



Enhanced Insider Security

Protect your Data Center, Your Data and Your Reputation

Stop a Critical Infrastructure Breach Before it Happens

In mission critical environments such as data centers, physical security is an increasingly important aspect of operations. One bad actor who can gain access to a server or cabling infrastructure could cause irreparable harm to a business and its reputation by compromising the privacy of its customer data or accessing commercially sensitive data.

A proactive security posture helps prevent security breaches before they happen. This requires a new approach to security that builds on the physical security capabilities that are already in place. Badge access alone cannot determine a person's movement once inside a controlled area or determine if suspicious behavior is being exhibited inside that area. Video surveillance needs to go beyond visual evidence to determine proactively if a security threat is forming.

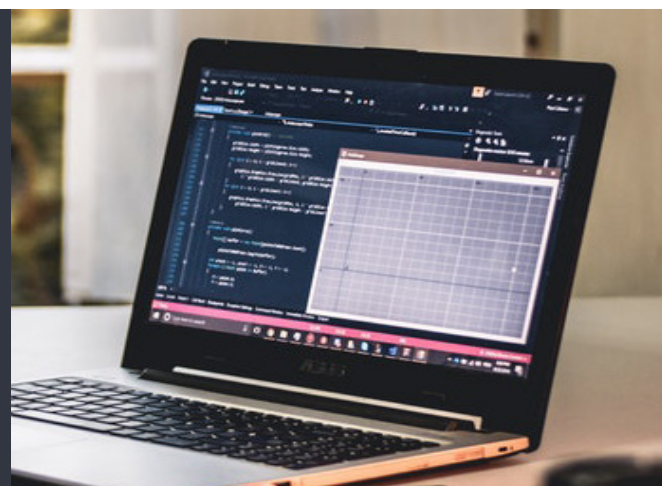
Introducing Enhanced Insider Security from Johnson Controls. This powerful and proactive solution generates real time locations of people and assets from unique wireless sensors, analyzes the data and creates custom alerts of suspicious or unauthorized behavior.



Analyze security information and create custom alerts of suspicious or unauthorized behavior to proactively protect your mission critical environment.

THERE IS SECURITY... AND THEN THERE IS **CONVERGED SECURITY**.

The Enhanced Insider Security solution looks beyond 'who badges in and who badges out' of a secure area; it tracks movement within the space and looks for behavior you deem to be unauthorized or suspicious. You make the rules — by determining how and when the system alerts your security team.



Unaccompanied Visitor

An alert is created if a visitor, who must be accompanied at all times within the data center or a defined space/zone inside the data center, is flagged as unaccompanied. A rule is set to alert security if this visitor is more than a set distance from the person who is assigned to accompany them. The alert can happen as soon as the distance threshold is reached or if the person is outside this range for more than a set amount of time.



Abandoned Badge

If a badge is removed by accident or for potentially malicious intent, this abandonment can be detected and an alert triggered.



Zoning and Rules

The data center may have multiple geo-fences or zones created, for which multiple rules can be applied.



Suspicious Rack Access

A set of racks can be defined as a special zone. A tamper-proof door movement sensor detects a door being opened and checks to see if an authorized employee is by the door, and if not, an alert is generated. In addition, tamper-proof movement sensors can be employed to detect if a door has been forced open or if there is an excessive force event on a rack structure.



Tailgating Reduction

Unauthorized persons can be detected even if they walked into a secure area behind someone else who opened the door with the swipe of a badge.



Unauthorized Dwelling

Dwell time can be measured and alerts can be triggered if a person spends an unusual amount of time in a defined area.



Unauthorized Movement of Assets

A tamper-proof tag facilitates the tracking of assets. Alerts can be triggered if an asset is moved outside a defined area and/or moved by an unauthorized person.

Your Security. Your Rules. Your Way.

Customize security rules.

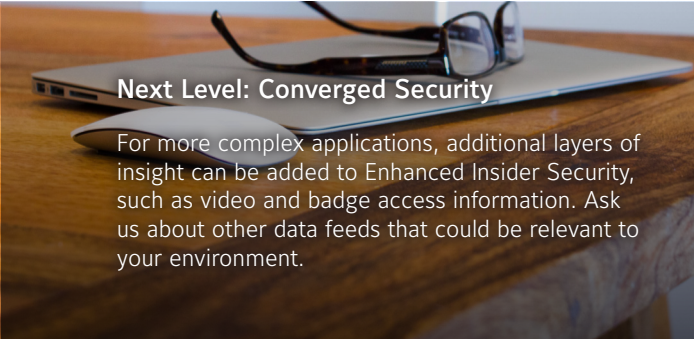
Within the secure area, you can establish zones that require varying levels of security. A 'green' zone, for example, might indicate low-value assets are present. A 'yellow' might indicate medium value and 'blue' zone might indicate high-value assets with the highest-level of access restriction. By geo-fencing the zones—even down to the level of a single workstation—you can apply different rules to each area which, when violated, would trigger prioritized alarms so the appropriate action can be taken.

Avoid vendor and technology lock-in.

The Enhanced Insider Security application is agnostic to any infrastructure or service provider, which means it can make use of sensors that are already in place. It reads location data from battery-powered beacons, Bluetooth badge trackers, smart plugs, mobile devices on WiFi, ultra-wide-band location systems and desk occupancy sensors.

Monitor events in real-time from a single interface.

When an event occurs, the application consolidates data from various feeds so you can quickly see if the priority event is something to be concerned about and if so, what actions you should take.



Next Level: Converged Security

For more complex applications, additional layers of insight can be added to Enhanced Insider Security, such as video and badge access information. Ask us about other data feeds that could be relevant to your environment.

Example: Add real-time social media feeds as an application input

As it analyzes the severity of security events, typically non-critical alarms may be elevated to higher importance. For example, an external door alarm may not, on its own, trigger a critical alarm. But it would take on added importance if the event happened during a nearby active-shooter event, violent protest, or weather emergency.

THE COMPREHENSIVE LOCATION-BASED SOLUTION

Personnel are limited to their authorized zones.



Approved Actions Include:

- Blue zone authorized personnel in Blue zone
- Yellow zone authorized personnel in Yellow zone
- Green zone authorized personnel in Green zone
- Visiting personnel (Orange) can be in any zone when accompanied by zone-authorized personnel



Restricted Actions Include:

- Yellow zone authorized personnel in Blue zone - **alert generated**
- Green zone authorized person in Yellow zone - **alert generated**

The Future of Data-Enabled Business

With more than 130 years of experience in the security and buildings industries, no other company offers a more comprehensive building technology portfolio than Johnson Controls.

Physical security systems such as access control, video surveillance and intrusion detection are designed to improve safety and protect high-value assets. But because each of these systems operates separately and speaks its own language, it has traditionally been difficult to take full advantage of the information provided by these disparate systems to proactively manage risk.

Develop a More Proactive Security Posture

Data centers and other mission critical facilities are expensive to build, maintain and secure. Enhanced Insider Security from Johnson Controls will help you make the most of the investments you've already made in sensors, beacons and gateways by merging real-time data from those sources, analyzing the events and delivering an unprecedented level of insight for a proactive security posture that manages risk in a totally unique way.



www.johnsoncontrols.com/digital