Admin By Request
ZERO TRUST PLATFORM

Secure Remote Access

Who We Are

Admin By Request creates Zero Trust SaaS-based solutions that eliminate security risks without killing productivity.

What the Product Is

Secure Remote Access extends our EPM solution with secure, browser-based remote access. IT teams get just-in-time connections via RDP, SSH, and VNC protocols, vendors receive scoped access to specific systems, and support staff provide live assistance through encrypted sessions.

Why You Need It

Traditional remote access creates permanent attack surfaces through persistent VPN connections and open firewall ports. Vendor access becomes a nightmare of shared credentials, overprivileged accounts, and complex firewall rules.

Remote support tools require software installations, create persistent backdoors, or rely on third-party services outside your control. IT teams waste time managing jump servers while compliance auditors flag always-on remote access as high-risk due to lack of visibility.

When You Need It

- When vendor access requires better security and audit controls.
- Before compliance audits (ISO 27001, NIST, Cyber Essentials Plus) that scrutinize remote access methods.
- When remote workforce support becomes business-critical.
- During incident response requiring immediate system access.
- When traditional VPN infrastructure creates more risk than protection.

Where It Works

Secure Remote Access integrates with Admin By Request infrastructure on Windows and Linux systems (macOS support Q3 2025). Deploy using cloud-hosted gateways or self-hosted Docker containers for complete control.

The solution works best for IT administrators managing distributed systems, organizations collaborating with external vendors, and support teams helping remote users across multiple locations.

How It Works

Three components handle different scenarios: Unattended Access for admin RDP/SSH/VNC sessions, Vendor Access for external parties through secure browser portals, and Remote Support for live screen-sharing and troubleshooting.

Connections route through secure Cloudflare tunnels with no persistent agents. Sessions automatically expire, all activity gets logged with optional video recording, and everything integrates with existing EPM approval workflows and audit trails.