Next-Gen access management

Five steps to close the gap in enterprise security with identity-based technologies

This is a pivotal moment for enterprise security

As building and business systems become increasingly networked, organizations are better positioned than ever to make use of that connectedness to deliver smarter, safer workplaces. And as they look for ways to take maximum advantage of the opportunities, a growing number of companies are turning to identity-based technologies.

Johnson Controls

Maximize the benefits of identity-based access controls

Identity-based technologies such as mobile credentialing, biometrics and wearables can help close existing security gaps through efficient access control and by offering unprecedented visibility into who's in the building and where. Yet these technologies also have the potential to introduce new vulnerabilities. Every device that's connected wirelessly within the workplace creates another point of access to the company's network. And therein lays the challenge for most organizations: How to take advantage of these security-strengthening technologies without inviting unnecessary risk that could lead to a security breach.

By properly evaluating security needs, evaluating potential weaknesses and focusing on clear goals, security teams can take effective steps to minimize the risk and maximize the benefits of implementing identity-based access controls.

Step 1: Consider how emerging technologies may fit into your security road map

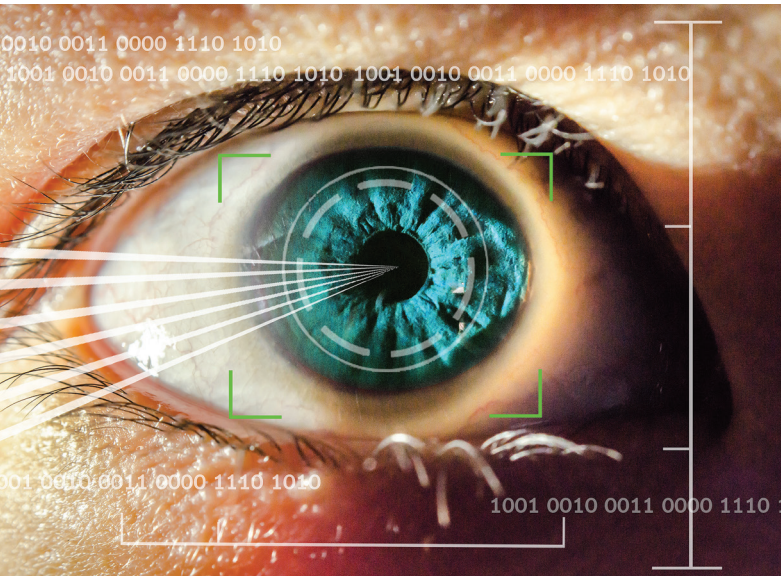
Mobile Credentialing

Everyone's got a handheld device these days and increasingly, people expect to run their lives through their smart phone. Mobile credentialing takes advantage of this new normal by replacing traditional access badges with virtual badges downloaded to a phone.

Because mobile credentialing mimics the personal experiences people already have with technology, virtual badges offer a familiar and convenient way for employees and guests to get in and out of a building with minimal disruption. Virtual badges can also be designed to track the movement of people within a building, alerting security teams to unusual activity or allowing them to more effectively respond in an emergency. For example, if high winds knocked out power to one section of a building (or to one building on campus), a text message could be sent to all badge holders who happened to be in that area at that moment, delivering specific instructions to their smart phones for the safest evacuation route.

There are inherent limitations and challenges with mobile credentialing, however, largely tied to policy and process. Organizations must determine whether they will provide corporate-issued phones to all employees; whether they will issue mobile credentials on an employee's personal

phone; and if so, how they will efficiently handle software issues like operating system incompatibility or the need to deploy upgrades. Because it takes time for these policies and processes to be developed and take hold, mobile credentialing – while growing at a steady pace[1] – is not expected to completely replace traditional badging for the foreseeable future.



Biometrics

Biometrics technologies, such as fingerprint readers and iris scanners, are typically used to strengthen authentication in high-risk areas of the building such as the IT data center, the manufacturing floor or the research and development laboratory. The more critical the asset (or the more severe the consequence if there is a security breach) the more value a layer of biometric security can provide.

The primary challenge with biometrics is this: Most organizations want to make it easy for people to move around quickly and with the least amount of interference possible. Adding layers of security slows things down. How much more time will it take for the user to be scanned and authenticated? Organizations must consider the tradeoffs when evaluating whether to deploy a secondary authentication tool.

Wearables

Wearable technology represents the next stage in the evolution of identity-based access controls. Wearables such as wristbands and watches are already being offered as part of corporate wellness programs by nearly half (46%) of the employers who responded to a 2016 survey.[2] It's no surprise that organizations are increasingly looking to take advantage of these lightweight, inexpensive, frictionless tools to enhance security.

The possibilities are endless: A wristband, pin or pendant could be programmed to grant access to parking, unlock a door, log into a PC, access a printer or use a cashless vending system in a cafeteria. Wearables have the potential to streamline the entire employee experience, creating efficiencies while seamlessly enhancing security.

Step 2: Assess your organization's risk

If mobile credentialing, biometrics or wearables will be deployed, the strategy should also include a plan to minimize the potential risks that accompany these technologies. A single cyber security breach can have devastating consequences, especially when company and customer data is compromised. Businesses lose money. Stock prices suffer. Brand reputations can be irreparably harmed. No organization wants to be the next Wall Street Journal headline.

So with a sense of what's possible through the use of these technologies, take a step back and thoroughly assess security gaps in the existing workspace. Consider bringing in third-party experts who can identify vulnerabilities, help prioritize the risks, and develop a strategy to address them, which may include the use of identity-based technologies.

[1] http://www.marketsandmarkets.com/PressReleases/mobile-user-authentication.asp

[2] http://hero-health.org/wp-content/uploads/2015/06/HERO-Wearables-in-Wellness-Report-Exec-Summary-FINAL1.pdf

Step 3: Get stakeholder buy-in

It takes a team of advocates to make the transition from traditional to identity-based access controls.

- ✓ **Recruit an internal champion.** Identify an executive sponsor that can carry the message across the C-level of the organization. That could be the Chief Information Officer, the Chief Risk Officer, Chief Compliance Officer or Chief Operating Officer.
- ✓ **Identify stakeholders.** Plan to create a cross-functional stakeholder team with representation from IT, risk management, privacy, compliance, human resources, legal and the business lines. Learn what drives each of the stakeholders and be prepared to deliver a personalized "What's in it for me?" message about the consequences of a security breach and the value of adding or transitioning to identity-based security tools.
- ✓ **Hold a value mapping session** and identify cross-functional points of alignment.

Step 4: Consider a phased approach

One way to minimize the up-front cost of transitioning to identity-based security is to consider a phased approach to implementation. For example, mobile credentialing could complement an existing badge infrastructure now with the potential to replace it later. Biometric scanners could be initially implemented only in high-risk, critical areas of the building where a secondary level of authentication is needed.

Making the transition in phases also gives organizations the opportunity to experiment with new technology before they go "all in", minimize disruption to business operations and benefit from the remaining, useful life of assets already in place.

To approach the transition in phases, recruit a team to pilot the new technology. Include respected people from various functional areas within the organization and who come from all points along the tech-savvy spectrum.

Step 5: Establish measurable return on investment

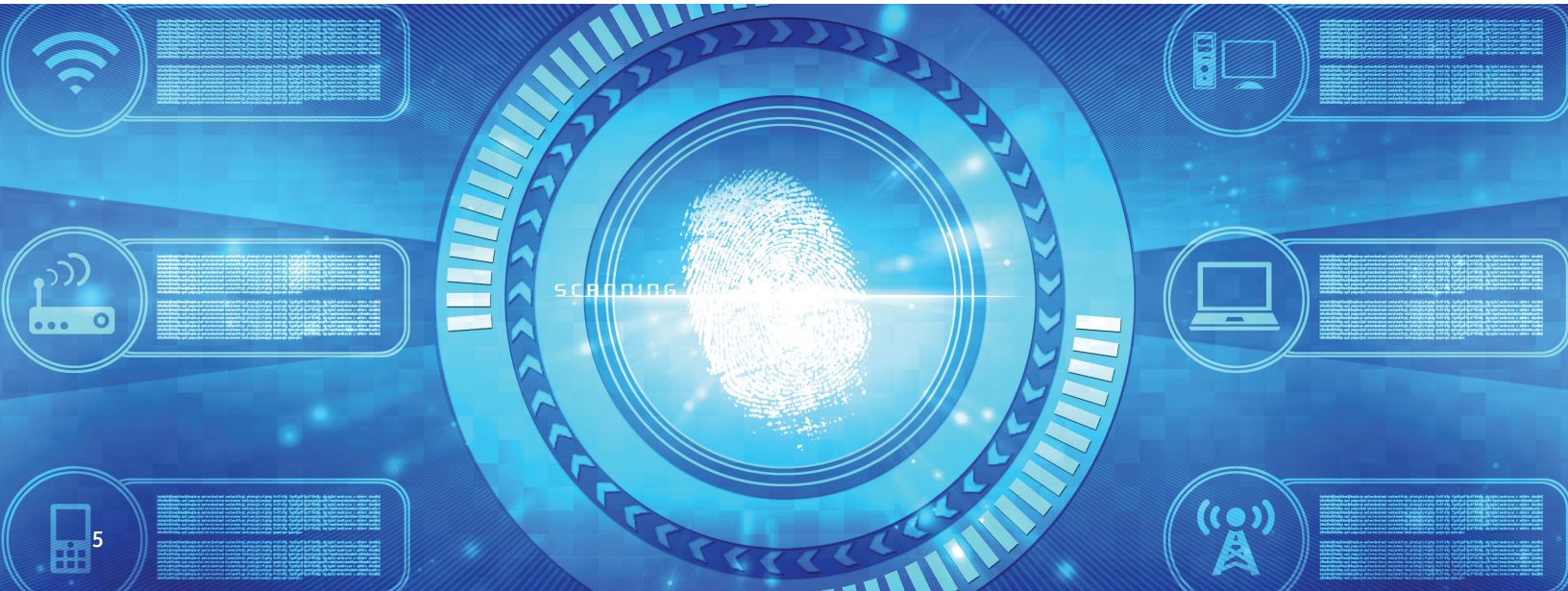
Establish a method to evaluate the success of the initiative and tie key performance indicators directly to the organization's goals. Some common metrics include:

- ✓ The per-user cost, on a monthly or annual basis
- ✓ The staffing required to maintain access controls
- ✓ The time it takes for people to move in, out and within the building
- ✓ Adoption rates
- ✓ The employee user experience
- ✓ The security team experience
- ✓ The cost and effectiveness of user training
- ✓ Any impact caused by issues with installation, integration or version control

The bottom line on identity-based access controls

No technology is infallible. But a well-designed, documented and comprehensive plan that takes advantage of the latest technologies can make an organization less of a target. It may also help to reduce liability in the wake of a worst-case scenario. An increasing number of boards of directors are taking an interest in cyber readiness and response plans, so that they can report to their auditors that they are doing everything possible to protect people and assets.

The challenge for organizations is to balance the benefits of introducing security-strengthening, identity-based technologies with their potential to introduce new security vulnerabilities. By taking the proper steps, security teams will be closer to achieving that balance.



For more information on next-gen access management, contact your local branch at www.johnsoncontrols.com.

About Johnson Controls

Johnson Controls is a global diversified technology and multi industrial leader serving a wide range of customers in more than 150 countries. Our 120,000 employees create intelligent buildings, efficient energy solutions, integrated infrastructure and next generation transportation systems that work seamlessly together to deliver on the promise of smart cities and communities. Our commitment to sustainability dates back to our roots in 1885, with the invention of the first electric room thermostat. We are committed to helping our customers win and creating greater value for all of our stakeholders through strategic focus on our buildings and energy growth platforms. For additional information, please visit http://www.johnsoncontrols.com or follow us @johnsoncontrols on Twitter.

About Johnson Controls' Building Technologies & Solutions

Johnson Controls' Building Technologies & Solutions is making the world safer, smarter and more sustainable – one building at a time. Our technology portfolio integrates every aspect of a building – whether security systems, energy management, fire suppression or HVACR – to ensure that we exceed customer expectations at all times. We operate in more than 150 countries through our unmatched network of branches and distribution channels, helping building owners, operators, engineers and contractors enhance the full lifecycle of any facility. Our arsenal of brands includes some of the most trusted names in the industry, such as Tyco®, YORK®, *Metasys*®, Ruskin,Titus®, Frick®, PENN®, Sabroe®, Simplex® and Grinnell®. For more information, visit www.johnsoncontrols.com or follow @JCI_Buildings on Twitter.

Johnson Controls