



AVTeleport

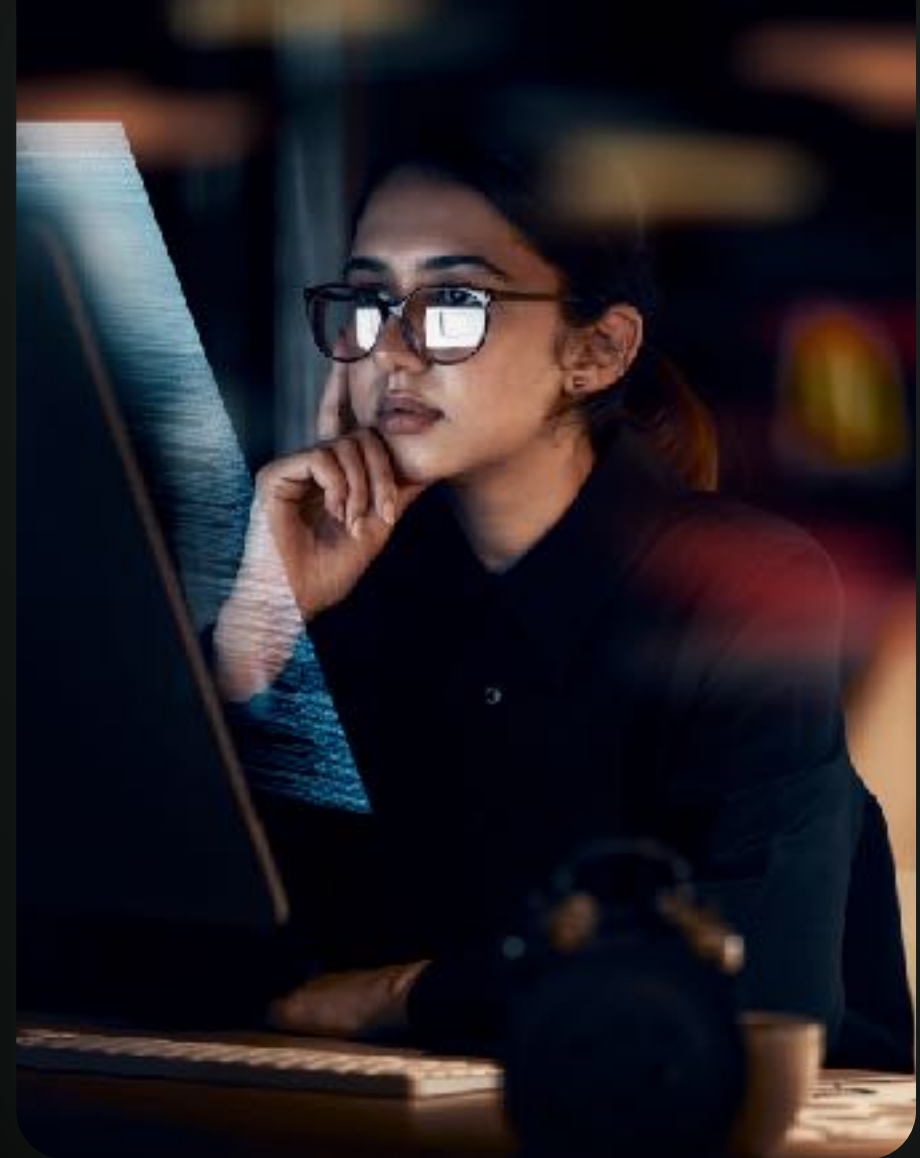
Security & Network Overview

Trusted, Secure, Remote AV Support



Why This Matters (IT Focus)

- ◆ AV systems are critical infrastructure on the corporate network
- ◆ Downtime creates helpdesk tickets, escalations, and productivity loss
- ◆ Traditional fixes rely on site visits → hours or days of delay
- ◆ AVTeleport enables secure remote support with response times measured in seconds, not hours
- ◆ This deck explains how AVTeleport works and why it's safe for your network





Security By Design

- » SOC 2 Type II compliant — independently audited
- » Zero-trust architecture — every user, device, and session verified
- » End-to-end encryption — WireGuard protocol (AES-256 / ChaCha20)
- » Optimized for outbound traffic:
 - Works over HTTPS (443/TCP) with no firewall changes
 - Optionally, UDP/41641 can be opened for improved performance
- » Built for enterprise IT standards, not consumer-grade remote access

If UDP/41641 is blocked, AVTeleport falls back to HTTPS relays ensuring connectivity without firewall changes

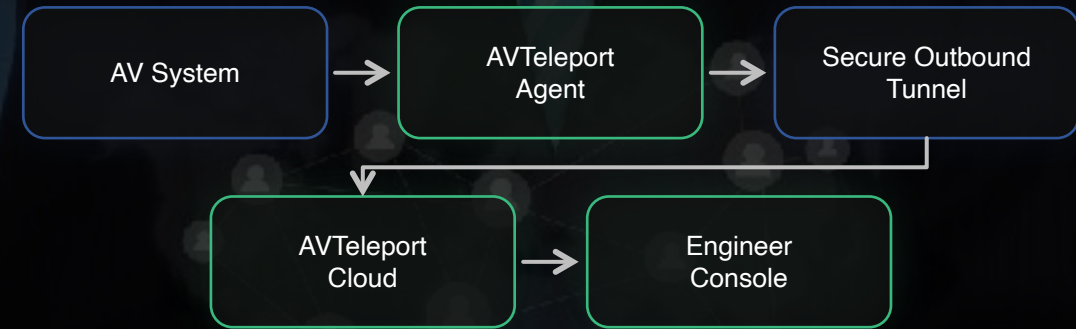




How the Connection Works

- » The AVTeleport Agent runs on the gateway
- » Establishes a secure, outbound-only encrypted tunnel to the AVTeleport cloud
- » Engineers connect only through the AVTeleport authenticated console
- » Connections are limited by robust Access controls (ACLs):
 - Defined in code (infrastructure-as-code model)
 - Version-controlled and change-tracked
 - Fully auditable for compliance and security review
- » No unsolicited inbound traffic ever enters the network
- » IT can revoke or block access or unplug the gateway at any time

Pairing Diagram



All sessions are encrypted, authenticated, access-controlled, & logged.



Network Requirements



Non-overlapping Ipv4 Ranges

- » Each site must use a unique internal IPv4 network range.
- » Avoid overlapping subnets across multiple customer locations.



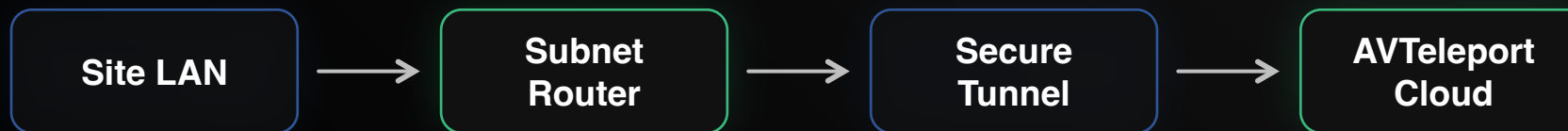
Defined IP Addresses/Ranges

- » Gateway must be connected in the same subnet as the AV equipment.
- » Accessible. – Access is limited to these approved addresses only.



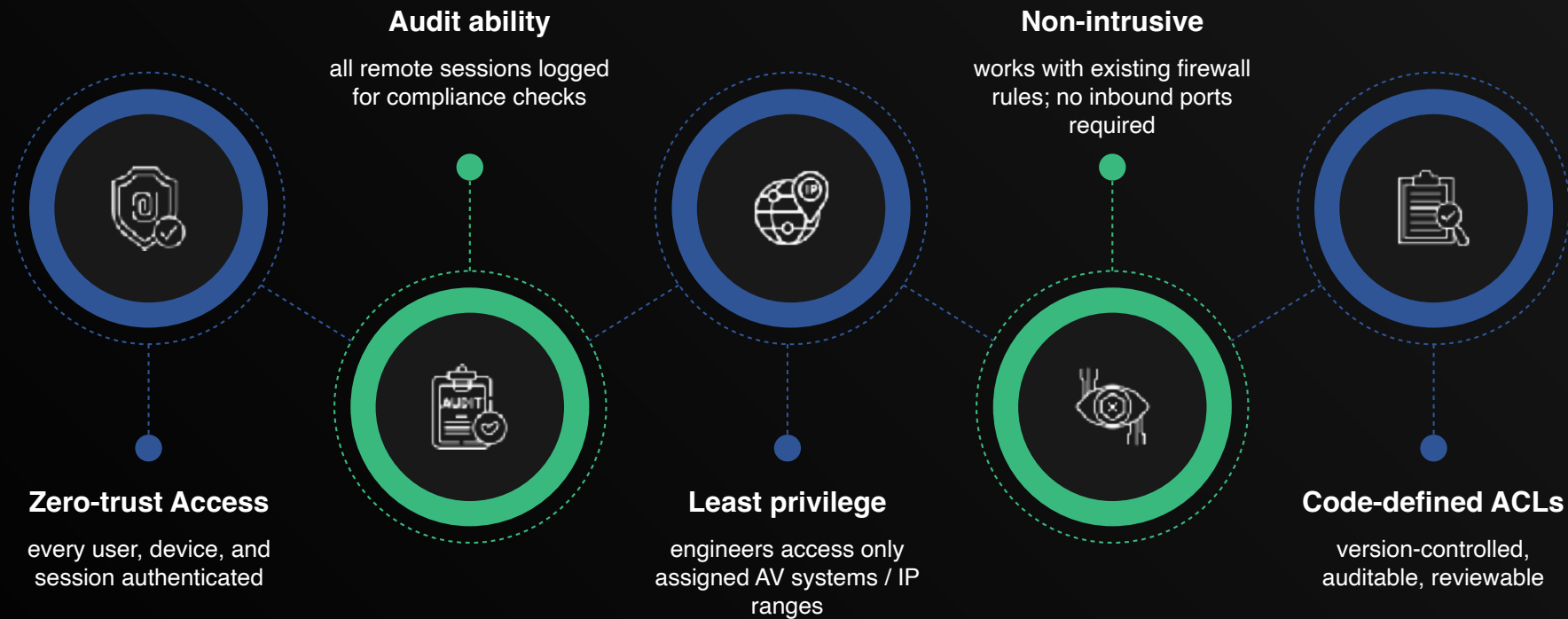
Single Tunnel Endpoint (Subnet Router)

- » One device is connected at each site to act as the subnet router.
- » This device creates the secure tunnel and provides access to the approved AV subnet.



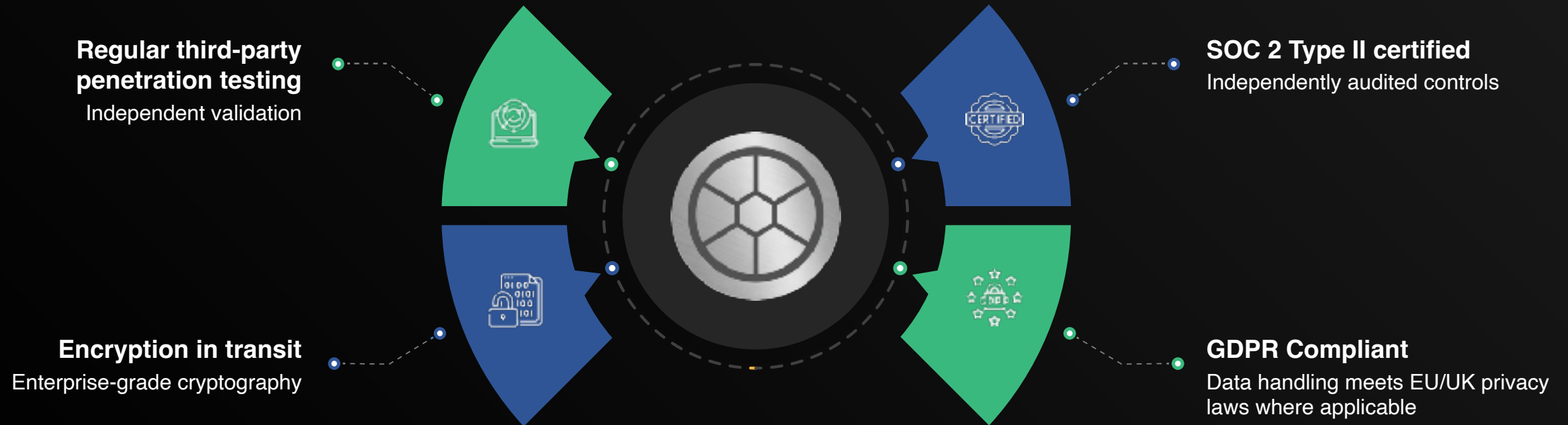


IT Security Principles





Compliance & Standards





Benefits for IT & Security Teams

01

Protects The Network

AV systems are critical infrastructure on the corporate network

02

Retain Control

IT can revoke or restrict access at any time. Or simply disconnect the gateway

03

Full Transparency

all sessions logged and tied to specific users

04

Compliance-ready

aligns with SOC 2, GDPR, enterprise frameworks

05

Operational Efficiency

faster fixes, fewer site visits, less disruption



Why This Matters (IT Focus)



Do we need to open firewall ports?

- No changes required. Works over HTTPS (443/TCP).
- Optionally, UDP/41641 improves performance.



Can AVTeleport see the entire network?

- No. Access restricted only to approved AV systems or IP ranges that are relevant to the AV systems.



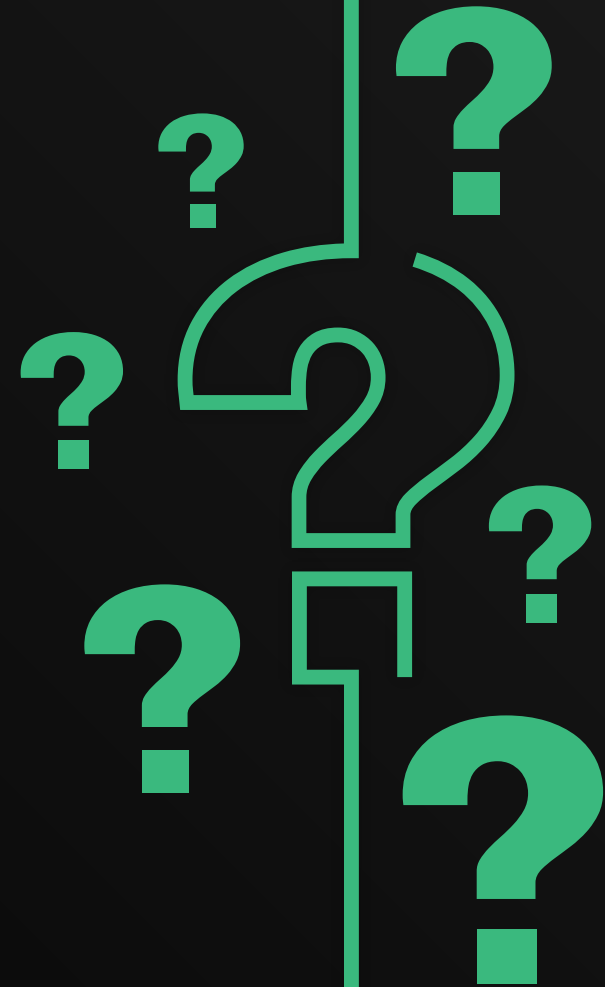
Where is data stored?

- Encrypted in SOC 2 certified cloud infrastructure.



Can IT audit sessions?

- Yes. All activity is logged





AVteleport



support@avteleport.com



www.avteleport.com

PROACTIVE. SECURE. RELIABLE.