

A Single Pane of Glass: Why Centralized Security is Necessary


Physical security is the barrier separating the outside world from your most valuable assets. From enterprises and commercial real estate buildings to schools and hospitals, they all depend on the cameras and notifications, software and hardware solutions that make up physical security. But a seismic shift, a transformation of sorts, is happening, and this metamorphosis is increasing efficiency, strengthening security and driving IT and security teams to reevaluate how they manage their systems.


In this whitepaper, we will explore how security is evolving, how you can centralize your systems behind a single pane of glass and why so many are embracing the shift in security.


WHAT IS PHYSICAL SECURITY AND WHY IS IT ESSENTIAL?


Physical security is comprised of the various techniques and technologies that keep property, people and assets safe. The techniques and technology vary depending on user requirements (government facilities require greater safeguards compared to an average small business). One of the first forms of physical security that might come to mind is the metal key and lock. Though some residential security systems still use these, nowadays, commercial buildings rely on card reader systems, biometrics and/or keypads. Proximity door readers unlocked by key card or smartphone are most commonly used.


But the scope of technology goes far beyond locks and keys, parking gates and metal detectors. Today, some of the most important technologies involve computer software. Commercial real estate firms, enterprises, schools, hospitals and more have integrated their hardware with software platforms used to collect data about door use, monitor access points and make sure only the people who need access to a facility have it. As you can imagine, these systems come in many types, including:

 **Door access control** - restricts or allows access to a physical space using authentication methods such as keycards, codes or biometric identifiers.

 **Video management** - is the recording and storing of video footage captured by surveillance cameras for security, monitoring or other purposes.

 **Identity management** - the process of authenticating, authorizing and managing digital identities and access privileges of users within an organization.

 **Communication/Notification** - receive instant alerts and send messages to colleagues.

 **Visitor management** - register, track and manage guest access to a facility to enhance security, safety and improve the overall visitor experience.

Today, with a greater variety of risks threatening the workplace, those responsible for physical security depend on multiple systems to provide well-rounded, multipoint security. However, the greater number of systems one uses, the more time and attention required – which brings us to the problem facing many security and IT professionals.

THE PROBLEM WITH PHYSICAL SECURITY

With so many security solutions available, teams must divide their time – managing multiple systems on a daily basis. For example, identity management systems -- like Okta and Azure AD – help organizations keep track of their employees' information (e.g., name, phone number, etc.). However, often IT and security teams end up inputting data like this into other systems, leading to unnecessary redundancies. With more redundancies come more opportunities for information to be misplaced, hacked or intercepted.

Sage Realty, a commercial real estate firm in New York, NY, experienced these redundancies firsthand. The CRE company had difficulties maintaining and organizing user credentials stored within their on-premises access control system. Sage's director of tenant experience described the Lenel S2 system as “fragmented” and “siloeed.” Consequently, their database contained many duplicate users, and in some cases, a single user's credentials appeared in the system as many as four times. Sage chose to replace the on-prem system with cloud-based access control. The new system streamlined the process of adding and removing credentialed users, allowing the CRE firm to clean up their database.

“The workflow for adding a new [user] is a massive improvement over the way we would do things with our old legacy system,” said Alec Fomin, director of tenant experience at Sage, about cloud access control.

But is transforming your security really as simple as migrating to the cloud? For the answer, let's take a step outside of the security industry and journey back to the 1980s.



THE SOLUTION TO DISPARATE SYSTEMS

The year was 1983. Mr. Roboto spilled over the radio waves, the VHS had taken over store shelves and off-the-shoulder sweatshirts were a thing. But at the time, an even greater, though less pronounced, cultural change had begun. On January 1, 1983, the United States Department of Defense released ARPANET, a technology now considered to be the precursor to the modern Internet. As we know, the internet has become a repository for everything from '80s hits to shopping for retro fashion. In effect, the internet created a single, centralized marketplace.

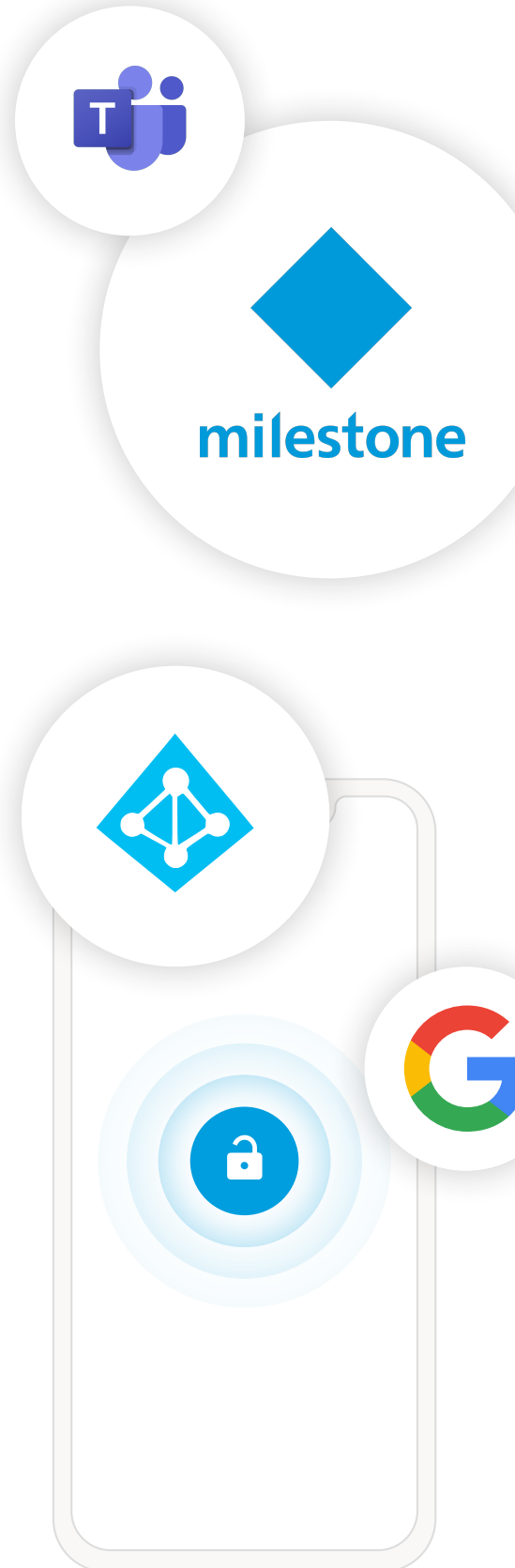
As it relates to security, the cloud is a similarly transformative power. It has the power to connect a wide variety of systems into one solution. For example, instead of managing information in both Azure AD and an access control platform, the same information sync in each.

Whether syncing video cameras to door access control or parking security platforms to visitor management software, the cloud makes it exponentially easier and faster to connect and operate security from a single pane of glass. Through the cloud, IT and security teams can create one interconnected security solution.

HOW DOES CENTRALIZED SECURITY WORK?

By now the benefits of connecting otherwise isolated software and hardware are probably pretty clear. Enterprises and organizations save time and operate more efficiently with the cloud. But what might not be as clear is how connecting these systems happens or why creating a centralized solution is so much easier with the cloud.

The answer comes down to integrations. Integrations allow IT and security teams to essentially patch their systems together. With traditional access control, integrations would take a long time to develop and deploy. However, cloud-based systems are ready for use immediately when a system gets installed. Unlike on-premises systems, cloud-based access control often comes with dozens of integrations ready for use. All administrators need to do is navigate to an integrations page within their access control software, click on the integration they want and enter an API key – a string of numbers and letters – to connect their systems. It's that simple.



HOW COMPANIES ARE BENEFITING FROM CENTRALIZED SECURITY

The enterprise, Pepsi G&J -- a production, bottling, marketing and distribution branch of Pepsi-Cola -- has already centralized their security with the cloud. To keep their security consistent across each of 13 locations, the enterprise uses the cloud to connect Genea Security and Azure Active Directory -- an identity management platform. Like Sage Realty, Pepsi G&J has eliminated duplicate credentials. However, they have taken their security a step further by integrating. Whenever an employee leaves the company and they are removed from Azure AD, the employee's badge credentials will also terminate.

"Now when we disable your user account, your physical access is disabled as well," said Hannah Holscher, Digital Technology Support Administrator at G&J. "It [used to take] HR five minutes to log in, type in somebody's name, the location they're in and add the badge. When we've got ten or fifteen people starting each week, that's about an hour a week we're saving [HR]. That's 60 hours a year we're saving just in badge creation."

The enterprise also decided to integrate their access control and Cisco Meraki video management platforms. When a door is opened, G&J Pepsi can pull up the corresponding, live video feed.

"If there's a question about somebody badging into a food sensitive area, we can just click on a link within the Genea portal and see if it's a problem," Holscher said. "Those value-added aspects where you can tie in a system like Meraki are incredibly important."

CENTRALIZING YOUR SECURITY

With an increasing variety of technology in the workplace, companies must juggle multiple hardware and software solutions. This leads to redundancies and inconsistencies in data management. The solution is an interconnected security system that can be managed from a single pane of glass. By centralizing your security through cloud-based access control, you can improve efficiency, reduce redundancies and enhance your overall security.



Interested in learning more about Genea's Cloud-based Security Software? Visit www.getgenea.com.