



Brivo Systems is a 10-year-old SaaS company providing trusted physical security and surveillance solutions to customers in industries ranging from retail to property management to federal, state, and local government. As such, the company operates at the intersection of three major trends within the cloud landscape: identity management, Internet of Things (IoT), and security. With increasing enterprise cloud acceptance and a strong federal drive for identity and access management, the company has enjoyed compound device, identity, and subscriber growth rates in excess of 35% annually.

*What sort of growth do you expect within the industry?*

Based on the increasing customer demand we've witnessed over the past several business cycles, we anticipate that growth rates of 30-40% are sustainable for at least the next three years, if not well into the five-year timeframe. Major drivers in our sector include: heightened concerns with security and terrorism; compliance-driven access control and data retention requirements; federal mandates for strong identity management and FIPS 201 compliance; and growing levels of buyer comfort with "the SaaS security question".

Generalizing on our own adoption trends over the three-plus year horizon, we see stronger drivers for the entire class of IoT applications. These are clearly enabled by more and better wireless technologies for connecting physical devices to web services such as our own Security

Management System (SMS), as well as reduced costs for wired solutions using POE. While the inescapably physical nature of physical security has long kept this market on electrical tethers, new products are freeing end users with low-power or network-powered devices, local and wide area wireless offerings, and the location independence that all SaaS backbones provide. The broad reach of SaaS has made it a favorite over traditional customer premise solutions for enterprises with far-flung assets requiring protection or monitoring.

*How does identity management play into this picture?*

We see the increasing 'democratization' of strong (or at least strong-er) identity tools as a driver for our own segment of the physical security sector as well as SaaS in general. With better tokens, widespread PKI, and better management tools, more value can be placed under the purview of automated security systems, with less reliance on expensive labor. We've witnessed this extensive growth as nearly three million identities have come under our own management for purposes as diverse as access to healthcare facilities, compliance testing, membership management, and federal facility protection.

*Are there other SaaS services being used in security?*

Yes, we could hardly do justice to the physical security market for SaaS without addressing the astounding growth in new entrants to hosted and managed video surveillance. While less celebrated than consumer-facing video success stories like YouTube, the transformation of the security video market from an industry of (literally) closeted, independent digital video recorders to one of centralized, networked storage is a watershed event, both in bandwidth and potential earnings as we follow Great Britain and others into the "surveillance society" era. In raw numbers, where there were only a handful of players as recently as two years ago, there are now upwards of 25 players offering SaaS solutions for physical security in the US alone, and a hundred more globally.

*What about the SaaS security question? This would seem especially relevant to your customers.*

Right, we cannot provide a proper outlook without addressing "the SaaS security question" that has haunted providers of all stripes since the inception of outsourced services. Having

launched our SaaS security offering in 2002, well before the current cloud explosion, Brivo witnessed dramatically changing customer attitudes over this eight year period. We have observed growing buyer awareness that, as a practical necessity, data security often must be evaluated on a comparative rather than absolute basis. That's not to say there aren't minimum thresholds that every system must meet. Rather, it's to point out a heightened customer understanding that things aren't always rosy on the *inside* of their own firewalls, and that outsourced providers with dedicated security specialists will consistently outperform multi-tasked in-house IT generalists. That this attitude is now prevalent in the federal sector-underscored by Vivek Kundra's recently sanctioned "cloud first" policy-illustrates how far we have come and is a triumph few would have expected when everyone was convinced that the federal government would never compute outside its own firewalls.

*This interview was published in SIIA's [Vision from the Top](#) , a Software Division publication released at [All About the Cloud](#) 2011.*