ENGAGE BLACK

BlackPiQ

Cyber-Physical Security

Encrypted Communications. Locked to the Controller.

BlackPiQ fuses authenticated IPsec encryption directly to a critical infrastructure asset's Ethernet port. The ramp and clamp electronic lock secures the physical connection, joining encrypted communications and port protection at the controller.

BlackPiQ protects the Ethernet interface against unauthorized local access, removal, replacement-cable bypass, and tampering.



BlackPiQ physically locked to the controller.

Stop lateral movement at the controller interface

Only the authorized control system network can communicate with the protected controller through its encrypted tunnel, preventing direct local access. **BlackPiQ** adds this protection without changing the controller's IP address or underlying logic.

Encrypted Path to the Control System

BlackPiQ creates an authenticated IPsec tunnel from the protected controller to a compatible IPsec gateway serving the control system, securing communications while locking the physical connection at the controller.



IPsec Interoperability

BlackPiQ connects to compatible firewalls, VPN gateways, and Ethernet encryptors using IKEv2 IPsec. The remote endpoint does not need to be another **BlackPiQ**. Both endpoints must use compatible security settings.

Post-Quantum Web Management

BlackPiQ supports hybrid key establishment using X25519 and ML-KEM-768 to protect its browser-based management interface. Controller traffic uses standard IPsec.

Engage Black • 9565 Soquel Drive, Aptos, CA 95003 • Tel: +1 (831) 688-1021 • sales@engageblack.com • www.engageblack.com

ENGAGE BLACK

BlackPiQ

Ethernet Port Vulnerability

An exposed connection can become a direct access path

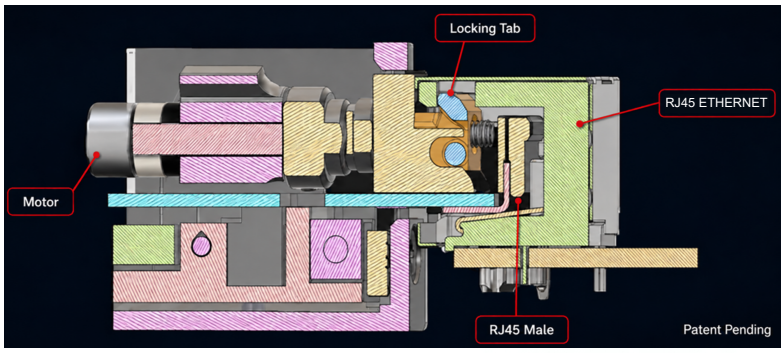
A reachable Ethernet segment can expose controller traffic and enable lateral movement. Without controller-level access controls, a compromised host or unauthorized physical connection may provide a path for unauthorized commands, configuration changes, or operational disruption.

Physical Ethernet Port Protection

Encryption locked to the asset.

BlackPiQ combines authenticated IPsec encryption with a Ramp & Clamp electronic lock to secure the controller's Ethernet connection.

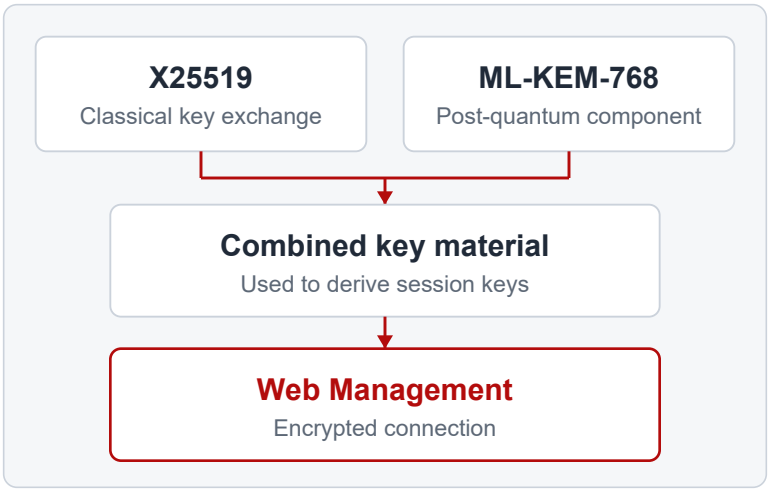
- **Active physical barrier**
- **Strict access control**
- **Intelligent tamper response**



Motor-driven RJ45 lock cross-section

Post-Quantum Protection

Post-Quantum Protection for Web Management



BlackPiQ combines classical X25519 key exchange with post-quantum **ML-KEM-768** to establish encryption keys for its browser-based management interface. Controller traffic uses standard **IPsec**.

This hybrid approach is designed to preserve key-establishment security even if one of the two methods is compromised. It helps protect against attackers capturing encrypted web-management traffic today for decryption with future quantum computers.

Engage Black • 9565 Soquel Drive, Aptos, CA 95003 • Tel: +1 (831) 688-1021 • sales@engageblack.com • www.engageblack.com

ENGAGE BLACK BlackPiQ

Identity, Control, and Accountability

BlackPiQ applies **Authentication, Authorization, and Accounting** to device management: verify administrators, assign permissions, and associate configuration activity with identity.

Centralized Authentication

Connect **BlackPiQ** to **TACACS+ or RADIUS** for centralized authentication to its management interface.

Local Authentication Methods

TOTP uses one-time codes from an enrolled authenticator app. **Client certificates** establish identity through a configured trust chain.

Authorization

Roles
Admin: device administration.
Super: device and user administration.

Management Visibility

Review device health, tunnel state, Ethernet traffic, security status, and active management connections.

Accounting

Record type	Operational visibility
Administrative access	Associate management access with the responsible user.
Configuration activity	Review administrative changes and system logs.
Security events	Inspect reported authentication, link, and tamper events.

Centralized SNMP Monitoring

SNMPv3 monitoring and notifications report configured authentication-failure, link-loss, and tamper conditions to authorized monitoring systems.

Modern Security for Legacy Controllers

BlackPiQ adds secure access and file-transfer capabilities to controllers that rely on legacy protocols.

- **SSH-to-Telnet:** Provides encrypted SSH access to the controller's existing Telnet interface for remote administration.
- **SFTP-to-TFTP:** Provides secure SFTP transfers to the controller's existing TFTP service for supported remote firmware and configuration updates.

Engage Black • 9565 Soquel Drive, Aptos, CA 95003 • Tel: +1 (831) 688-1021 • sales@engageblack.com • www.engageblack.com

ENGAGE BLACK

BlackPiQ

Technical Specifications

Product Web Page

Specification	BlackPiQ
Asset interface & uplink	• Protected asset: 10/100 Base-T Ethernet • Locking RJ45 with Ramp & Clamp. • Secure uplink: 10/100 Base-T Ethernet.
Power & mechanical security	• 24 V DC female input • PoE 802.3af Class 2 alternative power. • Patent-pending Ramp & Clamp • Zero-power bi-stable lock retention.
IPsec	• IKEv2 • Tunnel and transport modes.
Optional post-quantum	• Hybrid key establishment for the browser-based management interface. • Combines classical X25519 with post-quantum ML-KEM-768.
Management & monitoring	• Web UI for configuration and monitoring • MFA: TOTP / client certificates • Role-based access control • TACACS+ / RADIUS centralized device authentication • SNMPv3 monitoring and notifications.
Optional legacy controller security	• **SSH-to-Telnet:** Encrypted remote administration. • **SFTP-to-TFTP:** Secure file transfer for supported firmware and configuration updates.
Cryptographic hardware	• Trusted Platform Module (TPM) provides a hardware boundary for TPM-managed keys and supported cryptographic operations.
Module validation	• FIPS 140-3 Overall Level 2 • Physical Security Level 3. • CMVP Certificate #5109 • Validation applies to the incorporated module.
Operating temperature	• −40°C to +85°C.
Dimensions	• 2.2 × 0.75 × 1.5 in.