IoT Threat Defense for Smart Building Systems

System availability for people productivity

As workers opt to return to the office, your investment in those spaces must be realized with happy workers and improved productivity.

Your efforts to create an economically efficient and appealing space will only pay off if your smart systems are working to make those spaces a success. Your mix of vendors and service providers help to move people to where they are supposed to be and keep them out of where they should not. They arrive to a comfortable and well-lit work site. Rooms are reserved and monitored for comfort and cleanliness. In short, your smart workplace is an orchestration of efficiency and appeal. For that to happen and continue, all those specialized systems have to work without interference and that means smart things need smart security.

Cisco’s IoT Threat Defense recognizes the different systems and the things within. We understand who should and should not communicate with what and how to apply just the right amount of security to keep things running without interrupting operations.

Benefits

- Ensure smart building systems availability
- Enable segregation of systems by criticality
- Align system ownership to access controls
Get started with a review of your building system architecture today

We can help you find all the connections, intended and otherwise, into and out of your building systems and then apply the right measure of control while assuring continued operation. No system left unseen, and no risk left unaddressed. Ask your Cisco representative or partner for a discussion on where you would like to begin.

Assure building operations without obtrusive controls

Knowing what you have helps you know who should access it and what kind of protections it needs. Cisco has been identifying and segmenting building systems for over a decade. We can show you the communication patterns as they are and help you apply policy to reflect what that access should be.

Some systems are largely self-sufficient, while others interact with each other – but all can have positive and negative impacts if those interactions are not controlled across the spectrum of communication needs. Older systems may lack any form of authentication or authorization. They and their control stations could have significant vulnerabilities. Cisco can not only ID such issues, but also mitigate that exposure until you or your vendor can apply the proper levels of system security.

The Cisco solution is comprised of:

- Cisco® ISE with AI Endpoint Analytics – passively identifies building IoT devices and applies segmentation policies
- Cisco Secure Endpoint – protects workstations from malware and unwanted applications
- Cisco Secure Firewall – classifies traffic and protects needed applications while stopping exploitation of vulnerable systems
- Cisco DUO – the easy-to-deploy and easy-to-use multi-factor authentication system for your applications and users
- Cisco Secure Network Analytics – identifies anomalous network traffic as well as applies heuristic-based identifiers for known low and slow abuse patterns

© 2022 Cisco and/or its affiliates. All rights reserved. Cisco and the Cisco logo are trademarks or registered trademarks of Cisco and/or its affiliates in the U.S. and other countries. To view a list of Cisco trademarks, go to this URL: https://www.cisco.com/go/trademarks. Third-party trademarks mentioned are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (1119R) C45-745067-00 03/22