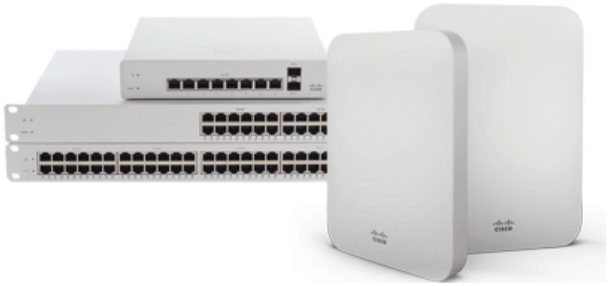
STRATOSPHERE NETWORKS

Preventive Smart Building Security for Real Estate Investment Firm Case Study



Client Background

The client is a private real estate investment firm with commercial buildings throughout the U.S. The company focuses on high-quality mid to high-rise office buildings in urban markets.

Business Challenge

The client needed preventive security solutions and services for a smart building in the Chicago area. Hacking and data breaches are a growing threat to these kinds of structures: In the first half of 2019, malicious attacks – including spyware, worms, phishing scams and ransomware – affected nearly 40 percent of the computers that control smart building automation systems, according to research released by Kaspersky.*

Without security measures in place, the networks that run a building's base systems are vulnerable to cyberattacks, especially since vendors and engineers connect devices to these networks on a regular basis. Cybercriminals can potentially shut down crucial systems (e.g., elevators or heating and cooling) or jump from the building systems network to the corporate network to get access to sensitive data.

*https://usa.kaspersky.com/about/press-releases/2019_smart-buildings-threat-landscape

Stratosphere Networks Solution

To meet the client's cybersecurity needs, the Stratosphere Networks team installed a full Meraki stack of firewalls, switches, and Wi-Fi for the building. We also provided the following solutions and services:

- Data switch installation
- WAP/wireless configuration
- WAP coverage
- Remote connectivity configuration
- Next-gen managed firewall with IPS/IDS
- Third-party vendor liaison services
- Enhanced security services
- Advanced malware protection
- Project management services
- Remote and onsite support

Benefits

- Full management and control of all ports for network protection
- Prevention of Internet of Things (IoT) device access to the network without approval from the client and Stratosphere
- Overall reduction of security breach risk level for the building and its networks
- Proactive monitoring of the infrastructure and internet
- Fully managed infrastructure stack, including updates to firewall