IBM Security

August 2020

Authenticate consumer and employee digital identities seamlessly

Transform your IAM program with identity-as-a-service

Contents

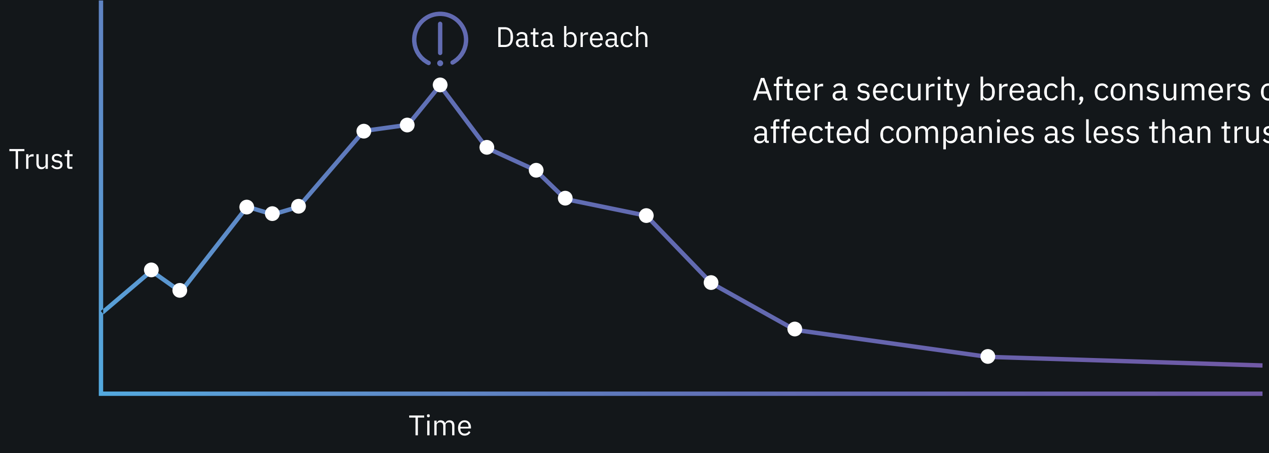
Validating user identities

"Securing identity online" is a phrase heard time and time again in the technology industry. Most organizations have implemented automated measures to validate user identities and protect their critical assets from attack. Yet many organizations still experience breaches or at the very least lack internal efficiency, which begs the question: What's missing?

Digital identity-related breaches are a top driver of consumer data loss, including personal information and financial loss, and internal company data loss, such as access to records and internal controls. The average cost of a data breach is $3.86 million, taking an average of 280 days to identify and contain.[1] Companies that are breached don't just lose data, they can lose public trust. After a security breach, consumers often view affected companies as less than trustworthy, which can lead to business loss.

As more companies migrate to the cloud, companies search for security measures to authorize and authenticate internal and external users, but they do not want to negatively impact the user journey with troublesome authentication methods.

Identity-as-a-service is expected to grow at a compound annual rate of 14.1% over the next few years as more businesses look to reap the benefits of cloud computing.[2] The goal for companies is to validate the identities of both consumers and employees from the cloud, but in a seamless and painless manner for users.



After a security breach, consumers often view affected companies as less than trustworthy.

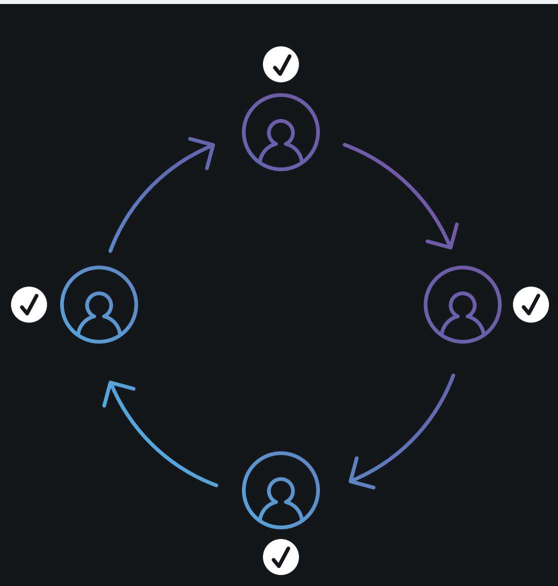
Secured and seamless made simple

Organizations today aim to implement zero trust strategies with identity as a central pillar. These implementations need to have secure processes while simultaneously offering all users a frictionless, productive experience. To provide these experiences, organizations should:

Confirm identities using context
Companies must be able to confirm and authorize all users logging in and provide continuous authentication throughout the user journey. They must be able to correctly and discreetly identify users without negatively impacting the user experience by implementing risk-based authentication.

Monitor authentication events
Identifying suspicious patterns of behavior is now a major challenge in the industry. To diagnose a fraudulent user, organizations need insight into all user activity as well as the ability to identify when unusual user behavior occurs and automatically take action.

Enforce security across digital platforms
Organizations are increasing mobile usage every day. As a result, more and more mobile devices need extended protection across applications, IoT and unified endpoint management. Companies are faced with the challenge of addressing growing mobile usage that requires digital identity enforcement and protection anywhere.



Companies must be able to confirm and seamlessly authorize all users logging in and provide continuous authentication throughout the user journey.

IBM Security Verify helps organizations deliver fast, secured access to business applications. See how IBM’s IDaaS technology connects users and apps in this two-minute video.

Watch video

Taking the pain out of passwords

Securing a user’s digital identity — whether an internal employee, partner or customer — is a challenge for businesses. **Customers in particular want to make sure their digital identities are secure when using any application, but they also want an easy-to-use, painless experience.**

Complex security measures

Security is key for customers to trust any organization. Users, however, do not want to see or interact with complex security measures — they expect that the security part of applications will run in the background and not be an inconvenience.

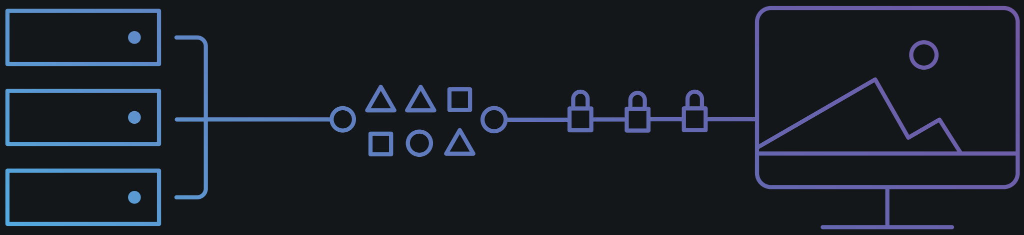
Keeping track of multiple usernames and passwords

Customers are faced with the challenge of remembering multiple usernames and passwords for each application they use. Each application that needs a separate set of log-in credentials serves as a negative blocker for the user.

Establish progressive trust

Users want a streamlined process, but they also do not want to provide more personal data than necessary. They expect to provide an appropriate level of data based on the transaction at hand, with the organization progressively learning more about a user throughout their journey.

Users expect that the security part of applications will run in the background and not be an inconvenience.



What to look for in an identity and access management solution

For seamless and secured IAM, confirm that your approach offers the following:

Single sign-on (SSO) options

– Eliminate username and password hassles with the ability to sign into all applications with a single set of login credentials

Multifactor authentication (MFA)

– Enhance security with modern user authentication methods, including passwordless options

Risk-based authentication and adaptive access

– Adapt levels of access and authentication based on deep, risk-based context

User lifecycle management

– Streamline the user onboarding and offboarding processes

Connections with existing user directories and identity providers

– Enable internal efficiency by building off existing implementations and user information

Integrations for zero trust initiatives

– Integrate with fraud protection, unified endpoint management and threat management portfolios to infuse identity into the heart of zero trust strategies

Support for consumer IAM scenarios

– Beyond traditional IAM, expand implementations for external users by leveraging capabilities for user registration, progressive profiling and privacy and consent management

Expertise to make your program successful

– Partner with a provider with built-in planning, support and deployment services

IBM Security Verify helps businesses analyze risks across their IAM environment. See how IBM's IDaaS technology identifies risks and offers suggested remediation in this short video.

Watch video

IBM Security Verify

The IBM Security Verify solution allows IT, security and business leaders to protect their digital users, assets and data in a hybrid multicloud world, while promoting internal process efficiency along the way. Beyond SSO and MFA, Verify is a modernized, modular IDaaS that provides AI-powered context for adaptive access decisions, guided experiences for developer consumability and comprehensive cloud capabilities, including access recertification and identity analytics. Future-proof your identity and access management investment for both workforce and consumer populations with Verify.

IBM **Security**

Sources

1. 2020 Cost of a Data Breach Report. Conducted by the Ponemon Institute. Sponsored by IBM Security.

2. Forrester Analytics: IAM Software Forecast, 2018 To 2023 (Global). Forrester Research, Inc. May 10, 2019. Sponsored by IBM.

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

Produced in the United States of America
May 2019
All Rights Reserved

IBM