SecurID™

2022
Ten Trends Defining Cybersecurity in the Year of Identity

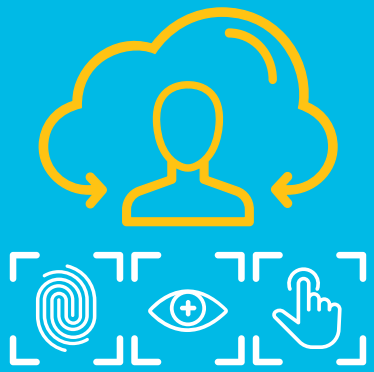
2022 began with remote and hybrid work continuing to shape how organizations do business; ransomware and other attacks doing more damage than ever; and business users and consumers alike demanding digital access that's easy, convenient—and secure.

The common denominator for cybersecurity in these challenging circumstances? Identity.

In a time when businesses must operate without a protective perimeter, when the stakes for protecting private data and intellectual property have never been higher, and when users are growing increasingly impatient with cumbersome access, identity has become central to how organizations secure their resources and enable their users.

On the following pages, we share ten trends that illustrate the ways in which identity both reflects and defines cybersecurity today. Read on to learn more about the challenges and opportunities in identity—and, by extension, cybersecurity—that are top of mind for 2022.

1 The Staying Power of Zero Trust



Prior to the pandemic, zero trust was often dismissed as hype. But that's changing, especially as organizations rely more on mobile connectivity, cloud operations and other security-sensitive ways of working. Zero trust—built largely on multi-factor authentication, governance processes and other identity-centric measures—is increasingly becoming accepted as a powerful means to a secure end.

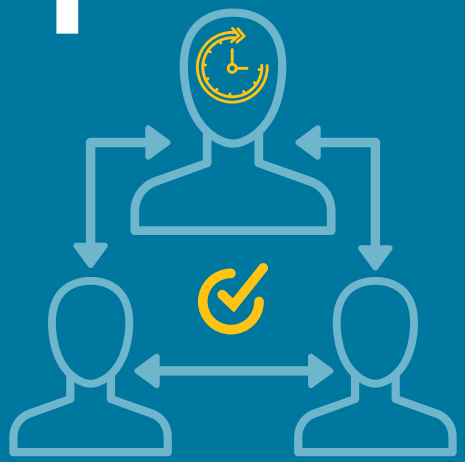
2 Toward a Passwordless Utopia

As long as passwords are hard for users to remember and easy for hackers to guess, they're going to continue to present a significant obstacle to secure access. Today, two forces are tipping the balance toward passwordless methods: business users and consumers who are less willing to accept inconvenience, and cybercriminals who keep finding more ways to abuse credentials.

3 MFA: From How-To-Do-It to How-To-Do-It-Better

After years of spreading the word about how to use multi-factor authentication to achieve secure, convenient access, we're now seeing MFA become even better established (and in some cases, required), with widespread acceptance of methods like push-to-approve, FIDO and biometrics. As a result, the focus is shifting to easy and secure rollouts for organizations, and increased convenience for business users and consumers.

4 Easy, Flexible, Agile Everything



No one wants to compromise online privacy and security, but everyone's patience with complex, time-consuming security requirements is wearing thin. Business users and consumers today are continuing to embrace passwordless and other ways to speed and simplify authentication, while organizations are looking to technology that helps streamline identity governance and compliance-related processes.

5 Mobile and Cloud: Growing Targets for Cybercrime

Organizations are moving more operations to the cloud, and people are relying more than ever on mobile devices for just about everything they do. That makes both those platforms increasingly attractive to cybercriminals—and underscores the need for organizations to prioritize investments in modern authentication, cloud infrastructure entitlements management (CIEM) and other capabilities to help manage cloud and mobile risk.

6 Locking Down Unstructured Data

Intellectual property is often stored in the form of unstructured data, which is hard to secure. Is it any surprise, then, that IP has become an especially enticing target for cyber attackers? Now more than ever, organizations benefit from employing data access governance, which provides the visibility into unstructured data needed to help stop IP exfiltration by bad actors.

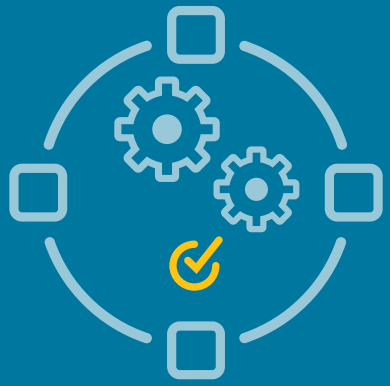
7 Around the World, Privacy Rules

Concerns about data privacy have not diminished since the adoption of the EU General Data Protection Regulation (GDPR) in 2016; if anything, they've accelerated. In Brazil, for example, where the General Data Protection Law (LGPD) recently went into effect, companies are exploring social logins, location-based authentication and other indirect ways of authenticating to address consumer data privacy concerns and comply with the new law.

8 Blockchain Finally Breaks Through. Or Not.

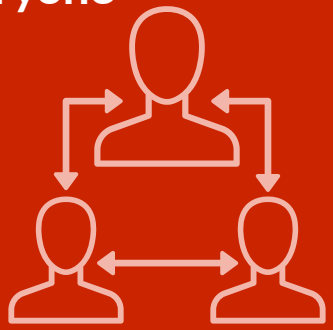
In the evolution of identity, 2022 is the year blockchain will be a resounding success—or a continuing disappointment, depending on how you look at it. Some see promise in blockchain as an enabler of secure digital identity; others anticipate privacy and data security problems with its use in authentication. Consider the challenges and opportunities—and keep an eye on this one.

9 Managed Services: More, Please



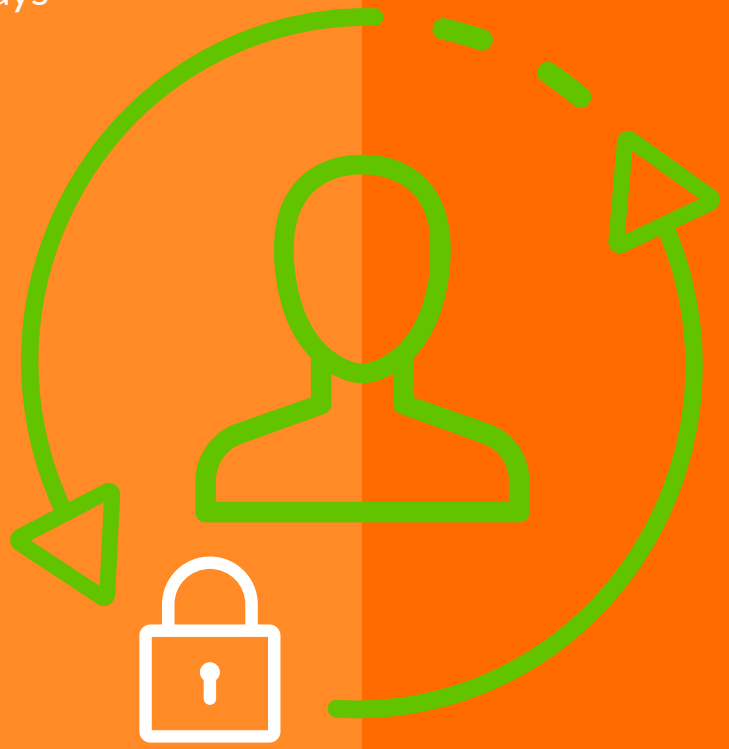
Identity governance and administration gives organizations of all sizes visibility into access and helps them fulfill regulatory obligations more easily. But for small and midsize organizations, the operational requirements to establish IGA may be more than they can reasonably take on. The result? Wider adoption of **managed services** offerings that let them reap the rewards of a mature IGA program without overcommitting their resources.

10 Welcome to the Age of Business-To-Everything-and-Everyone



Business-to-business, business-to-consumer, business-to-employee—after years of distinctions among use cases for authentication, we are now seeing a convergence in which one platform is configured to meet different needs. It's a perhaps long-overdue streamlining that recognizes the essential common thread underlying all markets, even if there are differences in specific capabilities and how they're delivered.

Here's to 2022 and the role identity will continue to play in delivering secure, convenient access, no matter what changes come. As your organization looks for new ways to seize opportunities and tackle challenges in the digital world, SecurID is here to help.



About SecurID

SecurID, an RSA business, is the trusted identity platform for 13,000 organizations around the world, managing 50 million identities and providing secure, convenient access to 30 million users. SecurID empowers organizations to thrive in a digital world, with complete capabilities for modern authentication, lifecycle management and identity governance. Whether in the cloud or on-premises, SecurID connects people with the digital resources they depend on everywhere they live, work and play. For more information, go to **securid.com.**

SecurID™
An RSA Business