EBOOK

RETHINKING **ACCESS CONTROL**

6 Steps to a Next-Generation Physical Access Control System (PACS)

RECONASENSE

TABLE OF CONTENTS

THE NEED FOR **NEXT-GENERATION ACCESS CONTROL**

Security professionals today face more responsibility with fewer resources than ever. Expectations continue to rise to secure perimeters, people, property, and digital spaces, while there simply are not enough trained personnel to keep up. And unfortunately, budget decisions are often reactive in nature, with funding awarded in the wake of troubling security incidents.

This is just one indication of an old model at work in the physical security industry. In reality, a host of challenges contributes to a pressing need to modernize physical access control. You likely know the issues firsthand, but let's review.

A MODERN WORLD COMES WITH MODERN RISKS

The complexity and severity of threats to physical security are ever increasing. According to the Occupational Safety and Health Administration (OSHA), 18% of all violent crime in the United States now occurs in the workplace. More disturbing still, 2018 saw a 54% increase in school shootings from the previous year, and the data continues to trend tragically upward. This is particularly concerning since, according to the FBI, the most deadly phase of an active shooter scenario occurs in the first 4-8 minutes – and it usually takes four or more minutes for first responders to arrive.

THREATS COME FROM UNEXPECTED PLACES

One of the most significant security threats arises from a seemingly unlikely source: inside the organization. The Verizon 2019 Data Breach Investigations Report estimates that 34% of all breaches in the last year were perpetrated by staff, employees, or affiliates of the company that suffered the attack.

THIS IS A WAR ON MANY FRONTS

Digital transformation has widened the playing field for potential security risk factors, and vulnerabilities can now be observed on multiple fronts at the same time. Incidents that exploit two or more domains of a business are known as multi-vector attacks. These incidents often comprise cyber and physical components, making them extremely difficult to predict, prevent, and contain.

LEGACY TECHNOLOGY LAGS BEHIND BUSINESS NEEDS

By and large, businesses rely on legacy physical access control systems (PACS) as their first line of defense in physical security. But, these systems are characterized by siloed information streams, lack of visibility across these streams, and limited processing power to address information overload. Additionally, these systems are generally inflexible, limited to static, role-based permissions that allow for forensic but not proactive security measures.

PACS INTEGRATION	LEGACY	MODERN
Video analytics	✓	✓
Operational technology	✓	✓
Weapons sensors (gunshot, chemical, biological, explosives)	✓	✓
Cyber security solutions	✓	✓
Visitor/Contractor management systems	✗	✓
Geolocation services	✗	✓
Gunshot and weapons detection	✗	✓
Communications	✗	✓
IoT sensors	✗	✓
HR systems	✗	✓
Weather applications	✗	✓
Social Media applications	✗	✓
Newsfeeds/Emergency systems	✗	✓

VIDEO SOLUTIONS PREDOMINATE THE INDUSTRY

Video-based solutions drive the physical security market, but these systems often do not have the sophisticated capabilities necessary to manage the modern risk landscape. In fact, 90% of security video footage is never seen until an incident investigation is initiated. VMS vendors have made efforts to fill gaps, but tacking on functionality to solutions not originally designed to address access control is a flawed response when so much is at stake.

HUMANS ARE IMPERFECT

Security measures are put in place because humans need support to stay safe. Yet, even with protocols in place, accidents and mistakes happen. 36% of executives report documents lost or stolen due to employees ignoring physical security protocols, and 55% of organizations fail to revoke access after an employee leaves the business.

IT AND SECURITY CONTINUE TO CONVERGE

The ground is shifting under our feet, bringing cyber and physical security increasingly under the same purview. However, tools and teams remain siloed. This is particularly concerning as threats continue to approach on multiple fronts at once. For example, when Sony was attacked in 2014, the data breach was preceded by a break-in at the Sony campus.

FUTURE-PROOF
ACCESS CONTROL

The challenges facing this industry are considerable, but not insurmountable, as long as decision-makers recognize the need for modern systems that address the limitations of legacy access control solutions. Historically, access control has been viewed as a "must have," relying on the passion and initiative of security personnel to go above and beyond to fully meet the needs of their organizations. We now know that proactive, adaptive systems that integrate cutting-edge technology are the way forward.

A CHECKLIST FOR MODERN ACCESS CONTROL

It's time to redefine physical access control – to better protect life safety, to get ahead of threats before they become incidents, and to contribute to efforts to build smarter cities and facilities. Let's take a look at a checklist for next-generation access control that will help your organization choose the right PACS for the future.

STEP #1 **RE**DEFINE	YES	NO
Does your access control go beyond the door to deliver the full picture?		
Does your access control unify all data streams into a common language and dashboard?		

STEP #2 **RE**DUCE	YES	NO
Is your access control proactive, not just reactive?		
Does your access control improve safety when conditions change?		
Can your access control detect insider threats and abnormal activity?		
Is your access control cost effective, sparing you the devastating cost of potentially avoidable breaches?		

STEP #3 **RE**SPOND	YES	NO
Does your access control give actionable recommendations to help you manage security incidents as they're happening?		

STEP #4 **RE**CLAIM	YES	NO
Can you customize your access control with automation rules?		
Is your access control prepared for governance and compliance detailed reporting functions?		

STEP #5 **RE**PURPOSE	YES	NO
Can your access control integrate with other tools?		
Is your access control evolution-friendly, preparing you for the future without requiring you to rip and replace existing systems?		

STEP #1

REDEFINE

It's time to think differently about access control, with systems that go beyond the door to give you a comprehensive picture of physical security.

ACCESS CONTROL IS MULTIDIMENSIONAL

The first step in future-proofing your access control is to recognize that the doors are just the starting point to holistic protection. Modern PACS must go beyond doors to provide sightline to the multiple data streams that contribute to the security landscape. As physical and cyber security converge (and threats span from doors to the network), visibility to all available information inputs is increasingly critical. A Microsoft study by Accenture explains that "these blended threats require connecting data, building new capabilities, and gaining new insights to allow security teams to better defend against attacks."

ACCESS CONTROL SHOULD EMPOWER, NOT BURDEN SECURITY MANAGERS

A system that allows you to see all security information in one elegant view is a critical first step to threat prevention and rapid response. Better still, a modern access control system should unify and "normalize" data across input streams.

This describes a single platform to organize and interpret data from all sources, using plain English. Not only does this optimize response time and planning, but it also democratizes security management by empowering personnel at every level to make proactive decisions and respond efficiently.

We've redefined access control by broadening its scope to protect **you better.** Now let's look at how next-generation access control helps to reduce risk.

STEP #2

REDUCE

Limit exposure to risk and reduce the number of threats that become incidents with proactive, risk-adaptive access control.

PACS SHOULD KEEP PACE WITH RISKS

The risk landscape is constantly evolving. Shouldn't your PACS? The second step in future-proofing access control is effectively managing risks in a world where threats are more numerous, sophisticated, and less visible than ever.

- Insider Threats and Collusion
- Intruders
- Active Shooters and Assaults
- Multi-Vector Attacks *(Physical and Cyber)*
- Drones
- Terrorism
- Natural Disasters
- Life Safety Hazards *(Chemical, Radiation, etc.)*
- Strikes and Protests
- Information Overload
- Connected World *(IoT)*

LEGACY SYSTEMS CAN'T KEEP UP

Risks are dynamic in nature; they can increase exponentially in severity in a matter of moments. Traditional PACS are not instrumented to address this new risk landscape. There are two key limitations in legacy systems:

1 Legacy PACS are Static

They cannot automatically adapt to changing environments, humans, or behaviors. Instead, they rely on human actors to make manual changes or react to alarms. This can cost seconds to minutes or more – and worse, lives.

2 Legacy PACS are Role-Based

Access to an area is assigned based on a role within an organization, without regard for additional factors (like changes in behavior or dangers in the area). This can cause businesses to be blindsided by bad actors within their ranks or to unnecessarily put their employees at risk.

GO FROM GATEKEEPER TO LIFESAVER

Unlike legacy systems, next-generation access control is dynamic and risk-adaptive. A modern PACS can integrate multiple criteria to adjust permissions in real-time – an impossible ask for humans.

Here's how it works: A risk score is assigned to individuals, actions, and environmental changes. Modern systems vigilantly calculate risk across dozens of factors and automatically react to lock down doors or adjust permissions based on a risk threshold. In this manner, risks are identified early and accounted for – before they become incidents.

To illustrate, let's say Ted usually comes in at 8am and clocks out at 5pm almost every day. Suddenly, Ted begins leaving the office around 11pm. A legacy system would make nothing of the change. But a modern PACS would flag the deviation and combine data from other sources that might add to the suspicious behavior. With a full picture of the risk, the system would adjust permissions appropriately and recommend actions to the security team.

In another scenario, imagine a chemical spill at a lab facility. A modern system would sense the presence of toxins and automatically shut down access to affected areas. A legacy system, in contrast, may sense the spill but would not proactively limit access to the exposure zone.

PROACTIVITY PRESERVES LIVES – AND JOBS

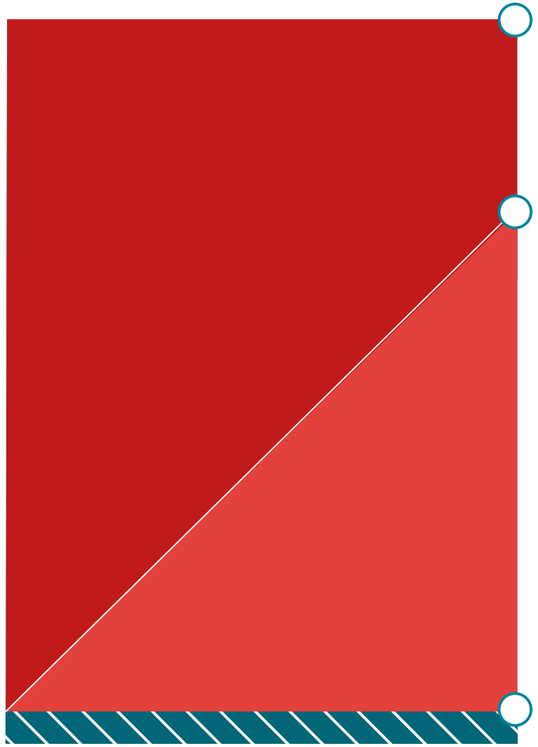
No one wants to be on duty when a security incident takes place. When accidents happen, lives and jobs are on the line. It's unrealistic to expect perfection (or clairvoyance) from human beings, but this is the beauty of a modern PACS. It's always on guard – looking, listening, analyzing behavior, and correlating patterns in real-time, so it's easier to protect lives, assets, and ultimately the bottom line.

MANAGE RISK AGAINST COST

Access control is an investment, so it's important to find a system you can grow into over a long period of time, while balancing the need to keep costs low today. As you weigh priorities and options, remember that modern access control protects more than people and property. It protects brands, too. Given that 81% of a public company's market value is held in intangible reputational factors, preventing security breaches is all the more valuable.

When breaches happen, the cost can be devastating and widespread, encompassing lost data, lost business, lost brand equity, and lost productivity. The cost of a modern PACS is negligible when you consider what a company stands to lose without one.

You've learned how a next-generation PACS reduces risks, so let's move on to how these systems respond when security incidents arise.



$7.91M[1]
Average cost of a data breach (US)
$3.86m (global)

UP TO $5M[2]
Cost to settle a negligent security case

$25-50K
Average cost of enterprise PACS

Sources
1. https://www.forbes.com/sites/niallmccarthy/2018/07/13/the-average-cost-of-a-data-breach-is-highest-in-the-u-s-infographic/#6202ea4b2f37
2. http://www.negligentsecurityattorney.com/verdicts-settlements

STEP #3

RESPOND

Revolutionize how you respond to threats by taking action early to mitigate (and even prevent) incidents with the help of intelligent, actionable, and automated access control.

MODERN ACCESS CONTROL IS ACTIONABLE

When threats become imminent, you need a plan. The next step in future-proofing your access control is developing an efficient incident response procedure for each type of possible security breach. This sounds intimidating, but next-generation access control makes this not just straightforward, but automatic.

A modern PACS can provide actionable, step-by-step guidance to address security incidents, keeping security personnel in control, even when panic sets in.

After taking in the risk reduction and response capabilities of a modern PACS, let's compare a legacy system response and a modern PACS response across two risk scenarios. Then we'll move on to how you can reclaim a sense of control with custom rules and risk profiles.

RISK RESPONSE SCENARIO #1

WHEN AN AREA BECOMES EXPOSED TO TOXIC CHEMICALS

1

In a research lab containing hazardous materials, an employee spills toxic chemicals, setting off a sensor.

RECONASENSE

2

Access for non-essential personnel is automatically revoked, leaving only HazMat certified employees and first responders with access.

3

No one is unnecessarily exposed to toxins and first responders can fluidly and rapidly address the problem.

TRADITIONAL ACCESS CONTROL

2

Anyone with role-based credentials is able to access the lab.

3

Four more staff members enter the exposed area and become ill, making the scene more dire and chaotic for first responders.

RISK RESPONSE SCENARIO #2

WHEN AN ACTIVE SHOOTER ATTACKS YOUR CAMPUS

1

Metal detection alarms sound and gunshot sensors activate as an attacker storms the building.

RECONASENSE

2

Turnstiles and doors automatically lock, while video surveillance is shared with first responders en route.

3

The shooter is confined and apprehended by law enforcement with minimal injury and no loss of life.

TRADITIONAL ACCESS CONTROL

2

The shooter moves freely across the campus with his previously obtained credentials, while first responders cannot access the area or view live surveillance feeds.

3

Several victims are critically wounded and a media firestorm erupts.

STEP #4

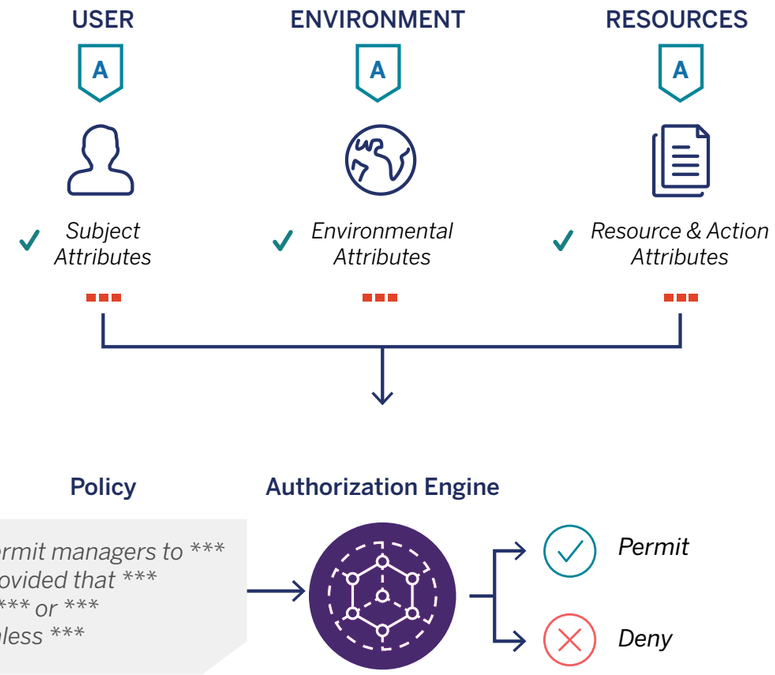
RECLAIM

Find a renewed sense of control and reclaim peace of mind with a PACS you can customize to fit your organization like a glove.

RECLAIMING PEACE OF MIND COMES DOWN TO TRUST

Security professionals carry an immense load on their shoulders, so the PACS they rely on should support them as comprehensively as possible. That's why the fourth step to achieving modern access control is reclaiming peace of mind with a system that can proactively address all key eventualities. The only way to realize complete confidence in your PACS is to build it to fit your organization like a glove.

Next-generation PACS are programmable to integrate custom rules, policies, and risk profiles. Authoring custom If/Then rules empowers you to design a security system that protects your organization best by drilling down on key areas of concern with granular commands and automated responses.



With customizations in place, a modern PACS is like having a sixth sense for security issues. When security managers can fully trust their system to support them, they can address other strategically high value concerns.

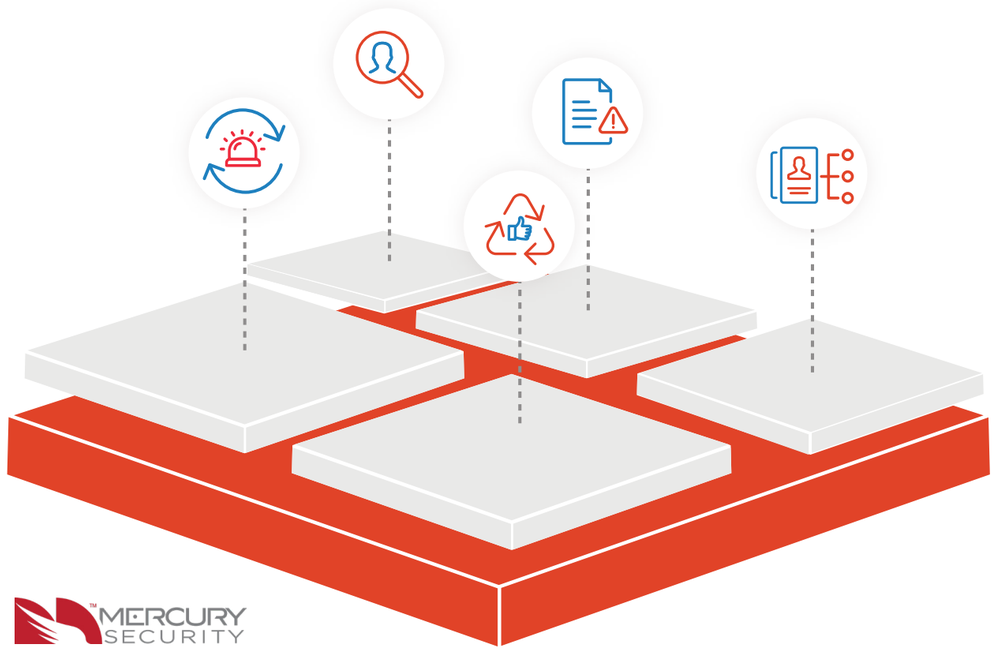
Detailed reports add to the peace of mind a next-generation PACS affords. This feature helps security personnel interface with key internal stakeholders as well as supports efforts around governance and compliance.

Having found full confidence with a modern PACS, let's turn to a topic that may still weigh heavily on your mind: your existing access control solution.

STEP #5

REPURPOSE

For organizations that wish to evolve rather than replace their PACS, there's a path to repurpose existing solutions and still reap next-generation rewards.



THERE'S AN INCREMENTAL WAY

Enterprise migration paths take time. For many, a "rip and replace" approach to achieving modern access control is infeasible. So, the fifth step is considering a hybrid model that harmoniously repurposes existing solutions. A modern PACS should integrate widely to cooperate with existing hardware and security systems. This is a cost-effective way to revolutionize your access control without a full upgrade.

In an environment secured with Mercury controllers, upgrading to intelligent access control can be as easy as a software upgrade with a modern PACS. Even layering on top of a legacy system, you'll reap these benefits:

- Proactive identification of potential threats
- Insider threat detection using access analytics
- Intelligent alarm management for all security technology
- Risk-adaptive security policies and procedures
- Confidence to fully transition to modern risk-adaptive PACS

STEP #6

RECONASENSE

One solution brings together the integrated, proactive, and risk-adaptive benefits discussed in this eBook to deliver next-generation access control.

RECONASENSE

A SOLUTION THAT CHECKS ALL THE BOXES

The final step on your journey to modern access control is requesting a demo of the only PACS that satisfies the next-generation access control checklist. ReconaSense delivers revolutionary access control that seamlessly unifies security data inputs, proactively identifies potential threats, and intelligently mitigates risks. With ReconSense, you can:

Unify Risk Management

Normalize all security data and sensor inputs across your enterprise for proactive safety analysis.

Modernize Access

Ensure safe interactions between people, facilities and assets with risk-adaptive physical access control.

Predict Threats

Get ahead of breaches and attacks before they wreak havoc with predictive insights and actionable guidance.

Improve Compliance

Implement safety policies and enforce procedural compliance with AI-enhanced security controls.

ReconaSense delivers the only intelligent, proactive, and risk-adaptive security platform that seamlessly unifies security data, alerts you to potential threats, and actively mitigates risk.

Let us show you how to make sense of it all with ReconaSense.

REQUEST A DEMO

ABOUT **RECONASENSE**

ReconaSense helps protect people, assets, buildings and cities with its next-gen access control and converged physical security intelligence platform. By leveraging intelligent data, ReconaSense identifies and mitigates potential threats and attacks before they happen, giving security teams the ability to go beyond managing data and individual alerts to achieving true situational awareness and rapid response capabilities.

LEARN MORE AT **WWW.RECONASENSE.COM**

+1 512.220.2010
insider@reconasense.com

RECONASENSE