EBOOK

DISCOVERING A PAINLESS PATH
TO MODERN ACCESS CONTROL

RECONASENSE

TABLE OF CONTENTS

INTRODUCTION

A ROADMAP TO MODERN ACCESS CONTROL

After over a decade of stagnation, the industry of physical access control systems (PACS) is finally transforming. From our digital devices like smart phones and smart home components, to the physical environments we live and work in, security protocols that started as locks and keypads have transformed along with today's technological advancements.

Enterprise organizations continue to face sophisticated threats, from both inside and beyond their facility. For facilities trying to maintain or modernize operations, a migration to a modern PACS may seem daunting and expensive to undertake.

However, a roadmap to modernized access control is not only possible, but cost-effective and intuitive. **This path forward makes it possible to transform dated, legacy products into an access control strategy that is integrated, proactive and dynamic.**

In this eBook, we will explore:

- **Challenges with physical access control systems for today's facilities**
- **What modern access control looks like**
- **How to transition to modern access control without starting from scratch**

THE CHALLENGES WITH PHYSICAL ACCESS CONTROL SYSTEMS FOR TODAY'S FACILITIES

This foundational element on its own poses multiple challenges in evolving your organization's access control policy forward. A majority of today's PACS were built on the foundation of role-based access control. But most vendors stopped there, creating some vulnerabilities in the modern risk environment.

STATIC NATURE OF ROLE-BASED APPROACH

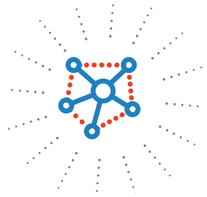
By managing access according to roles or groups, the ability to see access at an individual attribute or activity level is limited. Treating access control as a static whitelist of associations is no longer sufficient for today's dynamic environments. By assuming that all users are the same and that defining their access based upon their role is sufficient, the gap for a security threat becomes far more significant.

SINGLE-FACTOR AUTHORIZATION

Permissions are no longer black and white. Or at least they shouldn't be. Traditional PACS are typically operated with single factor authorization, typically a valid credential is present, and cannot look any further. In complex operations, this increases likelihood of hazards to life safety, and increases the probability of insider threats going undetected.

REACTIVE, BREACH-DRIVEN ALARMS

After the fact is too late. Post-event policy breaches are great for forensic investigations, but insufficient for proactive life safety and security postures. Existing PACS view of threats are static and therefore results in the alert of only known and predetermined threats—after the breach has already occurred. Any potential threats beyond the policies that the organization has defined can easily go unnoticed. These policies pull from a limited set of data, leaving the organization susceptible to increased risk or unrealized security violations.



LIMITED INTEROPERABILITY

Legacy access control systems also have traditionally been created to only have proprietary integration capabilities. This ultimately benefits the PACS and leaves the organization with significant gaps in a holistic security strategy. The lack of integration functionality not only adds considerable cost in requiring the oversight and maintenance of disparate systems, but limits the organization from having a comprehensive security perspective and intelligent access decisions.

Operating on physical role-based access controls alone also draws serious assumptions that can lead to more risk-accepting security protocols. By assuming that all users are the same and that defining their access based upon their role is sufficient, the gap for a security threat becomes far more significant.

So, how do we go beyond legacy approaches to close the gap?

WHAT DOES MODERN ACCESS CONTROL LOOK LIKE?

In order to redefine access control system technology, we must consider the process a revolution rather than an evolution of existing systems. Significant developments in technology, such as advanced architectures and artificial intelligence, have enabled us to secure our organizations more thoroughly than ever before.

There are four key attributes that modern access control systems have that distinctly differentiate them from their legacy counterparts:

1

INSIGHTFUL OPERABILITY

A foundation of increased interoperability presents the opportunity to gain meaningful insights. By seamlessly integrating with other security and non-security technologies, modern access control systems leverage a more complete data set to analyze activities taking place within the organization. By leveraging advanced analytics, data is quickly processed finding unknown risks through anomalous patterns that extend beyond policy-defined activity.

2

RISK-ADAPTIVE CONTROLS

By detecting patterns of unusual activity through the use of intelligent insights, risk can be mitigated in real-time. Attributes such as tardiness, activity time and locations, and even affiliations can all be monitored to identify and alert security teams to potential security risks. This proactive approach defies the abilities of conventional role-based access controls.

3

ENVIRONMENTAL AWARENESS

By assessing the environment for risks, safety can be improved in real-time. Environmental factors such as chemical levels, temperature, asset location, operational status, personnel present, etc. may represent risk to certain individuals at certain times. Permissions can adjust in real-time to assure individuals without the required attributes such as certificates, clearances or assignments don't cause harm to themselves or the operation.

4

ACTIONABLE GUIDANCE

Endless data insights can be overwhelming without a reliable course of action. Dependence on human intervention and legacy analytics can no longer compete at the speed required to make effective security decisions. By utilizing insights, policy-based actions can be triggered immediately without human intervention to boost the overall safety posture of the organization.

The transition from legacy access control to a modern solution can conjure up images of expensive software and time-consuming migrations. **Let's discover what is actually involved in the transition.**

HOW TO TRANSITION TO MODERN ACCESS CONTROL WITHOUT STARTING FROM SCRATCH

By using existing assets within your environment and the adoption of new technology, a transition to modern access control is easier than you think.

USE YOUR EXISTING DATA MODEL

You've worked for years to establish policies, define roles, and beyond. Don't lose the work you've already done. Rather, take it with you and migrate it to a new solution.

LEVERAGE YOUR EXISTING INFRASTRUCTURE

Keep your hardware while keeping up with threats. The fact remains that 90% of infrastructure, such as architecture, card readers, and controllers can still be used when migrating to a new access control system. Even the most complex legacy systems that have difficulty leveraging web services data can be migrated. Rip the term "Rip & Replace" from your vocabulary and advance your security posture with legacy equipment.

DEPLOY NEW ACCESS CONTROL TECHNOLOGY SYSTEMS

Understanding the security problem you're solving for will better enable you to define the needs that a new access control system can bring to your organization's security protocol. Ultimately, modern access control technology allows security teams to further define and reduce risk, better control costs, maintain compliance and improve life safety.

With a roadmap for modern access control success, you need a solution to get you there. **Let's get to know ReconaSense.**

CONCLUSION

PAVING THE WAY FOR NEXT-GENERATION ACCESS CONTROL

The time for intelligent access control is now. By applying an intelligent and responsive approach to access control, similar to other enterprise operations, ReconaSense delivers physical security's first and only risk-adaptive access control solution that ensures consistent and proactive security across the chaos of the modern enterprise.

With ReconaSense, organizations have a PACS with a modern database architecture that supports current and future policies and procedures. Finally, security operations can catch up with modern enterprise applications to improve life safety and mitigate risk with dynamic and intelligent access permissions across facilities.

THE RECONACCESS DIFFERENCE

- Compatibility with Legacy Systems
- Safety-enhanced Controls
- Advanced Threat Detection
- Real-time Intelligence & Analytics

READY TO START DOWN THE PAINLESS PATH TO MODERN ACCESS CONTROL?

Visit www.reconasense.com/getstarted

ABOUT **RECONASENSE**

ReconaSense helps protect people, assets, buildings and cities with its next-gen access control and converged physical security intelligence platform. 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®

©2019 ReconaSense. All rights reserved. ReconaSense and the ReconaSense logo, are registered trademarks or trademarks of Tranquility Ventures or its subsidiaries in the United States and other countries. All other trademarks are the property of their respective owners.