Mercury

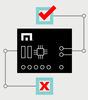
REVOLUTIONIZING ACCESS CONTROL

Mercury Embedded Application Environment

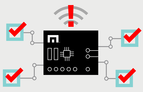
Redefining Security Through Intelligence at the Edge

- **Hosts applications on-device,** eliminating external dependencies
- **Enables new features through software** instead of hardware replacement
- **Supports a growing ecosystem** of developers and partners
- **Adapts to changing needs** with a flexible, future-ready architecture

Real-Time Edge Computing



Local decision-making: Processes access events on-device, reducing reliance on external servers



Offline operation: Maintains access control functions during network disruptions

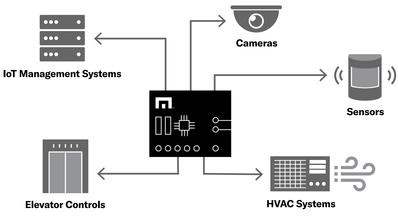
Suitable for sensitive environments: Functions in remote sites and restricted-network facilities

Simplifying IoT Integration

Links access control with smart building systems, enabling automation and efficiency

Unifies diverse devices under one platform to simplify management

Streamlines management and updates to eliminate security gaps



APIs Empower Connected Innovation

Host APIs: Facilitate management of core controller functions, such as access logic, event handling and system configuration.

Device APIs: Integrate locks, sensors, biometric readers and other hardware.

System APIs: Sync with IoT management systems databases, cloud platforms and identity systems.

Auxiliary Auth APIs: Enable PKI-based authentication, biometrics, multi-factor authentication and custom credentials.

Providing Robust Security at Every Level

Secure Boot: Verifies firmware at start-up, blocking unauthorized code

TrustZone: Isolates sensitive processes in a hardware-enforced secure enclave

API Validation: Authenticates and encrypts data to allow only trusted communication

Mercury's transformative platform is redefining security.

LEARN MORE