Securden

Secure Remote Assist

Zero Trust Secure Remote Access

A least privilege and zero trust based secure remote access platform to launch attended, unattended, and instant remote connections to devices and offer troubleshooting in a secure manner.

Instant Remote Access

Launch attended and unattended remote sessions to remote devices securely.

Collaborate Seamlessly

Invite specialists and collaborate to solve complex problems.

Least Privilege

Just-in-time privilege elevation for technicians on remote devices.

Product Datasheet

For enterprise security, IT helpdesk, compliance, and infrastructure leadership teams.

Secure Remote Assist

Product Datasheet

Platform Goal	Deployment Model	Primary Security Outcome
Allow technicians to launch secure connections to remote devices to offer troubleshooting, assistance and maintenance.	Software as a Service	Allowing technicians to launch secure attended, unattended, and instant browser based remote connections that are least privilege and zero trust compliant.

Product Overview

Secure Remote Assist is an end-to-end secure remote access and remote support solution for remote workforce and IT helpdesk teams. Securden Secure Remote Assist allows you to launch attended, unattended, and instant remote connections to remote endpoints and servers.

Core Technical Capabilities

Capability Area	Technical Functionality
Instant Remote Access	Allows technicians to code based remote sessions to any endpoint through standard web browsers.
Attended Remote Sessions	Allows technicians to launch remote troubleshooting sessions to manned endpoints that are managed using Securden. The agent running on the endpoint orchestrates the connection between the IT technician and the remote endpoint.
Unattended Remote Sessions	Allows users to access devices remotely through connections launched using the agent. Unattended access allows IT technicians to administer routine maintenance on servers and critical systems.

Capability Area	Technical Functionality
Vendor Remote Access	Zero trust third-party remote access without VPN with complete auditing and session recording.
Just-in-Time Admin Rights	Least privilege compliant sessions restrict technicians to standard user privileges on remote connections and allow technicians to gain admin rights on Just-in-Time basis.
Session Recording and Tracking	Remote sessions are recorded at the technicians end for complete activity tracking and visibility on remote sessions.

Architecture and Deployment

Area	Details
Deployment Models	Software as a Service
Backend Database	Amazon RDS. Encryption key managed through KMS.
Tunnel Server	Used for creating tunnel connections between remote client and remote server devices.
Agentless	Agentless, on-demand remote connections are supported.

Security Architecture

Security Area	SaaS Edition
Vault Model	Access-controlled, highly available vault instance hosted on AWS cloud with browser-based user access.
Data Encryption	Customer data is encrypted using AES-256 and stored in segmented encrypted database storage.
Encryption Key Management	Each customer segment uses a unique encryption key stored through Amazon KMS with cryptographic operations handled in an AWS CloudHSM cluster.

Security Area	SaaS Edition
Database Protection	Each customer's data is segregated and encrypted with a unique key so unauthorized access exposes only encrypted data.
Data Integrity	Encrypted customer data cannot be deciphered without the corresponding organization-specific encryption key.

Security Controls

Security Control	Details
Credential Encryption	AES-256 encryption.
Encryption Key Management	RDS database is encrypted using AES-256 and encryption key stored in Amazon KMS.
FIPS Mode	FIPS-compliant mode available for remote connector.
Certifications and Testing	ISO/IEC 27001, SOC 2 Type II, GDPR alignment, and periodic third-party penetration testing.
Access Governance	Remote assist policies that govern technician access to remote devices and just-in-time admin privileges.
Session Auditability	Audit trails for remote assist sessions, complete recordings of remote sessions.

Privileged Access Control Design

Control Layer	Technical Detail
Primary Authentication	Access to the remote assist web application can be controlled through LDAP-compliant services like Active Directory and Microsoft Entra ID, SAML-based SSO, RADIUS authentication, smartcard authentication, or native local authentication.

Control Layer	Technical Detail
Directory-Based Authentication	When directory authentication is used, the app authenticates through the configured directory and does not need to store directory user passwords.
User Lifecycle	Directory integrations support user onboarding, offboarding, authentication, and access provisioning workflows.
Second Factor	Supports MFA through any TOTP authenticator, Securden Authenticator, OTP through email, any RADIUS-based MFA, Duo, YubiKey, and others.
Access Policies	Granular role-based access controls, request-release workflows, just-in-time access, and passwordless privileged sessions reduce credential exposure.

Identity, MFA, and Integration Support

Integration Area	Supported Options
Primary Authentication	Local accounts, Active Directory, Microsoft Entra ID, LDAP, and RADIUS.
SSO	SAML 2.0 support for Okta, Microsoft Entra ID, ADFS, OneLogin, PingIdentity, Google Workspace, and other SAML identity providers.
MFA	TOTP apps such as Google Authenticator and Microsoft Authenticator, Securden Authenticator, Duo Security, RSA SecurID, YubiKey, email OTP, and RADIUS-based MFA.
RBAC	Predefined and custom roles.
Supported Browsers	Chrome, Edge, Firefox, and Safari.
Client Applications	Browser, Desktop application (Windows, Mac, Linux), iOS and Android mobile applications.

Product Specifications Snapshot

Specification	Details
Supported Access Types	Attended, Unattended, and Code Based, Instant remote access methods.
Remote Session Protocols	HTTPS – TLS 1.2 or 1.3; QUIC (UDP); TCP; WebSocket
Enterprise Integrations	Active Directory, Microsoft Entra ID, LDAP, Google Workspace, SAML SSO, SIEM, ticketing systems, MFA providers, SDKs, CLI access, and APIs.
Endpoint Controls	Removal of local administrator rights, application control, on-demand elevation for standard users, temporary administrator rights, and least-privilege enforcement.
Audit and Reporting	Visibility into who can launch remote sessions to which endpoints, servers, and systems. Reports on sessions launched, applications accessed and compliance support.

Commercial Notes

Commercial Area	Details
Licensing Model	Based on number of concurrent remote session
Non-Production Environments	No separate license required for test, staging, or DR instances.
Support	24x5 standard support; 24x7 premium support.
Upgrade Cadence	Minor monthly releases; major quarterly releases.
Free Trial	30 days; no credit card required.

Common Use Cases

Use Case	Description
Remote IT Support and Troubleshooting	Remotely access end-user computers to diagnose and resolve software issues, configuration problems, and system errors.
Unattended Remote Access	Access and manage computers or servers without requiring someone at the remote device to accept the session.
Attended Remote Support	Initiate a remote session with the end user's consent to troubleshoot issues while the user is present.
Third-Party Vendor Access	Provide external vendors or service providers with controlled remote access to systems that require maintenance or troubleshooting.
Remote Server Administration	Remotely access servers to perform administrative tasks, troubleshoot failures, manage configurations, and resolve performance issues.
Remote Workforce	Allow remote workforce to securely access internal IT resources.

See how Securden can help your organization

Book a Demo

Securden

+1 844 228 0327 +44 203 868 6147

support@securden.com www.securden.com

2810 N Church St, PMB 75693, Wilmington, Delaware 19802-4447, United States.