RSA

USER AUTHENTICATION TRENDS:

BLURRED BOUNDARIES AND NEW METHODS

BUSINESS-DRIVEN SECURITY™ SOLUTIONS

A CHANGING SECURITY LANDSCAPE

The landscape of user authentication is changing rapidly—and radically. A vanishing perimeter and the continuing explosion of cloud-based applications and mobile devices are blurring old boundaries around organizations and networks.

To keep up with the pace of change, lines of business are bypassing IT to deploy the applications they need to meet their business objectives—and in the process creating more islands of identity in a growing sea of shadow IT. And all of this is happening amid increasingly rigorous data protection regulation.

Yet how we access computers and networks hasn't changed much—passwords are still the dominant user authentication method, and more complex passwords do little to combat identity theft, which has become the number one attack vector: In 2017, 81% of hacking-related breaches leveraged stolen and/or weak passwords.[1]

Against this landscape, both IT and business face many challenges, and both require answers to a growing list of questions. This ebook is written to address several of today's most popular authentication questions:

- What's next for multi-factor authentication?
- Is single sign-on (SSO) like a house of cards ready to collapse?
- Will authentication standards accelerate adoption?
- Will biometrics (finally) live up to the hype?
- Will smartphones become the authentication method of choice?
- How will risk change the authentication game?
- And where will user authentication go from here?

[1] Verizon, *2017 Data Breach Investigations Report.*

WHAT'S NEXT FOR MULTI-FACTOR AUTHENTICATION?

Identity is today's most consequential attack vector. It's no surprise that the multi-factor authentication (MFA) market is rapidly expanding.

Vendors offer authentication methods ranging from traditional hardware tokens to risk-based techniques to support more users, devices and applications than ever before. In fact, 52% of American adults have used two-factor authentication.[2]

When it comes to MFA, one size does not fit all, and there looks to be room in the market for several options. With 44% of the world population owning smartphones,[3] it's no surprise that phone-as-a-token methods are becoming more popular, especially given increasingly flexible authentication choices. But traditional hardware tokens are still very much in demand. RSA, for example, has an active installed base of more than 50 million hardware token users, and Google recently introduced its Security Key hardware token.

MFA providers are also working to make authentication easier for users. End users have shown a willingness to switch service providers for more convenient authentication solutions. And while employees may be more of a captive audience, poor user access experience can limit business agility, reduce productivity, and damage morale.

[2] Pew Research Center, *Americans and Cybersecurity*, January 2017.

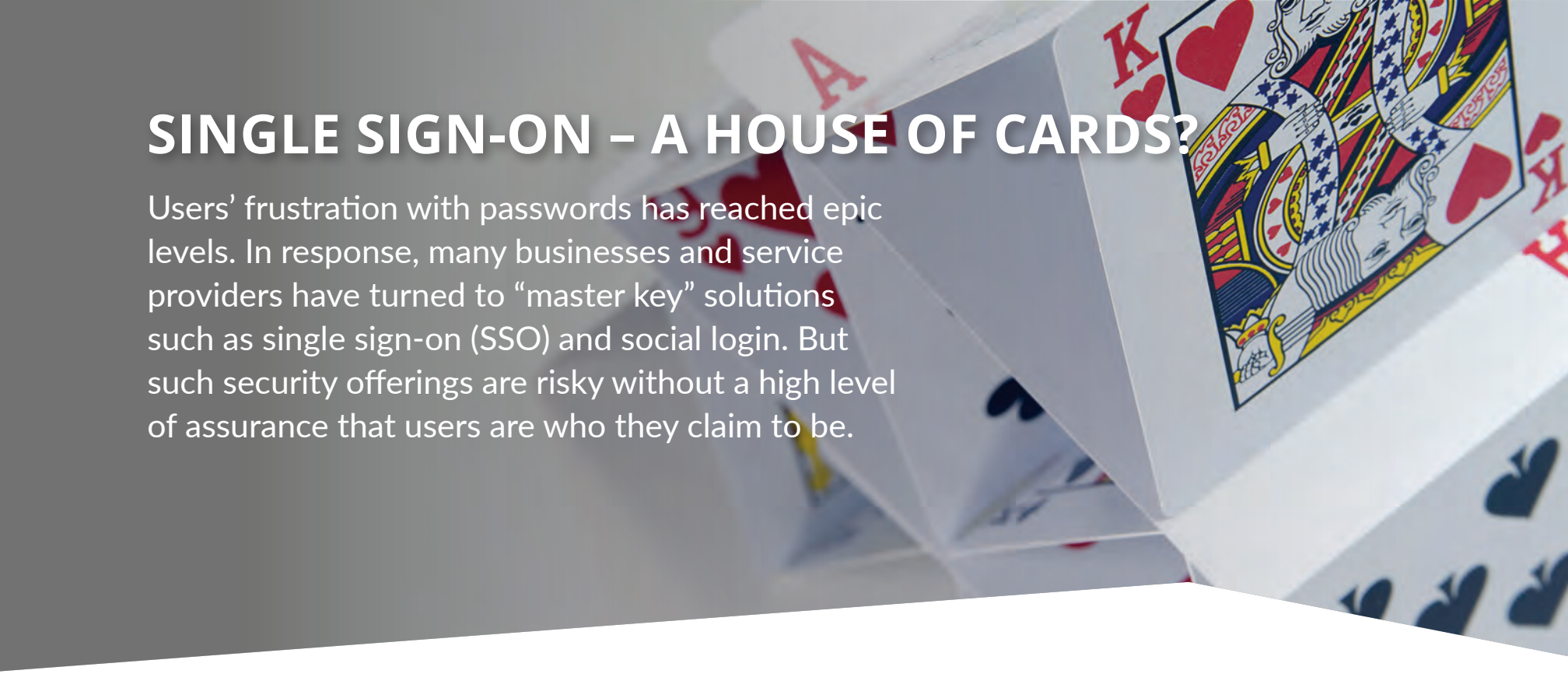
[3] Linda Sui, "44% of World Population will Own Smartphones in 2017," Strategy Analytics, December 2016.

THE MFA OUTLOOK

Most access or transaction requests are binary—users are in or they're out. With an expanding attack surface and the rise of increasingly sophisticated threats, such as spear phishing, organizations must factor in both context and risk when making access decisions. All MFA solutions are not created equal—be sure to choose a partner with deep expertise and an extensive track record. Moreover, look for solutions that certify interoperability with your on-premises and cloud applications, enable you to align identity assurance levels with risk, and give users the freedom to choose from a variety of easy-to-use authentication methods.

SINGLE SIGN-ON – A HOUSE OF CARDS?

Users' frustration with passwords has reached epic levels. In response, many businesses and service providers have turned to "master key" solutions such as single sign-on (SSO) and social login. But such security offerings are risky without a high level of assurance that users are who they claim to be.



Social login, using identities from social media sites such as Facebook and LinkedIn, is a well-established practice for providing low-risk access to consumer websites. At the corporate level, where identity proofing is much more comprehensive, and therefore more trustworthy, organizations tend to shy away from trusting such sites as identity providers.

Meanwhile, SSO adoption has kept pace with rapid growth in cloud apps and user mobility. Employees need to remember only one password, while IT gets centralized user access and increased visibility. But despite the user experience and cost savings benefits, a single password creates a single point of failure—and can expose organizations to a high level of risk.

This vulnerability hasn't gone unnoticed. Assuming similar effort, why would hackers go after a password to a single application when they can instead compromise dozens of accounts? Even well-respected SSO providers have been attacked, and there's no reason to believe such threats will abate.

In light of this reality, many organizations that use SSO are looking to reinforce access controls through MFA. Their best bet: best-of-breed solutions that cover all on-premises and cloud applications—and that won't negate the usability benefits of SSO.

THE SSO OUTLOOK

User experience is paramount in an SSO environment, and risks associated with a single point of failure are high. Expect to see SSO providers partnering with security and authentication specialists, increasing security and transparency with advanced analytics. With cloud and mobile services the new norm, organizations will expect mobile apps to share desktop's SSO capabilities. Emerging standards such as OAuth2 combined with Proof Key for Code Exchange (PKCE) should add a level of maturity to how users connect to native mobile applications.

WILL AUTHENTICATION STANDARDS ACCELERATE ADOPTION?

With identity being the number one attack vector, the need for multi-factor authentication has become ubiquitous—and demand for open industry standards is growing. The goal: ensure system interoperability while providing a common framework for users, applications and devices that can help accelerate technologies toward mainstream adoption.

With "something more than a password" the new default access choice, it's critical that strong credentials can be easily used across multiple systems and an increasingly diverse set of devices. Users expect seamless interoperability; if they don't get it, they'll switch service providers or circumvent IT. To ensure both security and service, providers and organizations need to offer a common MFA login experience across web, cloud, mobile and on-premises applications.

Several open industry standards and protocols are working to make interoperability a reality in user authentication:

OpenID Connect is an interoperable authentication protocol that enables apps and services to authenticate users without having to store or manage passwords.

FIDO (Fast IDentity Online) Alliance addresses lack of interoperability among strong authentication solutions and helps eliminate user password fatigue.

The World Wide Web Consortium (W3C) is an international community that develops open Web standards for enabling online services to create and use strong authentication.

NIST's Strength of Function for Authenticators (SOFA) initiative helps compare the security strength of two-factor and multi-factor authentication technologies.

THE OPEN STANDARDS OUTLOOK

There's no guarantee that open user authentication standards will be adopted on a wide scale. To succeed, they must provide clear and compelling benefits for end user organizations. In the meantime, reducing reliance on passwords, making phishing and other man-in-the-middle attacks more difficult for the bad guys, and increasing identity confidence are excellent reasons to rethink your authentication strategy.

WILL BIOMETRICS (FINALLY) LIVE UP TO THE HYPE?

Biometric user authentication has long been seen as a panacea. Its benefits are evident: a unique biological or behavioral trait, nothing extra to carry or remember, and more individual accountability.

But cost, complexity and spoofing concerns have often derailed adoption, and despite several large-scale consumer rollouts (including those from Aadhaar in India and Wells Fargo and USAA in the U.S.), adoption within the enterprise has been negligible.

With a maturing ecosystem of billons of biometric-ready smartphones, will 2018 finally be the year of biometrics? Android, Windows and iOS smartphones use biometric fingerprint sensors, and more and more consumers have embraced biometric modalities, trading privacy concerns for a more convenient user experience.

Open standards such as FIDO Alliance and SOFA-B (see page 7) aim to further adoption, enabling an interoperable ecosystem of biometrics-based authenticators for use across apps and websites. Within corporate environments, Microsoft's Windows Hello is paving the way with native support for biometric authentication to Windows 10 workstations and Active Directory (AD).

THE BIOMETRICS OUTLOOK

Even as the stars align for enterprise-level biometric authentication, several obstacles remain. Unlike passwords or tokens, biometric authentication is probabilistic, not deterministic—a "live sample" must meet a threshold that balances UX with security. And while fingerprint has been the modality of choice, up to 15% of users experience problems with it. However, in many cases the benefits unique to biometrics will outweigh the risks and frustrations. Look for more organizations to adopt biometrics as part of a layered authentication approach, combined with multi-factor and risk-based authentication methods for higher levels of identity assurance.

WILL SMARTPHONES BECOME THE TOKEN OF CHOICE?

With more than three billion smartphones in use today, it's well past time to know which we can trust and which are suspect. Mobile devices have become the new network perimeter; IT and security pros must be able to validate and trust devices with direct access to their systems and data.

Hardware-based security is a key ingredient in determining whether a mobile device is trustworthy. However, past initiatives such as Trusted Platform Modules (TPMs) and Intel Trusted Execution Technology (TXT) were seen as overkill and failed to gain meaningful adoption.

Fast-forward less than a decade, and phone-as-a-token authentication is becoming more popular. Current smartphones support secure processing of biometric data in hardware, providing tighter binding between user and device. But even as we confirm that John is in possession of John's phone, how do we know that said phone can be trusted? For a device to "attest" that it hasn't been compromised (and meets minimum security requirements), it needs capabilities at the hardware/firmware level—which are dependent on the device manufacturers.

We're getting there. Many smartphones now include hardware or firmware for strong protection of secrets and for measuring the integrity of their respective operating systems. Windows 10 Mobile uses TPMs for protected key storage and trusted boot, Apple has a "Secure Enclave" for secure data protection, and Samsung takes advantage of Qualcomm chipsets to establish a hardware root-of-trust via Samsung Knox.

THE DEVICE OUTLOOK

Devices are poised to play an increasingly important role in authentication. With cybersecurity defenses shifting toward automated and integrated models, application-to-application and machine-to-machine authentication will become more common, independent of any user. And as advanced analytics drive authentication to evolve from fixed to continuous, the need to trust device fingerprints will escalate. It's incumbent upon handset manufacturers to establish a verifiable ID, so that application and service providers can extend levels of trust to a device and its associated applications.

HOW WILL RISK CHANGE THE AUTHENTICATION GAME?

In today's evolving threat landscape, user authentication is moving from a fixed event to a dynamic, continuous one that factors in both context and risk. Meanwhile, advanced analytics enable increasingly sophisticated identity and access management (IAM) decisions while minimizing tradeoffs between security and convenience.

This evolution in strong authentication is being driven by three primary needs: to provide a less abrasive login experience for users, to protect access for an exponentially larger number of users (due to the rise of cloud and mobile apps), and to combat sophisticated phishing and pharming attacks, which continue to plague corporate IT departments at alarming rates.

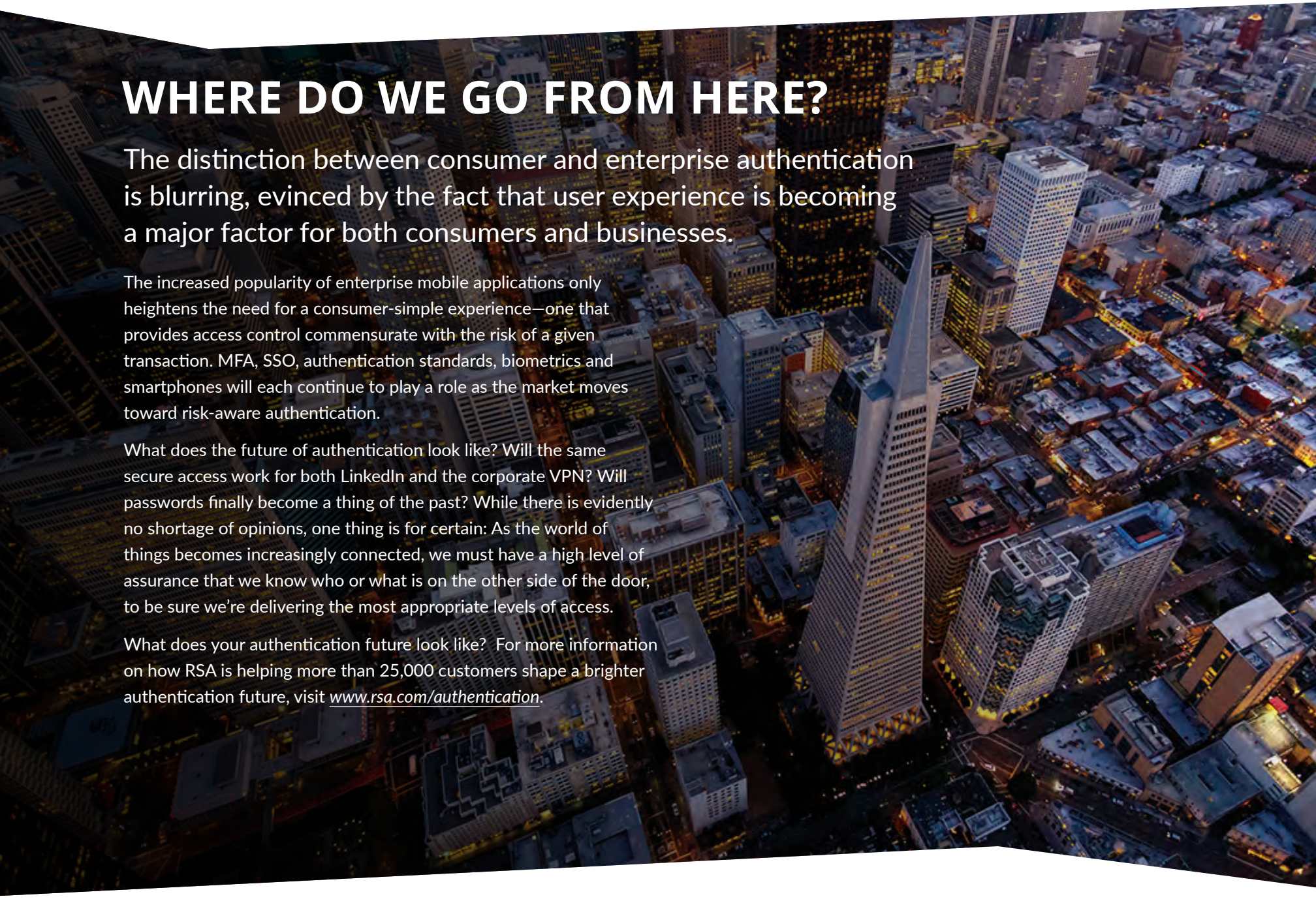
The concept of analytics for adaptive techniques isn't new. The retail banking sector has been using online fraud detection (OFD) tools for years, though aimed at financial fraud rather than authentication. Other corporate-level initiatives have used static rules such as IP address or whether a phone is under management. While such approaches were a step in the right direction, they omitted many risk factors, took too long to create new policies based on incidents, and had to be manually configured and maintained.

Another frontier: Advances in artificial intelligence have given us machine learning—a way to develop algorithms that draw inferences from data, then apply those learnings to new data sets to predict outcomes. With machine learning, user authentication systems can now apply user behavior and threat intelligence in near real time, supporting better decisions about current access requests and automatically adjusting or creating policies for the future. Since machine learning works in the background and is transparent to users, it can dramatically reduce user friction when accessing sensitive systems, applications and data.

THE AUTHENTICATION OUTLOOK

Any modern authentication solution must not only comb through data, but also interpret it and learn from the results, assessing complex scenarios and improving decision making without human intervention.

"Risk-based" has become the catchphrase du jour in the identity market, with virtually every provider taking a contextual/risk approach to IAM. But just as not all MFA solutions are created equal, risk-based authentication solutions vary widely in both capabilities and maturity. The security community must work to clear up the confusion—increasing visibility into offerings, showing how approaches differ, and offering guidance on how to choose the best one for your organization.



WHERE DO WE GO FROM HERE?

The distinction between consumer and enterprise authentication is blurring, evinced by the fact that user experience is becoming a major factor for both consumers and businesses.

The increased popularity of enterprise mobile applications only heightens the need for a consumer-simple experience—one that provides access control commensurate with the risk of a given transaction. MFA, SSO, authentication standards, biometrics and smartphones will each continue to play a role as the market moves toward risk-aware authentication.

What does the future of authentication look like? Will the same secure access work for both LinkedIn and the corporate VPN? Will passwords finally become a thing of the past? While there is evidently no shortage of opinions, one thing is for certain: As the world of things becomes increasingly connected, we must have a high level of assurance that we know who or what is on the other side of the door, to be sure we're delivering the most appropriate levels of access.

What does your authentication future look like? For more information on how RSA is helping more than 25,000 customers shape a brighter authentication future, visit *www.rsa.com/authentication*.

ABOUT RSA

RSA offers Business-Driven Security™ solutions that uniquely link business context with security incidents to help organizations manage risk and protect what matters most. RSA solutions are designed to effectively detect and respond to advanced attacks; manage user identities and access; and reduce business risk, fraud and cybercrime. RSA protects millions of users around the world and helps more than 90% of Fortune 500 companies thrive in an uncertain, high-risk world. For more information, go to *rsa.com/authent cat on*.