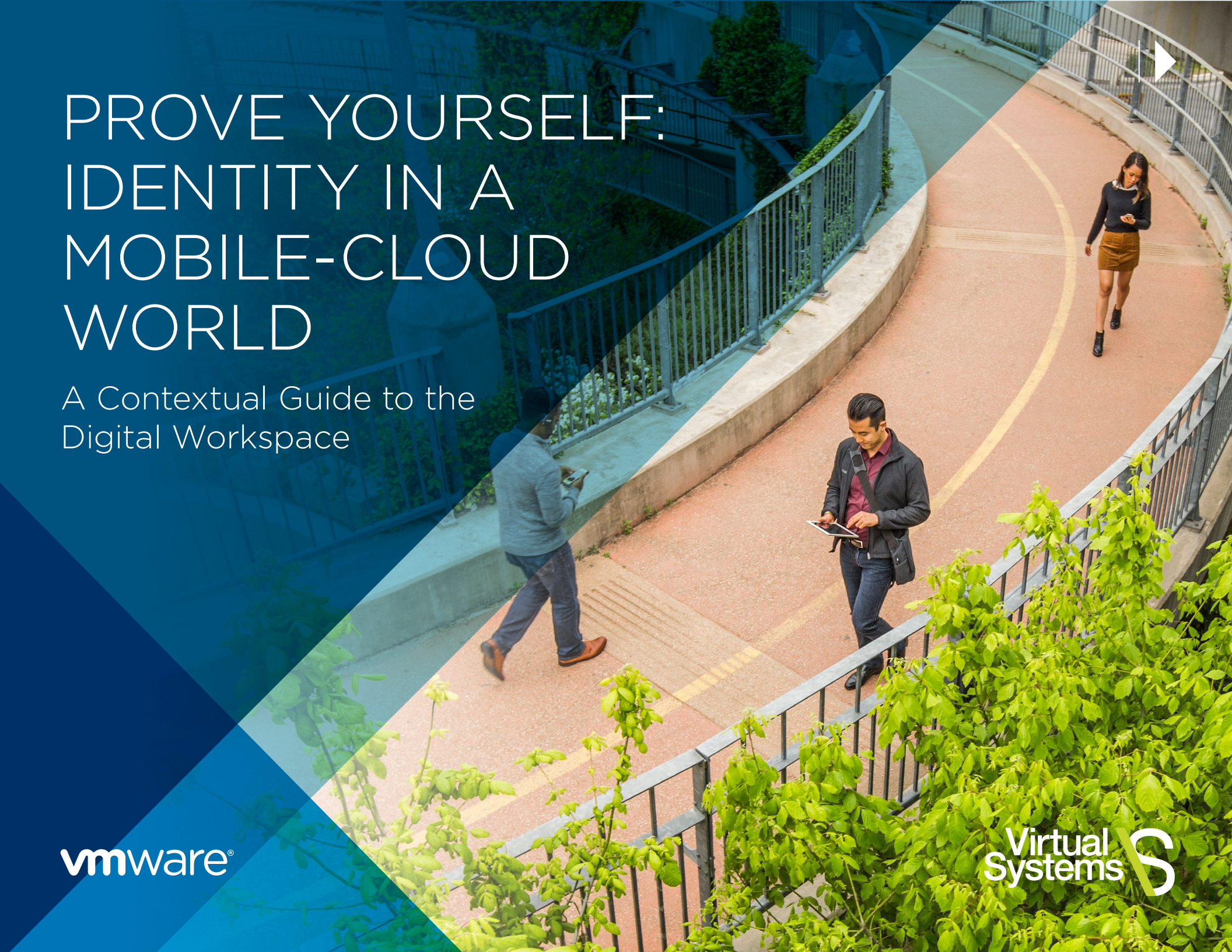
PROVE YOURSELF: IDENTITY IN A MOBILE-CLOUD WORLD

A Contextual Guide to the Digital Workspace



vmware®

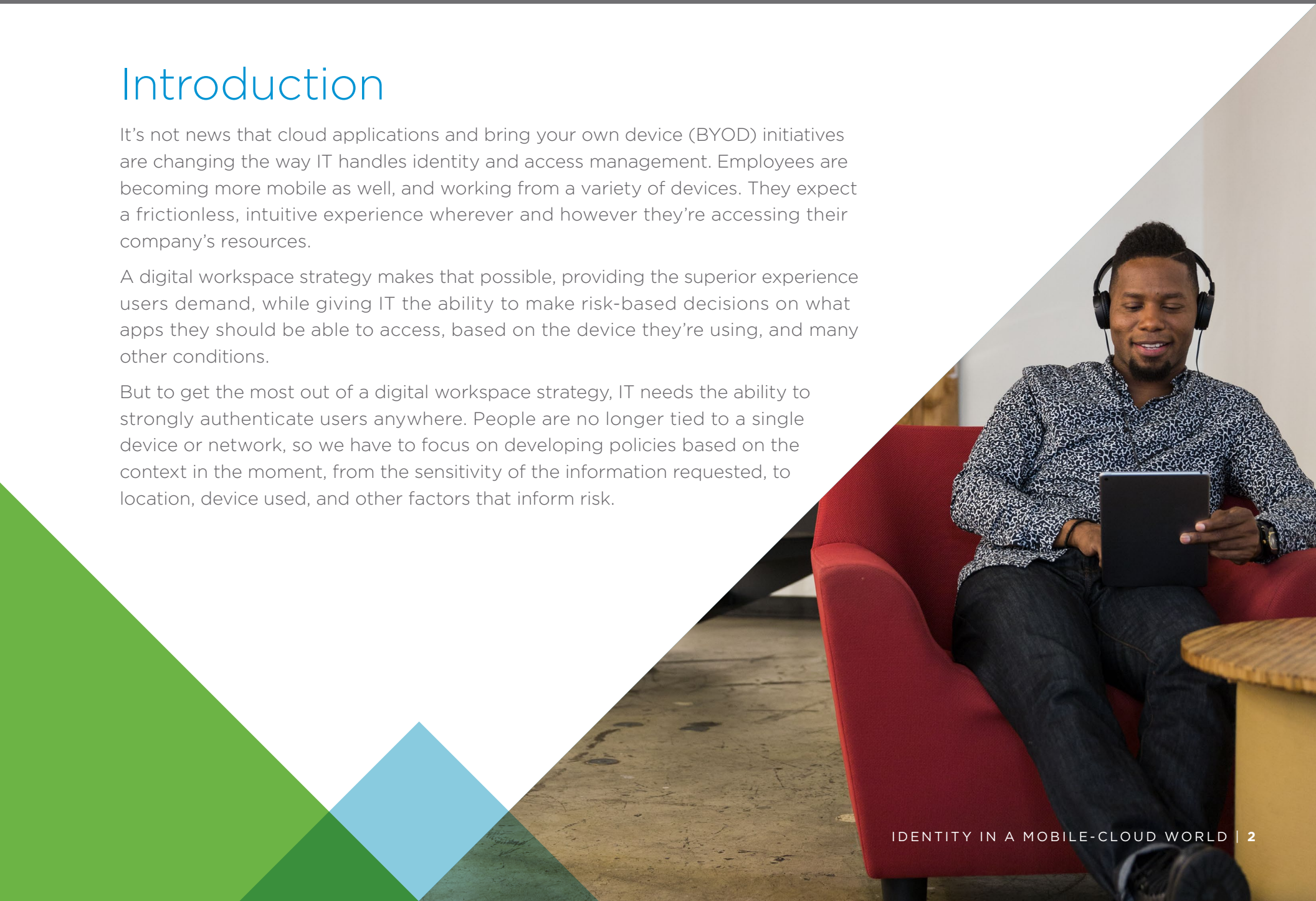
Virtual Systems

Introduction

It's not news that cloud applications and bring your own device (BYOD) initiatives are changing the way IT handles identity and access management. Employees are becoming more mobile as well, and working from a variety of devices. They expect a frictionless, intuitive experience wherever and however they're accessing their company's resources.

A digital workspace strategy makes that possible, providing the superior experience users demand, while giving IT the ability to make risk-based decisions on what apps they should be able to access, based on the device they're using, and many other conditions.

But to get the most out of a digital workspace strategy, IT needs the ability to strongly authenticate users anywhere. People are no longer tied to a single device or network, so we have to focus on developing policies based on the context in the moment, from the sensitivity of the information requested, to location, device used, and other factors that inform risk.



Identity and Access Management Powers Security with Simplicity

As people use more and more devices and apps outside the traditional office space, it's more important than ever to truly trust and know who is accessing your sensitive company assets. Identity and access management is the key to enabling secure, mobile access for today's cloud-savvy users, without compromising security and compliance.

Identity and access management means knowing who you are, what you have access to, and being able to utilize what it knows about you, your device, and a host of other information necessary to grant, deny or provide limited access to corporate resources. Since end users are often tethered to their phones, identity and access management can leverage possession of a unique device and even an individual's fingerprint (or other biometrics) to provide stronger authentication. Mobile authentication technologies become new ways for users to prove they are who they claim to be, and enable broader enterprise security while enabling continued user simplicity.

Authentication

Common authentication issues that cause security problems include inherent weakness in passwords, the clunkiness and expense of hardware or software token-based two-factor authentication, and conflicts occurring from multiple user identities across multiple apps.

Governance

In a mobile-cloud world, the ability to accurately grant and revoke access is imperative. Timing is also critical in the rapidly moving world of business technology—how long do user updates, edits, and changes take? For example, can you immediately verify exactly what programs Bob had access to at 8:30 this morning?

Contextual Access

Once authenticated, IT can determine who you are and to which apps you have access. But further consideration still needs to be made regarding restricting access based on a host of conditions. In the mobile-cloud era, contextual access means application admittance is no longer all-in or all-out, but rather fluid and dynamic. Additionally, access needs to be monitored beyond the time of initial authentication, so IT can revoke or force a risk-based authentication as appropriate.

The multitude of apps and devices used to accomplish prime productivity, alongside the need for a credible way to continuously manage risk, leads directly to the need for a single platform that can capture detailed information for system monitoring while providing real time visibility via advanced analytics.

Single Sign-On Transforms the Mobile Experience

The old system of identity involved individual accounts, and often, passwords written longhand and taped to a monitor for convenience. Many organizations have also invested in identity federation for on-premises enterprise applications using custom software pointing to complex directory infrastructure, but because of the cloud and mobile devices, there is now a tremendous increase in options and account types.

CONSIDER THE TYPICAL USER EXPERIENCE TODAY...	....COMPARED TO THE POSSIBILITIES THAT A DIGITAL WORKSPACE STRATEGY OFFERS
Download an app (such as Microsoft OneDrive) from the Apple App Store or Google Play. Launch it from your home screen.	More than simply a one-click login, SSO systems come in three forms:
Respond to the app's request for your email address, followed by a prompt to enter your username and password.	Enter the same username and password for every app, every time.
Type in an overly complicated password—including capital letters, numbers, and symbols. Receive error message that username and/or password is incorrect. Curse at app and re-enter aforementioned complex password.	-or-
	Enter your username and password once and launch multiple apps.
Verify using two-factor authentication. Realize you have to go into the other room where the alternate device with verification code is currently located.	-or-
Finally gain access to the app.	Username and password are irrelevant because your identity is established through a managed certificate and a minimum PIN code installed on your personal device.
Repeat process next time you have to access a different app.	

Identity can wholly change the mobile experience when the user doesn't have to remember and enter their username and password for as many apps as are installed. Instead, mobile identity federation can enable a single sign-on (SSO) system, enabling easy access to necessary programs.

With VMware Workspace ONE™, the device is provisioned with a secure cryptographic token in the form of a certificate to verify the user. After authentication, the system can decide whether or not the device is trusted based on compliance criteria from VMware AirWatch® Unified Endpoint Management™. If conditions are met, the Workspace ONE platform enables or denies access to the application.

This is a form of the patent-pending technology called "Secure App Token System" built for native iOS and Android devices that do not permit browsers to share information like cookies used in Windows and Mac OS. It enables a business to establish trust between a back-end cloud app (either internal or external) where application data lives, the device that the user possesses (whether corporate or personally owned), and the enterprise digital workspace solution (such as VMware Workspace ONE). Through a combination of tokens and certificate management, the digital workspace solution intercepts the authentication flow and provides the user with a one-touch single sign-on anchor via a unique certificate on their device.

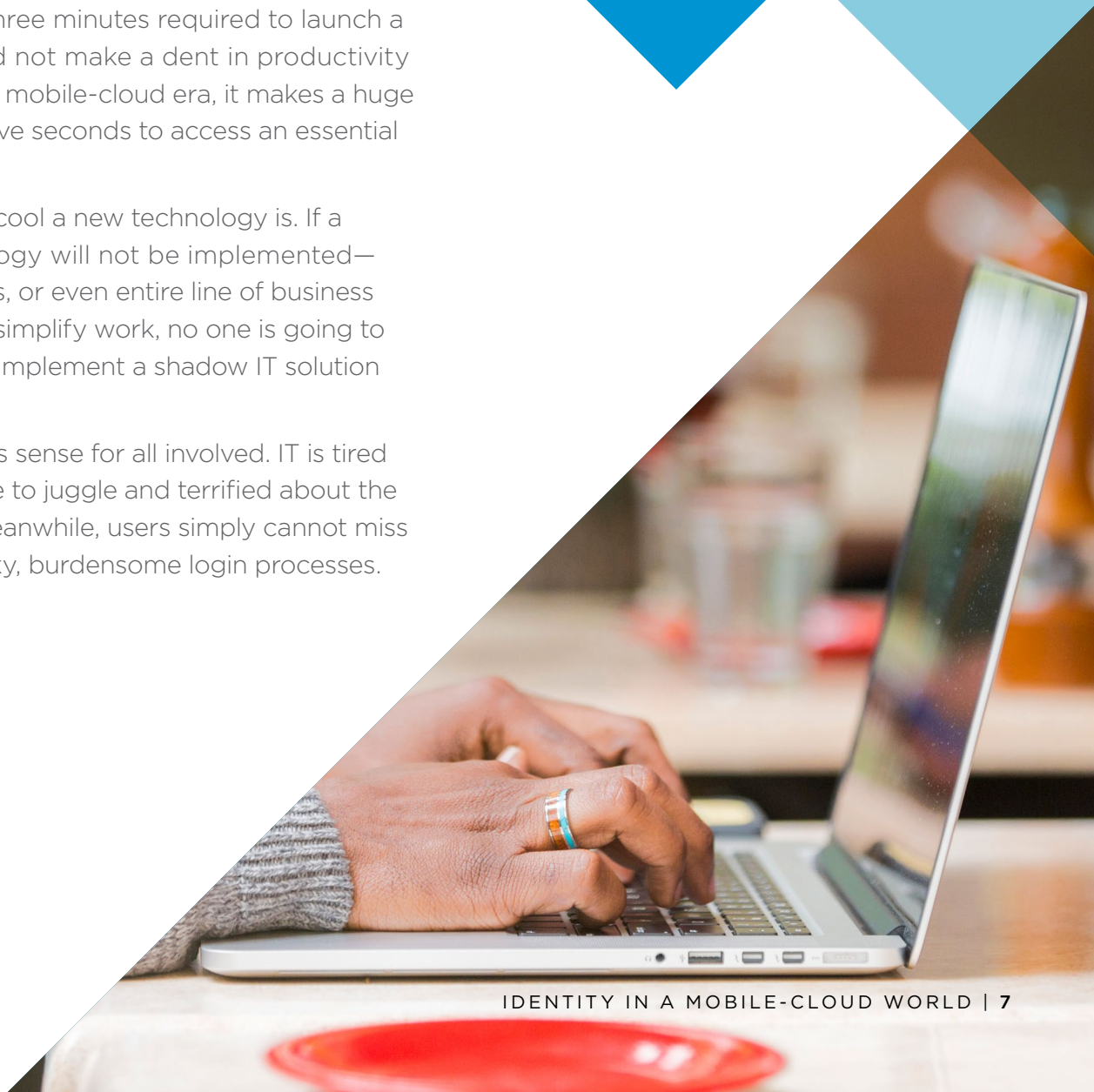
In short, it means that the end user is getting a much better experience than trying to negotiate a lengthy password with numbers and letters and characters. More importantly, that password can easily be spoofed. And anyone who has that password can use it on any device. The significance of certificates is that they are closely associated with their individual user, who may now be a simple PIN or biometric ID device unlock away from accessing an application, much like the ease of any consumer app.

Identity and access management—and SSO technology in particular—isn't new. It's actually been around quite a while. So why the sudden increase in interest?

During the days of the desktop era, the extra three minutes required to launch a corporate virtual private network (VPN) would not make a dent in productivity based on the scope of one's day. But in the new mobile-cloud era, it makes a huge difference in efficiency if it takes only an extra five seconds to access an essential task on one's device.

For enterprise IT, it's never really mattered how cool a new technology is. If a business is uneasy about security, the technology will not be implemented—regardless of end-user demands. For employees, or even entire line of business functions, if the technology IT provides doesn't simplify work, no one is going to use it. Or worse, they may even sidestep IT and implement a shadow IT solution that can introduce new security risks.

Modern identity and access management makes sense for all involved. IT is tired of resetting the many passwords end users have to juggle and terrified about the potential consequences of a security breach. Meanwhile, users simply cannot miss opportunities to be productive because of clunky, burdensome login processes.



Supporting Diverse Apps with Identity and Access Management

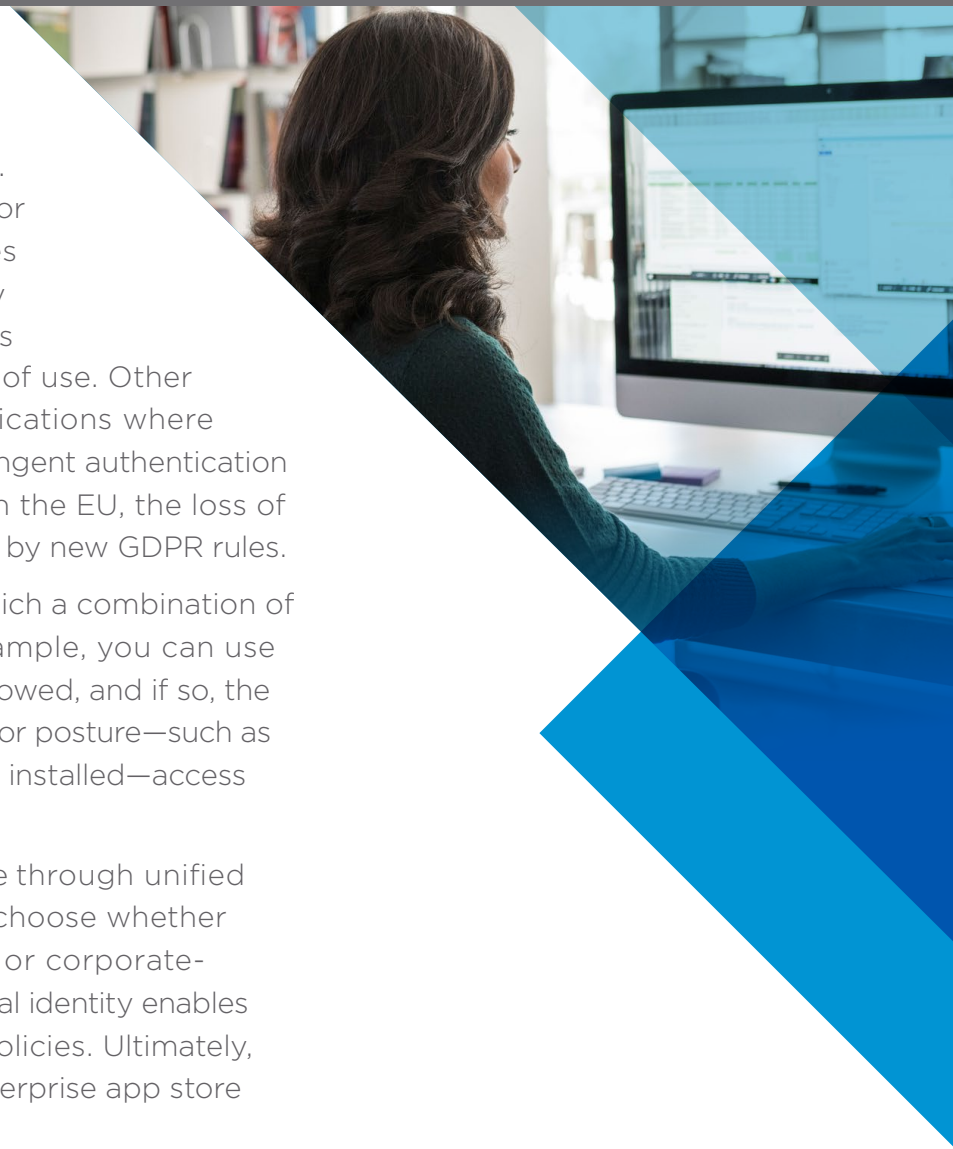
The tipping point for requiring an access management solution for web and mobile apps is when the organization begins to develop their own applications, or incorporate third-party applications that may have mixed architectures. What's driving identity and access management priorities?

Software-as-a-Service Apps Come of Age

There's been a tremendous interest in using access management to support moving to software as a service (SaaS) apps. Every application that gets put into the cloud has its own identity administration, access enforcement and reporting needs. When working with an amalgamation of endpoints that are mobile, non-mobile, and include native application architectures, you need an access management solution that can support native apps as well as traditional browser-based access, leveraging standards like SAML, or legacy apps that likely require a bridge from existing federation or password management solutions.

Users Are On the Move

App security is no longer simply about the user authentication. Organizations must now consider under which circumstances specific users should be granted access. Even once you're able to confirm who a user is, there may still be questions about things such as location—such as where information is being accessed in a hospital, or which country a sales director is visiting to meet with a client.



Different Apps Require Different Security

Some applications may not need to be restricted as much as others. For example, if you're on the road using an application like Concur for continuing expense management, you're constantly taking pictures of receipts to submit to accounting. In the case of such minimally sensitive information, the company wants the authentication process and policy rights as liberal as possible to enable the greatest ease of use. Other activities may be much more sensitive, such as ERP or CRM applications where customer information may be regulated, requiring much more stringent authentication management to minimize the possibility of data loss. For instance, in the EU, the loss of customer information could constitute a breach of privacy regulated by new GDPR rules.

A key feature of Workspace ONE is contextual access control, in which a combination of identity and device contexts are used to regulate access. For example, you can use network location or device type to determine if access should be allowed, and if so, the type of authentication to be used. Similarly, based on device context or posture—such as whether the device is managed or jailbroken or if a blacklisted app is installed—access to a particular app can be allowed or denied.

Additionally, with device awareness and control of compliance posture through unified endpoint management via VMware AirWatch, organizations can choose whether they wish to permit access on unmanaged, personally managed, or corporate-managed devices. Having awareness of both device posture and global identity enables IT to balance flexibility for end users with corporate compliance policies. Ultimately, this gives IT a choice to scale up or down the capabilities of the enterprise app store to best suit the needs of their business.

Give Users Freedom of Device Choice

Employees now expect to be productive anywhere, from any device. The innovation and ease-of-use found in consumer devices have outpaced the experience and equipment IT can provision within a traditional corporate-owned model. What IT needs and users expect is a scalable self-service model that enables users to get work done on the device of their choosing while maintaining enterprise standards for management and security.

Consider the experience of a new hire. Instead of having to trek to the IT department and dust off a refurbished laptop that is stacked up in the recesses of a closet (that may or may not have been imaged recently), the employee receives a drop-shipped device to bring with them—ready to work. Or, based on preference, they can simply use their own device by downloading the necessary IT-configured applications and using the provided user credentials.

It is important to note that there is a spectrum to this idea of managing a device. In some cases, it means that a user should be able to approach any machine—at home, at the neighbor's, at the library—and be able to navigate to a website, log in, and have some level of access. On the far end of that spectrum is a device that is completely supervised or locked down and owned by a corporate department. It may mean that a user has no administrative rights or ability to change any configuration on that device, because the enterprise wants to ensure the device always remains in a state of homeostasis. This approach has the potential of being the most secure, but it certainly doesn't leave a lot of room for user flexibility.

What's Key to an Effective Solution?

When it's time to make a decision about which identity and access management solution is right for you, consider whether it delivers the intuitive, frictionless experience your users want, together with the robust security and manageability IT requires.

SIX SOLUTION-CRITICAL CRITERIA

- ✓ Single sign-on
- ✓ Directory integration
- ✓ Multi-factor authentication
- ✓ Policy management
- ✓ Cross-device catalog and launcher
- ✓ Analytics/Reporting

AND DOES THE SOLUTION...

- Automate and streamline on-boarding and revocation?
- Increase productivity?
- Reduce complexity by being easy to use?
- Meet security and compliance requirements?
- Support any type of device and OS?
- Support any type of application?

Identity Access Management Layers

The Workspace ONE app gives employees instant access to their personalized enterprise app catalog. The built-in VMware Identity Manager™ offers a deep range of identity access management layers.

Build an App Catalog

- Install app directly onto springboard or access through responsive HTML5 app portal
- Auto-provisioning workflows

Federate User Identity

- SSO with domain login
- Permits strong authentication - provision and revokes access instantly

One-Touch Authentication

- No configuration or login required
- Leverage device ownership and unlock to establish authentication

Multi-Factor Authentication

- Strengthen security by employing multiple components to authenticate
- Support biometric or other multi-factor authentication methods for more sensitive applications

Conditional Access

- Managed or unmanaged devices, network scope, authentication strength
- Set policy levels by app

Conclusion

Identity and access management is about more than just proving you are who you claim to be. But from an enterprise perspective, management and access control perform a delicate balancing act between what employees will merely tolerate and what they will actually use.

Most enterprises have purchased SaaS services and mobile apps. Most of these live in "shadow IT," and some may even be integrated into the help desk ticket system for account creation and password resets. However, many enterprises are now reaching a breaking point. The need for mobile-cloud identity and access management becomes quite clear to IT when:

- They get to the fourth or fifth app and the tickets pile up
- There is a reported "breach" by an ex-employee who still has access
- The line of business pushes IT to simplify the user experience because mobile access is too cumbersome and yet mission critical

IDENTITY AND ACCESS MANAGEMENT

- **Empowers employees to be productive by removing the traditional barriers to mobility (VPNs, multiple passwords, tokens, and use of non-managed/non-domain-joined laptops and mobile devices).**
- **Increases security by strengthening authentication for apps beyond passwords while simplifying the user experience.**
- **Frees business to roll out new apps and services and grow confidently—both organically and inorganically—with the assurance that IT systems can immediately support new users.**

Ready to Learn More?

VMware Workspace ONE lets you unlock the potential of a digital workspace together with fully integrated identity and access management. It delivers the adaptive, conditional access you need to ensure the right level of security based on authentication strength, data sensitivity, user location, and device posture. By integrating identity and access management deep within the solution, Workspace ONE makes it easy for you to modernize your IT operations for the mobile cloud era.

Building out a complete digital workspace strategy is the key to managing user access from one place, enabling users to self-subscribe to apps they need, while IT builds centralized access policies based on user and device type.

At VMware, we reject the notion that security and usability are mutually exclusive. It is not user versus IT, but rather the joining of consumer-simplicity and enterprise-security within the digital workspace.

Try VMware Hands-on Labs for Simplifying App and Access Management

Join Us Online:

vmware® Virtual Systems

VMware, Inc. 3401 Hillview Avenue Palo Alto CA 94304 USA Tel 877-486-9273 Fax 650-427-5001 www.vmware.com