MOCANA

# Driving Operational Device Security Revenue and Margins

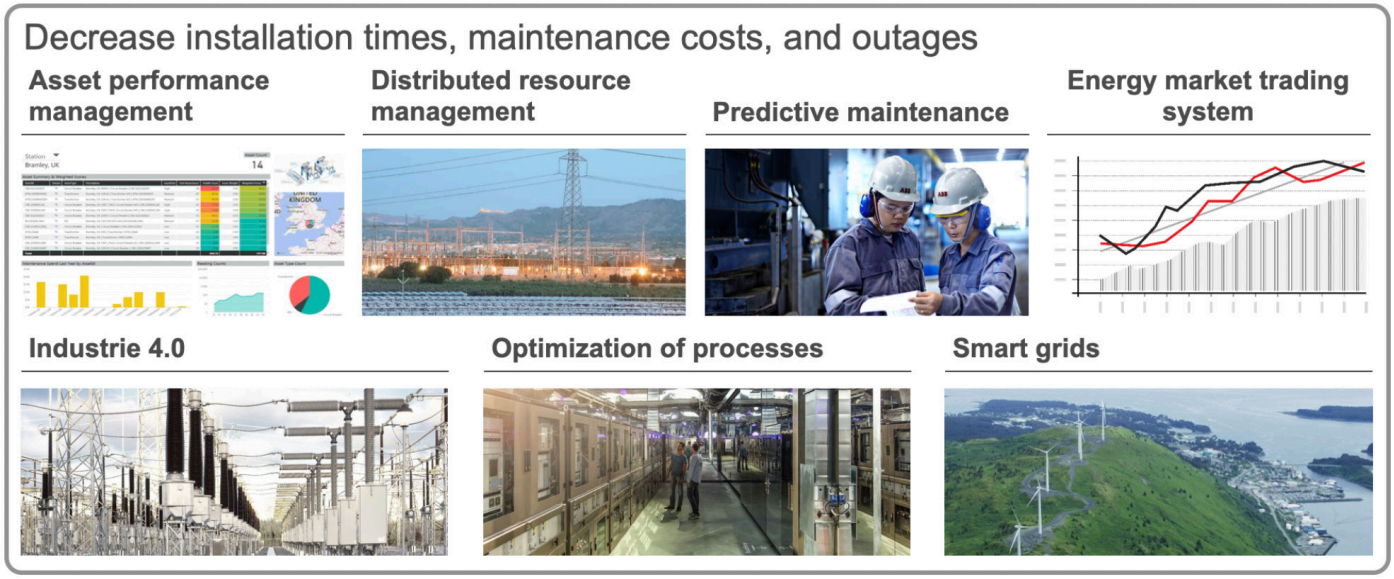


Figure 1. Challenges of Managing the Device Security Lifecycle

## Digital Transformation and Security

Industrie 4.0 has ushered in a wave of innovation that is helping industrial operators to improve installation times, reduce maintenance costs, and improve productivity and uptime. The need for artificial intelligence and cloud computing is increasing the need to connect industrial systems to the Internet, expanding the surface of attack and making the systems more vulnerable. The United States Council of Economic Advisors estimates that malicious cyber activity costs the U.S. economy between $57 and $109 billion per year.[i]

## Operator Challenges of Security Management

Protecting and managing the security of industrial and Internet of Things (IoT) devices is challenging. According to IMS Research, 85% of all industrial devices in the field are considered to be legacy, and critical infrastructure operators and industrial automation companies are struggling to protect decades-old equipment. Securing the supply chain requires an understanding of the device security lifecycle.

## High Costs of Managing Device Security

Aging devices with limited security protections need to be updated and patched. Oftentimes, these devices are patched manually by field technicians using insecure methods that are costly. Dispatching a field technician may cost $300 to $1,000 per incidence to simply manually implement a software patch or to update credentials and keys. Furthurmore, field technicians with access to private keys or device credentials can be compromised, allowing keys to get into the hands of malicious actors who can use the information to stage man-in-the-middle (MITM) attacks.

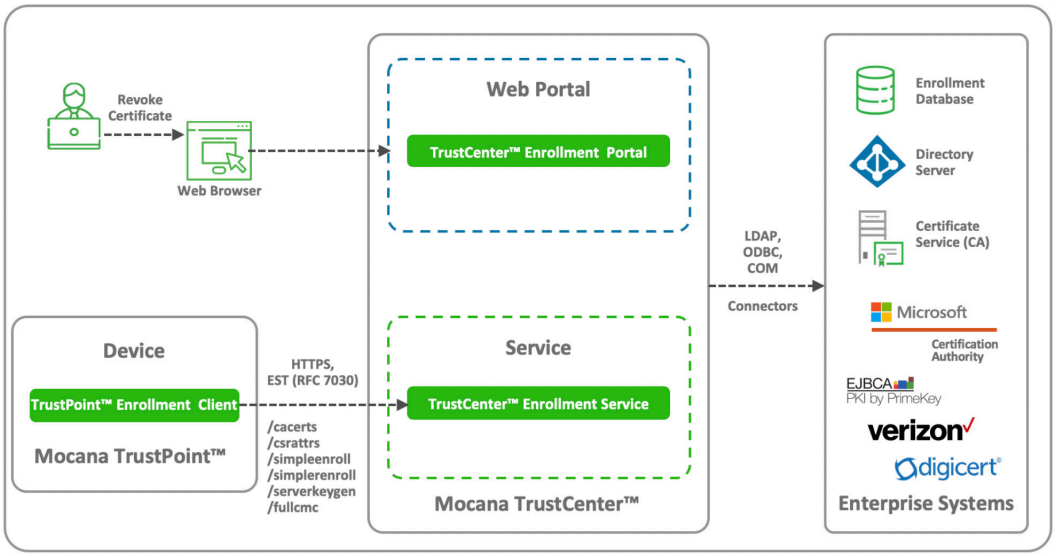


Figure 2. Mocana TrustCenter™ Automated Lifecycle Management

### Drive Operational Device Security Revenue

Given thedifficulty of managing the security lifecycle, OEMs, industrial operators, and service providers have the opportunity to introduce new security services for asset owners to help them decrease the cost and risks associated with device security.

### Mocana TrustCenter™ - Automated Device Security Lifecycle Management

Mocana TrustCenter™ is a services platform that automate the device security lifecycle. Mocana TrustCenter™ Enrollment Service (TCES) automates key, certificate and credential management. Mocana TrustCenter™ Update Service (TCUS) automates secure firmware updates. These services run on private or public cloud servers.

Mocana TrustCenter™ automates certificate enrollment, renewal, and rekey operations that enable secure device onboarding, trusted updates, secure transport and data protection required by IoT applications.

### Mocana TrustPoint™ - Device Security Software

Mocana TrustPoint™ is comprised of comprehensive embedded security software that is delivered as binary clients or source code that runs on Linux, Windows or a real-time operating system. TrustPoint™ includes a FIPS 140-2 level 1 validated crypto engine.

### Simple Credential Management and Updates

Operators and asset owners can use Mocana TrustCenter™ to securely and remotely provision and manage keys, digital X.509 certificates, device credentials, and software updates. Using TrustCenter™ simplifies the management of the device security lifecycle. This dramatically lowers the cost of operational device security management.

### Easy Device Management System Integration

Mocana TrustCenter™ can be integrated with vendor device management systems (DMS), certificate authorities (CA), and backend directory servers and business ERP systems using the Mocana's REST APIs and connectors.

---

[i] https://www.whitehouse.gov/wp-content/uploads/2018/03/The-Cost-of-Malicious-Cyber-Activity-to-the-U.S.-Economy.pdf

**Mocana Corporation**
111 W Evelyn Ave, Ste 210
Sunnyvale, CA 94086
tel (415) 617-0055 toll free (866) 213-1273
**iotsales@mocana.com**

 