SECURITHINGS

CYBER PROTECTIONS

Secure and harden your physical security and enterprise IoT devices at scale

SecuriThings Cyber Protection enables organizations to proactively secure their physical security devices against evolving cyber threats, ensuring continuous compliance, reduced risk exposure, and resilient operations across the enterprise.

Protecting Diverse Fleets from Modern Cyber Threats

Physical security devices—cameras, access control systems, NVRs, and more—are increasingly targeted as entry points into enterprise networks. SecuriThings delivers a unified platform to identify, prioritize, and remediate cyber risks across all connected devices.

Reduced cyber risk exposure

Continuously detect vulnerabilities, misconfigurations, and outdated firmware across all devices. Prioritize and remediate risks before they can be exploited.

Automated security enforcement

Apply and enforce security policies at scale, including password rotations, certificate management, and firmware updates—without disrupting operations.

Continuous compliance assurance

Align with internal IT policies and regulatory requirements through automated controls, audit-ready reporting, and real-time compliance monitoring.

Improved operational resilience

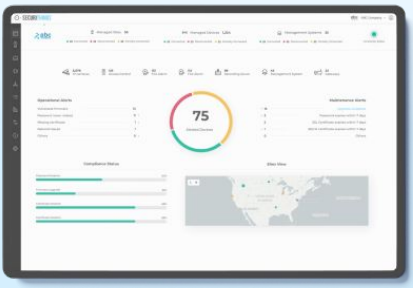
Prevent security incidents that lead to downtime or system compromise. Maintain secure, stable, and continuously available physical security systems.

Centralized visibility and control

Manage cyber posture across all sites, devices, and vendors from a single platform, with real-time insights and actionable intelligence.

Consolidate, automate & secure your physical security devices

SecuriThings Platform provides real-time security and operational efficiency to improve system availability, organizational compliance, and cyber protection while reducing costs and streamlining future planning.



Vulnerability detection

Automatically identify known vulnerabilities, weak configurations, and outdated software across all devices. Prioritize risks based on severity and impact.

Device hardening & policy enforcement

Standardize and enforce security baselines across your environment. Ensure devices are configured according to best practices and organizational policies.

Password & credential management

Eliminate weak or static credentials with automated password rotations and secure credential enforcement across all devices.

Automated remediation workflows

Remediate vulnerabilities at scale with automated actions such as firmware upgrades, credential updates, and configuration changes.

Compliance and audit readiness

Generate detailed reports on vulnerabilities, remediation status, and compliance posture. Support audits with accurate, up-to-date documentation.

Firmware lifecycle management

Ensure devices are always running secure and supported firmware versions, reducing exposure to known exploits.

Deployed across many industries including:

- Technology companies
- Financial institutions
- Healthcare
- Manufacturing
- Education
- Oil and energy
- Pharmaceutical
- Logistics
- Transportation
- Sports & Venues
- Entertainment
- Retail

For more information,
please visit us at **www.securithings.com**

SECURITHINGS