TOP 5 REASONS WHY MOBILE WILL TRANSFORM ENTERPRISE AUTHENTICATION

Simply Better Authentication

Table of contents

Introduction: a mobile world

Currently, around 25 percent of the world's population uses a smartphone. By 2017, that number is projected to reach one-third.[1] Today, the average person spends the better part of three hours a day on his or her mobile device.[2] Of these 162 daily minutes, the vast majority — 86 percent — will be spent on mobile apps. For the typical person, 23 days of the year will be spent on their phone. [3]

Simply put, the mobile device is part and parcel of daily life. It's fundamentally changed the way consumers behave, and this influence has spread to the enterprise sector as well. For instance, patron-owned mobile devices have largely helped pave the way for the widespread emergence of bring-your-own-device (BYOD) policies. Ten years ago, the idea of a company employee logging into the enterprise system while they're on an airplane over the Atlantic would seem far-fetched, but today such behavior is relatively commonplace. Mobility is changing how we shop, work and live our daily lives.

And contrary to what some people think, mobility is secure for businesses — provided they take the proper steps to protect devices within the enterprise network. There's no denying that the proliferation of mobile devices presents new safety challenges for enterprises and consumers alike. But these potential challenges can be mitigated - paving the way for mobile to become a trusted, convenient and multi-purpose enterprise digital ID.

1 http://www.emarketer.com/Article/Worldwide-Smartphone-Usage-Grow-25-2014/1010920
2 http://www.geekwire.com/2014/flurry-report-mobile-phones-162-minutes/
3 http://www.mobilestatistics.com/mobile-news/23-days-a-year-spent-on-your-phone.aspx

Securing digital identities with mobile

Mobile solutions are fundamentally changing the way we live. For many people, they've replaced devices like cameras, voice recorders and music players. Now, a person's smartphone or tablet is more of an all-purpose media portal. And with the emergence of mobile pay solutions and other innovations, the various applications of mobile devices are becoming even more wide-ranging.

But mobile devices aren't only versatile for individual users — they can also play a key role in the enterprise. In fact, within a corporate network, mobile devices can replace things like hardware tokens, building access cards and passwords. Beyond that, they can be harnessed to defeat more advanced malware and even to streamline business processes -- eliminating email or paper-based approval processes.

Here's why mobile technology is set to transform enterprise authentication.

Reason 1: mobile is a secure platform to deploy enterprise identities

Five key reasons for enterprises to leverage mobile devices in the office.

It's easy to assume that because devices like iPhones and tablets are used outside of the company network — in places like subway cars, airplanes and homes — that they're automatically less secure than PCs. In fact, this is not the case. As a recent InfoWorld report pointed out, by far the vast majority of enterprise breaches happen due to compromised computer systems.[4] This is largely due to the fact that mobile devices are more secure than computers. Their security stems from sandboxing (more on that later). If an app is maliciously infected, for example, the infection is contained to that app alone and does not spread elsewhere on a device.

This is hardly the case for computers, where one app being targeted can often mean the entire device gets commandeered. Yet as a Dark Reading piece pointed out, the idea that mobile devices are less secure persists among company IT departments, even though it's a misconception.[5]

The reason why mobile devices are often presumed to be vulnerable is because most individuals and businesses aren't taking the proper (and basic) steps to secure them. Basically, what you want to avoid at all costs is jailbreaking your phone. Jailbreaking is a practice in which one uses a software application which 'breaks open' the phone's file system to allow you to modify it.[6] The problem with doing this is that you then immediately lose the built-in security tools provided by your carrier — and those features are there for a reason. As long as you don't jailbreak your mobile device, you can be sure that it'll be more secure than a PC. Here are some of the reasons why:

- **Signed/vetted applications:** Legit applications that you download onto a mobile device will have been signed and vetted before you even put them on your system.[7] As long as you're getting the app from an official store — such as the Apple App Store — you can guarantee that it'll have gone through a vetting process that ensures its security.
- **Application sandboxing:** Whether you're leveraging Android, BlackBerry or iOS, you can rest assured that apps you're downloading will have been secured via sandboxing.[8] What this means is that the app and its contents will be autonomous from other apps. Therefore, in the unlikely event that one app gets infected, that virus won't spread to other apps you use. Conversely, if another app in your docket gets hit by malware, the app you have downloaded won't be exposed.
- **Mobile Device Management / MDM:** Enterprise IT needs control over mobile devices accessing company resources and MDM gives them the ability to provision security policies and remotely manage devices to mitigate risk. Along with company "partitions" on the phone and the ability to ensure security scanning occurs, features such as remote wipe help ensure IT is not "opening up the barn door" with mobile.

4 http://www.infoworld.com/article/2845956/mobile-security/the-safest-computers-are-iphones-and-ipads.html
5 http://www.darkreading.com/mobile/industry-trends-research-confirm-mobile-devices-can-be-more-secure-than-pcs/d/d-id/1139728?
6 http://cellphones.about.com/od/glossary/f/jailbreak_faq.htm
7 http://www.entrust.com/wp-content/uploads/2013/08/Entrust-White-Paper-Why-Mobile-is-the-Next-Digital-Identity-May-2014.pdf, 8
8 Ibid, 9

- **Embedded security:** By using embedded security features like PINs and digital certificates to get into various apps, you can take a significant step toward solidifying mobile security.[9] For enterprises, it's absolutely imperative to harness embedded security options. And for employees using a mobile device as a BYOD resource, it's vital to have a four-digit passcode in order to even get access to a device. That way, if a smartphone or tablet is left somewhere like the subway, someone outside the company system won't be able to get access to it.
- **Alternative technology:** We're moving toward an exciting future in which other means of verifying identity are cropping up. These include tools like facial recognition and retina/fingerprint scanning.[10] For Apple, this is already popularly taking shape in the form of Touch ID, an iPhone and iPad solution that enables users to have their device recognize their fingerprint.[11] This is quickly becoming a popular — and more secure — alternative to the traditional four-digit passcode, and it represents arguably the most advanced and dependable identity verifying technique out there.
- **Evolving security:** Mobile architectures are constantly growing on both the hardware and software sides when it comes to enhancing security. One recent advancement, for instance, is the emergence of Trusted Execution Environment (TEEs) on mobile devices. TEEs offer an isolated and highly secure area where individuals and businesses can ensure that trusted transactions occur safely.[12] You can think of a TEE like a firewall — except that TEEs are meant for isolating sensitive transactions whether that be access a locked room, logging into the network, or approving a large money transfer etc.

Additionally, there are some basic security principles to follow that can curb the threat of malicious intrusions on mobile devices. Here are a few, as outlined by an expert team:[13]

- ✗ **Don't click suspicious email links:** This is pretty straightforward advice, and it holds true as much for smartphones as it does for computing devices
- ✓ **Only download apps from trusted sources:** Sometimes a strain of malware will try to dress itself up as an app. But again, the signing/vetting employed by legit app repositories will weed such imposters out. So make sure to only download apps from trusted sources.
- ✗ **Don't choose easy PINs:** Make sure workers know that PINs should be as robust as possible or better yet take advantage of embedded biometrics to secure access to the phone.
- ✗ **Don't join just any Wi-Fi hotspot:** Be sure to confirm the legitimacy of any Wi-Fi network you're joining. This should be a relatively simple process — if you're at a cafe, for instance, just go up to the counter and ask an employee to identify the store's official Wi-Fi.
- ✓ **Authenticate Wi-Fi-connected devices:** If a mobile device wants to gain access to your corporate network, you must ensure that it's properly authenticated. The absence of an authentication platform could lead to malicious users gaining access to your Wi-Fi network.

9 Ibid, 10
10 Ibid, 10
11 http://support.apple.com/en-us/HT5883
12 https://www.cl.cam.ac.uk/~sjm217/talks/rhul14tee.pdf
13 https://www.us-cert.gov/sites/default/files/publications/cyber_threats-to_mobile_phones.pdf

Reason 2: mobile offers cost savings

Within the workplace, mobile devices offer a far more cost-effective means of two-factor authentication than the conventional hard token. Hard token-based authentication is a cumbersome and expensive process. First, the physical tokens have to be made, and then disseminated — sometimes via armed guard. Once the tokens are in the hands of the users, that doesn't mean 100 percent security. After all, if a user happens to lose his or her hard token, then the whole process has to start all over again. This is not the case for mobile users, who can self-provision authentication and even easily carry out a reset/upgrade. This is something that will come naturally to most employees, since they've already become accustomed to such processes through downloading apps from the app store.

Smartphones offer a more robust and easier authentication wall than physical tokens. By leveraging software-based tokens on mobile devices, you get rid of the risks inherent in physical tokens, as Infosecurity Magazine points out.[14] With smartphone-based authentication, businesses can say goodbye to shelling out big bucks on costly and clunky hard tokens — not to mention having to always make help desk calls — and instead embrace the ease and cost savings that accompany mobilizing the process.

Reason 3: mobile offers stronger, more convenient authentication

A single mobile device encompasses a whole host of functionalities, and that creates an unprecedented level of access control for businesses harnessing mobility. With a device like a smartphone or tablet, you can enjoy these different types of access:

- **Secure Logical Access:** Within the business sphere, logical access ensures that privileged information contained on computer networks and systems is limited to those individuals with the authority to view it.[15] With a virtual mobile based identity solution, logical access can be easy, secure and always in hand. Along with accessing VPN networks, secure intranets and even public cloud applications, a mobile credential can be your virtual smart card for true password-less access to your Windows computer. And it's also a highly secure solution. For instance, your computer will automatically lock when you walk away from it through smart Bluetooth integration.
- **Secure Physical Access:** Mobile solutions don't only help ensure logical access, but also access entry to physical spaces as well. Whether you're a government or enterprise, protecting the physical area where business happens and is contained is absolutely vital. Luckily, this too can be accomplished via mobile credentials which can operate as a building access card to regulate access to privileged areas like physical doors and work areas.[16] And whereas physical access cards present yet another thing to be carried around — not to mention another thing that can be easily lost — mobile credentials are always with you and virtually impossible to duplicate.

14 http://www.infosecurity-magazine.com/magazine-features/hard-soft-or-smart-evaluating-the-two-factor/
15 http://findbiometrics.com/applications/logical-access-control/
16 Ibid

Reason 4: mobile means quicker/better user adoption

For most workers out there, using a mobile device is already second nature. Because things like smartphones and tablets are mainstream technologies, they're things that the average employee already has some measure of lay expertise using. For that reason, the typical staffer is likely to use an app/mobile device for security. In fact, employee use of mobility is so widespread that a Government Information Group survey found that government workers can't even do their jobs well without their mobile device.[17] Therefore, by embracing mobility, businesses and governments aren't only taking a proactive business step, but are catering to the desires and working habits of their employees. Because of this, a company policy based around mobility will be more popular among staffers – and its use will be more intuitive.

Most people are glued to their smartphone, which means that the likelihood of a staffer leaving his or her device at home or losing it is relatively low. However, even if that happens, it doesn't have to be a disaster scenario. By following the suggestions outlined earlier — including embedded security and alternative technologies like TouchID — companies can protect against a lost phone becoming a compromised one.

Reason 5: mobile future-proofs your enterprise

Any company that wants to succeed will be as mindful of the future as they are of the present. And mobile solutions offer the ultimate means of future-proofing your business. The first thing to point out is that apps are a lot easier to update on mobile devices than they are on computers — and they come out more frequently. Think about your personal phone use and how often updates for apps appear. In order to install them, it's as simple as clicking a button. The same principle holds for businesses. And just as apps are easy to implement and update, so too is new security technology like taking advantage of emerging biometric or TEE capabilities. With resources like this in place, companies can take advantage of the most cutting-edge security methods out there — such as fingerprint identification technology — in order to create the simplest and safest enterprise environment possible. Here are some future-focused use cases that mobile will be able to tackle:

- **Anywhere, anytime dual controls:** Let's say you're in the midst of a business deal that requires you to wire $50,000. Because of the amount of money involved, you need approval from your company's financial director, who's unfortunately out of town. In the past this kind of situation would have slowed down the transaction, but with mobile, an approval request can be sent to the out-of-town financial director remotely, and she can approve it and digitally sign it on her mobile device.
- **Remote work with top-tier security:** Because credentials can be embedded into mobile devices in your network, this allows for a tablet to become a secure desktop. This means that traveling employees and mobile field workers — like inspection agents — can enjoy security that's as robust as that on computers in the physical office.
- **Strong authentication for privileged users:** Increasingly, criminals are targeting IT administrators to compromise enterprise systems – successful attacks have been executed on Fortune 1000 retail, banking and media companies. With a mobile based smart card, not only can IT administrators authenticate with strong PKI based credentials, the transaction can be sent out-of-band to the mobile device to defeat account takeovers.

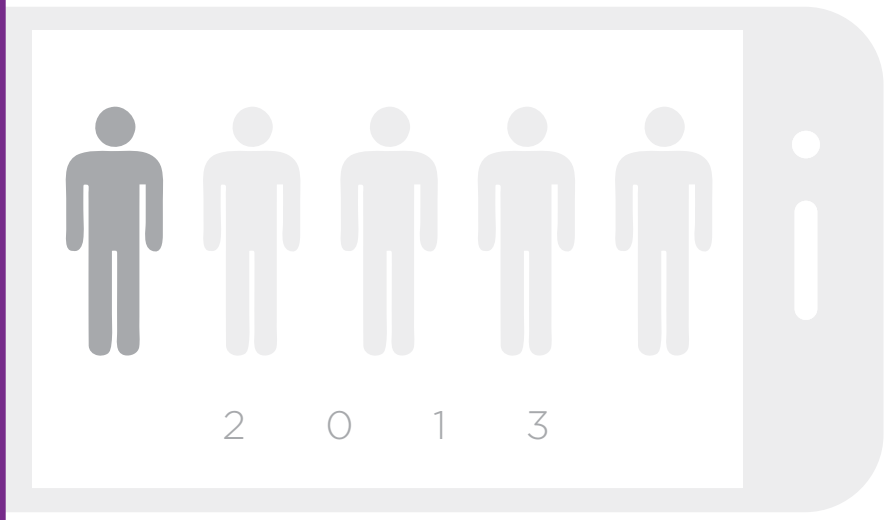
17 http://fcw.com/microsites/2012/download-mobile-and-wireless/01-employee-mobile-device-needs.aspx

Conclusion

Mobile the next generation in Enterprise Authentication

Mobility is the way of the present – and of the future. Back in 2013, 1 in 5 people around the world owned a smartphone.[18] By 2017, it'll be 1 in 3. These days, smartphones and tablets aren't peripheral elements of daily life — they're right in the center. They're helping to regulate our homes, open our doors, start our cars, and conduct payments. And fortunately for businesses, they offer tremendous transformative potential to improve how enterprise security is achieved as well.

As we've outlined here, mobile devices are secure — in fact, more secure than PCs. And their transportability makes them more convenient too. By leveraging mobile devices in your enterprise authentication, you can take significant strides toward both bolstering efficiency and strengthening security.



18 http://www.businessinsider.com/smartphone-and-tablet-penetration-2013-10

About Entrust Datacard

Consumers, citizens and employees increasingly expect anywhere-anytime experiences — whether they are making purchases, crossing borders, accessing e-gov services or logging onto corporate networks. Entrust Datacard offers the trusted identity and secure transaction technologies that make those experiences reliable and secure. Solutions range from the physical world of financial cards, passports and ID cards to the digital realm of authentication, certificates and secure communications. With more than 2,000 Entrust Datacard colleagues around the world, and a network of strong global partners, the company serves customers in 150 countries worldwide.

For more information about Entrust products and services, call **888-690-2424**, email **entrust@entrust.com** or visit **www.entrust.com**.

Headquarters
Entrust Datacard
1187 Park Place
Shakopee, MN 55379
USA

Twitter Facebook Youtube LinkedIn Google+ RSS