

# CLAROTY FOR BMS

## Why Building Management Systems (BMS) are Uniquely Difficult to Secure, and how Claroty’s Portfolio of Cybersecurity Solutions Tackles this Challenge

The world’s leading financial firms, data center colocation companies, healthcare systems, commercial real estate enterprises, airports, manufacturers, and IT services providers, and public sector organizations are among the many global organizations with at least one thing in common:

**They all rely on The Claroty Platform to help secure the building management systems (BMS) that underpin the functionality, habitability, and safety of their most critical physical facilities.**

This brief details the top challenges these types of organizations face in securing their BMS and how Claroty helps customers overcome such challenges to achieve and maintain effective and efficient BMS security.

### Top BMS Security Challenges

#### 1. BMS are Typically Designed for Engineering Efficiency – Not Security

The inherently insecure nature of most BMS creates cyber and operational risk. Key concerns and areas of exposure include:



##### Physical Security Concerns

- Physical access to the BMS console tends to be poorly controlled; adequate role-based access controls and user monitoring are rare
- BACnet, a predominant protocol through which BMS enables access and control of all building systems, is cleartext and unauthenticated; this increases exposure to physical security and other risks associated with compromises

##### Password Retrieval Vulnerabilities

- BMS often comprise legacy technologies that are infrequently patched and thus highly prone to password retrieval vulnerabilities
- These types of vulnerabilities can enable unauthenticated users to easily retrieve and reset device passwords, thereby leading to the compromise of a BMS’s underlying systems

##### Poor Security Hygiene

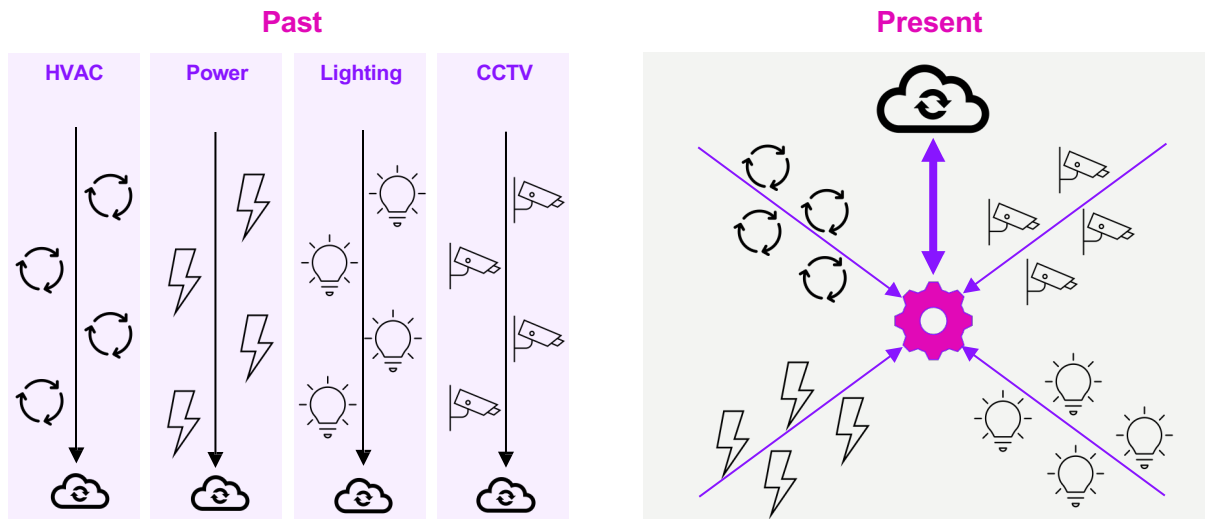
- The pervasive practice of prioritizing efficiency over security has led many BMS technicians to use weak, default, and/or shared credentials
- Since BMS technicians typically have administrative credentials, this practice significantly increases the most critical systems’ and devices’ risks of compromise via credential theft and privilege escalation attacks

##### Logical Connectivity Exposures

- BMS are often connected to IT networks and the Internet in order to enable cloud-based analytics, remote monitoring and maintenance, etc.
- Such connectivity – when combined with the inherent insecurity of BMS – expands the attack surface, making a BMS highly accessible and susceptible to a vast range of targeted and opportunistic external threats

## 2. The Rise of Smart Buildings is Amplifying the Security Weaknesses of BMS

Smart buildings are quickly transforming the status quo. In the past, buildings merely contained their HVAC, lighting, power, elevator, and security systems – among others – independently. But presently, smart building technologies are enabling more and more buildings to connect, integrate, and control all of these systems from one central console: the BMS.



The popularity of this approach is fueled by its benefits, which range from energy and maintenance efficiency, to enhanced comfort and safety, to cost savings. These benefits, however, often overshadow the real risks: By converging a building’s previously siloed – and in many cases, inherently insecure – systems into one heterogenous network shared with IT, smart building technologies can further expand the attack surface and amplify the existing security weaknesses of a BMS.

## 3. The Potential Impact of a BMS Compromise is High

Regardless of the attack type or vector, the impacts of a BMS compromise can be severe. Some common scenarios include:



Type	Description	Potential Impacts
<b>Vector for attacks on the IT network</b>	<ul style="list-style-type: none"> <li>Unsecured building automation devices can be used as steppingstones for attackers seeking to penetrate the corporate IT network</li> </ul>	<ul style="list-style-type: none"> <li>Compromise of proprietary data such as intellectual property, financial information, PII, credentials, etc.</li> <li>Downtime of IT-connected systems</li> </ul>
<b>Collateral Damage</b>	<ul style="list-style-type: none"> <li>Unsecured connectivity between a BMS and IT network, as well as certain types of vulnerabilities in building automation devices, can create pathways for IT attacks such as ransomware to spillover into the BMS</li> </ul>	<ul style="list-style-type: none"> <li>Downtime of the BMS and/or connected systems</li> <li>Compromise of critical assets whose availability, integrity, and/or reliability depend on the BMS</li> </ul>
<b>Targeted Sieeware</b>	<ul style="list-style-type: none"> <li>Remotely exploitable vulnerabilities in building automation devices can be susceptible to Sieeware, which is a form of ransomware that targets building automation systems</li> <li>Sieeware can facilitate extortion and give an attacker full control of the BMS and all connected systems</li> </ul>	<ul style="list-style-type: none"> <li>Downtime of the BMS and/or connected systems</li> <li>Compromise of critical assets whose availability, integrity, and/or reliability depend on the BMS</li> </ul>
<b>Insider Threat</b>	<ul style="list-style-type: none"> <li>Inadequate role-based access controls and the use of default or shared credentials can provide unrestricted access to a BMS for technicians and other users</li> <li>Limited visibility can enable both malicious insiders and unintentional errors to go unnoticed</li> </ul>	<ul style="list-style-type: none"> <li>Downtime of the BMS and/or connected systems</li> <li>Compromise of critical assets whose availability, integrity, and/or reliability depend on the BMS</li> </ul>

## How Claroty Addresses BMS Security Challenges

Claroty empowers customers to overcome their BMS security challenges by implementing the following controls:

<b>DISCOVER:</b> The full contents of the BMS, everything connected to it, and everything that relies on it	<b>PROTECT:</b> Against vulnerabilities, risky actions by BMS technicians, and other security weaknesses	<b>DETECT:</b> The earliest indicators of threats that could impact the BMS and/or connected systems	<b>OPTIMIZE:</b> BMS security to IT security and GRC programs via existing tools, people, and processes
<ul style="list-style-type: none"> <li>Automatic discovery and cataloging of all components of the BMS environment – including all connected systems and devices, related processes, and connected users’ sessions</li> <li>Creation of a centralized, easy-to-manage, and always up-to-date inventory of the BMS environment</li> <li>Definitive insight into what normal looks like</li> <li>The extensive caliber of visibility required to support all subsequent – and essential – aspects of an effective BMS security program</li> </ul>	<ul style="list-style-type: none"> <li>Automatic identification of BMS risk factors: unpatched vulnerabilities, insecure protocols, misconfigurations, poor security hygiene among staff, use of inadequate remote access tools, etc.</li> <li>Ongoing risk and vulnerability assessment with prioritization and mitigation guidance</li> <li>Secure remote access with RBAC, live monitoring, and an emergency disconnect mechanism</li> <li>The ability to implement and optimize BMS network segmentation based on device communications</li> </ul>	<ul style="list-style-type: none"> <li>Ongoing monitoring of the entire BMS environment for the earliest indicators of both known and unknown threats</li> <li>Actionable context – including a full root-cause analysis and risk assessment – for all alerts</li> <li>The ability to quickly detect and disconnect risky sessions from remote technicians and vendors</li> <li>A resilient threat detection model backed by Claroty’s renowned research team to ensure the latest signatures and remediation guidance are always accessible and built-in to BMS defenses</li> </ul>	<ul style="list-style-type: none"> <li>A vast integrations ecosystem and robust API that provide the ability to achieve and maintain effective BMS security via existing (and familiar) tools, infrastructure, and workflows</li> <li>A flexible, scalable architecture with cloud and on-premises options, all of which support multi-site deployments and all manner of BMS specifications</li> <li>Actionable analytics on risk posture, hygiene, and overall performance that are suitable for executive consumption and shed light on the enterprise-wide impacts of BMS security</li> </ul>

### Common Use Cases for The Claroty Platform among BMS Customers

	Providing external vendors of BMS equipment with a secure, frictionless, highly controlled means through which to remotely access the equipment for maintenance purposes	Enabling SOC analysts to receive and respond to BMS alerts seamlessly and confidently with actionable context through their existing SIEM and SOAR tools	
Monitoring the process values of data centers’ HVAC systems to ensure rapid detection of any temperature changes that could be harmful to servers	Identifying critical vulnerabilities in building automation devices and implementing zero trust-based controls to compensate for the risks until the next maintenance window when patching can safely occur	Using custom alerting rules to quickly pinpoint maintenance issues and end-of-life indicators in power systems and all connected devices	

### About Claroty

Claroty empowers industrial, healthcare, commercial, and public sector organizations to secure all cyber-physical systems in their environments: the Extended Internet of Things (XIoT). The company’s unified platform integrates with customers’ existing infrastructure to provide a full range of controls for visibility, risk and vulnerability management, network protection, threat detection, and secure remote access. Backed by the world’s largest investment firms and industrial automation vendors, Claroty is deployed by hundreds of organizations at thousands of sites globally. The company is headquartered in New York City and has a presence in Europe, Asia-Pacific, and Latin America.