Five cloud-based physical security measures for healthcare organizations

Steve Van Till

New tools such as cloud-based access control have created new opportunities for changing the way that electronic security systems can interact, according to the author. He describes how such software has made it easier and less costly for health systems to cope with change and how IT and physical security can work together in this critical area.

(Steve Van Till is the Founder, President and CEO of Brivo, a global leader in cloud-based physical access control and Software-as-a-Service solutions. He has previously served in a variety of senior management roles in high technology companies spanning Web development, healthcare, and satellite communications. A Board Member of the Security Industry Association, he been selected by Security Magazine as one of "The Top 25 Most Influential People in the Security Industry.")

Modern healthcare organizations are challenged like never before to manage physical security across large campuses, multi-location regional healthcare networks, and affiliated labs and clinical settings. Any one of these contexts presents a large set of challenges, but taken together they often test the limits of conventional physical access control systems. Add to this the torrent of change from the rise in merger and acquisition activity, and you have a perfect recipe for gaps in physical security.

Modern cloud-based Software as a Service (SaaS) platforms and mobile applications have made it much easier for organizations to cope with change regardless of which IT functions are affected by removing the physical data center and local server from the equation. But how do these cloud platforms apply to the fundamentals of security? Do the same

benefits apply?

1. PREVENT

Prevention is always job one in physical security. In the case of access control, this starts with ensuring that locked doors are locked, and that only authorized personnel can gain entry. Surprisingly, however, we find that many organizations struggle with this most fundamental of security principles. One of the primary culprits in rapidly changing multi-location institutions is synchronization of user database across disparate security systems. This is a common side-effect of acquisition, growth into new territories, or the addition of new types of clinical services that take place at distinct facilities.

Cloud-based systems are, by their very nature, location-independent, which facilitates centralized control and supervision. Adding access control protection to entry points miles or even half a continent away is the same as adding new controls in your primary facilities. Monitoring responsibilities can be easily shared between local security personnel and a central SOC. Multiple logins to a cloud solution with fine-grained permissions management allows the balance of local and central management to be tuned to an organization's needs.

At the budgetary level, the fact that cloud systems are typically priced on a per-door per-month basis means that there are fewer "surprises" than with a large per-location or per-server licensing fees.

2. PROTECT

Protection takes on many forms in electronic security. Access control is fundamental, but it usually is not sufficient to stand alone. Most of the other disciplines in physical security--video, alarms, mass notifications, compliance monitoring--have all seen movement toward the cloud as well. What this does for security organizations is to create additional partnerships between cloud companies--so called cloud-to-cloud integration between vendors allows them to integrate their systems once and for all, rather than as a unique, one-off solution that your organization has to pay for and maintain.

The integration of multiple security functions in a single platform, or a group of cloud-

connected platforms, provides tremendous protective leverage for security departments. In the context of multi-site organizations, these alliances provide the same benefits to the security organization that we see with cloud-based solutions now becoming widespread on the clinical and financial sides of the organization.

3. DETECT

Detection systems are only as good as their ability to deliver the right information to the right person(s) at the right time. This is another area where cloud-based systems excel across distributed organizations, such as today's healthcare landscape. Cloud or SaaS applications are distance and location independent, and they are the natural platform to serve as a back end to mobile applications. In fact, it's a safe bet that that every non-corporate application on your mobile phone is cloud-backed, and that the remainder are quickly migrating.

With security becoming as mobile as any other information-intensive discipline in a healthcare organization, the ability to easily deploy mobile solutions is essential. That's why the combination of cloud and mobility are the logical conclusion to crafting and effective detection--and notification--infrastructure.

4. MONITOR

Now that we've covered delivering the right message to the right person at the right time, what's next? Ongoing monitoring is often required for incidents that unfold over longer periods of time. Collaboration among the multiple parties that may be part of a response team is often one of the most challenging aspects of incident response.

Here again, if we look to the effectiveness of cloud-based collaboration versus nearly anything else, cloud is miles ahead. Slack has become a runaway success based on simple collaboration across workgroups, but there are many other cloud-based contenders in this space who are all leveraging the same fundamental cloud characteristics of being able to communicate to all the right people at all the right time. Tools of this sort make monitoring far more effective when multiple parts of the organization must all participate in real time.

5. RESPOND

Effective response is highly dependent on the type of security incident being managed. At the systems level, it must often also tie into other IT functions or systems used by department outside of security, such as personnel. For many generations of information technology, it has been a challenge to create these links unless the two vendors had a partnership between them and offered it as a product option.

Cloud application providers, however, have made it standard to include open APIs (Application Programming Interfaces) as a core part of their products. They have become as standard to cloud products, as electric windows are cars. They are no longer an option, but rather just "the way things are done". The benefit to security organizations is that these APIs make it much easier for your own IT department or a 3rd party integrator to build out the connectivity your organization needs.

CONCLUSION

The fundamental challenges of providing effective security have not changed greatly since the dawn of security. What has changed are the tools we can use to accomplish our mission. New tools such as cloud-based access control have created new opportunities for changing the way that electronic security systems can interact, and the ways we can use them across our growing multi-location security responsibilities.