SOLUTION BRIEF

DRAGOS
SAFEGUARDING CIVILIZATION

Cybersecurity for Building Automation Systems

Integrated technology, intelligence, and services from Dragos

The Challenges

Building Automation Systems (BAS) have helped facility owners and tenants maintain and improve the safety, operations, and performance of connected environments for decades. While BAS systems are critical to the safe and efficient operation of modern buildings, they also face significant cybersecurity risks. BAS systems are typically comprised of interconnected devices, including controllers, sensors, valves, and related networking equipment. These systems are critical to the operation of modern buildings, as they provide a centralized way to manage and optimize energy usage, control building access, and monitor environmental conditions.

Operational and business risks exist due to threats which could cause harm to occupants and have significant negative impact to the systems that rely on a building's expected level of operations. To mitigate these risks, a comprehensive cybersecurity strategy for BAS is essential. This strategy should include architecture reviews, regular cybersecurity assessments, carefully planned and executed monitoring for comprehensive OT visibility, and ongoing evaluation of intended and actual readiness.

Dragos has worked with customers who have some of most complex and highest profile facilities in the world – everything from the largest managed data centers (case study referenced on next page), to landmark attractions and national labs. Our professional service teams are regularly consulted in the design and assessment of network architecture, endpoint protection, and operational resilience.

Your Frontline Ally

Your success is our success. We're committed to ensuring you're empowered to identify, mitigate, and respond to vulnerabilities and threats in your environment. With Dragos as your ally, you are a part of the mission - where ecosystems are empowered, adversaries are outsmarted, and civilization is safeguarded.

Given the increasing complexity and interconnectivity of BAS systems, it is critical to identify and mitigate cybersecurity risks associated with these systems. Failure to implement adequate cybersecurity measures could potentially lead to significant financial and reputational damage, as well as cause harm to the safety and well-being of building occupants.

Case Study

Dragos conducted a series of assessments to evaluate the overall cybersecurity maturity of the operational technology (OT) environment for several leased datacenters (LDCs) using the Cybersecurity Maturity Model Certification (CMMC)

The assessments examined 12 different LDCs, covering a total of 16 different regions.

Recurring trends in the vulnerabilities were found in the LDCs.

Download Case Study

Asset Visibility – What is on my network?

The Dragos Platform identifies industrial assets and their activity through passive traffic monitoring within the BAS network. Backed by our exclusive ICS/OT vulnerability knowledge base, you'll know precisely which vulnerabilities to remediate, and those that can safely be mitigated by other means based on our team's recommendations.

Threat Visibility – Who is on my network?

Leveraging our exclusive, industry-leading threat intelligence, the Dragos Platform detects threats and provides security teams with expert guided investigation and response with our playbooks. Our codified expertise arms your team with the insight and information to manage active cyber risks within BAS environments.

World-class Professional Services

We understand the differences between teams who manage corporate IT systems, and ones who are responsible for the security of building automation systems. Our teams can help integrate the unique requirements of both sides through expert-lead assessments, architecture reviews, and table-top exercises.

The Solution

Visibility into BAS networks provides the ability to identify and correlate suspicious network, host, and control events and can assist in identifying intrusions as they occur. It's important to prioritize security controls based on operational criticality. Addressing the OT visibility challenge requires a technology platform that provides comprehensive visibility of assets, vulnerabilities, and threats in the context of business priorities.

Our Expertise

Dragos offers the largest and most trusted global team of ICS/OT experts with front-line practitioner experience, who also regularly contribute to recognized standards and frameworks such as: IEC-62443, NERC CIP, NIST CSF, and C2M2. Our team of solution architects and technical account managers have worked for some of the largest and most recognized companies that supply and protect Energy Management Control Systems (EMCS), Heating Ventilation and Air Conditioning (HVAC) systems, Fire and Life Safety (FLS), and Electronic Security Systems (ESS) in regions worldwide.

To learn more about how Dragos can help secure your facilities, contact sales@dragos.com

About Dragos, Inc.

Dragos, Inc. has a global mission to safeguard civilization from those trying to disrupt the industrial infrastructure we depend on every day. Dragos is privately held and headquartered in the Washington, DC area with regional presence around the world, including Canada, Australia, New Zealand, Europe, and the Middle East.

To learn more about our technology, services, and threat intelligence offerings, visit **dragos.com** or connect with us at **sales@dragos.com**.