Access Control Integration

Securing the Physical and Digital World

Challenge

Access control systems play a vital role in securing physical spaces and protecting sensitive information. With the advent of cloud computing, a new era of access control integration has emerged, revolutionizing how organizations manage and monitor their security infrastructure. In this blog post, we will explore the benefits of integrating access control systems with Azure Active Directory and other cloud-based network devices.

Overview

- Enhanced Security with Cloud-Based Systems

- Advanced Integration Using Software Architecture

- Ensured Convenient Remote Managment and Monitoring

- Transformed Organizations with Scalable Cloud Solutions

- Provided Peace of Mind with the Pavion Experience

Solutions

Cloud-Based Access Control

Cloud-based access control integrated systems can enhance security, provide remote management capabilities, and facilitate scalability. Integrating access control systems within a single-sign-on (SSO) system architecture such as Azure Active Directory enables organizations to streamline their security protocols. Most security leaders think of SSO as a way to improve user experience; however, SSO also plays a critical role in delivering security for data and applications. By leveraging Azure's robust authentication and authorization capabilities, organizations can ensure that only authorized personnel have access to restricted areas or sensitive data. Active Directory integration allows for seamless user management, making it easier to provision and restrict

access rights across multiple systems. SSO further enhances security by providing a unified authentication experience, reducing the risk of weak passwords or unauthorized access attempts. It essentially replaces multiple usernames and passwords with one set of corporate credentials to access resources securely, ultimately decreasing the chance of a security breach.

Software-Derived Architecture and Cloud-Based Network Devices

One of the key advancements in access control integration is the adoption of a software-derived architecture, particularly with the deployment of cloud-based network devices at entry points. With ongoing work-from-home initiatives, the proliferation of software

as a service (SaaS), and an influx of mobile apps and internet of things (IoT) devices, it's easy to see why cloud computing is considered the "new normal" for today's businesses. Traditionally, access control systems relied on on-premises (on-prem) hardware devices that required manual configuration and maintenance. Most businesses no longer need expensive on-premise (on-prem) application servers to provide essential business applications and software, not to mention, there's the cost of maintaining and upgrading that technology every few years. With cloud-based network devices, organizations can leverage the scalability, flexibility, and remote management capabilities of the cloud. This Managed IT Services approach centralizes access control management, allowing administrators to monitor

and control access to multiple locations from a single interface, regardless of physical proximity. Managed IT services help companies get off the technology life-cycle treadmill and migrate to an integrated suite of platforms based in the cloud. This eliminates time spent on IT support so that companies can focus on what's important.

Remote Management and Monitoring

Cloud-based access control systems also benefit companies by enabling remote management and monitoring, empowering organizations to oversee their security infrastructure from anywhere, at any time. Through a web-based interface or dedicated mobile applications, administrators can grant or revoke access rights, view real-time activity logs, and receive instant notifications of security events. This remote accessibility provides flexibility, convenience, and improved response times, ensuring that security measures can be swiftly implemented in case of an emergency or security breach.

Scalability for Growing Organizations

As organizations expand and undergo changes in their physical infrastructure, scalability becomes a critical

consideration for access control systems. Cloud-based solutions offer unparalleled scalability, allowing organizations to easily accommodate growth or adapt to evolving security requirements. Whether it's adding new doors, integrating additional locations, or scaling up user access, cloud-based access control systems can flexibly adjust to meet the needs of growing organizations without the need for extensive hardware upgrades or complex reconfigurations.

Cloud-based access control integration has transformed how organizations manage and enforce security protocols. By leveraging the power of SSO, and a software-derived architecture, organizations can experience enhanced security, streamlined administration, and the flexibility to scale their access control systems. Embracing cloud-based access control solutions enables remote management, improves scalability, and empowers organizations to proactively

connect and protect their physical spaces and valuable assets while managing an IT infrastructure from the cloud.

Traditional on-prem systems require a network configuration that may heavy, unauthenticated communication over insecure forms of connectivity. This creates a lot of insecure vulnerabilities in a company's network infrastructure. Cloud-based access control systems operate in highly secure data centers, leaving a very small hardware footprint. To stay ahead of the curve, companies should embrace the benefits of cloud computing in access control to reinforce their security infrastructure for a safer, more connected, and more efficient environment.
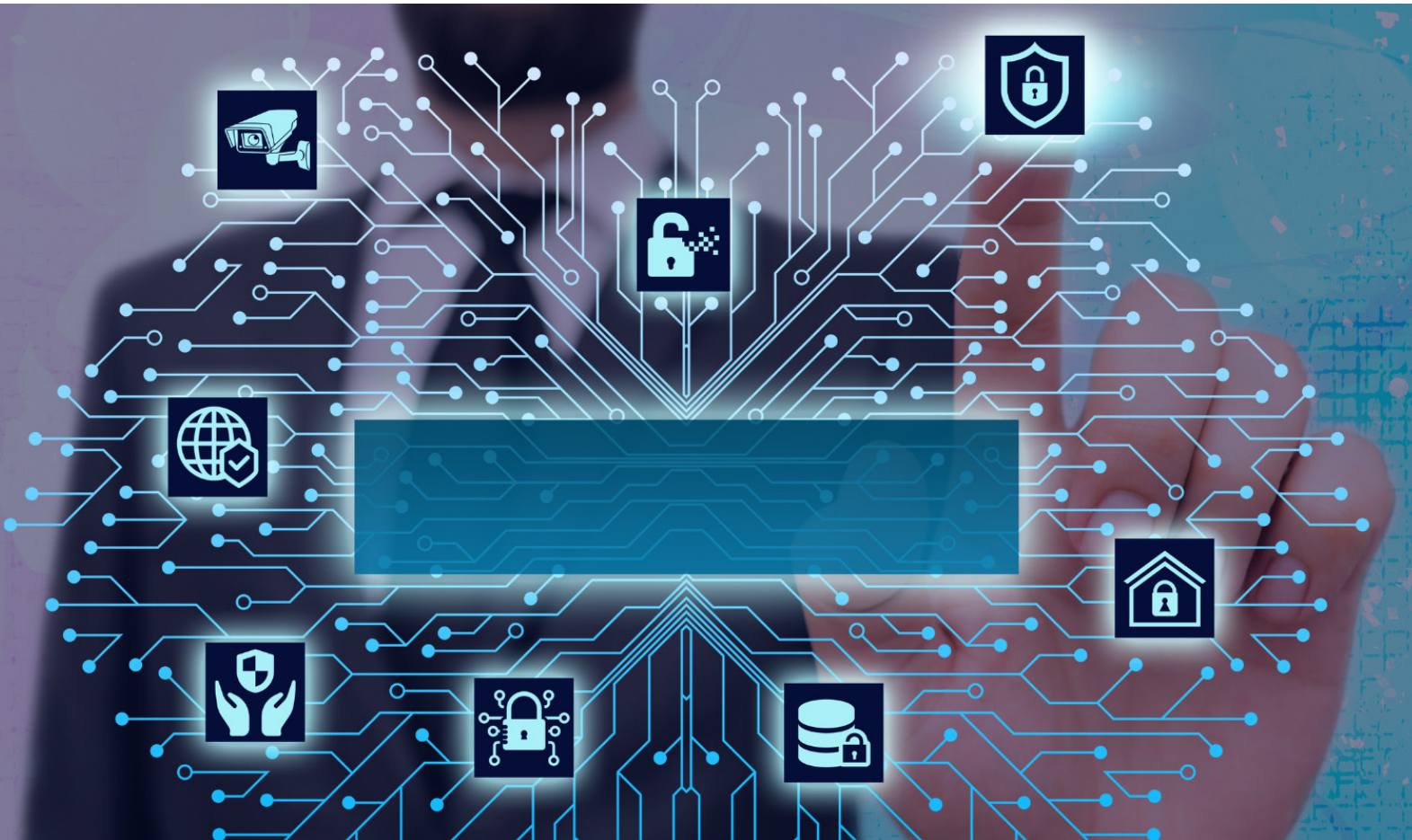
PAVION EXPERIENCE

We've Got You Covered

We call it the Pavion Experience. The lifecycle of services we deliver, from design through ongoing support, that helps keep your fire, security, and integration systems running while saving you time and money.

Pavion brings best-in-class solutions together. Through the entire project lifecycle, we work with our customers to solve their problems and help them overcome their challenges. So no matter your project, we meet your needs with a partner you can trust.

Design

From the initial project kickoff to understanding your requirements, we'll design a solution that meets your needs with clear scope, bill of materials and comprehensive drawings.

Technology & Integration

Once your design is approved, we deliver your technology with first-class implementation, engineering, change management and training.

Service

With your solution fully implemented, Pavion offers multiple service offerings to make sure you get the most out of your Pavion Experience, with the highest level of reliability and customer service offered.

About Pavion

Pavion connects and protects
by providing Fire, Security, and Integration
solutions to customers in 55+ U.S. locations
and 22 countries. The company brings
industry-leading experience to clients in the
enterprise, healthcare, education, government,
data center and retail industries. Its mission
is to bring clarity and transformation to
safety, security, and communication through
technology and radical service.
Learn more at Pavion.com.

Our Industries

We've built solutions for many
different industries, and we're
ready to provide you with
the service and solutions you
need to connect and protect
what's important.

Healthcare
Tech/Data Center
Property Management
Financial
Retail
Education
Distribution & Storage
Govt & Defense

PAVION™
CONNECT AND PROTECT

pavion.com
SCAN ME

SDM
SYSTEMS INTEGRATOR 2022 OF THE YEAR

scn TOP 50 SYSTEMS INTEGRATORS