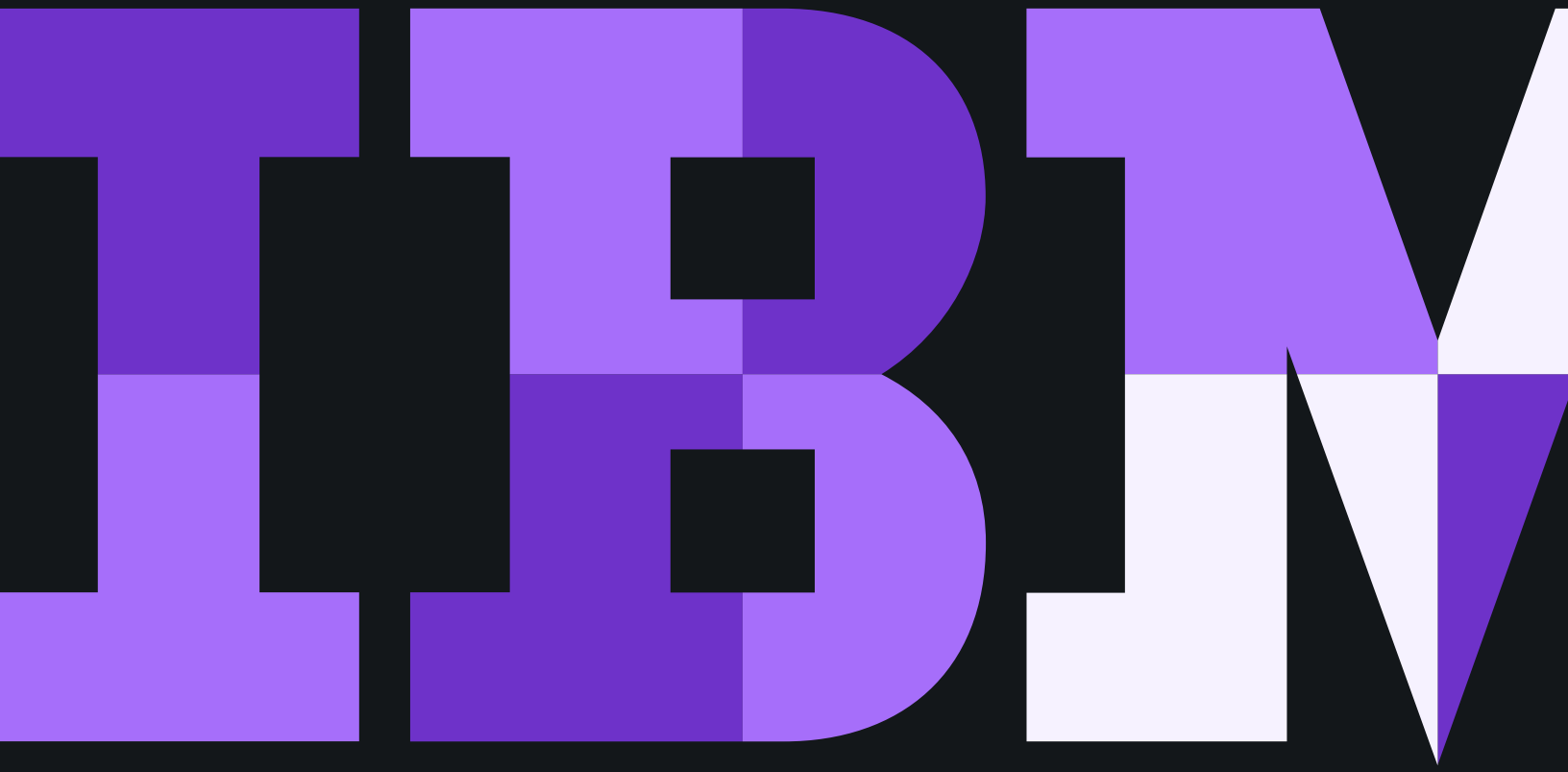
IBM Security

January 2020

Building digital trust into better experiences

Unlock revenue opportunities through seamless, secure digital trust



IBM

Contents

3 Creating trust in a digital world

3 Unlocking context to establish trust

4 Aligning enterprise security around trust

5 Keeping your business safe

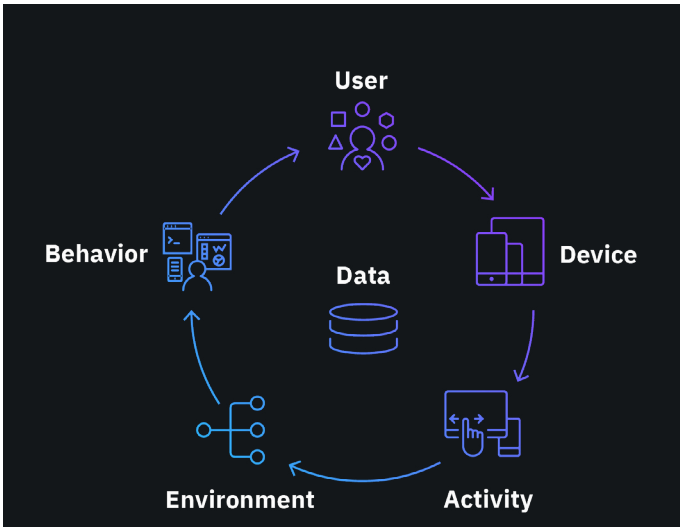
6 Driving digital transformation through a foundation of trust

7 Security can unlock opportunity

Creating trust in a digital world

As human beings, we rely on our senses, memory and intelligence to establish trust. But what happens when those tools are taken away? In the digital world, a complex set of information, identification and security tools are needed to establish trust.

Digital trust is an alignment of privacy controls and privileges that occurs when the right user has the right access to the right data for the right reason and the right purpose. The benefits of digital trust extend beyond security. When implemented thoughtfully, seamlessly and with the user experience in mind, digital trust can deliver better engagement that unlocks higher productivity and more opportunities for revenue growth.



Gain the context needed to analyze risk and establish digital trust

Unlocking context to establish trust

You have a mandate from customers to protect their personal information. Moreover, as a security professional, you've been entrusted to protect your business. There are privacy and compliance requirements to consider, business changes to navigate around and, in the midst of it all, increasingly sophisticated cyberattacks emanating from a global community of fraudsters. Yet users still expect security mechanisms that are seamless and simple.

In the past, your business may have looked primarily to identity and access management (IAM) solutions to build trust. **But digital trust is more than establishing identity. It's a combination of analysis and understanding that layers contextual insights on top of identity** by considering:

- The user and their unique attributes
- The device and endpoint-specific authentication such as digital fingerprinting
- The activity as it relates to the data, application and user
- The user's environment as well as the network environment
- The user's behavior as determined by usage analysis.

Aligning enterprise security around trust

Just like any relationship, digital relationships are comprised of many small interactions over time. Together, these interactions provide a cumulative insight into who we are: our behaviors, interests, responsibilities and roles. In a digital world, however, companies need to continually test and validate those relationships as individuals move between devices, networks, applications and channels. This can create friction when users are repeatedly prompted for passwords, additional authentication steps and, sometimes, denied legitimate access to applications.

The goal of digital trust should be to create a secure, frictionless experience for users. To achieve this, organizations need to combine the right security technologies and processes to automate trust mechanisms rather than rely on manual controls. For example, replacing a password for each application with single sign-on or using advanced analytics to initiate step-up authentication are effective ways to turn on security controls without turning off users.

Achieve silent security with IBM Security Identity & Access Management

As a business, you need to ensure that the right people have the right access to data at the right time. Do the right thing for your employees with IBM Identity & Access Management.

Watch video

The right digital trust framework leverages advanced technology such as AI-infused fraud detection, strong and seamless identity and access management, data security with an integrated suite of capabilities and mobile security with unified, multidevice management. When combined, these technologies can help your business:

- Extend security and identity seamlessly between on-premise and cloud-based systems
- Bridge legacy and new technologies together to create a shared foundation of trust
- Reduce security costs and streamline security processes across the organization
- Provide cross-functional visibility to security teams so they can truly work as a team

IBM Security helps businesses create a world-class digital trust platform with our solutions and services. We offer IBM Security Guardium to protect data and ensure compliance, IBM Security Identity & Access Management to efficiently manage identities and validate user behavior and IBM Security MaaS360 to manage mobile security across the enterprise and beyond.

Keeping your business safe

You've spent years building trust with your customers, and you want to maintain that trust. Meeting compliance requirements and preventing fraud can do more than protect your reputation — it can improve your bottom line. You can strengthen security and simplify log-in and authentication processes, all while navigating within the confines of privacy, consent and compliance. By leveraging advanced technologies such as artificial intelligence and behavioral analytics, you can equip silent mechanisms for establishing digital trust.

Because identities are constantly on the move between locations, devices and apps, security controls need to be agile and invisible. This agile, invisible security can take a variety of forms, including:

- Easy-to-implement single and multifactor authentication controls that support seamless experiences
- Strong step-up authentication mechanisms that activate only for at-risk users
- Single sign-on screens and unified application launchpads that simplify access across devices and between applications

IBM Security can protect your business while preserving great user experiences. IBM Security services can help you identify, classify and protect critical data. IBM Security Guardium monitors user activity and alerts security teams to unauthorized access, while guarding your data through security controls such as encryption, masking and tokenization. IBM Security Identity & Access Management supports regulatory compliance (FFIEC, 2FA, PSD2, etc.), centrally manages access certifications, simplifies onboarding and exiting, and prepares your business to adapt to new regulatory requirements as they arise. IBM Security Trusteer delivers advanced fraud protection using AI and data consortiums to track trends in the fraud landscape across different organizations, then shares that data to protect and set up lines of defense.

Get smarter data protection with IBM Security Guardium

Smart data protection sees with insight, automates with purpose and scales as you innovate. Learn how IBM Security Guardium can protect your world.

Watch video

IBM Security Guardium monitors user activity and alerts security teams to unauthorized access

Driving digital transformation through a foundation of trust

The drive toward digital transformation is led by the promise of innovation, efficiency and richer experiences. Implicit in that promise is the existence of security and trust. **Companies that successfully deliver secure, seamless digital experiences will win in the digital marketplace, whether it's in the form of higher employee productivity or higher customer loyalty**. Similarly, those companies that fail to align their security mechanisms with user expectations will find that transformation plagued by growing pains.

What do digital users expect? Security with simplicity. They want the protection of multifactor authentication without the manual work of authenticating themselves multiple times. They want self-help tools that are simple to use, whether they've lost a wallet or simply lost a password. And they want their identity to move seamlessly with them across devices and applications.

IBM Security can help you build that digital foundation of trust. IBM Security Identity & Access Management delivers secure single sign-on so users can log in once to applications without repeated password prompts. IBM Security MaaS360 gives users the freedom to access applications from anywhere without sacrificing security. IBM Security Trusteer protects against fraud while providing seamless onboarding and login that intelligently activates step-up authentication only when risk factors are present.

Create digital identity trust with IBM Security Trusteer

With IBM Security Trusteer, your customers can bring their identities and trusted relationships with them on their digital journey with your business.

Watch video

Security can unlock opportunity

The right approach to digital trust looks beyond security to see the opportunity that lies in building better user experiences. In the past, security in the form of lengthy registrations and multiple password prompts was viewed by users as a barrier to better experiences. What users really want are security mechanisms that happen behind the scenes, whether it's a digital identity that follows them across devices, or discreet behavioral analytics that screen for subtle anomalies, like how a user is holding their device.

Think of how digital trust is established today. In many cases, the burden of proof is on the user. **They enter a password, enter a code, respond to a prompt, etc. But imagine a different experience, where passwords are replaced by silent authentication that happens automatically as part of a broader fabric of contextual trust** — one that the user never touches and never sees. Instead of presenting the same trust challenges to every user, only the small percentage of users who present risk would be challenged. Data would still be protected, accounts secured and trust established, but without the negative experience of treating every user as a potential threat.

What users really want are security mechanisms that happen behind the scenes

Businesses that get digital trust right have the potential to create stronger, longer and more profitable relationships with their users.

IBM Security's digital trust solutions can help you create those trusted relationships and extend them seamlessly across devices and applications. IBM Security delivers a complete digital trust solution that combines data discovery, data protection, identity and access management, authentication, risk management, fraud detection and global threat intelligence, featuring:

IBM Security Trusteer — cloud intelligence, AI and machine learning combine to help deliver continuous digital identity assurance with seamless authentication and powerful fraud detection

IBM Security MaaS360 — an AI-powered solution for unified endpoint management delivered in the cloud and designed to protect data, support privacy and compliance and deliver secure, seamless mobile experiences

IBM Security Guardium — a complete protection platform that analyzes privacy and compliance risks, protects your data and continuously monitors for vulnerabilities

IBM Security Identity & Access Management — deliver silent security with behind-the-scenes identity and access management features that include single sign-on, multifactor authentication and access control

IBM **Security**

IBM Global Services
Route 100
Somers, NY 10589
U.S.A.

Produced in the United States of America
January 2020

WAGXLGAJ