INDUSTRY PERSPECTIVE

Security Challenges
Smart Buildings

Security Practices for Smart Buildings: Good, Better, Best

Ensure solution providers are implementing the right cybersecurity products

Implement a comprehensive, cybersecurity approach

Property owners and managers are beginning to use smart building technologies to increase operational efficiency and enhance tenant comfort. These technologies bring greater intelligence and automation to buildings, making them more energy-efficient, environmentally friendly, and reliable. Whereas operational savings can be significant, smart buildings can also increase property values by providing added services to occupants, such as personalized office environments, connected conference rooms, intelligent parking, and integrated security and surveillance.

These benefits stem from actionable insights, generated through detailed analysis of building data, which can be performed by a central building management system (BMS). The BMS, often located in a data center or cloud, must first be connected to all major building systems and sensing devices. This can be done with software-as-a-service (SaaS) solutions, based on the Internet of Things (IoT), which bring building data to the cloud.

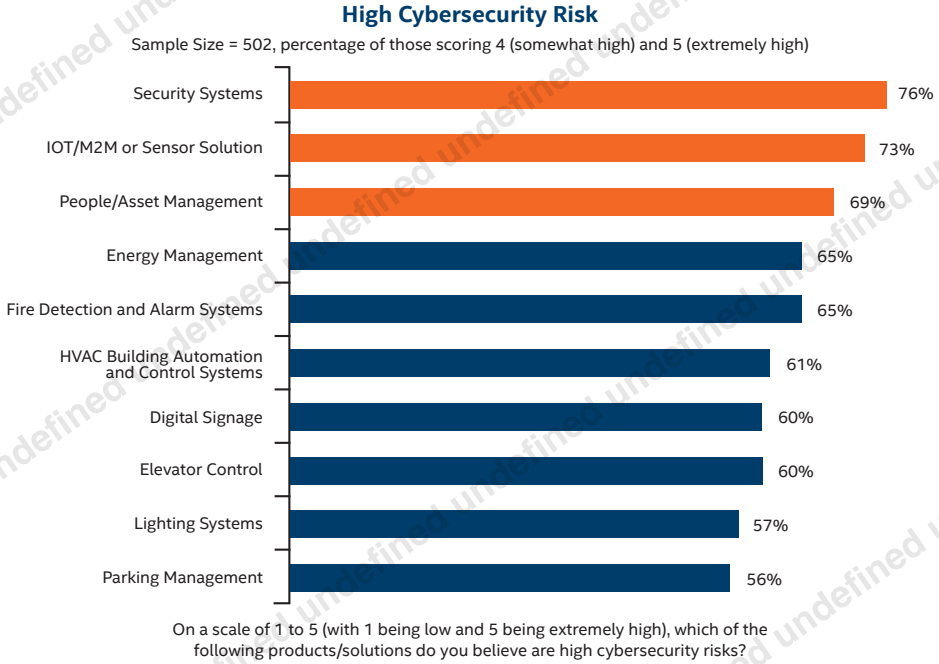

Figure 1. Building elements perceived to be at high risk[1]

Source: Compass Intelligence and the CABA Intelligent Buildings and Cybersecurity Research Report

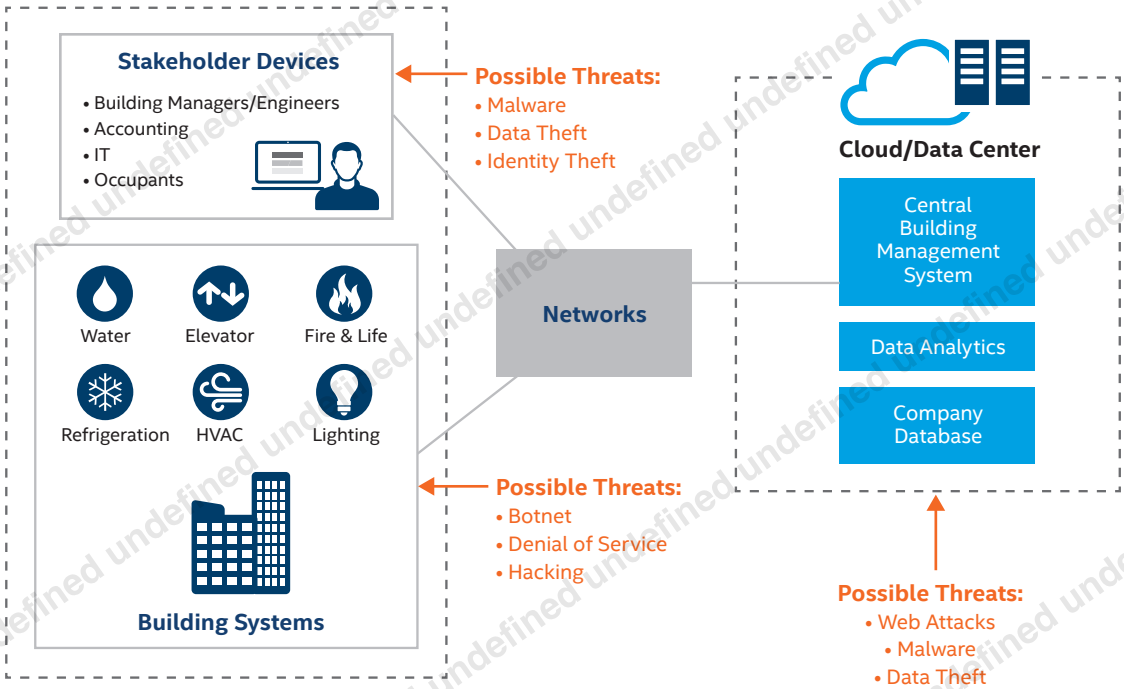

Figure 2. Possible security threats for smart building solutions

However, many of these SaaS solutions operate outside of IT-managed enterprise processes, making it imperative to proactively protect against cybersecurity risks that span customer premises, the Internet, and the enterprise. Cause for alarm, the number of cyber incidents involving industrial control systems, which includes building and access control systems, is on the rise, increasing by 74 percent from fiscal year 2011 to fiscal year 2014, according to the U.S. Department of Homeland Security (DHS).[2] Building systems with the highest risk of cybersecurity attack are shown in Figure 1, based on a recent survey conducted by Compass Intelligence and published by Continental Automated Buildings Association (CABA).[1]

To help prevent these attacks, connected devices and their data must be tamper-resistant, and the chain of custody must remain secure throughout—from devices to cloud services and enterprise applications. Intel® Security technologies for IoT solutions were expressly designed to help address these security challenges.

This paper discusses security practices for smart buildings, identifying the types of cybersecurity products available to implement robust, end-to-end protection for building systems, stakeholders, networks, and data centers.

Possible Security Threats

There is a wide variety of ways that hackers and cybercriminals could potentially attack a network through a smart building solution. Figure 2 shows some of the possible threats by potential targets.

Building Systems and Stakeholder Devices

Smart buildings will connect together a variety of building systems (e.g., HVAC, lighting, refrigeration, and surveillance) and stakeholders, including building managers and engineers, accounting, finance, IT, and occupants. Possible threats include:

Malware

Although building systems do not surf the web or open emails, they still need to be safeguarded against malware hiding in message payloads that could create serious problems, like sabotaging mission-critical data or causing equipment damage. It is also important to ensure malware cannot gain access to building systems through removable storage media such as USB drives, CDs, and DVDs. Many believe this is the way the Stuxnet virus was transmitted.

Also requiring security protection are personal computing devices used by stakeholders to connect to building systems or the BMS via a user interface. An infected device could allow malware to infiltrate the smart building. Malware typically attacks personal devices via websites, email attachments, executable files, etc., making it necessary to secure all devices that connect to the network, whether private or public (e.g., 4G, Internet).

Most stakeholders are aware of cybersecurity risks, but when it comes to phishing attacks, the user is still the weakest link.[3] The Verizon Data Breach Investigation Report, 2014[4] notes that nearly one in five users will click on a link within a phishing email.

Identity Theft

Identity theft by individuals, either internal or external to the organization, can wreak havoc if they gain administrator privileges that allow them to control the system in any fashion they desire. Often this happens via an unsuspecting user or administrator clicking on a phishing email and giving up their login credentials. Once on the network, thieves can plant a virus, steal data, control the system, eavesdrop on data being sent, or a multitude of other nefarious offenses.

Without the proper controls, an unauthorized individual can masquerade as a systems administrator, or rogue devices could connect to the network and mirror a legitimate device.

Data Theft

Databases are an attractive target for cybercriminals, especially if they contain personally identifiable information that can be sold or credentials that help them gain access to physical or intellectual property.

Networks

Smart building networks may face advanced, stealthy attacks that can evade traditional detection methods, including:

Botnets

Robot networks, popularly known as botnets, have a varied history. Essentially, a bot is simply a series of scripts, commands, or a program that is designed to connect to something (usually a server) and carry out various functions.[5] Although bots need not be harmful, some malicious programs set up a botnet system once they have breached a network. The result is a command-and-control architecture capable of spreading an infection within the network, making cleanup considerably more difficult and damage potentially much greater.[6]

Denial-of-Service Attack (DoS)

An attacker can cause a network to fail for a period of time by sending a barrage of requests and useless traffic that slows it down to the point of being unusable.[7] A distributed denial-of-service (DDos) attack on a network is typically carried out by multiple cybercriminals or machines. These attacks are usually done using botnets (remote computers that are under their control) to bombard the site with requests. Cybercriminals create botnets by infecting a collection of computers—sometimes hundreds or thousands—with malware that gives them control of the machines, allowing them to stage their attack.

Hackers

Some hackers try to use "brute force" to access networks. This is essentially the high-tech version of trying every password combination within the parameters of the organization to thwart login credential verification.[8]

Data Centers and the Cloud

Facing many of the same possible threats previously discussed, data center and cloud infrastructure with a large attack footprint (e.g., servers and storage) can be susceptible to more attacks, such as:

Web Attacks

In addition to malware and data theft, web pages used by stakeholders to interface to smart buildings should be protected. As the web continues to grow and evolve, web-borne malware attacks keep pace, threatening networks and critical data. McAfee Labs identifies hundreds of thousands of new pieces of malware each day, and most are transmitted via the web.

Layered Security Model

Due to the wide range of building systems, applications, and stakeholders, there is no single security product that will protect smart building infrastructure in its entirety. A collaborative approach to defense is needed to safeguard the building and its occupants from identifiable, emerging, or even unknown threats. A well-designed layered defense also helps contain malware, thus increasing the possibility a building system can continue to perform even when attacked.

Many legacy building systems were not designed with the security features needed to securely communicate over a common network. In these cases, an IoT gateway can be used to connect to these systems and transmit their data in VPN tunnels to the data center or cloud, as shown in Figure 3.

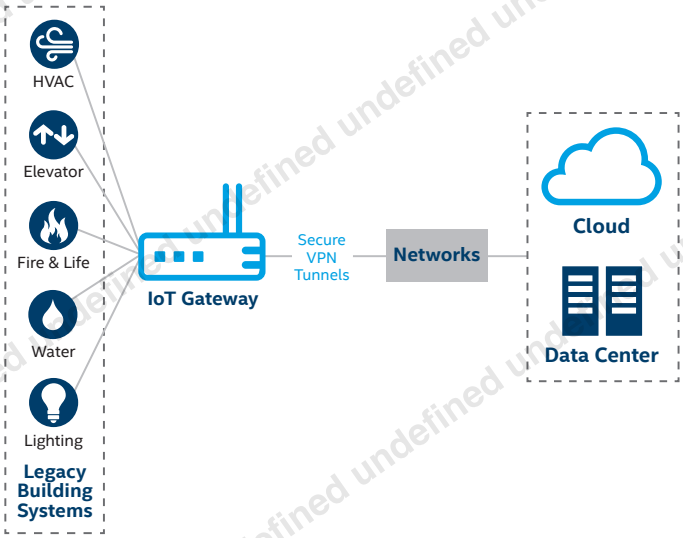

Figure 3. An IoT gateway securely sends building system data to the data center or cloud

Security Implementation: Good, Better, Best

It is easy for property owners and managers to become overwhelmed by the scope and complexity of securing a smart building. Helping to bring context to cybersecurity, Figure 4 groups the relevant security product types into three categories: good, better, and best. The "good" category captures the essential or minimum capabilities property owners and managers should ask their solution vendors to incorporate. The following briefly describes these product types and the threats they help mitigate.

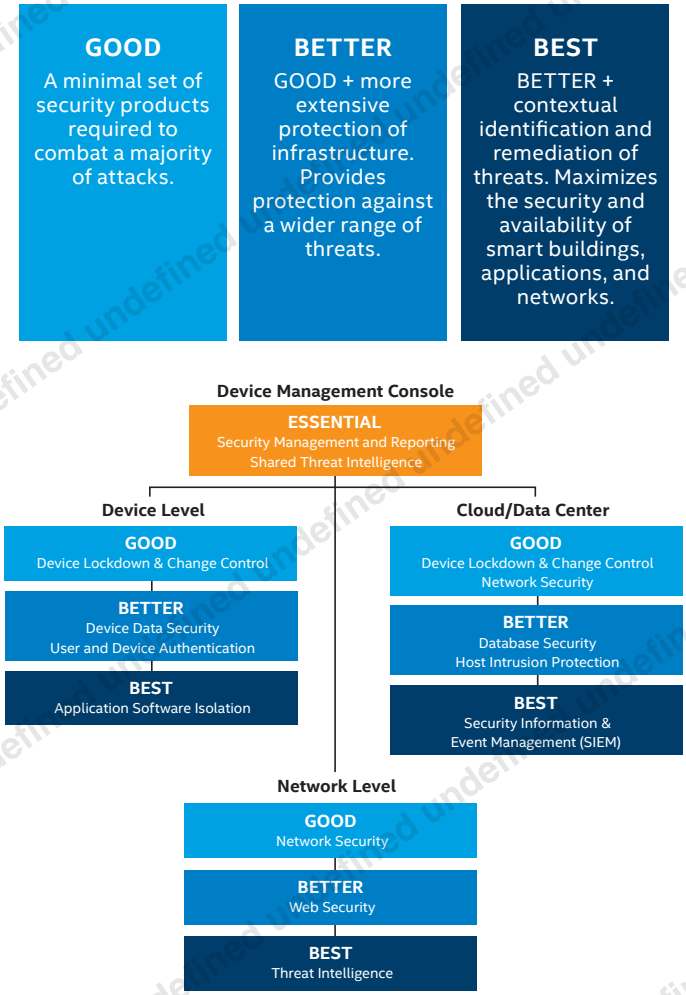

Figure 4. Types of security products categorized by good, better, and best

Device Management Console

The building management solutions should have a central console that provides a unified view of the security posture across assets in the enterprise, including device, data, user, network, and data center visibility delivered by the BMS solution vendor.

Security Management and Reporting – Good

Simplify security operations, detect vulnerabilities, and take prompt action, when needed, with help from device manageability software with automated management capabilities. Configure alerts and security responses based on the type and criticality of security events in the smart building, as well as create automated workflows between security and IT operations systems to quickly remediate outstanding issues.

Example product

Wind River Helix Device Cloud is a ready-made, cloud-based platform for the Internet of Things (IoT) that greatly reduces the complexities of building and rolling out large-scale embedded device networks.*

Shared Threat Intelligence – Best

Integrate security intelligence from multiple sources (firewalls, gateways, networks, cloud, and building systems) and have them work as one. Automatically generate self-learning, contextual knowledge that pinpoints threats and quickly adapts. Maximize protection when systems are able to learn about threats collectively.

Example product

McAfee Threat Intelligence Exchange optimizes threat detection and response by closing the gap from malware encounter to containment from days, weeks, and months down to milliseconds. Alongside, McAfee Data Exchange Layer (DXL) combines multiple threat information sources and instantly shares this data out to other connected security solutions, including third-party solutions.

Device Level

Security products are loaded on building systems and stakeholder devices.

Device Lockdown and Change Control – Good

Block malware and unauthorized applications and changes to building systems. Minimize security risks by controlling what runs on building systems and protecting their memory.

Example product

McAfee Embedded Control uses a simple, lightweight, yet highly effective whitelisting technology to protect against malware attacks.

DEVICE INTEGRITY THROUGH WHITELISTING-BASED SECURITY

There are two popular ways to protect against malware:

Antivirus (AV) is a traditional security approach that blocks (and often eradicates) malicious code or data containing a known or suspicious character string documented in a regularly updated malware signature file.

Whitelisting maintains a carefully controlled list of permitted, trusted code (i.e., whitelist), which is allowed to execute, while unknown or unauthorized software is prevented from running. Once the whitelist is created and enabled, the system is locked down to a known baseline—no program or code outside the authorized set can run, and no unauthorized changes can be made.

Whitelisting is a good choice for building systems since they are typically fixed-function devices that run a predefined set of applications. Whitelisting software has a small footprint and low overhead, and there are also no signature file updates that need to be managed on a regular basis.

Device Data Security – Better
Protect against the theft of mission-critical and occupant data and intellectual property stored by the network, storage systems, or building systems. Gain visibility on how smart building data is being used and how it may be leaking out. Encrypt building data to render it unreadable and unusable in case a malware or a hacker gains access. Prevent unauthorized use of removable storage devices. Ensure the software that runs on the IoT gateways or IP-connected edge devices sends data to the data center or cloud in digitally signed or encrypted tunnels such as SSL/HTTPS.

User and Device Authentication – Better
Enable secure and user-friendly access to business-critical information. Give users a set number of attempts to enter their password, locking the system when unsuccessful to stop hackers using brute-force login attacks. Authenticate devices to ensure only those approved can connect to the network.[8]

Example products
McAfee Enhanced Infrastructure Protection for Intel® IoT Gateway verifies the identity of devices, secures the network with a stateful firewall, and allows SSL/TLS tunnel management to ensure secure device-to-device and device-to-cloud communication.

Intel® Enhanced Privacy ID (Intel® EPID) allows building systems to authenticate other systems using a fixed, hardware-based identity similar to a fingerprint.

Device and Application Software Isolation – Best
Avoid unintended interactions between applications running on a building system, like an application (possibly malware) accessing another's memory space and corrupting or stealing its data.

Example product
Intel® Security Enterprise Infrastructure Protection (Intel® Security EIP) separates the security management functions of the platform from the operational applications, allowing the operational layer to be secured, monitored, and managed. This sophisticated solution is easy to use, cost-effective, and works with both new and legacy infrastructures.

Network Level

Network security prevents access to the system via the network itself. It is the practice of restricting access to a private network at its entry points. This involves firewalls, antivirus programs, intrusion detection and prevention systems, and security information and event management programs. This security generally addresses access from outside the system.[9]

Network Security – Good
Discover and block sophisticated threats with intrusion prevention system (IPS). Perform deep inspection of network traffic to combat botnet and DoS attacks. Identify hackers with behavior analysis.

Example product
McAfee Network Security Platform helps block more intrusions, detect and remediate breaches faster, and maximize security and performance.

Web Security – Better
Keep smart building portal free of viruses and malware. Perform deep content inspection on uploads into the portal. Web Security Gateways usually can deploy multilayered defenses incl. pattern based malware scanning but some can provide additional security services based on behavioral engines to detect unknown threats based on code behavior. These can also inspect mobile code and can provide detection for threads embedded into scripting languages not only in HTML but also PDF, office documents or flash. In addition these can help securing portals by controlling access based on the geo location of the client making a request, can act as reverse proxy to provide AAA-functionality and SSL security when acting as a reverse proxy.

Example product
McAfee Web Protection scans the web traffic of every device, user, and location for known viruses and zero-day malware.

Threat Intelligence – Best
Detect when malware writers use packing to change the composition of the code or to hide it in order to evade detection.

Example product
McAfee Advanced Threat Defense detects targeted attacks and shares threat intelligence among management, network, and endpoint systems.

Data Center and the Cloud

Servers in data centers and the cloud are increasingly the target of attacks because they house large amounts of corporate data and are also critical for performing day-to-day activities.

Device Lockdown and Change Control – Good (see Device Level description)

Network Security – Good (see Network Level description)

Database Security – Better

Keep databases safe and available. Improve visibility into all database activity, including local privileged-user access and sophisticated attacks from within the database. Terminate sessions that violate security policy, while creating a reliable audit trail of all database user activity.

Example product

McAfee Database Security provides real-time protection for business-critical databases and compliance without downtime.

Host Intrusion Protection – Better

Defend data center and cloud servers against known and new zero-day attacks. Examine database queries to prevent attacks, such as SQL injection. Ensure normal behavior and prevent tampering of data using shielding policies and rules.

Example product

McAfee Host Intrusion Prevention for Server boosts server security and lowers costs by reducing the frequency and urgency of patching.

Security Information and Event Management (SIEM) – Best

Get real-time visibility into all activity on all systems, networks, databases, and applications. Identify stealthy attacks through real-time situational awareness. Use data analytics to turn data and network traffic analysis into security intelligence.

Example product

McAfee Enterprise Security Manager delivers a real-time understanding of the world outside—threat data, reputation feeds, and vulnerability status.

Cloud-based data centers, like Microsoft Azure* or Amazon AWS*, may require a targeted security solution to protect the associated elastic assets (e.g., servers, storage) through their lifetime.

Example product

McAfee Public Cloud Security protects Windows and Linux* instances using various capabilities, such as antivirus, host firewall, intrusion prevention, application control, file integrity monitoring, and encryption management of EBS volumes. Security policies are managed centrally using McAfee ePolicy Orchestrator (ePO), a versatile central console with powerful reporting, alerting, and policy management.*

Improving Smart Building Cybersecurity

The smart building industry is at the point where cybersecurity is no longer an option. Buildings are already under attack by cybercriminals, and this is expected to increase over time.

On the whole, cybersecurity can be complex; building managers are not IT experts, and training may be needed to comprehend cybersecurity in the solutions. Building managers should partner with their IT departments to ensure that cybersecurity is designed into their solutions. Companies that do not have IT departments should ensure their cloud service providers comprehend cybersecurity into their solutions. Intel Security portfolio offers a solution with cybersecurity and allows property owners, managers, and other stakeholders to safely enjoy the benefits of smart buildings. The Foundstone Services team, part of Intel Security Professional Services, brings an objective perspective and a unique combination of tools and training to provide assessments, incident response and restoration, plus training courses in industrial control systems (ICS) cybersecurity.

For more information, visit intel.com/iot/smartbuilding.

1. CABA, "Intelligent Buildings and Cybersecurity," Landmark Research Report, 2016.
2. U.S. Government Accountability Office (U.S. GAO), "DHS and GSA Should Address Cyber Risk to Building and Access Control Systems," December 2014, http://www.gao.gov/assets/670/667512.pdf.
3. McAfee Email Protection data sheet, page 1, www.mcafee.com/us/resources/data-sheets/ds-email-protection.pdf.
4. https://dti.delaware.gov/pdfs/rp_Verizon-DBIR-2014_en_xg.pdf.
5. "The New Era of Botnets," page 3, McAfee white paper, www.mcafee.com/us/resources/white-papers/wp-new-era-of-botnets.pdf.
6. "Cybersecurity in Smart Buildings: Preventing Vulnerability While Increasing Connectivity," CABA white paper, page 13, www.caba.org/CABA/DocumentLibrary/Public/CybersecuritySmartBuildings.aspx.
7. Robert Siciliano, "What Is a Denial-of-Service Attack?" March 18, 2014, https://blogs.mcafee.com/consumer/denial-service-attack.
8. Page 13, www.caba.org/CABA/DocumentLibrary/Public/CybersecuritySmartBuildings.aspx.
9. Page 9, www.caba.org/CABA/DocumentLibrary/Public/CybersecuritySmartBuildings.aspx.

0516/MS/CMD/PDF 334327-001US