ARISTA CYBER

SERVICES

SECURE DESIGN & DEPLOYMENT

REMOTE ACCESS WITH ZERO TRUST

ZERO TRUST WHEN REMOTE BECOMES ROUTINE

Remote access is often the weakest link in OT, whether it is for vendors, maintenance, or offsite monitoring. Legacy VPNs or open connections can expose systems to undue risk. When trust is implicit, one compromised credential or connection can open the door to significant damage.

Arista Cyber helps you implement a Zero Trust remote access framework that verifies every user, device, and connection. We collaborate with your network, operations, and vendor management teams to identify all remote access paths and users. Together we define Zero Trust rules and test configurations. We outline policies, micro-segmentation, continuous authentication, and least-privilege access. We also incorporate audit logging and monitoring to keep visibility over remote access, so that remote does not mean risky.

KEY BENEFITS

- Protect OT networks while enabling safe remote operations
- Centralized monitoring and control of remote connections
- Time based access
- Control over file transfer
- Compliance with ISA/IEC 62443 and internal policies
- Reduce exposure to cyber threats

DELIVERABLES

- Evaluate existing remote access methods
- Design secure, segmented remote access using ZTNA
- Integration with multi-factor authentication
- Integration with Windows Active Directory for Centralized Authentication
- Integration with SIEM for logging
- Provide documentation and training

PARTNER WITH ARISTA CYBER TO DESIGN, DEPLOY, AND PROTECT YOUR OT OPERATIONS WITH BUILT-IN SECURITY AND LASTING CONFIDENCE.

HAVE A QUESTION?

Contact our industrial cybersecurity professionals for more information.

REQUEST A CONSULTATION

CONTROLLED, CENTRALIZED, AND COMPLIANT REMOTE ACCESS FOR RESILIENT OPERATIONS

VISIBILITY. INTEGRITY. RESILIENCE.

Let’s Fortify Your Future.

More information

Email us: info@aristacyber.io
Or visit aristacyber.io

The Cutting Edge of OT Cybersecurity