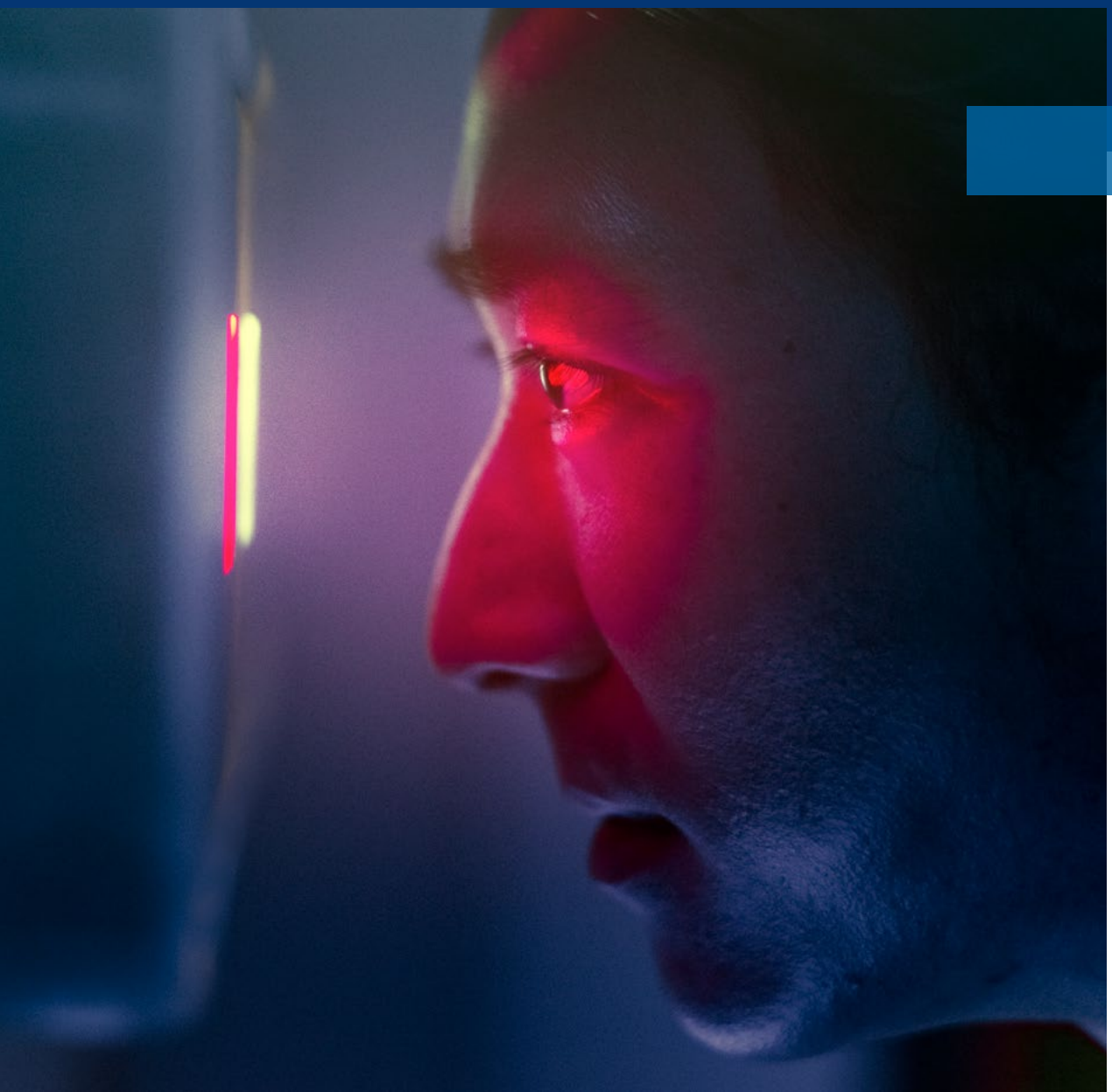
princeton IDENTITY

ACCESS CONTROL EXECUTIVE BRIEF

WHITEPAPER

THE PATHWAY TO BIOMETRIC ADOPTION IN THE SECURITY MARKET IS SELLING CONVENIENCE FIRST

By Bobby Varma and Lee Odess

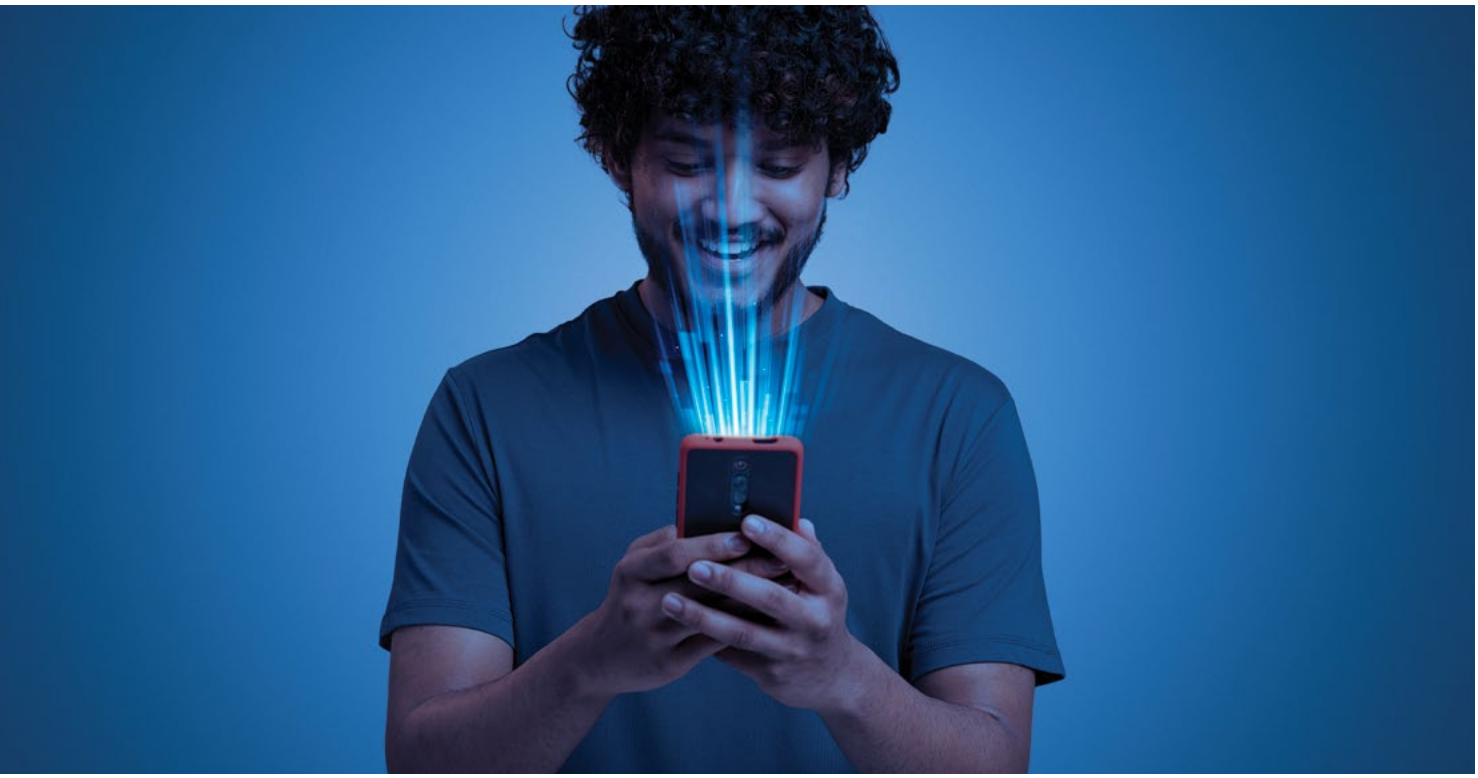


INTRODUCTION

SMARTPHONE DEVELOPERS CREATED A "MUST-HAVE" MOMENT FOR THE TECHNOLOGY BASED ON CONVENIENCE. TODAY, OVER 80% OF SMARTPHONES HAVE BIOMETRICS ENABLED.

When Apple introduced Touch ID on its iPhone 5S a decade ago, it was a seminal moment for biometrics. Almost overnight, the technology moved from the realm of high-security and government applications into the mainstream. Soon, all smartphones let users unlock their devices with a touch or a glance. Smartphone developers created a "must-have" moment for the technology based on convenience. Today, over 80% of smartphones have biometrics enabled.

Why hasn't that moment yet occurred within the physical security industry? There are countless applications in which biometric identity solutions could deliver a superior user experience, yet few applications have become mainstream. This whitepaper addresses what manufacturers could have done differently, how and why the pace of adoption is now picking up speed, and offers a forecast for the future.



[1] https://www.biometricupdate.com/202211/cisco-report-81-percent-of-all-smartphones-have-biometrics-enabled

LEARNING FROM MISTAKES

Everyone agrees that biometric identity solutions are convenient. They eliminate the need to carry or remember anything, and today's readers are fast – authenticating one's identity in seconds. The user experience is seamless.

These systems eliminate administrative headaches too. Databases remain free of duplicates. Access cards can't be lost or stolen. Event logs are highly accurate. So why aren't biometric identity solutions everywhere? Here are five reasons:

1. The biometric industry should focus more on problem-solving. Companies like Apple started with a specific user need and then leveraged biometrics to develop a solution. To this point, Apple has rarely, if ever, used the word "biometric" in its advertising. Touch ID used a "fingerprint." Today's iPhones use "Face ID." These are terms the consumer understands. Conversely, biometric solution manufacturers have tended to focus on their technology, toss it into the marketplace, and then say, "Hey, here's a great tool. Figure out where to use it." It's been a solution looking for a problem. Biometric manufacturers should prioritize identifying particular applications in which biometrics could add value and then tell stories about the value created by using biometrics.

2. Many of the applications where biometrics excel are already using other technologies that do the job "well enough." Most notably, mobile credentials have become a mainstay of access control systems, augmenting the need for cards and fobs and offering users and system administrators a more convenient experience. While one can legitimately argue that biometrics would deliver an even better experience in 99% of installations, mobile raised the bar so much that the incremental value of biometrics has become a hard sell.

3. Manufacturers mistakenly assumed that technological innovations within the security industry would continue to penetrate markets horizontally. Historically, that's how things worked. As new solutions launched, they began in high-end verticals, like government facilities, banking, and utilities. Then, they gradually made their way to other industries like retail, education, and multi-tenant commercial. That pattern has changed.

Today's security solutions are primarily software-driven and frequently integrated within vertical-specific platforms. For example, access control for a multi-tenant residential building may be part of a Tenant Engagement App that includes rent payment, community postings, repair scheduling, lease management, and more. Biometric manufacturers have been slow to embrace this reality, assuming their technology's successful adoption by verticals like airport security and border control would seamlessly spread to others, despite the need to function as part of a vastly different ecosystem.

4. Biometric companies needed to work more closely with integrators to ensure their technology was easy to implement and install. That's now changed, but compared to devices like IP cameras that have been plug-and-play for years, biometrics has catching up to do. Also, some security integrators may have been resistant to the technology for fear that it would cannibalize a profitable piece of their access control business.

5. Then, there's the elephant in the room. Social media has amplified perceptions that biometric identity solutions violate user control over Personally Identifiable Information (PII). The security industry should more aggressively counter the narrative with education while refocusing the conversation on convenience. We know that when the story becomes about convenience rather than security, the public is largely willing to push its worries about PII and privacy aside. Growing enrollment in the CLEAR program at airports is a perfect example. Biometrics are being used for a security application – screening passengers. However, the benefit to the public is one of convenience – breezing through TSA checkpoints.

A GOLDEN OPPORTUNITY

For years, companies internally debated whether to upgrade their systems. The pandemic forced their hands. The pandemic hastened the adoption of technology solutions in many ways. Management teams were suddenly motivated to reduce labor costs by automating processes, make the in-office experience more frictionless, and support the security requirements of a hybrid workforce. Those genies are not going back in the bottle.

Biometrics can help achieve these goals. Here are some applications where we'll see adoption most quickly.

Access Control

In many environments, biometrics are the ideal access control credential. Manufacturers now recognize that flexibility is vital to user acceptance and have begun offering a choice of modalities within a single reader. Rather than force a biometric solution on users who aren't comfortable with it, multi-modal readers let users interact with readers in the way they prefer, whether via a biometric, access card, or other credential. Over time, more users will ditch their cards in favor of using a biometric because they'll see their colleagues doing so with no adverse effects.

Logical Access

"Zero Trust" policies are gaining traction as the preferred network architecture. It requires users to verify and authenticate their identity whenever they open software, opena file, edit a file, save a file, send an email, or perform any other distinct network interaction. While Zero Trust greatly enhances network security, it can be a massive hassle for users who must repeatedly enter a password all day. Glancing at a camera or touching a fingertip reader requires much less effort. Even for networks not implementing Zero Trust, biometrics make remote login by employees working from home more convenient and secure.

Visitor Management

Biometrics can automate visitor management, reducing lines for visitor screening and badges. Self-serve kiosks can match a visitor's face with their photo ID, eliminating the need for a security officer to perform that task. Once inside, biometric readers positioned at doorways, stairwells, and elevators limit visitors' access to areas where they are permitted.

Time and Attendance

Biometrics readers integrated with Time and Attendance tracking solutions speed up the time it takes for employees to "punch" in and out. They can spend more time on break and less time waiting to punch back in. For management, the solution eliminates time clock fraud, buddy punching, and administrative tracking errors. Some Time and Attendance solutions already have a biometric reader built into their hardware.

Point-of-Sale (PoS)

When connected to PoS technology, enrolled users can make purchases without a credit card or mobile app. Lines speed up in cafeterias, and vending machines become incredibly convenient. Amazon has already introduced a biometric PoS solution at its Amazon Go stores. At the cash register, enrolled users hold their open hand a few inches above a specialized scanner that analyzes the palm's surface characteristics and subcutaneous features. Within seconds, the system identifies the shopper and bills their linked account for their purchases.

WHERE TO BEGIN

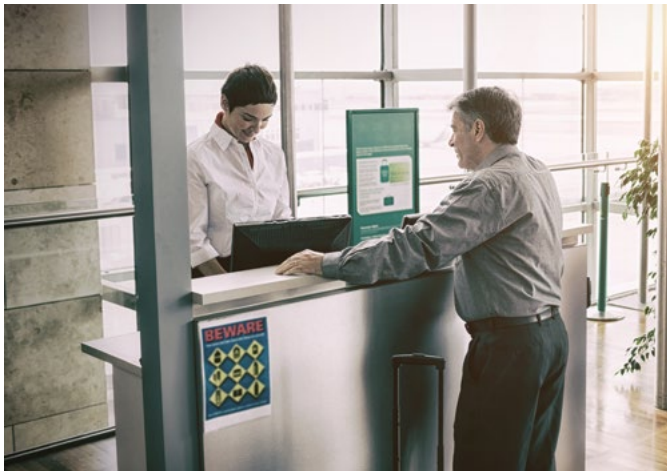
By learning from past mistakes and capitalizing on this moment of opportunity, biometric manufacturers can speed up the pace of adoption.

The first places to make inroads are where people feel the pain – from long lines or cumbersome operational processes. **Best bets are in verticals where integration with broad, industry-specific software platforms can deliver a host of conveniences.** These include:

Higher-Ed Campuses

Universities and colleges are ahead of most other verticals in embracing biometrics. They are self-contained communities where students and faculty use their identity cards for just about everything, making biometric identity solutions a welcome addition. User demographics skew young, equating to fewer concerns about PPI and privacy. Twenty-somethings have grown up with social media; they'll gladly share their data if it makes daily life more convenient – particularly with institutions, organizations, and companies that have proven to handle data properly and have earned their trust.

Biometrics are unlikely to replace more traditional credentials across entire campuses, but they're an ideal option for some locations. Adding biometric readers to exterior doors of residence halls ensure students never get locked out. Their use in locker rooms and training facilities allows student-athletes to move about freely while wearing pocketless uniforms, swimsuits, or workout gear. Stadiums, theaters, and cafeterias can offer "fast track" lines at entrances and cash registers. High-security areas, like data centers and research labs, can leverage biometrics as part of dual-factor authentication. And, on-campus healthcare facilities can immediately identify patients when they check in for appointments, reducing sign-in paperwork and ensuring accurate record-keeping.



Commercial Real Estate

Here, the use of biometrics for access control is becoming more common in single-tenant facilities where fewer stakeholders require buy-in. In large industrial and manufacturing plants with thousands of workers, biometrics are ideal for access control and time and attendance applications. Workers spend less time funneling in for their shifts; administrators save hours no longer dealing with lost cards and inaccurate event logs.

Multi-Family Residential

Developers, owners, and operators now promote their properties' high-tech features as selling points. Biometric readers that provide seamless access to community spaces like laundry rooms, gyms, pools, mail rooms, and storage facilities improve the ease of daily life while instilling a sense of security for residents. The systems also generate revenue. Residents late paying rent risk having their access turned off.

Life-Sciences

In medical and research environments, biometrics can make it much easier for staff to adhere to cleanliness and security protocols. Some biometrics, like the iris, can regulate entry to operating rooms and clean rooms with just a glance. Gloves and masks can stay on. Biometrics can also harden access to restricted areas like pharmacies and drug storage rooms without inconveniencing the workers authorized to enter.

MAKING IT HAPPEN

Biometrics in security are clearly gaining ground. Here's what manufacturers and systems integrators should keep in mind as they attempt to clear the final market hurdles:

Maintain an "AND," not "OR" mindset.

Users need a choice of which modality is best in different situations: keys, pins, cards, mobile, or biometrics. No solution is right in all conditions. It's necessary to consider lifestyles and how users interact with technology. Biometrics are an excellent addition to the identity verification toolkit, but there's no need to pit them against other solutions. When stakeholders focus on marrying security with convenience, leaving all suitable options open, all boats will rise.

Focus on problem solving.

The technology will sell itself if it's the best solution for a specific issue. For example, Mercedes is introducing fingerprint biometrics to adjust the driver's seat, steering wheel, mirror settings, and navigation in its C-class models. The public welcomes practical, hyper-targeted solutions. By contrast, having great specs and a "cool" factor do nothing to scratch an itch.

Think beyond security.

The most successful security integrators have evolved into technology integrators. They have broadened their offerings with the IoT, smart home solutions, and multi-purpose apps. With each of these, they are selling convenience.

Biometric identity solutions can harden security, but first and foremost, they too are "convenience" solutions. Rest assured, once the public experiences them applied to solve everyday problems, there will be no turning back!