TECHNICAL BRIEF

insight.tech

POWERING IoT AND EMBEDDED INNOVATION

7 Ways to Secure Smart Buildings

Patrick Mannion

IoT-connected smart buildings face serious security risks. For example, a recent white-hat exercise by the IBM X-Force Ethical Hacking Team found that building controllers often use the same login as their network router. Once hackers get access to a network, they can quickly take over the building automation system (BAS).

To make matters worse, routers often leave administration ports open—giving hackers an easy entry point. Such vulnerabilities let hackers do things like:

- Shut down cooling systems to overheat servers
- Shut off security systems or gas sensors
- Stop elevators and turn off lighting systems
- Gain access to the IT network and corporate data

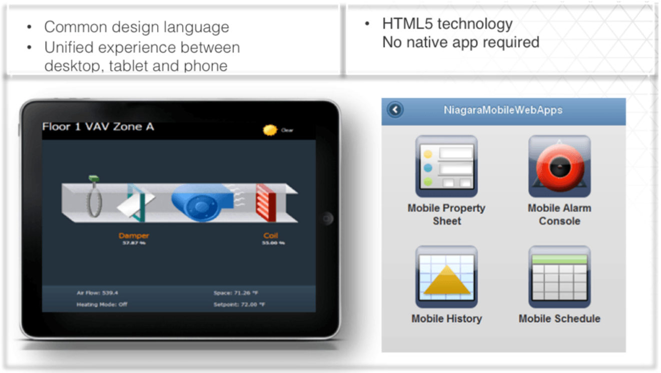
Protecting the smart building is difficult because these security risks span multiple levels: the BAS itself, the cloud connection, and the remote management interface. What's more, smart buildings are often part of a real estate portfolio, so any security solution must be able to scale across all locations.

According to Ron Victor, founder and CEO of IoTium, there are seven keys to success:

1. **Use encrypted certificates** to access the BAS instead of usernames and passwords.
2. **Eliminate VPNs and APNs** (similar to VPN but for cellular networks), again to avoid usernames and passwords—everything needs to work on certificates and keys.
3. **Don't rely on existing routers** in the building; instead, connect to the cloud using a secure gateway.
4. **Avoid changes to firewall or proxy settings** as this can make the IT network vulnerable to attack—and can require lengthy approval.
5. **Use a book-ended architecture** with software running at the data source and sink to avoid DDOS attacks.
6. **Ensure data isolation** such that every subsystem (lighting, HVAC, security, etc.) is separate all the way to the cloud, so that if malware affects one subsystem, it won't affect the others.
7. **Encrypt all traffic** to prevent unauthorized users from accessing data.

The Niagara 4 Solution

To illustrate these techniques, Victor points to his experience with the Niagara 4 building control framework. Niagara 4 is a management and control framework developed by Tridium (now part of Honeywell). It enables the integration of building systems into a unified platform with an HTML5 interface. Features include analytics, visualization, and custom dashboards **(Figure 1)**.



- Common design language
- Unified experience between desktop, tablet and phone

- HTML5 technology
  No native app required

Figure 1. Niagara 4 provides full data analysis, visibility, and control of smart buildings. (Source: Tridium)

IoTium and Kodaro recently worked together to bring Niagara 4 to the Dell Edge gateway. Among other features, these gateways are equipped with Intel® Trusted Platform Module (TPM 2.0) for secure boot and BIOS-level lockdown of unused ports.

Each TPM has a unique RSA cryptographic key burned into it, enabling use of certificates and keys instead of usernames and passwords. "You can't afford to have usernames and passwords if you have to connect millions of buildings," said Victor. "They're hard to remember and store, and it just doesn't make sense, so you need to eliminate those."

The Dell gateways provide a number of other capabilities useful for BAS. These include the ability to connect to any legacy building ecosystem (BACnet, Modbus, CANbus, Z-Wave, 6LoWPAN), as well as an advanced Intel Atom® processor for local analytics.

The combination of Niagara 4 and the Dell gateways provides many of the key requirements of a smart building, including data acquisition, processing, analysis, visualization, and remote access and control.

Securing the Endpoints

Once Niagara was ported to the gateway, the next step was to secure the network and make the solution scalable across hundreds or even thousands of facilities. This required a full understanding of vulnerabilities, elimination of truck rolls, and avoiding the need to change enterprise proxy and firewall policies.

This is where IoTium iNodeOS comes into the equation. Residing on the gateway, this Debian Linux-based OS allows secure networks to be deployed at scale by eliminating usernames and passwords, managing updates, and isolating the IT and OT networks. **(Figure 2)**.

As a managed OS, iNodeOS takes care of updates and security patches automatically, without requiring a command-line input. "You need a service that's 24/7 that is looking for vulnerabilities and patches in real time," said Victor. "We built it only because there is no OS out there that can be completely cloud-managed without the need for any command line interface."

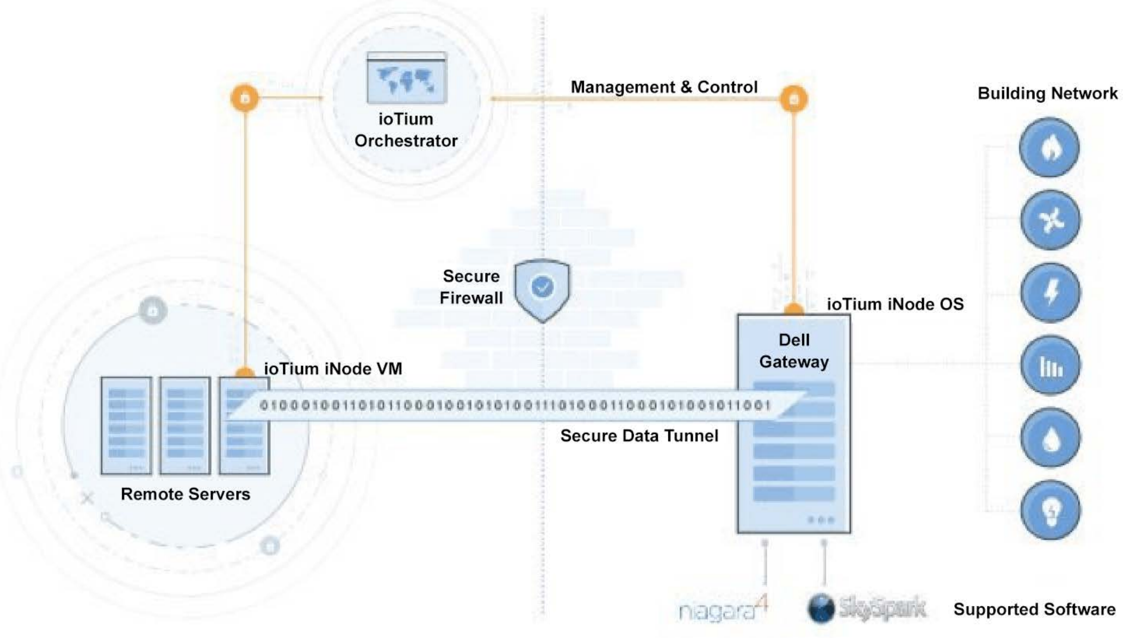


Figure 2. IoTium's solution offers multilayer security. (Source: Kodaro)

Secure Data Transmission

At the next level up, IoTium has a built-in firewall. This firewall ensures that BAS assets are neither visible on the Internet nor exposed to backdoor threats. Instead, all data runs through a secure data tunnel—a "book-ended" approach that requires authorized software at both ends.

Additionally, IoTium uses a containerized architecture that isolates each subsystem. Thus, a compromise to one subsystem will not impact other subsystems or the wider IT network. Adding encryption to the mix further protects the BAS by ensuring that any data that falls into the wrong hands will be unusable.

Avoiding Insider Attacks

Despite all the technological security measures that can be undertaken, the easiest way to compromise a system is a malicious employee. "People think it's someone from the outside that will hack the system, but the easiest way to compromise traffic is to pay off someone inside the building," said Victor. "You have to presume this is going to happen, and then protect yourself."

IoTium's bookended architecture, where a source can talk only to a sink with the same client software, helps here. It prevents data from being read if an employee simply taps into the network with his or her own device without the right client software installed.

Migrating to new IoT Deployment Paradigm

Of course, security is not the only place where scalability matters. As IoTium points out, its zero-touch provisioning and one-click application deployment can save considerable time and expense.

All in all, it's clear that a truly smart building does more than manage BAS systems. Instead, smart buildings must be designed with scalability and security in mind.