Get Back to Business with Confidence

How to fully leverage your security platform when you return to the office, classroom, or local business

As organizations begin to transition more of their workforce back to the office, security practitioners are wrestling with new challenges and questions:

1. What do full scale operations look like going forward?
2. How do we get there safely?
3. Will this be affordable?
4. Are there new best practices that do not disproportionately inconvenience our staff, customers, or visitors?

Many of the adjustments you'll face will be guided by variables such as your environment, risk tolerance, and regulatory compliance requirements imposed by outside agencies. In any case, whether you are a Fortune 500 organization with a global footprint, a local boutique business, school, religious organization, or health club, your future operations will likely look much different than a year ago.

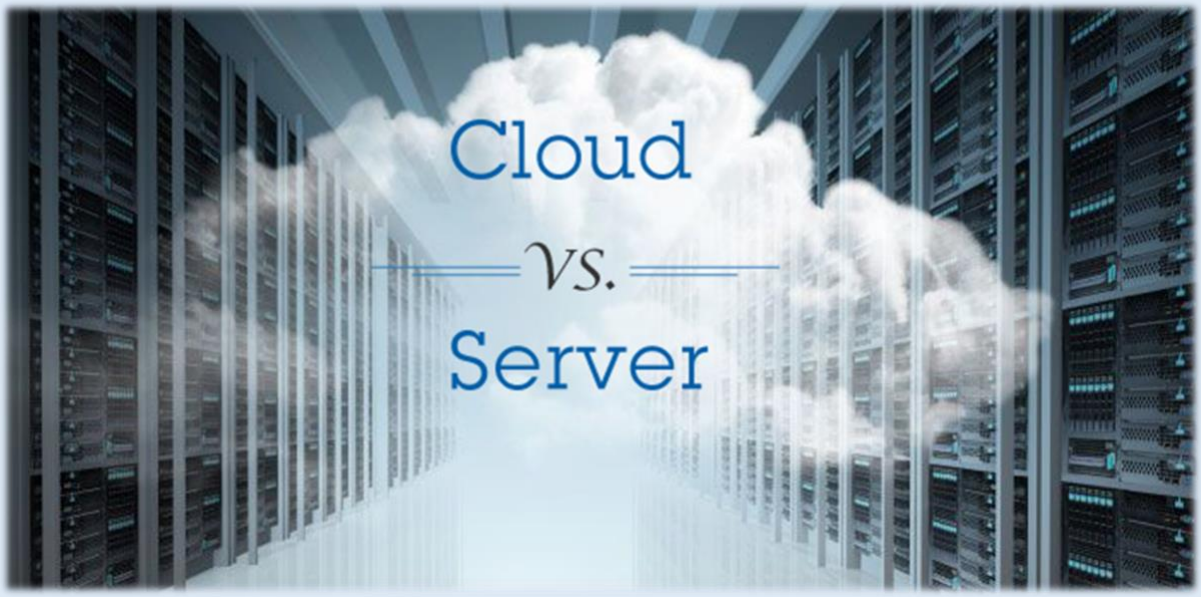
Feenics has been leading the security innovation charge since 2011… from being one of the first manufacturers to bring cloud-based access control solutions to the market, to our Access Control as a Service (ACaaS) delivery model, and even to our decision to host on Amazon Web Services (AWS).

And as we continue to navigate the current environment, we stay committed in making sure our ***Keep by Feenics*** flagship access control as a service platform can help get us all back to business!

With that, let's explore some security & operational elements that can best prepare you for the future.

Cloud-Based Security

A fundamental category battle is occurring between legacy client-server security systems and forward-looking cloud-based solutions. While many business systems are already in the cloud (banking, CRM, web hosting, and productivity tools like Office, Slack, and Asana), security as is often the case, has lagged behind due to many unfounded concerns/myths.



However, the pandemic has brought areas into focus where cloud-based security shines in comparison to legacy client server systems… including reliability and uptime, serviceability, ease of use, adaptability, deployment flexibility and daily operation. In short order, cloud-based solutions have risen from "nice to have" to "absolute must have" and the category now appears ready to tip in favor of the cloud, while client server goes the way of MS-DOS, Bear Stearns, and the VHS player.

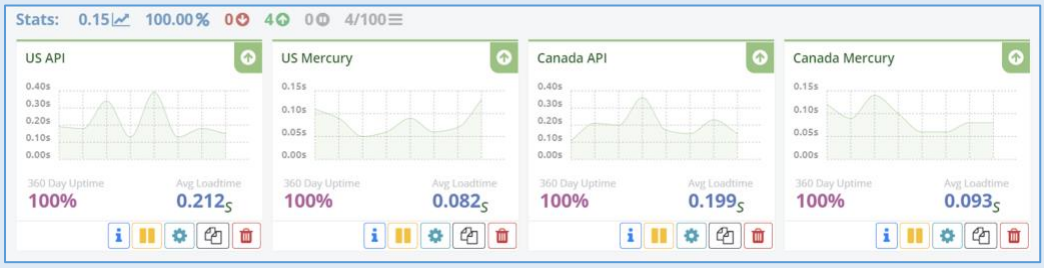
Here are a few benefits that cloud-based solutions offer to maximize your security operations:

1. **Hands off, hassle free maintenance:** Perhaps the greatest benefit a cloud-based solution offers is that the backend architecture is entirely maintained by the manufacturer. There are no operating systems or databases to purchase, install, or maintain; no patches to apply; and product updates are applied with zero system downtime… allowing security practitioners more time to focus on what they do best.

2. **Manage from anywhere there is an internet connection:** With cloud-based systems, you can manage and monitor your system from virtually anywhere. 100% of your security operations can be run from your office, your home, or anywhere in between using a web client, lightweight Win app, or iOS/Android mobile app. You can remotely unlock a door, monitor alarm activity, change door schedules to allow for deliveries, and run reports… whenever and wherever you are located.

3. **Security:** Certain individuals believe their security data is safer locked in an IT closet, but the opposite could not be more true. On-prem IT personnel are typically not dedicated to security, could get distracted by other tasks, and are not solely focused on protecting your network. Conversely, hosting platforms such as AWS spend millions of dollars to ensure the security and integrity of their infrastructure. Their datacenter employees are there solely to protect your data. In addition, they employ top tier cyber-hardening experts tasked with staying current with emerging vulnerabilities. Thus, cloud-based solutions enjoy the best of both worlds… protection through their native security implementations plus the additional layers of security inherent with hosting providers.

4. **Always-on:** Properly architected cloud-based systems offer near 100% system uptime, even during system upgrades and maintenance. The chart below illustrates uptime data from Keep, our flagship Access Control as a Service platform.

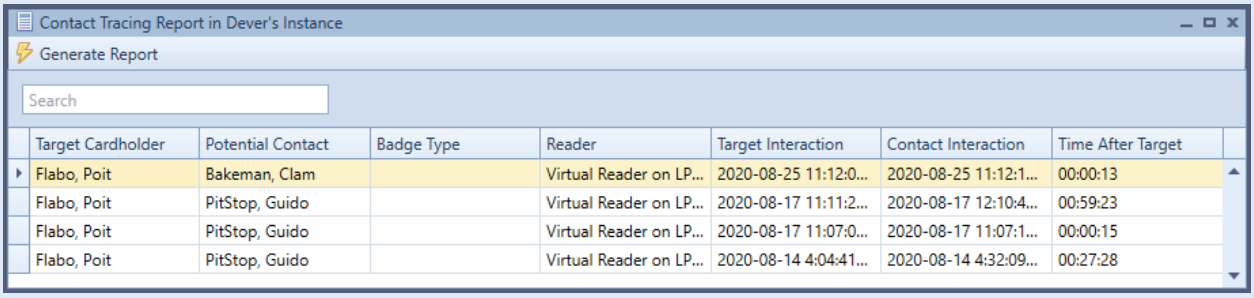


5. **Regular feature updates:** Native cloud systems can push feature updates at a pace not feasible by its client-server counterparts. Lightweight cloud architectures allow for frequent updates that keep the product fresh, feature rich, and current with the latest technology and security standards.

6. **Ultimate scalability:** Cloud solutions scale with ease. Updating licenses is accomplished in real time from the app's license manager. In the unfortunate scenario that requires you to scale back operations, licenses can be downgraded for the amount of time you aren't using a facility.

User Contact Tracing and Reporting

Tracking the potential spread of infectious diseases to minimize exposure will continue to be a requirement for many organizations. **People Proximity Reports,** like the ones offered by Keep, allow you to identify individuals who may have come in contact with someone with a known or potential exposure. You can determine who may have been in the same area (during specified time periods) as an exposed individual. You can then proactively inform your staff to take proper precautions. Based on the movement of an exposed individual, filters can be applied on individual rooms, areas, or time frames.



Target Cardholder	Potential Contact	Badge Type	Reader	Target Interaction	Contact Interaction	Time After Target
Flabo, Poit	Bakeman, Clam		Virtual Reader on LP...	2020-08-25 11:12:0...	2020-08-25 11:12:1...	00:00:13
Flabo, Poit	PitStop, Guido		Virtual Reader on LP...	2020-08-17 11:11:2...	2020-08-17 12:10:4...	00:59:23
Flabo, Poit	PitStop, Guido		Virtual Reader on LP...	2020-08-17 11:07:0...	2020-08-17 11:07:1...	00:00:15
Flabo, Poit	PitStop, Guido		Virtual Reader on LP...	2020-08-14 4:04:41...	2020-08-14 4:32:09...	00:27:28

Occupancy Controls

Occupancy controls are one way to help enforce physical distancing requirements, capacity constraints and other regulatory compliance mandates. Options include:

1. **Occupancy count via anti-passback:** This function leverages “in” and “out” readers. It allows you to define the maximum number of people permitted in defined areas. Real time dashboards and reports show both the current occupancy count and identity of the occupying individuals. Real time alerts can be configured to notify managers when an area has reached capacity.

2. **Reconfigure access privileges:** Cloud-based systems allow the ability to easily reconfigure access privileges, from anywhere, to minimize traffic within a building or common area. Privileges could be segmented by time of the day (shifts) or days of the week.

3. **Reroute traffic from high density areas:** Re-routing traffic is another way to control occupancy. For example, specifying different entrance points for different groups allows you to effectively control the flow of people. Visitors could have even greater restrictions placed on their movement.

4. **People counters:** Organizations can leverage people counting technology such as physical counting sensors placed around doors and/or through video analytic people counting software.

Suspend Access Rights of Suspected, Exposed, and Close Contact Individuals

Cloud-based systems like Keep allow you to suspend access privileges for exposed credential holders and/or those deemed at risk based on a People Proximity report. Additionally, an integrated video management system can be leveraged to verify a person's presence in an area by reviewing associated video for the reader(s) in question.

Once an individual is deemed safe to return, their access rights can be easily restored.

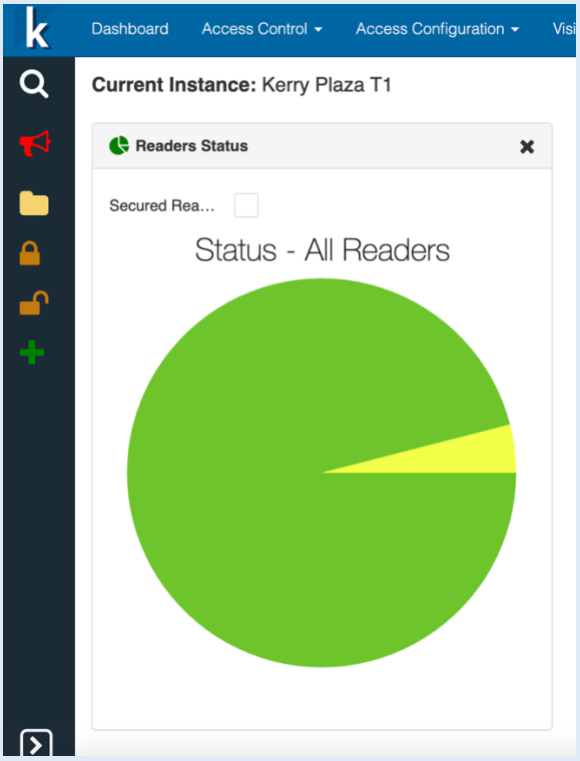
Wellness Attestation

Electronic attestation survey completion can be required prior entering a facility. Wellness forms can be required daily, and attestations can be stored in the system's audit logs. For additional protection, credentials can be deactivated nightly and reactivated the next day after a wellness attestation has been completed.

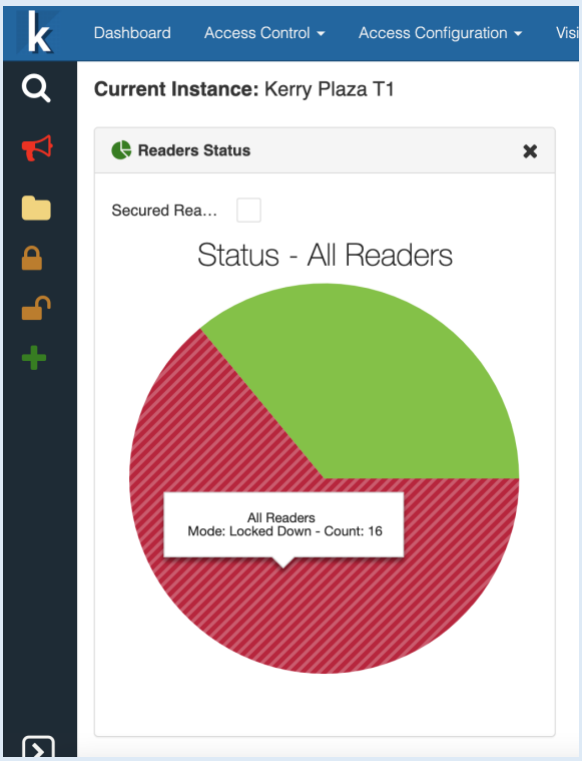
Efficient Lockdown Functionality

Immediate lockdown capabilities of potentially contaminated areas are central to an effective containment strategy. Once an exposed area is identified, you can efficiently lock it down using a mobile app, web client, or Win App.

Prior to Area Lockdown



Post Area Lockdown



Remotely Onboard New Employees

A popular benefit of cloud-based access control systems, such as Keep, is the ability to remotely onboard new employees. Core employee information can be imported via an HR system, photos can be captured using hi-res mobile phone cameras, and access rights can be assigned from a home office. Mobile credentials can even be issued in lieu of traditional badges.

Touchless Access Control

Touchless access control is becoming increasingly popular for organizations looking to minimize contact surfaces and other common touchpoints. For this, two options to consider are Mobile Credentials and Touchless Entry Points:

1. **Mobile Credentials:** Mobile credentials streamline efficiencies from issuance to usage at the door and offer numerous benefits over their physical credential counterparts:
    a. Virtually no one forgets their phone, thereby greatly reducing the number of times someone needs assistance to enter the building.
    b. Nobody goes “days” without noticing they lost their phone, thereby minimizing the time their credential could be compromised.
    c. Unlike a physical credential, lending someone their phone to gain unauthorized access is highly unlikely.
    d. Access to entry points is more convenient.
    e. Mobile credentials are more secure, particularly when paired with a phone’s multi-factor authentication.
2. **Touchless Entry Points:** All the advanced safety protocols in the world will be in vain if everyone flows through a single door, each touching the handles and crash bars as the enter/exit. Designing high traffic entry/exit points for minimal contact requires outfitting them with automatic door openers, PIR sensors and touchless request to exits.

Temperature Monitoring / Fever Detection

For certain organizations, temperature monitoring technology is an important component of their security tech stack in order to create a “first line of defense” at the door. Options are available using biometrics (leveraging facial recognition), video management systems (using thermal camera analytics), and traditional temporal scanning devices. In an integrated scenario, solutions like Keep can enforce entry policies based on temperature readings. Each solution offers a unique set of pros/cons that should be carefully vetted to ensure the validity of accuracy claims.

Bear in mind that temperature detection is an emerging technology (particularly thermal cameras) and has valid accuracy concerns (readings in non-controlled environments), reliability issues (inability to detect asymptomatic people) and privacy issues (particularly in regard to HIPPA compliance). Be sure to consult your legal team and local regulatory agencies before deploying these solutions.

Visitor Management

Visitor Management adds a critical layer of protection to a comprehensive security operation.

Here are a few considerations to help you maximize your environment, whether you choose to utilize Keep's native Visitor Management module or one of the many 3rd party Visitor Management systems integrated into the Keep ecosystem:

1. **Touchless Check-in:** Visitor check-in using mobile phones eliminates the need to interact with self-service kiosks or receptionists. With proper setup, visitors can self check-in, e-sign required attestation questionnaires or consent forms and use their mobile credential to access secure areas.

2. **Wellness Attestation:** Electronic wellness attestation or other consent forms can be required prior to check-in with results stored in the system's audit logs. Visitor access can be deactivated nightly and reactivated the next time attestation or consent forms are completed.

3. **Temperature Checks:** Temperature readings can be recorded as part of the check-in process. A visitor with an elevated temperature can be denied access with alerts sent to proper authorities.

4. **Visitor Tracking and Reporting:** All visitor activity is stored in system audit logs. As such, visitors can be included in People Proximity reports if exposure to/from a visitor is suspected.

Bringing it All Together

Ensuring your facilities, schools, medical offices, etc. are safe to occupy requires a new way of thinking. Taking the necessary steps today can also prepare you for tomorrow's challenges.

It's become increasingly clear that cloud-based technologies are best suited for tackling our latest challenges. With a properly architected ACaaS platform, you can manage your security system from your home office, your work office, or company command center (without loss of functionality or degradation of security).

And while the many themes covered in this paper will help to get our organizations on the right path, we must not become complacent. As we look to the future, new technologies will emerge to help tackle ever-evolving challenges. Technologies including, but not limited to:

1. Machine Learning and Predictive Analytics
2. Beacon and GPS sensing technologies
3. Health focused IoT devices (Apple Watch, Oura Ring, Whoop Strap)
4. Continued evolution of Responsive Environments and Intelligent Workspaces

We'll need to explore what roles these and other technologies will play and how they can be leveraged to keep us, and our buildings, safe long after we return to work in full force.