) with a gateway element (private or global) empowers organizations to adjust access and security controls in the way that best fits their structure and industrial architecture. Whether they prefer to centralize access control and management or to grant it per site, Cyolo supports multi-tenancy that allows maximum flexibility, all while keeping data insides the organization's trusted boundaries.

> *"Ten percent of users create 90% of the risk for organizations. That's why we focus on securing remote privileged access."*
>
> - Almog Apirion
> CEO & Co-founder, Cyolo



CYOLO GLOSSARY:

IDAC (Identity Access Controller):
The "brain" of Cyolo PRO. This lightweight software component remains on-prem within the organization's trusted boundaries and holds all configuration, secrets, policies, and keys. The IDAC can be deployed in any environment and has no inbound connection, only a TCP 443 outbound connection to the gateway.

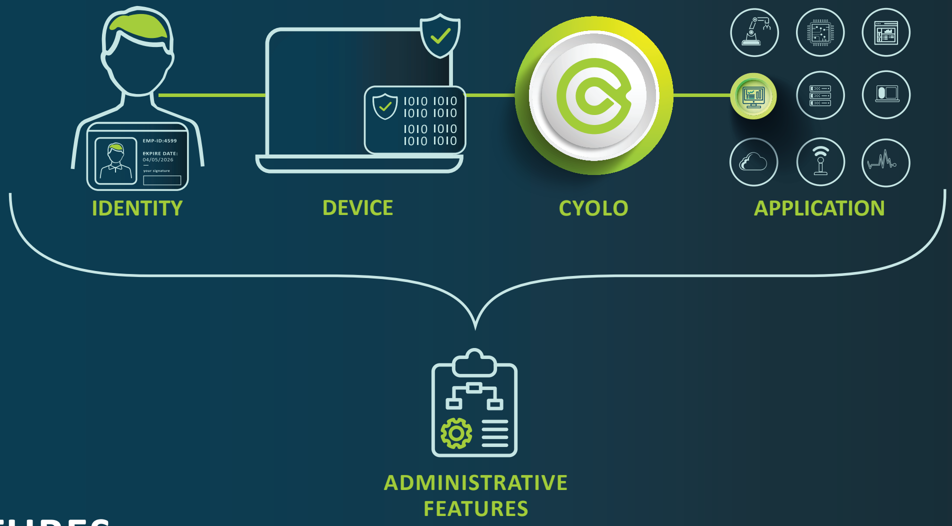
Private Gateway:
A software component that is placed in the DMZ and routes packets to the proper IDAC without transmitting information to an external cloud or performing decryption.

Global Gateway:
A router component that leverages a wide network of Points of Presence (PoPs) around the globe. Cyolo PRO quickly and seamlessly routes remote user connections to on-premises IDACs via global gateways.

Cyolo Connect:
An optional agent that adds device posture and management capabilities.

CYOLO PRO: FEATURES & CAPABILITIES

Cyolo PRO ensures security throughout the entire connection cycle — from the user via their device to the application.



MAIN FEATURES

IDENTITY

Feature	Technical Description
Multi-factor authentication (MFA)	Integrates with any MFA service, including Duo. Native solution also enables MFA for legacy apps
Single sign-on (SSO)	Supports SAML, Kerberos, secrets, user credentials and more
IdP integrations	Supports any IdP solution - LDAP, SAML, OpenID, RADIUS
Local identity provider (IdP)	Allows Local Identity Federation between all IdP solutions used and fast addition of users
Vault	Self-hosted on-prem vault that allows safeguarding all accounts secrets including shared accounts
Password rotation	Password rotation policy set by the admin at the app, user or group level
Just-in-Time (JIT) access	Grants temporary real-time access permissions for specific assets
Lifecycle management	Enables simple provisioning and deprovisioning of user identities
Self-service profile & password management	Provides tools for users to manage their passwords and profiles with no need for IT support
Agentless access	Allows web-based access to SSH, RDP, VNC, HTTP, HTTPS, SMB or Telnet applications

DEVICE

Feature	Technical Description
Device posture	Enforces access policies based on device compliance status
Device policy	Allows to determine policy per device based on user network and captive portal
Device management	Allows Local Identity Federation between all IdP solutions used

CYOLO SOLUTION

Feature	Technical Description
Supported secrets	Password, private key, certificate, API keys and generic secrets
Secure file transfer	Securely transfer files through the Cyolo platform
File scanning	Scan files before uploading within the Cyolo platform or through an ICAP integration
Conditional access	Granular access policy on the user, group, app or apps group level
Custom conditional access (webhook integration)	Allows extra custom access conditions via Webhooks
Session management	Manage sessions with scheduled or supervised access; Record sessions or terminate a connection in real-time
Zero-trust access	Connects user only to approved apps and assets without full network exposure

APPLICATION

Feature	Technical Description
Assets protocols	RDP (web/native), SSH (web/native), VNC, HTTP/HTTPs, SMB, PostgreSQL, and other applications
Native apps support	Through SSH tunnels
Web Application Firewall (WAF)	Protects web applications by managing HTTP traffic
Application analytics	Monitors application usage and security statistics
Custom domain	Allows publishing applications using a custom domain
Access approval	Requires approval for access attempts
Session audit logs	Provides detailed logs of user sessions for every app for incident response and compliance. Easily integrates with any SIEM and SOAR solution
Session recording	Enables session recording by policy

APPLICATION

Feature	Technical Description
Recordings search	Allows quick search of commands within recorded SSH sessions
DevOps CLI access	Enables command-line access for DevOps tasks
Integrations	Extensive integration capabilities
Application analytics and insights	IP addresses/ports users accessed
Wildcard web applications	Configured address/URL without redirecting to different addresses
Risk Score Analysis	Advanced AI-based risk score analysis evaluates the security risk of each session and provides a summarized report of the actions taken
AI Session Monitoring	Proactive AI monitoring capabilities dynamically oversee ongoing sessions and warn supervisors about risky or unusual activity

ADMINISTRATIVE FEATURES

Feature	Technical Description
Role-based access control (RBAC)	RBAC introduces 5 role levels: Super Admin, Operation Admin, Read only Admin, Helpdesk Admin, and Log Admin. These roles apply to both the Admin Portal and API for streamlined access management
REST API	Provides easy API integration
Multi-tenancy architecture	Supports multiple tenants to allow local or central management
Log shipping to Syslog server or AWS S3	Ships audit and activity logs to external servers for storage and analysis
Branding capabilities	Allows customization of the user interface according to the client's needs
Notifications - admin system events	Sends notifications for important system events
Topology view	Provides a visual representation of the network topology
Secrets sharing	Enables admins to securely share secrets with users
Monitoring	Provides tools for monitoring system performance and security
Secrets retrieval from the system vault	Allows authorized individuals to retrieve secret values from the secure system vault
Digital experience measurements	Latency measurements

GRANULAR ACCESS AND ACTIONS POLICY:

Cyolo PRO's comprehensive policy framework enables administrators to exercise granular control at the category, application, and user levels. Beyond static policies (such as time, IP, and geo), Cyolo PRO supports the enforcement of access, based on contextual factors such as device posture. Additionally, Cyolo PRO provides maximum flexibility and control through API-based custom query policies.

Access Policy Controls:

- ☒ Device posture check
- ☒ Require MFA
- ☒ Require device certificate
- ☒ Geolocation
- ☒ Source IP address
- ☒ Users require approval from an approver to access the application
- ☒ User must fill out the access request form before they can access the Application
- ☒ API — Verify this policy with external integration
- ☒ Time
- ☒ Supervisors can join active sessions
- ☒ Native session access token will be valid for ___ minutes
- ☒ Allow camera
- ☒ Allow audio input
- ☒ Allow COM redirection
- ☒ Allow smart card redirection
- ☒ Log successful user access
- ☒ Anti-malware scan

Actions Policy Controls:

- ☒ Block file uploads or downloads
- ☒ Enforce session fingerprinting
- ☒ Log successful user access
- ☒ Block clipboard (copy/paste)
- ☒ Block drive redirection
- ☒ Block printer redirection
- ☒ Use multiple monitors
- ☒ Record session
- ☒ Supervisors can join active sessions
- ☒ Native session access token will be valid for ___ minutes
- ☒ Allow camera
- ☒ Allow audio input

SUPPORTED PROTOCOLS:

Web Applications
1. HTTP
2. HTTPS
3. SaaS
4. Link

Networks
1. TCP
2. Network
3. DesktopApp
4. SSH Tunnel

Servers
1. RDP
2. SSH
3. VNC
4. TELNET

Databases
1. PSQL

Files
1. SMB

OUTCOMES

Modernized Security

Granular controls enable true least privilege access across the entire enterprise

Better User Experience

- Agentless, web-based access with a single consolidated login
- Enable safe and secure third-party access
- Support remote work and BYOD

Operational Safety

- Reduce risk of life-threatening equipment incidents
- Minimize downtime/ manual mode

Reduction of Compliance Headaches

- Audit logging/forwarding
- JIT and recorded sessions
- Comply with CMMC/NIST, ISO, NERC CIP, NIS2 and more

Increased Productivity, Reduced Cost & Complexity

- Reduce hardware, VM costs
- Save time with centralized management
- Eliminate cumbersome vendor risk assessments

Enterprise-Ready Deployment

- Deploy in any environment – cloud-connect, on-prem, isolated
- Supports legacy systems & applications
- Scalable across 100+ sites in under 90 days

ABOUT CYOLO

Cyolo provides secure remote privileged access for cyber-physical systems (CPS), enabling industrial enterprises to simply connect employees and third-party vendors to critical assets.

Cyolo offers stronger security and more control than traditional secure remote access and deploys in any environment without causing disruptions or requiring change management.

Cyolo delivers improved security, productivity, and operational agility – without compromise.

Visit cyolo.io to learn more.