Cybersecurity for Smart Buildings

FIVE-YEAR MARKET ANALYSIS AND TECHNOLOGY FORECAST THROUGH 2023

DIGITIZATION SPURS DEMAND FOR CYBERSECURITY

Buildings require reliable 24-hour operation, and the move to innovative technologies such as the IoT, cloud computing, edge computing, and analytics is driving a shift to remote building management and monitoring.

Adoption of new technologies like edge computing devices, intelligent sensors with wireless capabilities, smart lighting systems, and more is all creating a huge technology shift in the once relatively unchanging world of building automation. Most commercial buildings today implement at least some aspect of "smart" technology or intelligence, even if it is only wirelessly connected thermostats.

The big push to adopt IoT and remote connectivity has resulted in many connected buildings with remote access, but these remote connections are not always secure. Building automation systems are also frequently left exposed and, historically, have been a vector for cyber-attacks where the attacker gains entry to a building automation system and then uses that to move to the corporate network

Within the smart cities sector, smart building owner-operators are more aggressive about adopting new technologies such as IoT and remote monitoring, sometimes without fully considering the impact of cybersecurity.

The sophistication of cyber-attacks and vulnerabilities are incredibly dynamic, driving an ongoing need for more sophisticated tools and services. Successful attacks on large, cyber-sophisticated organizations have also demonstrated the limitations of defensive efforts to block intrusions and the importance of active strategies to minimize their impact.

Early detection of changes in endpoint devices and abnormal communications is fundamental to these efforts. Tools to help defenders efficiently investigate and address these events are equally important.

For more information, please visit us at www.arcweb.com/market-studies/.

STRATEGIC ISSUES

End users and owner-operators of today's intelligent buildings are starting to realize the importance of cybersecurity at the IT and OT layers. The OT layer has marked differences in requirements for cybersecurity and continuous, uninterrupted operations. End user and owner-operators must consider the following:

- Which solutions are right for me?
- How does IoT affect cybersecurity?
- How do I effectively choose suppliers?
- What are the differences in approaches for new projects vs. legacy installed base?
- What standards and industry norms should I follow?
- What scope of controls and sensors should I consider for cybersecurity?
- How can I assess my level of program maturity versus my competitors?

RESEARCH FORMAT

This ARC research is available in the form of a concise, executive-level Market Analysis Report (PDF).

RESEARCH FOCUS AREAS

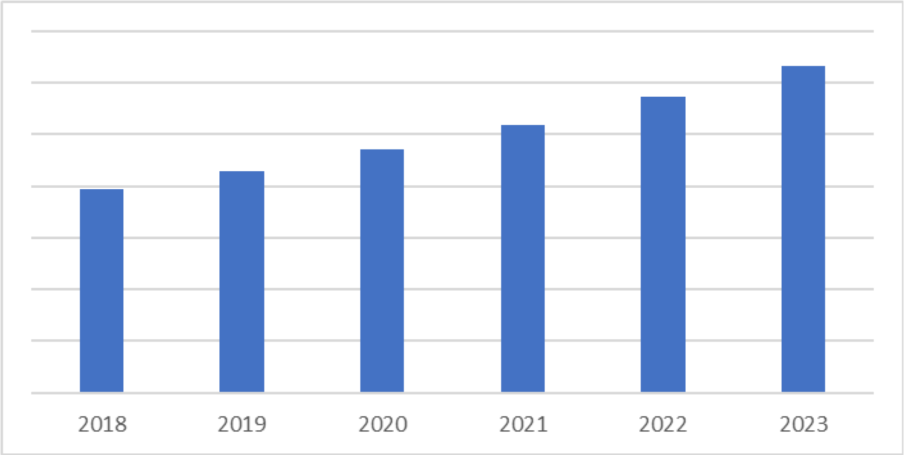
STRATEGIC ANALYSIS
Success Strategies for End Users, Owner-Operators
Success Strategies for Suppliers
Major Industry Trends
Types of OT Level Cybersecurity Solutions

SCOPE OF RESEARCH
Segmentation by Region
Segmentation by Product Type
Segmentation by Supplier Type

MARKET SIZE & FORECAST
Total Cybersecurity for Smart Buildings Business
Revenues by Region
North America
Europe, Middle East, Africa
Asia
Latin America
Revenues by Product Type
Hardware
Software
Services
Revenues by Supplier Type
ICS Cybersecurity Supplier
Building Automation Supplier
Third-party Service Provider

INDUSTRY PARTICIPANTS
The research identifies all relevant suppliers serving this market.

Worldwide Cybersecurity Market for Smart Buildings


2018
2019
2020
2021
2022
2023