

EBOOK | Symantec Identity Security

# Winning the Digital Transformation Race

3 TIPS TO MAKE SECURITY A COMPETITIVE ADVANTAGE

# Winning the Digital Transformation Race



**Consumer behaviors and expectations have changed in recent years.** The mobile generation wants access to data and services anywhere, at any time, and they don't want to spend time logging into systems and going through lengthy security and authentication requirements to do so. Yet at the same time, consumers want to know their data and information is secure, and not at risk of theft or fraud. In order to satisfy these demands, organizations must be able to provide the right balance of security and user experience to consumers—**frictionless web and mobile app authentication that ensures sensitive data remains safe**, all without slowing development speed.

As organizations increasingly focus on their digital offerings through web and mobile applications, the risk of theft and fraud continues to rise. Regular news headlines of major data breaches further reinforce that this risk will not go away anytime soon. Security breaches break the trust of consumers, and result in lost customers, revenue, and market share. In order to remain competitive, digital-focused businesses need a security and authentication strategy that meets the demands of consumers. Enterprises today must build strong authentication in their web and mobile apps to protect enterprise and consumer data, increase user trust, and ensure customer retention.

*Security breaches break the trust of consumers, and result in lost customers, revenue, and market share.*

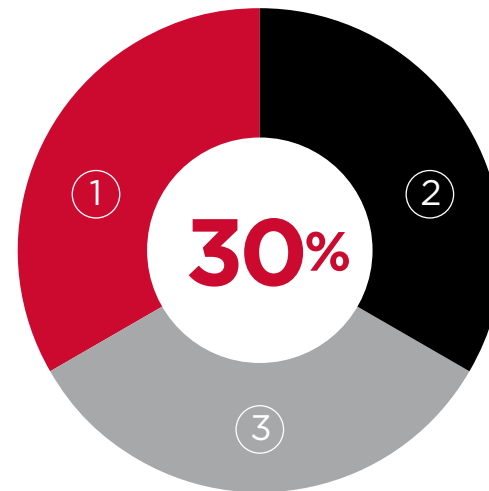
# The Digital Transformation Race

The advent of web, mobile, and IoT apps today has made nearly every business a software-first, **digital organization**.

If you're part of this digital transformation race, it's important to understand the changing landscape, and align your digital strategy with your overall business goals. Likely, your businesses' goals will include meeting the demands of customers on all channels. On web and mobile apps, it is vital to gain consumer trust to encourage adoption of digital services. Providing convenient security for customers will help give you a competitive advantage and grow your business. The reality of competition in this new digital arena means that "40 percent of today's businesses will fail in the next ten years; 70 percent will attempt to transform themselves digitally, but only 30 percent will succeed."<sup>1</sup>

**To be part of the 30% of businesses that are successful in digital transformation, there are three key ideas to keep in mind.**

Increase customer trust with built-in, risk-based security



Make authentication and security foolproof yet frictionless

Don't slow down the development process—work alongside it





*“Digital transformation is about sweeping change. It changes everything about how products are designed, manufactured, sold, delivered, and serviced—and it forces CEOs to rethink how companies execute, with new business processes, management practices, and information systems, as well as everything about the nature of customer relationships.”*

- McKinsey & Company





## Tips for Successful Digital Transformation

# 1. Increase Customer Trust with Built-in, Risk-based Security

Payers, providers, pharmaceutical companies and medical device manufacturers now find themselves in a hyper-connected ecosystem where once well-defined boundaries have blurred. Data no longer sits in static paper records. The new normal is an environment where medical devices can instantly connect with a patient's Electronic Health Record, transmitting physiological data in real time.

A strong, risk-based authentication solution should include:

- **User behavior profiling**—identify users based on behavior patterns, including geo-location, device, time-of-day, and velocity.
- **Mobile risk authentication**—have access to device data to validate user identity.
- **Dynamic rules**—update rules on the fly to match business policies and respond to new threats or user requests.
- **Immediate access to data**—feedback on what triggered fraud rules, so action can be taken to adjust fraud thresholds.



# Tips for Successful Digital Transformation

## 2. Make Authentication and Security Foolproof Yet Frictionless

Research reports prove that customers want a frictionless, easy authentication experience in order to continue doing business with an organization. But, surprisingly, they also want to be able to see strong security. In fact, 66% of consumers said, “I like all the security protocols when I interact online because it makes me feel protected.” Alongside this, 27% of customers abandoned a transaction due to a lack of visible security.

Clearly, strong security is necessary. But simultaneously, customers also want an easy authentication method that doesn't require them to spend time answering repetitive security questions or going through steps that slow down their access. “Inputting usernames and passwords in a mobile device is a clunky user experience, so many consumers willingly embrace biometrics and other technologies that are both easier and more secure.”

Consumer preference for secure and frictionless authentication, and businesses' understanding of these preferences, make it essential for all digital businesses today to think through the customer experience, the security of web and mobile apps, and the implications of a repetitive and time-consuming authentication process.

A frictionless authentication solution should:

- **Offer multiple authentication options**, including desktop OTP, FIDO support, fingerprint (Touch ID), OAuth tokens, OTP over email or SMS, push notification, and risk-based authentication
- **Enable a seamless**, omni-channel consumer experience
- **Include consistent policies** across environments
- **Be appropriate** for the level of activity being performed—for example, requiring step-up authentication for high risk transactions



## Tips for Successful Digital Transformation

### 3. Don't Slow Down the Development Process—Work Alongside it

**Mobile teams are coming under increasing pressure to build and release more capabilities via apps at an increasing pace. At the same time, they must manage the risk of this increased access.**

And they also must improve security within the app, without slowing innovation. Businesses that attempt to force cumbersome development methods to ensure security may end up causing a developer revolt.

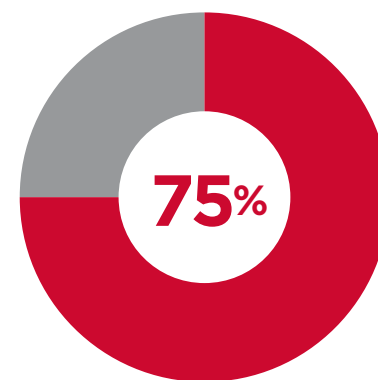
And as we've seen, customers today demand secure apps with easy, frictionless authentication. To strike this difficult balance, development teams need security solutions that allow them to increase the velocity of app development while maintaining the needed security strength.

Does your development team have the right tools to accomplish this?


A security solution should enable the development team to:

- **Accelerate the pace** of innovation to maintain competitive advantage by delivering new products, features, and experiences more quickly.
- **Reduce cost** and complexity in development processes.
- **Easily embed security** into mobile apps to simplify the coding experience.s

**75% of businesses want advanced authentication and security measures that have little or no impact on the digital customer experience**







*Quickly build and  
maintain modern,  
frictionless, and  
secure apps*

# Introducing a Solution from Symantec Identity Security

**Symantec Authentication allows your developers to quickly build and maintain modern, frictionless, and secure apps for your customers. The solution provides one easy step to rapidly integrate device security and comprehensive multi-factor and risk-based authentication.**

Symantec Authentication protects mobile communications, supports a variety of authentication methods, and can be quickly embedded into apps via a streamlined, universal mobile SDK. This allows developers to deploy apps much faster by eliminating dozens of complex steps normally required for coding device security.

Key features include:

- **Embed security, easily.** Symantec Authentication includes a universal SDK that developers can use to easily embed security into web, mobile, and IoT apps.
- **Provide frictionless authentication for users.** Minimize security friction via transparent two-factor authentication credentials and contextual risk-based evaluation.
- **Choose the security that works best for you.** Symantec Authentication provides options. Supported web and mobile app authentication methods include desktop OTP, FIDO support, fingerprint/facial scan (Touch ID/FaceID), OAuth tokens, OTP over email or SMS, push notification, and risk-based authentication. These choices ensure you have multiple secondary authentication methods that you can pick and choose, so you don't have to make any sacrifices.
- **Decrease time-to-market without compromising security.** Get apps to market faster by limiting repetitive and complex app development tasks. Built-in security ensures developers can focus on building winning features, not spending time becoming security experts.



# Is your enterprise building and supporting apps that are frictionless, secure, and quick to deploy?

With Symantec, A Division of Broadcom, win the digital transformation race and gain a competitive advantage.

LEARN HOW AT [BROADCOM.COM/SYMANTEC-IAM](https://broadcom.com/symantec-iam)



For product information please visit our website at: [ca.com](https://ca.com)

Copyright © 2020 Broadcom. All Rights Reserved. Broadcom, the pulse logo, Connecting everything, CA Technologies, and the CA technologies logo, are among the trademarks of Broadcom. The term "Broadcom" refers to Broadcom Inc. and/or its subsidiaries.  
BC-0548EN-0120 January, 2020

