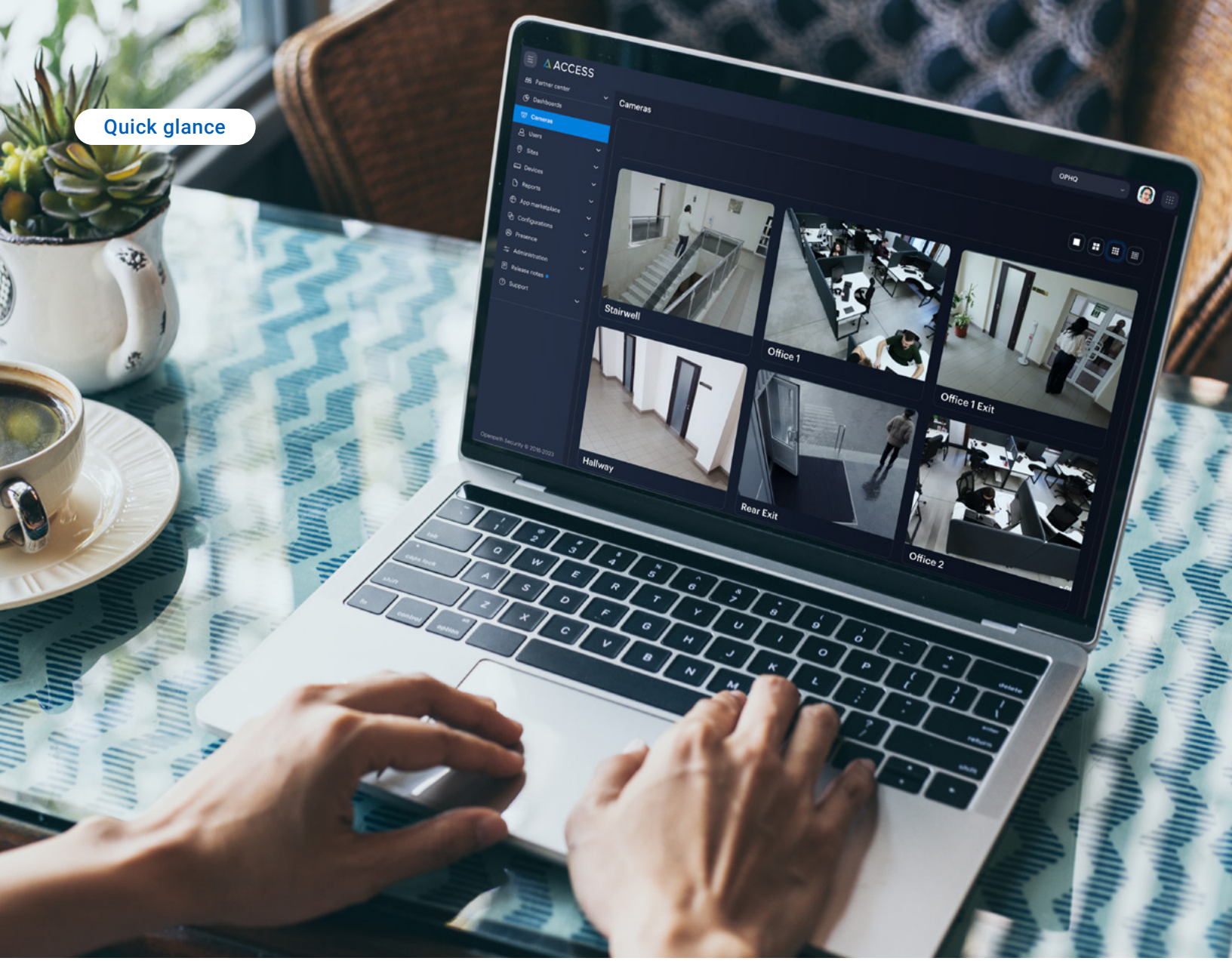
Quick glance



AVIGILON™

Physical & Cyber Security with Avigilon Alta Access

Avigilon Alta Access is designed to help keep your people and data safe, period. From the ground up, our infrastructure is built with cloud-native technology and encryption. New updates are auto-installed as they are released, meaning your access control system always has the latest security protocols to keep up with evolving threats. Behind the scenes, we proactively test areas of concern across multiple layers, staying ahead of potential vulnerabilities while maintaining the best possible experience for end-users.

MOTOROLA SOLUTIONS

At the door, our core architecture relies on the latest encryption techniques for secure key management, while tamper-resistant hardware protects unlocks and safeguards data privacy. We don't wait for threats to emerge; we proactively anticipate and mitigate risks to your data and people.

Avigilon Alta Access' comprehensive security features include:

Robust architecture

Alta Access is designed for hostile environments, assuming that readers are deployed in public areas and have insecure communication channels. Access is secured through end-to-end encryption, multi-factor authentication and offline capabilities to protect against both passive and active attackers across all mediums.

Advanced encryption

The system employs TLS 1.2 with NSA Suite B Cryptography algorithms for most communications. Unique end-to-end encryption is used for Bluetooth Low Energy (BLE), protecting against wireless eavesdropping and man-in-the-middle attacks, ensuring secure data transmission even over potentially compromised networks.

Secure credentials

Alta Access enhances security through mobile credentials, MIFARE DESFire EV3 key cards and SAML SSO support for centralized authentication. Mobile credentials use strong cryptography with multi-factor and biometric authentication. DESFire key cards employ unique cryptographic keys, ensuring high resistance to cloning.

Tamper-resistant hardware

Smart Readers act as secure proxies without storing sensitive data, minimizing tampering risks. Smart Hubs generate their own public/private key pairs and require physical access for initial provisioning. This design significantly reduces the risk of unauthorized access to critical information.

Offline functionality

Alta Access maintains functionality during outages through backup batteries and local credential storage. It can receive updates to user permissions offline via signed data transmitted through mobile devices, ensuring continuous secure operation even without network connectivity for up to 60 days.

Compliance & data privacy

Alta Access hardware complies with standards from regulatory bodies like FCC, ISED and CE Directives. It meets UL294 and IP65 standards for quality and protection. The system is CCPA compliant and offers EU data residency options, supporting various compliance requirements including PCI, MPAA, CJIS and HIPAA.

As the threat landscape evolves, so does our commitment to physical and cybersecurity. To dive deeper into the security features of Avigilon Alta Access, **access the whitepaper here.**

MOTOROLA SOLUTIONS

AVIGILON™