WHITEPAPER

Done waiting?

Invisible security for efficient workflows and happy customers

imprivata®

It's an age-old story: technology meets workflow; workflow is no better – perhaps even worse – with technology; no happily ever after. Not quite the fairy tale we'd like, despite technology being "the great enabler."

Technology innovation has long been central to the advancement of security (best) practices, often to the detriment of workflow efficiency. And today that makes sense, due to the increasing attack surface introduced by some of those same technologies.

But technology – and specifically technology built for the purpose of security – shouldn't just be a necessary evil. Instead, the right solutions can usher in an era of improved workflow efficiency, productivity, and customer experience. All while, yes, still improving security.

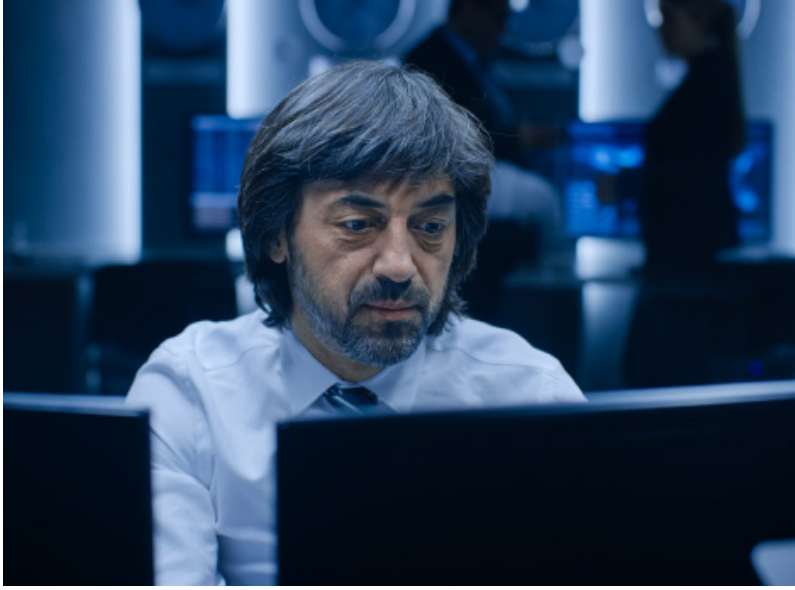
Striking a balance between security and workflow efficiency

End users often equate the idea of security with barriers and frustration – inefficiencies, long wait times, and sometimes even dreaded side-eye glances from customers. They're going as fast as they can; the system's just slow; sorry, there's really nothing they can do.

"Security friction," a concept that suggests that most people will default to convenience when an extra effort is required, often leads to workarounds that compromise protections adopted for security in the first place. This means that the security technologies that were put in place are actually being ignored completely, and entirely new – and inefficient and unsecure – workflows are being built.

For example, when IT and security teams design systems that force end users to contend with frustrating, repetitive manual username and password entry multiple times during their shifts, workarounds really are inevitable. If IT and security teams do nothing to head off these threats, both the organization's risk and impact of a breach can increase.

It's a key challenge in every industry – trying to balance the protection of huge amounts of data with users' need for fast access to that data.



END USER ADOPTION IS ESSENTIAL TO A STRONG SECURITY INFRASTRUCTURE

What is most important to security professionals? Ensuring that their organization is as secure as possible without slowing down end users, which often delays customer satisfaction.

Leading businesses are using strong authentication and single sign-on (SSO) to make it easier for end users to adopt technologies put in place for security's sake. With a platform like this in place, users can simply tap their badges or scan their fingerprints to authenticate into their critical systems and applications. This capability enhances their experience with technology, bolsters security, and improves the end customer experience.

Many organizations globally have already taken this step and invested in a single sign-on and authentication management platform to:

- Enable organizations to implement strong, 16+ character passwords, avoiding credential breaches without introducing security friction
- Stop waste of end user time that comes with manual username and password entry
- Empower end users with self-management of their passwords to reduce calls to your help desk

In addition, there can be significant cost savings associated with this type of technology as well. Just imagine: if you can save even 10 seconds on every login, performed by every end user, every day, the time savings quickly add up. And, as the old aphorism goes: time is money.

Implementing virtualization technology without introducing security barriers

Virtualization allows organizations to provide users with access to information, anywhere. It's no surprise that the use of virtual desktop infrastructure (VDI) has increased over the past decade. Virtual desktops can have the following advantages:

- Improved security
- Enhanced user experience
- Reduced IT maintenance costs

> **Burnout is not about working too much, it's about working ineffectively...**

Securely implementing virtualization across your organization is not without its challenges, though. The biggest hurdle to overcome is ensuring the successful adoption of the system despite security protocols that often force users to take multiple steps to authenticate and gain access to the system.

The goal of any good IT program should be simplicity and expediency – ultimately, to facilitate fast, efficient use of technology, not block it. To get there, organizations need systems that are stable, secure, and fast to deploy. By combining single sign-on with virtual desktop access, organizations get more secure and stable systems that can be easily deployed, modified, and quickly adopted by end users.

Preventing technology fatigue with a smarter approach to security

As a senior member of your organization, retention of employees is part of your job description, whether you know it or not. But there's good news: by creating frictionless workflows that prompt the fast, efficient use of technology, end user experience will improve.

All of that wasted time and workflow disruption leads to often intense frustration for your hard-working employees. In fact, it's not unheard of for frustrated employees to leave, is it? Every little bit – like creating a positive technology experience – helps.

"Burnout is not about working too much, it's about working ineffectively," said psychiatrist Dr. Alok Kanojia. "Burnout is when someone who wants to do a good job and is capable of doing a good job [can't because] there's a system that prevents them from doing it, and then they get exhausted, then they give up."

Earlier, we stated that technology can be a great enabler – and that's true – but it can take some intentional effort to allow it to be that way. Putting solutions that actually enable the use of technology in place that also improve security? That's the goal.

When systems are locked behind prohibitive security barriers, one of three things will likely happen:

1. Customers will not feel satisfied with their experience due, at least in part, to long wait times
2. Users will share login credentials or accounts with each other
3. Users will leave systems unlocked so that they always have access to systems and data whenever they need it

Security friction causes these problems that can be as far reaching as to affect your employees' – and your customers' – overall satisfaction with your organization. But when new technology innovations are combined with authentication management and SSO, the benefits are clear: no workarounds by users, and even some ROI. What's more, the security of your organization will be improved.

imprivata®

Imprivata, the digital identity company for enterprise, provides identity, authentication, and access management solutions that are purpose-built to solve hyper-complex workflow, security, and compliance challenges.

For more information, please contact us at 1 781 674 2700
or visit us online at www.imprivata.com

EAM-DS-done-waiting-0124