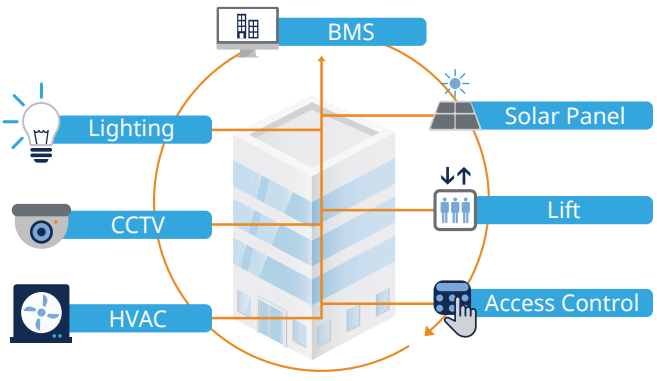
In-Depth Device Visibility & Cyber Resilience for Building Automation Networks

With many installations worldwide, Forescout's SilentDefense delivers in-depth device visibility and risk management for building automation systems (BAS) in real-time.

SilentDefense passively analyzes building automation network communications to provide in-depth device visibility and enable effective management of a full range of cyber and operational threats, including potential safety risks to building occupants.

Landscape

Today's buildings are becoming integrated cyber-physical systems (CPS), where previously isolated physical components such as HVAC, access control, elevators and surveillance systems are now connected in a unified system. Building automation systems (BAS) orchestrate this integration by connecting and controlling the building's different sub-systems to facilitate management operations. Today, data centers, hospitals, airports and other critical facilities are growing accustomed to the power of networked building automation systems (BAS) and are embracing the advent of smart buildings and the Internet of Things (IoT). For this reason, several countries are developing regulatory frameworks for BAS cybersecurity.



Device Visibility and Control

Challenge

This smart integrated connectivity makes buildings more comfortable, energy-efficient, and secure but it has also increased their exposure, with the number of identified vulnerabilities in BAS increasing over 500% in the past three years [1] and issues arising, such as:

- The exposure of legacy systems with limited security mechanisms
- The integration of technologies originally devised to address different issues
- The increasing complexity and criticality of the managed processes

Cases of cyberattacks to BAS are on the rise, and so are malfunctions, misconfigurations and operational errors. Malicious actors can now hack into this digital infrastructure and cause disruption and downtime, even forcing a data center to go offline, shutting off IP cameras or disabling security systems to grant unauthorized access to critical areas.

Solution

SilentDefense is the only solutions of its kind, offering specific benefits for building automation systems. Its non-intrusive asset inventory capability, combined with advanced machine learning, patented anomaly detection technology and extensive threat library empower building owners and managers with visibility, detection and control of their BAS to prevent cyber incidents.

SilentDefense instantly identifies BAS-connected assets in a building and provides the vendor, model, firmware and other information. SilentDefense detects misconfigurations, operational issues and both known and zero-day cyberattacks, alerting in real time if a new node appears on the network or communication patterns become abnormal.

By implementing SilentDefense, building managers can reduce risks, streamline network security operations and gain immediate ROI. It will also help them meet increasingly stringent compliance and regulatory requirements.

Benefits of SILENTDEFENSE™

SilentDefense empowers facility operators with unrivaled visibility, threat detection capability and control of their network.

VISIBILITY

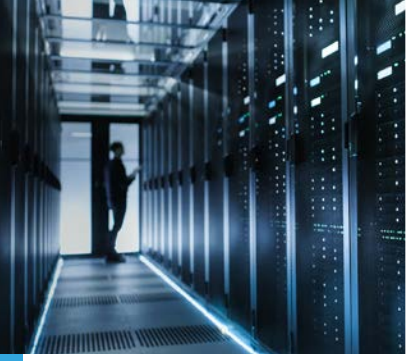
- Passively establish a complete asset inventory
- Establish a network baseline of normal communications
- Understand the current resiliency of your network

DETECTION

- Catch known and unknown threats at their earliest stages
- Pinpoint weak spots and current inefficiencies
- Gather all evidence required for incident response

CONTROL

- Prioritize incident response and mitigation activity
- Ease standards compliance with real-time asset inventory and advanced reporting capabilities
- Anticipate problems and threats




Applications

Asset Inventory

- Automatic asset and communication inventory and network map
- Passive device fingerprinting, including device model, firmware version and module
- At-a-glance view of host properties, network activity and configuration change logs

Network Assessment

- Automatic assessment of building automation device vulnerabilities, exposure to cyber threats and existing networking and operational problems
- Quick and comprehensive input for risk assessment with zero impact on the monitored network

Network Monitoring

- Continuous network monitoring and real-time alerting for operational and cyber threats
- Deep packet inspection for standard and proprietary building automation protocols and vendors such as BACNet, Fox, LonTalk
- Rich alert details facilitate root cause analysis and reduce mitigation effort and cost
- Integration with major SIEM solutions and Syslog-enabled devices in a matter of minutes

Threat Hunting

- Comprehensive search for indicators of incidentsin network traffic and protocol messages
- Continuous traffic recording for real-time and historical analysis
- Flexible framework for definition and identification of recurring suspicious behavior
- Periodic updates of IoC and Threat libraries
- Automatic, back-in-time threat searches and individuation of past compromises

Incident Response

- Identification of incident source and spread through interactive network map
- Visual real-time and historical data analysis to speed up recovery and mitigation
- Enterprise case management with smart grouping and automatic assignment of alerts to cases

Compliance & Standards

- Inventory information and controls enabling compliance with standards and guidelines such as NIST Cybersecurity Framework
- Support network segmentation, policy enforcement and timely response for compliance with IEC 62443

Product Deployment and Operation

Integration and Support

Firewalls & Data Diodes

paloalto NETWORKS
FORTINET
Check Point SOFTWARE TECHNOLOGIES LTD.
PHOENIX CONTACT
WATERFALL

SIEM Solutions

Radar IBM
splunk>
ArcSight
ALIEN VAULT

Asset & Security Management

CISCO
SKYBOX SECURITY
leidos

Building Automation Vendors

CREATING A CLIMATE FOR GROWTH PRIVA
WAGO
Honeywell
SIEMENS
TRIDIUM

[1] https://media.kasperskycontenthub.com/wp-content/uploads/sites/43/2016/07/07190426/KL_REPORT_ICS_Statistic_vulnerabilities.pdf

FORESCOUT

Forescout Technologies, Inc.
190 W Tasman Dr.
San Jose, CA 95134 USA

Toll-Free (US) 1-866-377-8771
Tel (Intl) +1-408-213-3191
Support +1-708-237-6591

Learn more at Forescout.com