

# MOCANA

## Case Study: Ruggedized Networking Equipment Provider Hardens Devices and Secures Communications

### Challenge

This networking equipment provider designs, manufactures and sells industrially hardened networking equipment that can be used in industrial environments. Their products include ruggedized Ethernet switches, servers and media converters that can withstand a wide range of temperatures and high electromagnetic interference. Each of these products are typically installed or used in environments that are difficult to physically secure. The company was concerned about hackers being able to physically compromise a device and install malware that would give them control of the device or access to private data.

The company needed a way for network and system administrators to access and manage the network devices securely. They also wanted to make sure that someone who gained unauthorized physical access to the device or a serial port could not tamper with the device, implement malware, or access private information. They required support for SSL and SSH. They also wanted to ensure that passwords were authenticated against a RADIUS server to support multi-factor authentication.

### Mocana Solution

This networking equipment manufacturer selected Mocana's IoT Security Platform, an embedded security software solution optimized for use in industrial control and IoT devices. The software is designed to compile into the firmware of the device. The Mocana solution provides the manufacturer with:

- FIPS 140-2 Level 1 validated crypto engine that is free of open source security software
- Support for secure SSL and SSH for encrypted data communications
- Support for extended authentication and multi-factor authentication
- Ability to support digital identities and certificate management using X.509 certificates.

### Impact

The manufacturer was able to harden their networking devices with strong cybersecurity controls and secure communications. Mocana's solution enabled the manufacturer to differentiate their product by providing system administrators with a secure method to access and manage the device.

### About the Networking Equipment Provider

This networking equipment provider is part of a multinational conglomerate that serves industrial and commercial companies. The parent has more than \$80 billion in revenues and 300,000 employees. In addition to manufacturing networking equipment, the company produces controllers and heavy machinery for power generation, industrial automation, medical technologies, railways and water treatment.

### Challenge

- Harden ruggedized networking equipment
- Prevent tampering
- Secure communications with multi-factor authentication and encryption

### Solution

- Mocana IoT Security Platform enabling device integrity, SSL communications
- Multi-factor authentication and extended authentication

### Impact

- Enabled product differentiation
- Reduced surfaces for attack
- Improved the company's cyber risk profile