



SECURING YOUR REMOTE EMPLOYEES WITH CLOUD-BASED AUTHENTICATION

Table of Contents

I. The Right Authentication Solution at the Right Time	2
A. Market Trends	3
B. Use Cases	3
II. Questions to ask When Considering Multi-Factor Authentication	4
III. Is Cloud Right for Your Organization?	5
A. Costs	
B. Security	
C. Interoperability	
IV. Top Features to Look for in a Cloud-Based Multi-Factor Authentication Solution	6
A. IT Agility and Flexibility	
i. A Choice of Authentication Methods	7
ii. Modern, Multi-Level Authentication Approaches	7
iii. Configurable and Adaptive Risk-Based Policies	8
iv. Availability	9
v. Extensibility	9
vi. Authentication Oversight and Reporting	10
B. User Experience	11
i. Striking the Right Balance Between Security and User Experience	11
ii. Mobility in the Workplace	11
iii. Mobile Innovation	11
iv. Self-Service Capabilities	12
C. Business Impact	12
i. Deploy how you Want When you Want	12
ii. Compliance	13
iii. TCO	13
V. A Vendor I Can Trust	14

The right authentication solution at the right time

In this time of social distancing, those who can are being asked to work from home — some for the first time. Similarly, more and more businesses and consumers are interacting and transacting online. In fact, many enterprises have gone entirely virtual. Which means you can expect cyber criminals to take advantage of the situation.



So how do you protect your enterprise, remote employees, customers and partners while also ensuring business continuity, productivity and exceptional user experiences? By choosing the right authentication solution.

This buyer's guide will help you determine if a cloud-based authentication solution is right for your organization, whether temporarily during the current spike in WFH programs and online commerce, and details the top features to look for in an authentication solution.

A. Market Trends

The digital evolution has enabled organizations to innovate and streamline processes with greater dependency on mobile and cloud, and IT has an increased impact on business success. But the reality of distributed applications and connected devices, especially in the current environment, has introduced new security challenges. To secure information and provide users seamless access to data, you need to reevaluate your approach to authentication.

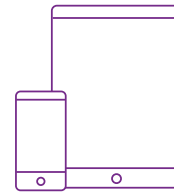
You need a modern authentication solution that is agile and secure, enabling trusted identities and transactions for business continuity.

B. Use Cases

As businesses continue to evolve and become more complex, IT managers need to rethink their authentication strategy and consider new use cases such as unified SSO for cloud and on-prem apps, adaptive risk-based authentication, and passwordless authentication.



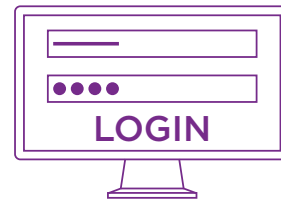
Streamline VPN access
with frictionless authentication



Unlock the power of mobile
as your new desktop



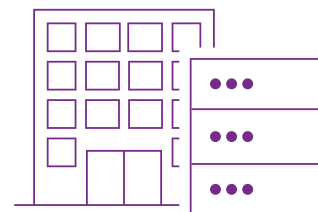
Transition to cloud SSO for a competitive
edge and easy access to all apps



Provide seamless and
secure workstation login



Digitally connect and collaborate
with customer and partner portals



Provide privileged users access
to critical systems and apps

II. Questions to ask When Considering Multi-Factor Authentication

A. How will Multi-factor authentication affect our customers?

No doubt there is a perception that authentication can cause friction for your customers. You need to ensure your authentication solution of choice is secure and frictionless. To exceed customer expectations, look for **a transparent, contextual authentication solution that opens up new experiences and services** to the end user while ensuring security.

B. What types of users do we need to authenticate?

Depending on what type of users you need to authenticate, you will want to consider different types of authentication methods. Typically, applications in your organization require different access methods based on the type of user. Look for a solution that gives you **the flexibility to provision identities based on user needs**.

C. What applications and resources fit into our immediate authentication plans? Future authentication plans?

A majority of companies will look for a solution that meets their immediate authentication needs, but it's important to be aware of and plan for future authentication use cases. For example, you may need VPN access today, but you might eventually need a patient, customer or partner portal. Make sure to find a solution that **supports you both today and in the future to reduce your costs and the potential hassle of switching vendors**.

D. What is our IT maturity when it comes to authentication skills, resources and initiatives?

Not sure how you want to deploy your authentication solution? Depending on your IT department's bandwidth and resources, your deployment model will vary. If you have a mature IT department and want control over your data, an on-prem solution is probably best. Not ready to move to the cloud but still want a turnkey solution? You're probably looking at a virtual appliance. Want to streamline IT and move to the cloud? Cloud-based authentication is your best bet. The key is to **ensure you have a solution that will protect your investment**, allowing you to **transition to the cloud when necessary**.

E. How do we rate cost, security and UX priorities?

Your organization's priorities can help you determine which authenticator is right for your users. But don't think that if you want security you have to sacrifice cost and user experience. **Modern authentication solutions such as mobile are more secure, more cost effective and provide a better user experience**.

F. How important is enterprise mobility to our organization?

As your mobile workforce continues to grow, consider enabling your employees with mobile as the computing platform — a virtual smart card embedded on your users' devices. By giving your employees secure, seamless access to the devices they use the most, your organization will be able to **better serve customers, drive revenue and optimize productivity**. Look for a vendor that is integrated with an EMM to provide an even more secure, frictionless experience for you and your employees.

III. Is Cloud Right for Your Organization?

The advent of cloud presents organizations an opportunity to consider alternatives to traditional IT services and delivery methods. Whether you are looking to innovate more quickly, save costs or more closely align with other business units, moving aspects of your business to the cloud can accelerate your digital transformation.

But there are several considerations to make when deciding whether to keep initiatives on-premises or move them to the cloud, including costs, security and interoperability.

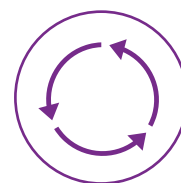
Key Cloud Considerations



Costs



Security



Interoperability

A. Costs

When deciding whether to make the move to a cloud-based authentication solution, consider the financial impact on your organization. Ask yourself the following questions:

- What are the immediate costs?
- Are there recurring or long-term costs?
- Will there be additional infrastructure, location or headcount costs?
- What ongoing maintenance costs might there be?
- What cost savings might my organization experience?

B. Security

The security of your organization's data is of utmost importance and should be a key consideration when determining where to host your authentication solution. Consider:

- What regulations do I have to meet?
- How will my data be secured?
- Could implementation result in potential loss of data?
- Is the solution slick, secure or both?

C. Interoperability

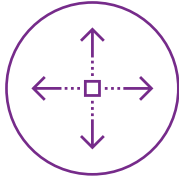
Your authentication solution is just one of many solutions within your organization, and it will need to work in tandem with many other business critical applications. Ask yourself:

- What applications and services need to interface with the authentication solution?
- Are these applications and services on-premises or cloud-based?
- Do they require specific software versions?
- What upgrade cycles are they on?

IV. Top Features to Look for in a Cloud-Based Multi-Factor Authentication Solution

Once you've determined that a cloud-based authentication solution best meets your organization's needs, you need to assess the individual solution.

The top features you should look for in a cloud-based multi-factor authentication solution are:



1. IT agility and flexibility



2. User experience



3. Business impact

“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.”

Modern Authentication Methods Protect and Enable The Business
Andras Cser, Forrester
June 2018

A. IT Agility and Flexibility

All about the choices

When it comes to an authentication solution, you want choices. You need a flexible solution that can be adapted to meet your needs now and moving forward. Consider your existing use cases. How many users and devices do you need to authenticate? Where are they located?

Your authentication solution should be able to handle all use case scenarios for your business, whether they be business to employee (B2E), business to business (B2B) or business to consumer (B2C).

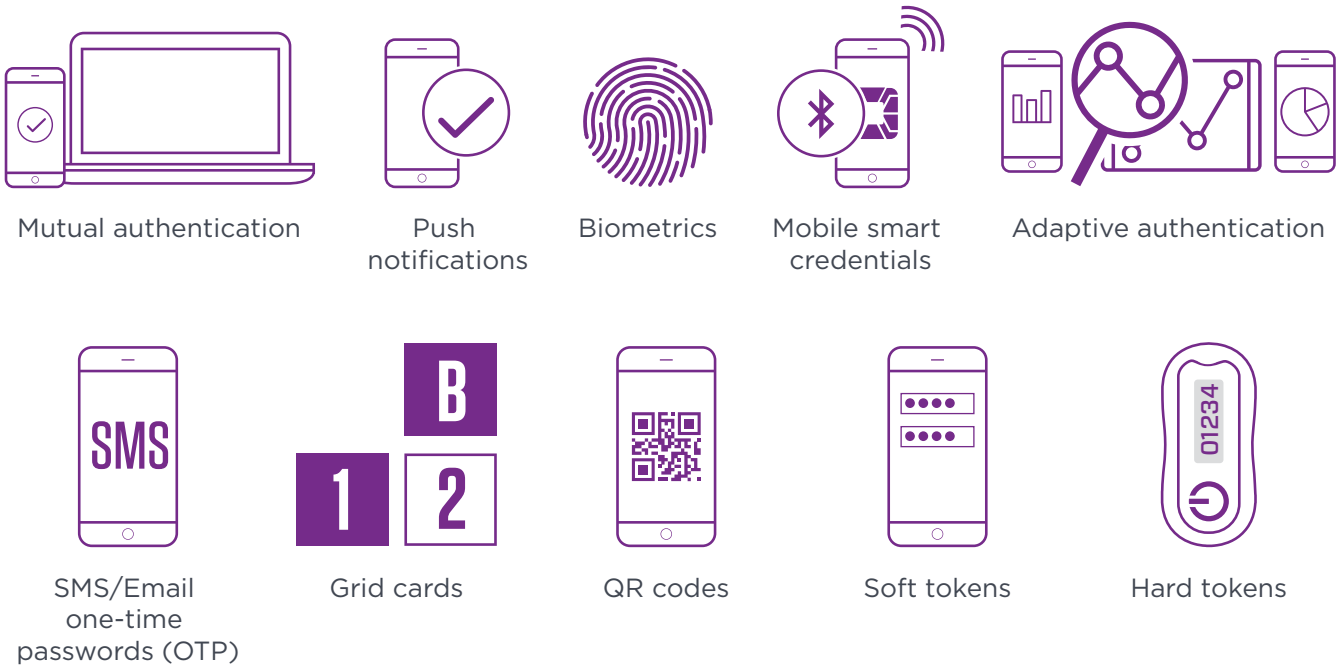
You also need an authentication solution that is easily configurable. Authentication solutions should be able to discern which assets and applications require multi-factor authentication, depending on real-time risk, and provide configurable policies to secure access.

Cloud-Based Authentication - Buyer's Guide

Helping you Navigate the Possibilities

i. A choice of authentication methods

It's important to have a choice when it comes to authentication methods. Depending on varying factors such as the asset being accessed, the device the asset is being accessed from and the level of technical ability of the user accessing the device, you may want to choose different methods of authentication. Various options include:



Your authentication solution provider should offer you as many authentication options as possible. To help reduce operation costs, make sure that authenticators can be managed by end users and alternate authenticators of equivalent strengths can be configured for accessing specific applications and assets.

ii. Modern, multi-level authentication approaches

The most secure authentication solutions will also offer multi-level authentication, which is crucial in cases such as transaction approvals. Types of multi-level authentication include:

- **Device reputation:** Recognizes and detects fraud across internet devices based on patterns to stop fraud and abuse in real time, prior to login. This allows you to verify the integrity of a device before a trusted identity is provisioned to a user. Ex: BYOD and mobile precheck
- **Transactional analytics and behavioral biometrics:** Analyzes points of user interaction, such as frequency of logins, adding an abnormal number of payees or different touch/swipe motion on a mobile device, to gain a complete picture of potentially fraudulent behavior.
- **Step-up authentication:** If risk is elevated for a user, it's important to enable step-up authentication that is still frictionless for the end user such as mobile push authentication, touchID or Bluetooth wireless login.

iii. Configurable and adaptive risk-based policies

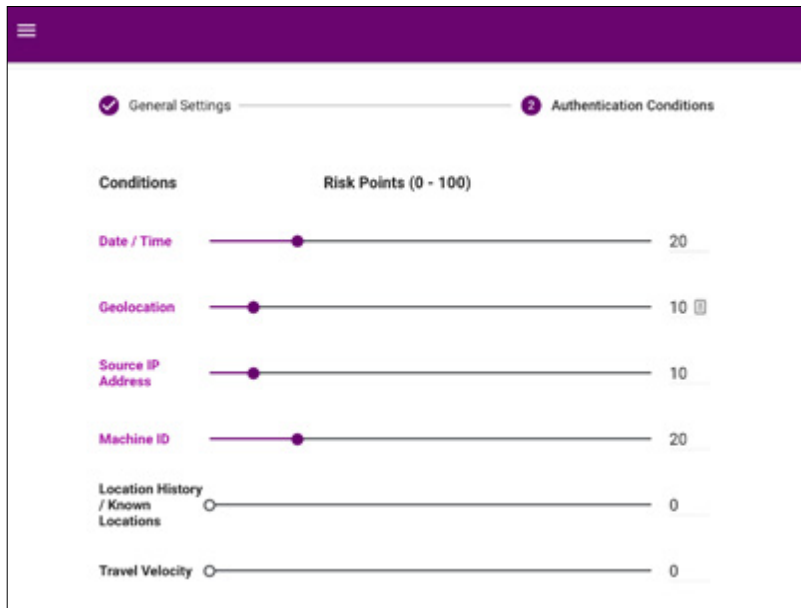
Authentication solutions are not one size fits all, especially when it comes to security. Effective authentication solutions provide easy to configure and adaptive risk-based policies that allow administrators to define access control policies on a per application, per user group basis using:

- **Weighted risk factors:** Risk factors can be weighted differently within the same application or asset, depending on the user group.
Ex: Contractors may need to be time-of-day and day-of-week limited for certain applications, while administrators might need 24/7 access to those same applications.
- **Risk-level definitions:** Administrators can define risk-levels such as low, medium and high based on application and user group.
- **Authentication decisions:** At each risk level, the authentication should be able to allow, block or challenge the access. Each risk level should also have defined authenticators and additional defined authenticators required in challenge scenarios.

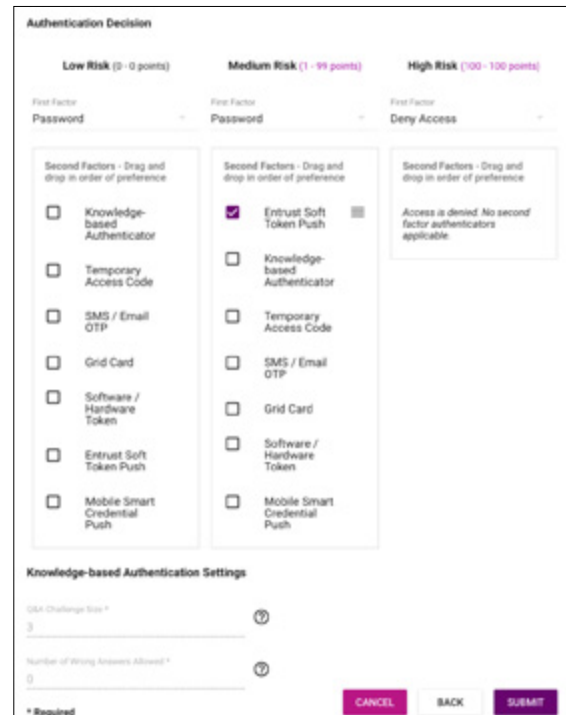
With a flexible authentication solution, you are able to assign varying levels of authentication based on real-time user access in accordance with configured policies.

IntelliTrust — Sophisticated Yet Simple

Raising the bar with advanced click-and-drag policy definition



Fine control over risk factors and risk weight



Full control over defining risk range (Low/Medium/High)

iv. Availability

Managing authentication threats is a critical aspect of digital business. The speed of digital business, as well as the any-time, anywhere demands of users, increases risk and puts more pressure on the authentication solution to be constantly available, as any moment of unavailability is experienced by a user as a failure to deliver your product or service to them.

Research by Gartner indicates that "By 2020, 60% of digital businesses will suffer major service failures, due to the inability of IT security teams to manage digital risk."

Special Report: Cybersecurity at the Speed of Digital Business
Paul E. Proctor and Ray Wagner, Gartner, Inc.
Refreshed: December 7, 2017 | Published: August 30, 2016

A good security solution is highly available and resilient against security incidents and downtime. If you select a cloud-based authentication solution, ensure that the solution is hosted on a well-known, highly available platform distributed across multiple geographic regions and various availability zones. You should expect an uptime of 99.9%, backed by the provider's SLA (service level agreement).

To be trusted to give your users what they want anywhere, anytime while not taking on unacceptable risk, choose an authentication solution that is:



Highly available
(at least 99.9 percent uptime)



Resilient against security
incidents and downtime



Hosted on a well-known, highly available platform
that is distributed across multiple geographic
regions and provides various availability zones
within each geographical region

v. Extensibility

Implementing a SaaS solution shouldn't be frustrating. It's important to find a solution that easily extends its capabilities into your environment so that you don't have to expend unnecessary time, money or resources.

You must choose a solution that allows for integrations with on-premises and cloud-based applications. You should be able to enable your legacy on-premises and cloud applications with multi-factor authentication without having to rewrite them. Cloud applications (SaaS) should be able to integrate using standards like OIDC, SAML, OAuth, etc.

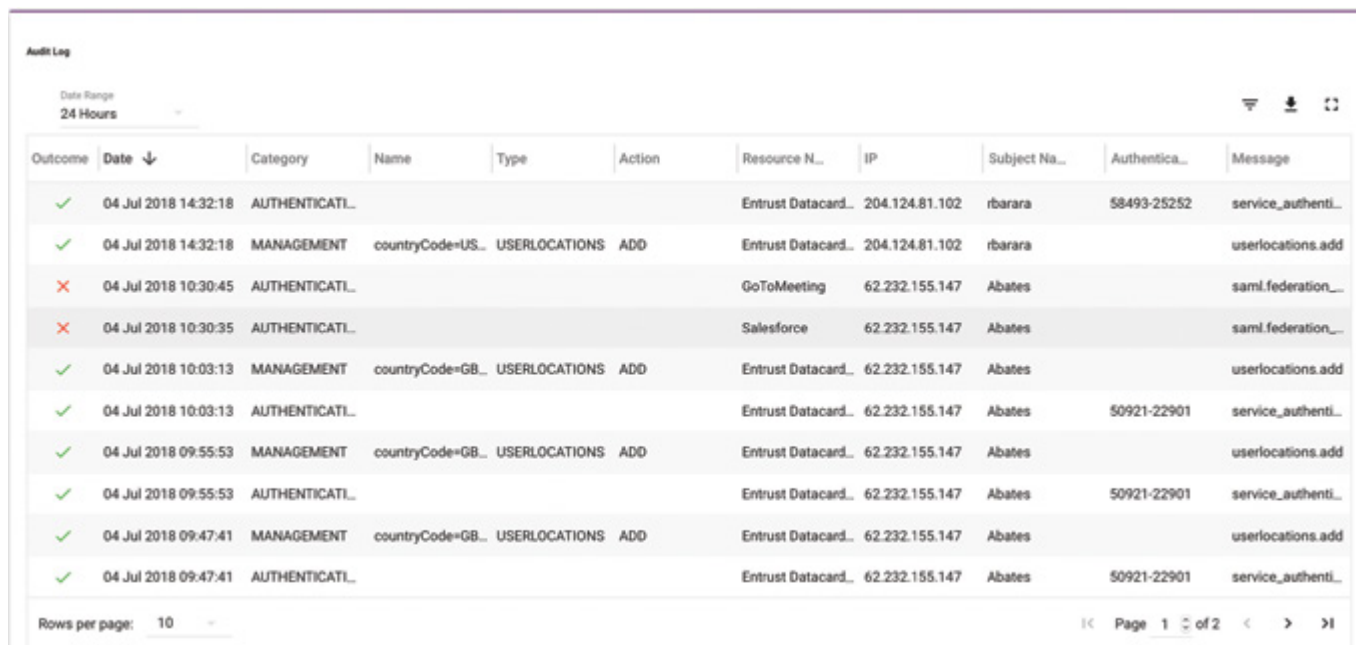
Ensure that your provider is able to integrate with all your applications through configuration and also provides RESTful APIs for automation of workflows.

vi. Authentication oversight and reporting

You also want to ensure your authentication solution gives you oversight into all actions performed by all system users, such as analytics, trends and patterns, as well as any authentication attempts, so your team can stay on top of any attempted breaches.

All authentication attempts should be traceable to their source (device, application, firewall, server, etc.) and contain data such as IP address, network, geographical location, type of action, access attempted, date and time of attempt, and user and authenticator ID.

You should have access to audit logs and dashboards with system reports, and the solution should integrate into your existing security information and event management solution for a single point of interface to better understand and react to recognized patterns and events.



The screenshot displays an 'Audit Log' interface. At the top left, there is a 'Date Range' dropdown set to '24 Hours'. On the top right, there are icons for filtering, downloading, and refreshing. The main content is a table with the following columns: Outcome, Date (with a downward arrow), Category, Name, Type, Action, Resource N..., IP, Subject Na..., Authentica..., and Message. The table contains 10 rows of data. The first row shows a successful authentication (green checkmark) for 'Entrust Datacard...' on '04 Jul 2018 14:32:18'. The second row shows a successful management action (green checkmark) for 'countryCode=US...' on the same date and time. The third and fourth rows show failed authentication attempts (red X) for 'GoToMeeting' and 'Salesforce' on '04 Jul 2018 10:30:45' and '04 Jul 2018 10:30:35' respectively. The fifth row shows a successful management action (green checkmark) for 'countryCode=GB...' on '04 Jul 2018 10:03:13'. The sixth and seventh rows show successful authentication (green checkmarks) for 'Entrust Datacard...' on '04 Jul 2018 10:03:13' and '04 Jul 2018 09:55:53' respectively. The eighth and ninth rows show successful management actions (green checkmarks) for 'countryCode=GB...' on '04 Jul 2018 09:55:53' and '04 Jul 2018 09:47:41' respectively. The tenth row shows a successful authentication (green checkmark) for 'Entrust Datacard...' on '04 Jul 2018 09:47:41'. At the bottom left, there is a 'Rows per page' dropdown set to '10'. At the bottom right, there is a pagination control showing 'Page 1 of 2' with navigation arrows.

Outcome	Date ↓	Category	Name	Type	Action	Resource N...	IP	Subject Na...	Authentica...	Message
✓	04 Jul 2018 14:32:18	AUTHENTICATL...				Entrust Datacard...	204.124.81.102	rbarara	58493-25252	service_authenti...
✓	04 Jul 2018 14:32:18	MANAGEMENT	countryCode=US...	USERLOCATIONS	ADD	Entrust Datacard...	204.124.81.102	rbarara		userlocations.add
✗	04 Jul 2018 10:30:45	AUTHENTICATL...				GoToMeeting	62.232.155.147	Abates		saml.federation_...
✗	04 Jul 2018 10:30:35	AUTHENTICATL...				Salesforce	62.232.155.147	Abates		saml.federation_...
✓	04 Jul 2018 10:03:13	MANAGEMENT	countryCode=GB...	USERLOCATIONS	ADD	Entrust Datacard...	62.232.155.147	Abates		userlocations.add
✓	04 Jul 2018 10:03:13	AUTHENTICATL...				Entrust Datacard...	62.232.155.147	Abates	50921-22901	service_authenti...
✓	04 Jul 2018 09:55:53	MANAGEMENT	countryCode=GB...	USERLOCATIONS	ADD	Entrust Datacard...	62.232.155.147	Abates		userlocations.add
✓	04 Jul 2018 09:55:53	AUTHENTICATL...				Entrust Datacard...	62.232.155.147	Abates	50921-22901	service_authenti...
✓	04 Jul 2018 09:47:41	MANAGEMENT	countryCode=GB...	USERLOCATIONS	ADD	Entrust Datacard...	62.232.155.147	Abates		userlocations.add
✓	04 Jul 2018 09:47:41	AUTHENTICATL...				Entrust Datacard...	62.232.155.147	Abates	50921-22901	service_authenti...

B. User Experience

i. Striking the right balance between security and user experience

Above all, an authentication solution should keep your organization and users secure. Good security solutions weigh the risk of a security threat in real time against the risk of requiring or not requiring action. For example, requiring a user to provide two factors of authentication every time they access an application might result in unnecessary frustration. A good authentication solution should be able to provide strong security behind the scenes while maintaining a good user experience.



ii. Mobility in the workplace

As more and workers work remotely or in the field, it's important to provide a secure, frictionless solution that enables them to work more efficiently with quicker response and turnaround times — ultimately providing better customer service. Utilize a virtual smart card embedded on their mobile device that provides access to their VPN, email and applications.

iii. Mobile innovation

Mobile access to applications and portals is driving an evolution of use cases. Recent survey data shows that employees use an average of three mobile devices daily to access applications. When selecting an authentication solution, **pay close attention to mobile innovations that you will eventually need to offer your users, such as:**

MOBILE PUSH NOTIFICATIONS	BIOMETRIC AUTHENTICATION	SEAMLESS INTEGRATION WITH EMM SOLUTIONS	MOBILE SMART CREDENTIALS	DEVICE REPUTATION
Mobile push notifications require a click or push of a button to verify access/transactions.	Biometric authentication such as fingerprints and facial recognition enable a transparent experience for your users.	EMM solutions such as VMware and MobileIron provide a more comprehensive solution for you and a better user experience for your customers.	Mobile smart credentials act as a virtual smart card, increasing security and streamlining user endpoints such as physical and logical access.	Device reputation provides users a transparent, secure experience by only enabling step-up authentication when a user's registered device is identified as a risk.

“By the end of 2022, 70% of enterprises will combine biometric methods with analytics and with either mobile push models or embedded public key credentials across multiple use cases, up from almost nil today.”

Technology Insight for Biometric Authentication
Ant Allan and Tricia Phillips, Gartner, Inc.
September 6, 2017

iv. Self-service capabilities

With an optional self-service module, users can self enroll, recover their account and reset passwords, without the assistance of a help desk — ultimately reducing calls to the IT helpdesk. Users are empowered to manage their authentication needs anytime, anywhere — when it's most convenient for them.

C. Business Impact

You need an authentication solution that not only meets your current device and user needs but can scale to meet future needs. As the number of users and devices increases, new use cases might be introduced, all representing potential points of authentication and integration. Choose an authentication solution that can handle a wide variety of use cases.

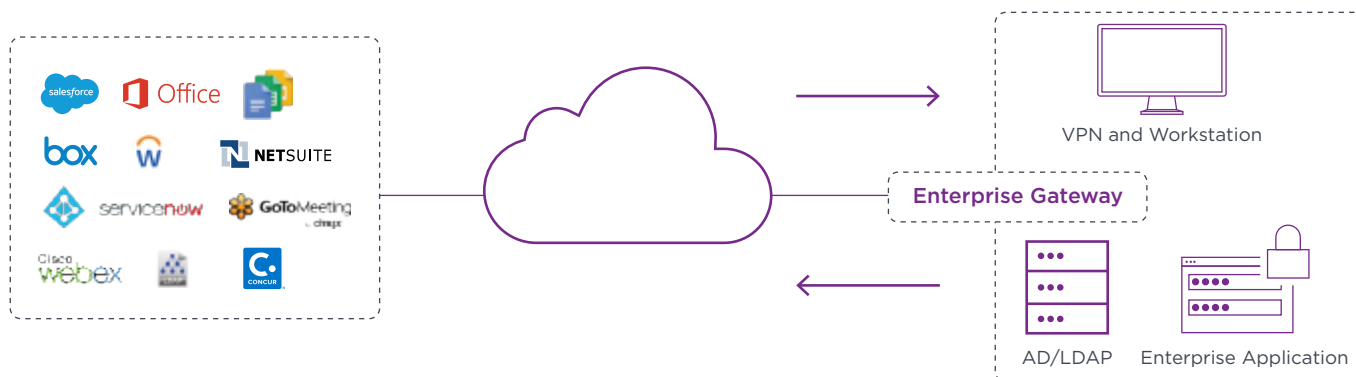
i. Deploy how you want when you want

Whether you want cloud-based authentication today or in the near future, it's important to find a solution that can grow with you as your business evolves. Find a provider that equips you with the flexibility to choose your authentication methods and deployment models so that you don't have to switch vendors down the road, ultimately reducing hassle and costs.

Your authentication solution should also allow for integration with all your applications, no matter where they are. 70-80 percent of companies are operating within a hybrid architecture in which some applications are hosted in the cloud while others are hosted on prem. Your authentication solution must cater to your needs of integrating with cloud applications while securing your on-prem applications. You should be able to enable your legacy on-premises and cloud application with multi-factor authentication without having to rewrite them.

Cloud applications (SaaS) should be able to integrate using standards like OIDC, SAML, Oauth, etc. Ensure that your provider is able to integrate with all your applications through configuration and also provides RESTful APIs for automation of workflows.

Your authentication solution must support your transition to the cloud and your digital business transformation without disrupting ongoing operations.



ii. Compliance

The right authentication solution can help you meet the growing number of regulation requirements while also expanding your reach to attract and retain customers. Look for a solution that can help you meet the following regulations:

- PSD2
- FFEIC
- PCI-DSS
- PIV Derived Credentials
- Swift Alliance
- GDPR
- HIPAA

iii. TCO

It's important to determine your upfront, onboarding, maintenance and support costs when evaluating a new authentication solution. The right authentication solution will support new, profitable use cases that you should weigh against the cost of implementation.

- 1. Determine the upfront costs** by analyzing the authentication solution pricing model and whether it supports flexible, user-based transactions. The model should support all applications that you need now, and in the future, with a clear understanding of what is already covered and where there will be extra costs.
- 2. Once the upfront costs are established, determine the onboarding, maintenance and support costs** for a complete picture of your authentication investment. Look for a scalable solution that allows you to forecast future costs and develop plans to capitalize on new use cases. Cloud solutions allow you to spend less on IT speciality skills because the brunt of the work happens in the cloud.

The cost of implementing security should never outweigh the importance of supporting new authentication use cases when those use cases help make your business more competitive or unique. A trusted partner will always ensure you are aware of what the future holds both in terms of challenges as well as opportunities.

Future-proof, scalable authentication platforms are those that can **anticipate areas in which you will grow and have a wide variety of authenticators ready to deploy** into your environment without extra effort from your development team. A strong authentication platform creates opportunities for digital businesses that have an impact both today and for the future of your digital business.

Make sure you choose the platform that will not only support where you are now, but where you want to go next. Find an authentication partner that:

- **Has a product that grows with your growing needs**
- **Is a thought leader**
- **Brings innovative solutions to the market**
- **Has a roadmap that takes advantage of best-in-breed components**
- **Provides a modular approach to support your overall IAM needs**

V. A Vendor I Can Trust

The key to your organization's digital transformation is choosing the right authentication solution partner, and Entrust Datacard has been a leader in trusted identity for more than 20 years.

Our strong authentication solutions offer the capabilities, assurance levels, deployment options and mobile innovations you need to enable digital business — and protect what's important to you.

The breadth of our portfolio, including on-premises, virtual appliance and cloud-based authentication solutions, allows you to trust one solution partner for all of your identity needs. And our commitment to continuous innovation means we are with you every step of the way, from where you are today to the realization of your ideal digital enterprise.

A Leader in Trusted Identity



Over 20 years
of trusted identity
solution experiences



Serving global organizations
from world governments
to digital business innovators



With an innovative,
end-to-end solution

About Entrust Datacard Corporation

Consumers, citizens and employees increasingly expect anywhere-anytime experiences — whether they are making purchases, crossing borders, accessing e-gov services or logging onto corporate networks. Entrust Datacard offers the trusted identity and secure transaction technologies that make those experiences reliable and secure. Solutions range from the physical world of financial cards, passports and ID cards to the digital realm of authentication, certificates and secure communications. With more than 2,000 Entrust Datacard colleagues around the world, and a network of strong global partners, the company serves customers in 150 countries worldwide.

For more information about Entrust Datacard products and services, call **888-690-2424**, email sales@entrustdatacard.com or visit entrustdatacard.com.

Corporate Headquarters

Entrust Datacard
1187 Park Place
Minneapolis, MN 55379
USA



Entrust Datacard and Entrust are trademarks, registered trademarks and/or service marks of Entrust Datacard Corporation in the United States and/or other countries.
©2020 Entrust Datacard Corporation. All rights reserved.

AT21Q1-WFH-Cloud-Auth-Buyers-Guide-BG