

Cyber-Physical Security

Secure Remote Console Access

BlackEdge combines authenticated remote access over Ethernet with a motor-driven RJ45 lock that physically secures the equipment's RS232 serial-console connection.

Authorized operators reach the attached serial console remotely through **BlackEdge**. Authentication, assigned roles, command policies, and activity records bring identity and accountability to the console workflow.

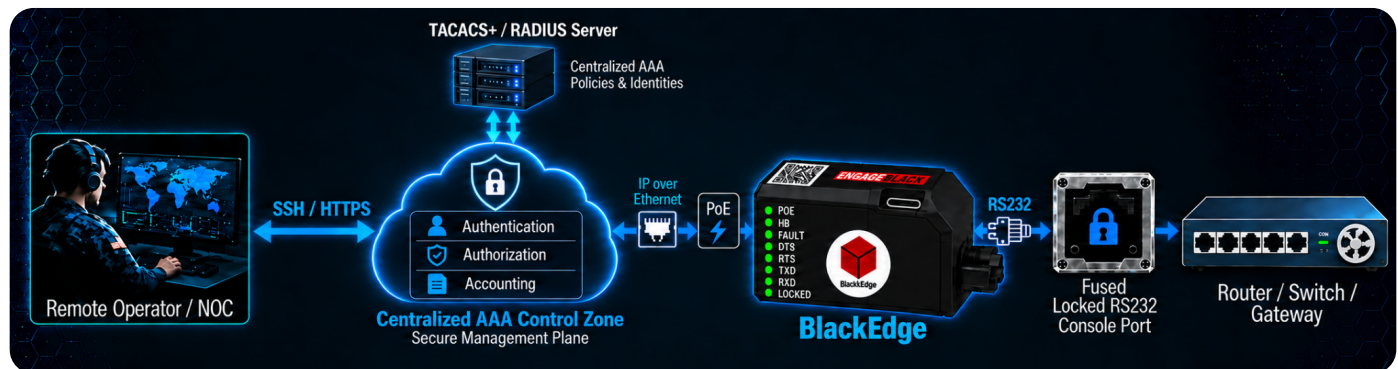
BlackEdge protects the console connection against unauthorized physical access, malicious access, unauthorized commands, and tampering.



BlackEdge at a protected serial-console connection.

Remote-To-Console Architecture

Connect **BlackEdge** to the equipment's serial console and management network. Authorized operators reach the protected console remotely, with identity validated locally/on-device or through TACACS+ / RADIUS.



Operational Technology

Secure serial-console paths across SCADA and other critical systems in utilities, manufacturing, transportation, oil, gas, and mining.

Defence Communications

Protect serial-console access across tactical routers, SATCOM, command posts, mobile systems, and radio base stations.

Network Infrastructure

Protect privileged serial-console access to routers, switches, and gateways across distributed network infrastructure.

Console Port Vulnerability

Serial console ports provide direct access to equipment management

The underlying RS232 connection carries console data in plaintext.

Physical Exposure

Without physical port protection, unauthorized access is easily achieved.

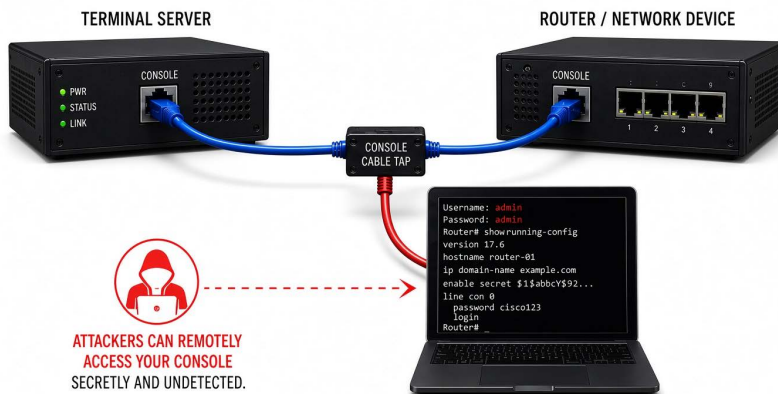
Persistent Login Sessions

Sessions may remain open when automatic timeouts are not configured or supported.

Weak Authentication

Basic, static, or shared passwords can weaken individual identity verification.

INSECURE CONSOLE CABLE



- A hidden cable tap can turn local access into a remote attack path
- Commercial cable taps are readily available
- Reveal login credentials
- Direct unauthenticated access
- Expose critical infrastructure

Physical Console Port Protection

Fused authenticated console access.

BlackEdge secures RJ45 connectors with a tamper-reactive electronic lock that uses cryptographic multi-factor authentication to restrict access.



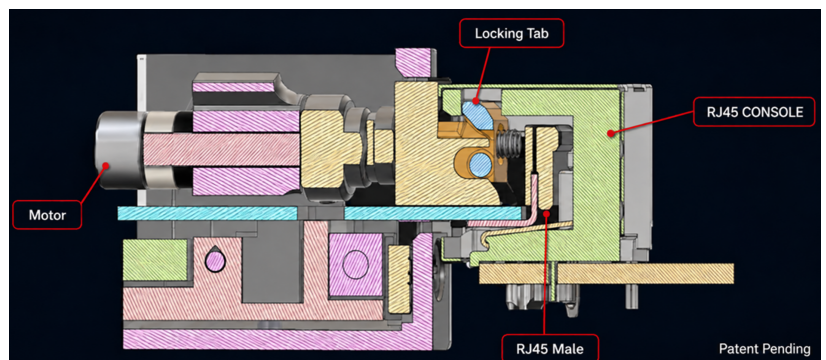
Active Physical Barrier



Strict Access Control



Intelligent Tamper Response



Motor-driven RJ45 lock cross-section

Identity, Control, and Accountability

BlackEdge applies **Authentication, Authorization, and Accounting (AAA)** to remote console access: verify identity, control permitted actions and commands, and record activity for attribution.

Centralized Authentication

Connect **BlackEdge** to **TACACS+ or RADIUS** servers for centralized operator authentication.

Local Authentication Methods

TOTP uses a time-based code from an enrolled authenticator app for the configured MFA workflow. **Client certificates** are validated under the configured trust policy.

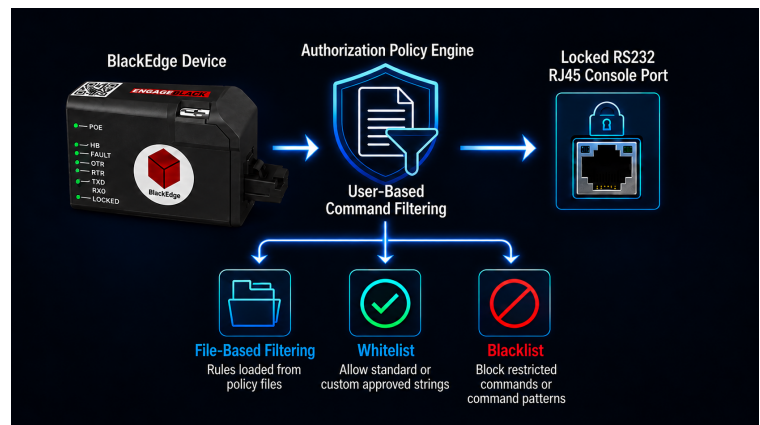
Authorization

Roles

Super-Admin, Admin, and Operator roles define administrative and console permissions.

Command-Level Control

File-based command policies specify allowed commands and block commands outside the user's assigned policy.



Accounting

Record type	Operational visibility
Session history	Who connected, when, and where the connection originated.
Command audit trail	Commands entered and their allowed or blocked outcomes.
Security events	Authentication, access, and tamper events alongside console activity.

Centralized SNMP Monitoring

SNMPv3 monitoring and traps bring remote device status and security events into a central management system for distributed visibility.

Tamper Response

When physical interference is detected, **BlackEdge** blocks console access while the tamper condition is active, records the event, and sends an SNMP trap to the configured monitoring system.

Technical Specifications


[Product Web Page](#)

Specification	BlackEdge
Console	• RS232 via locking RJ45 • DB9-to-RJ45 adapter
Network	• Ethernet management-network connection • SSH access to the attached serial console
Power	• USB-C or 24 V DC, depending on configuration • PoE as an alternative with Ethernet connectivity
Authentication	• Certificate-based authentication or TOTP • Local/on-device validation or TACACS+ / RADIUS
Authorization	• Role-based administrative and console permissions • File-based command filtering
Dashboard & Terminal Clients	• HTTPS dashboard for status, access settings, authorized lock/unlock, and browser terminal • Compatible SSH terminal clients include Rocket Reflection, SecureCRT, MobaXterm Pro, PuTTY-CAC, and others
Monitoring & audit	• SNMPv3 monitoring and traps • Session records, command audit information, and security events
Cryptographic hardware	• FIPS 140-3-validated secure cryptographic coprocessor (TPM) • Dedicated hardware boundary for TPM-managed keys and cryptographic operations
Validation	• FIPS 140-3 Overall Level 2 • Physical Security Level 3 • CMVP Certificate #5109 • Common Criteria EAL4+ in compliance with TPM 2.0 • Trusted Computing Group (TCG) certification
Dimensions	2.2 x 0.75 x 1.5 in

Accessory: DB9-To-RJ45 Adapter

Use the DB9-to-RJ45 adapter with compatible legacy DB9 serial ports while keeping **BlackEdge** inline with the protected connection.

