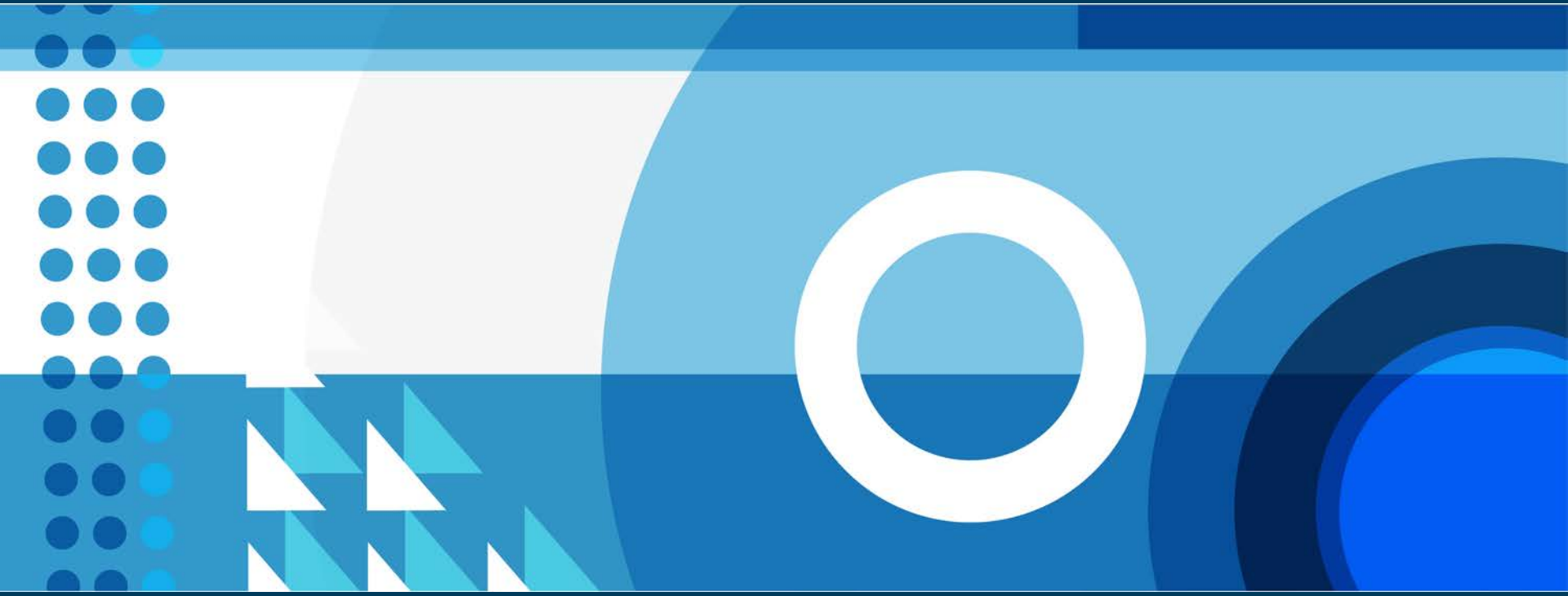
FORRESTER®

Forrester Opportunity Snapshot: Entrust Datacard | June 2018

Modern Authentication Methods Protect And Enable The Business

GET STARTED ▶



Forrester Opportunity Snapshot: Entrust Datacard | June 2018

Modern Authentication Methods Protect And Enable The Business

Evolve Your Authentication Approach

IT and security executives understand they need to manage identities in an automated fashion to achieve regulatory compliance, boost employee productivity, and improve customer experience. Firms' interactions with employees, contractors, and suppliers are increasingly digital — and rely on data from mobile, cloud services, desktop applications, and other devices to connect fast and effectively. But finding the right approach requires an effective and modern identity and access management (IAM) strategy. Firms without a modern IAM strategy risk a security breach of sensitive data, such as personally identifiable information (PII), intellectual property, business plans, etc., due to outdated authentication methods. This lack also puts strain on users due to a cumbersome process inconsistent across applications. To better serve users and protect the enterprise, firms must modernize and adopt the right authentication solutions for their environment — a best-in-class solution that is easy to use and protects business interests into the future.

In March 2018, Entrust Datacard commissioned Forrester to conduct a study exploring approaches and challenges of user authentication and access management. The study surveyed 100 IT and IT security executives in North America who are responsible for authentication and identity access strategy and technology and/or security at their organization. The demographics of the study are:

Company size (# of employees)

- **28%** - 20,000 or more
- **29%** - 5,000 to 19,999
- **43%** - 1,000 to 4,999

Industry (top 5)

- **17%** - Healthcare
- **16%** - Financial services
- **15%** - Technology
- **10%** - Manufacturing
- **9%** - Retail

Title

- **32%** - C-level executive
- **16%** - Vice president
- **52%** - Director

Job function

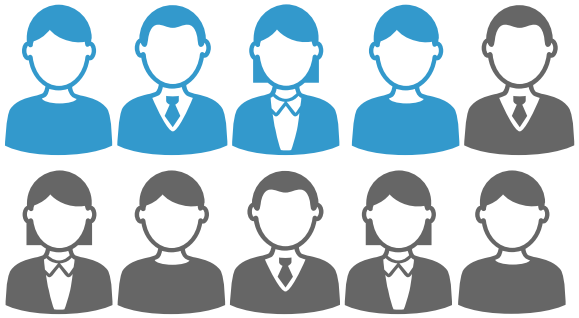
- **89%** - IT
- **11%** - IT security

Modern Authentication Methods Protect And Enable The Business

Security Falls Short As Firms Over Rely On Outdated Authentication Methods

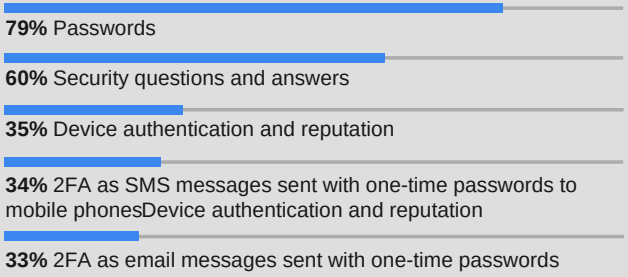
Ineffective authentication security comes with significant direct and indirect risks including compliance penalties, data theft, loss of customer and employee trust, and loss of revenue. It's alarming then that nearly 40% of the decision makers we surveyed feel their authentication methods fall short of protecting user access today.

This gap in security may be due to an over reliance on insecure forms of authentication, like passwords and security questions. It's worrisome that the majority of firms continue to use passwords despite that: 1) they are easily cracked or stolen by criminals and 2) users struggle to remember them — leading them to either decrease security when they write passwords down, or increase costs calling the help desk to reset forgotten passwords. Although typically deployed as two-factor authentication (2FA), user-entered security questions are also problematic: they can be rendered useless with the quick search of a user's social media accounts.



Four out of 10 firms say their current methods **are moderately effective or worse** at protecting internal users

"What authentication methods does your organization use to identify internal users? (Select all that apply)"
Top 5 shown.



Base: 100 North American IT decision makers responsible for authentication and identity access strategy and technology and/or security at their organization
Source: A commissioned study conducted by Forrester Consulting on behalf of Entrust Datacard, April 2018

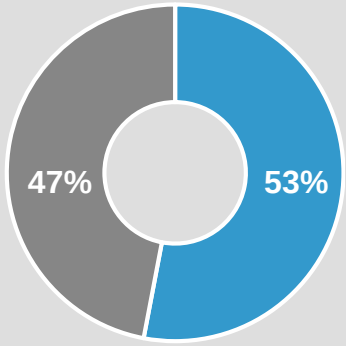
Modern Authentication Methods Protect And Enable The Business

To Plug Security Holes, Firms Employ Disparate Authentication Methods

Recognizing the need for greater security, most firms we surveyed have attempted to mature their IAM by adopting modern authentication methods in addition to passwords and security questions. However, many firms still lack a unified strategic approach to authentication. With more than half using four or more different methods to authenticate internal users, it's clear that firms are attempting to get more security with more methods — even if they are increasingly outdated (i.e., passwords, tokens, gridcards, etc.). This "more-is-more" approach is misguided, as the more methods employed, the greater the risk of increased friction and complexity for the user.

Many firms bolt on disparate authentication methods, rather than assess their IAM strategy holistically across devices and identities.

Many firms are bolting on several modern approaches simultaneously in pursuit of more effective security.



53% of firms use four or more types of authentication to identify internal users.

Base: 100 North American IT decision makers responsible for authentication and identity access strategy and technology and/or security at their organization

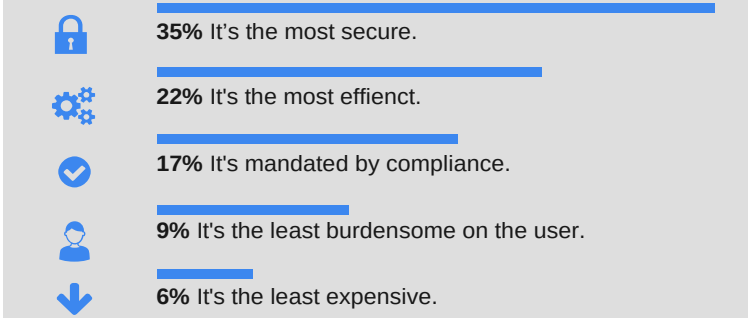
Source: A commissioned study conducted by Forrester Consulting on behalf of Entrust Datacard, April 2018

Modern Authentication Methods Protect And Enable The Business

Ease Of Authentication Is A Secondary Consideration, Resulting In Unnecessary User Frustration

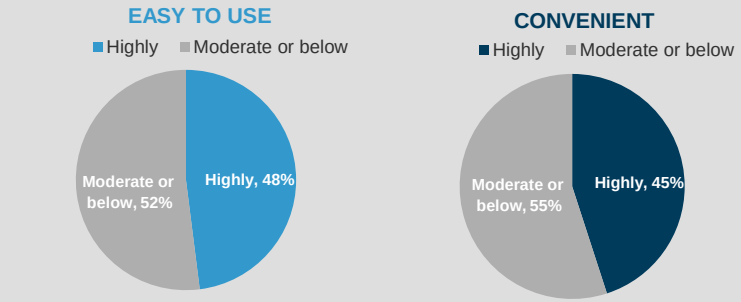
While internal users expect quick and easy access to job-critical applications no matter the device they are using, our study found that firms prioritize the security of their methods far above ease of use. In the case of the 53% of firms using four or more methods, inconsistent experiences may prevent users from getting what they need. For example, users might need a complex password that must be reset every 90 days for on-premises workstation access, but need a different password and a one-time-password (OTP) token for accessing the VPN. As a result, more than half of decision makers feel there is room to improve in both ease of use and convenience. Firms with frustrating security controls risk alienating employees, partners, and customers, driving up support costs, and slowing down the speed of business.

"What are the key reasons your firm chooses to use your current authentication methods? (Rank top 3)"
Showing top 5, rank 1 only.



Base: 100 North American IT decision makers responsible for authentication and identity access strategy and technology and/or security at their organization
Source: A commissioned study conducted by Forrester Consulting on behalf of Entrust Datacard, April 2018

"In your opinion, how easy to use and convenient are your organization's current authentication processes and technologies for internal users today?"



Base: 100 North American IT decision makers responsible for authentication and identity access strategy and technology and/or security at their organization
Source: A commissioned study conducted by Forrester Consulting on behalf of Entrust Datacard, April 2018

Modern Authentication Methods Protect And Enable The Business

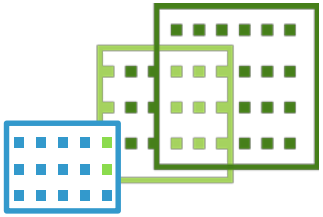
Authentication Complexity Will Grow For Foreseeable Future

Compounding the ineffective security and poor user experience caused by today's "more-is-more" approach, firms don't foresee the situation getting easier: 29% say complexity will stay the same in two years, while 44% believe that complexity will in fact increase over the next two years.

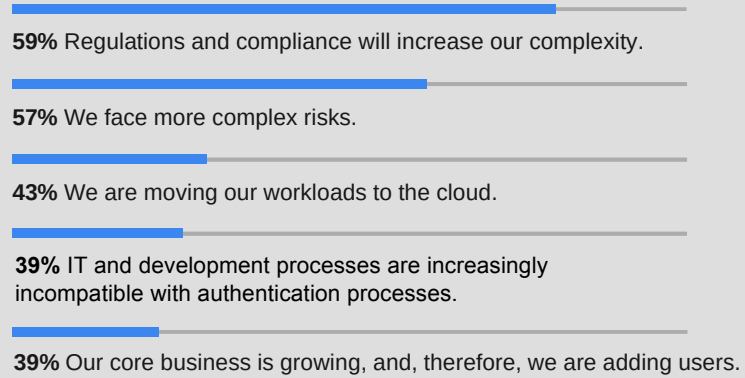
AUTHENTICATION COMPLEXITY DRIVEN BY RISK AND REGULATION

Decision makers who believe user authentication is growing in complexity believe it is driven by greater:

- **Regulation.** Compliance mandates (i.e., GDPR, FERC/NERC, GLBA, HIPAA, PCI DSS, PSD2, etc.) are getting more numerous and complex.
- **Risk.** Increases in computing power have already improved the success of brute-force attacks. Moreover, today's systems of authentication may be ill-equipped to detect future forms of attack.



"You indicated that authentication and identity access will become more complex over time. What do you think drives this? (Select all that apply)" Top 5 shown.



Base: 44 North American IT decision makers responsible for authentication and identity access strategy and technology and/or security at their organization
Source: A commissioned study conducted by Forrester Consulting on behalf of Entrust Datacard, April 2018

Modern Authentication Methods Protect And Enable The Business

1 2

Firms Recognize The Essential Nature Of Modern Approaches, But Strategic Adoption Is Key

Passwords frustrate both users and administrators, who devote valuable time to dealing with password issues instead of tasks that serve customers. However, a password-free world is not likely in the short-term. Our study found that passwords and security questions remain critical to most enterprise authentication strategies.

Encouragingly, firms place growing importance on modern methods that increase security and are convenient for the user — and could replace passwords in the long term. To future-proof their methods, decision makers must plan strategically to adopt the fewest methods required to provide the greatest security and UX. A modern approach prioritizes:

- **Push notifications.** By alerting the user with a mobile application, you take the guesswork out of the experience.
- **Biometrics.** Both highly secure and easy for the user.
- **Bluetooth-based physical-logical access.** Automation that provides frictionless access while maintaining high assurance.
- **Behavioral anomaly and device reputation.** Enable continuous authentication that's invisible to the user.

The difference between table stakes, modern approaches, and the frontier depends on current adoption and importance to strategy.

Method	% Adopted	% Important
Table Stakes: used alone, considered an antiquated strategy **Adoption and importance high**		
Passwords	79%	80%
Security questions and answers	60%	71%
Modern Approaches: the foundation of an updated authentication approach **Adoption low to medium, but importance medium to high**		
Device authentication and reputation	35%	69%
2FA as push notification in mobile token	26%	66%
2FA as push notification built into a business mobile app	23%	60%
2FA using physical biometrics	21%	60%
2FA using physical smartcards	23%	54%
2FA as mobile Bluetooth-based proximity sensing	15%	51%
The Frontier: next generation methods **Adoption and importance both low**		
Behavioral biometrics	19%	47%
Geolocation-based geo-fencing	20%	43%

Base: 100 North American IT decision makers responsible for authentication and identity access strategy and technology and/or security at their organization

Source: A commissioned study conducted by Forrester Consulting on behalf of Entrust Datacard, April 2018

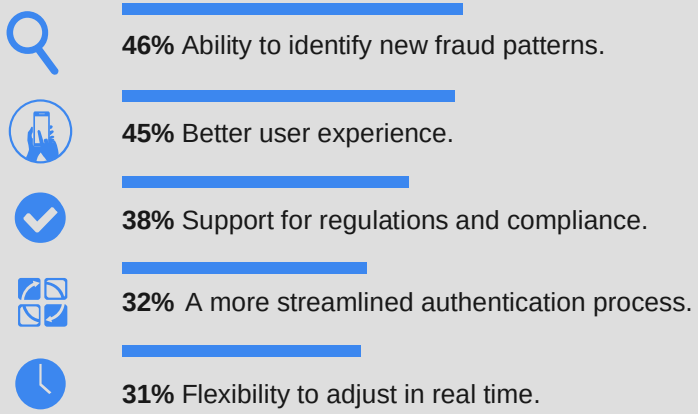
Modern Authentication Methods Protect And Enable The Business

Modern Authentication Means Stronger Security And Better User Experience

Decision makers believe a modern approach to authentication will bring their enterprise:

- **The ability to keep up with new threats.** Firms fight an uphill battle against emerging fraud methods, but modern authentication can help identify new patterns. For example, behavioral biometrics monitor typing speed and mouse movements for suspicious activity.
- **Better user experience.** With modern 2FA in place, users don't need to follow complicated password requirements that change every 90 days — and organizations may be only able to force password changes once every 180 or 365 days. Plus, administrators can reduce the resources required for password-related support calls.
- **Greater support for regulations and compliance.** Modern methods make it easier for auditors to get answers to critical compliance questions like: 1) who is granted access to what system and 2) how is access policy reliably enforced.

"What are, or would be, the benefits of modernizing your organization's approach to authentication? (Select all.)"
Top 5 shown.



Base: 100 North American IT decision-makers responsible for authentication and identity access strategy and technology and/or security at their organization
Source: A commissioned study conducted by Forrester Consulting on behalf of Entrust Datacard,April 2018

Forrester Opportunity Snapshot: Entrust Datacard | June 2018

Modern Authentication Methods Protect And Enable The Business

Your Authentication Strategy Must Meet The Demands Of A Changing Business Environment

The changing nature of business is pushing the boundaries of traditional identity. More and more, employees and partners engage with firms digitally. Their expectation, to easily access business-critical applications and data from anywhere, forces firms to manage identities and access across a variety of devices and hosting models — even as regulation and threats change and grow. A strong IAM strategy must protect the firm from sophisticated cybercriminals and support Zero Trust security architecture with greater user intelligence and transparency, all while providing the ease of access users need to accelerate business results. However, our survey found that today's outdated or bolt-on approaches to authentication are not sufficient because they are: 1) ineffective at protecting users, 2) burdensome on users, and 3) hinder users' ability to access an increasing number of applications without having to reauthenticate. Instead, firms should turn to a modern approach to authentication — one that centers on protecting sensitive data and unifying treatment of access across devices and populations. In modernizing their IAM strategy, firms stand to gain a stronger enterprise through greater security and frictionless user experience.

METHODOLOGY

This Opportunity Snapshot was commissioned by Entrust Datacard. To create this profile, we surveyed 100 IT decision makers responsible for authentication and identity access strategy, technology and/or security at organizations with 1,000 or more employees. The custom survey was completed April 2018.

Project Director
Emma Van Pelt
Market Impact Associate
Consultant

ABOUT FORRESTER CONSULTING

Forrester Consulting provides independent and objective research-based consulting to help leaders succeed in their organizations. Ranging in scope from a short strategy session to custom projects, Forrester's Consulting services connect you directly with research analysts who apply expert insight to your specific business challenges. For more information, visit forrester.com/consulting.