Buyer's Guide

Cloud-Based Identities

Helping you Navigate the Possibilities

ENTRUST

SECURING A WORLD IN MOTION

Table of Contents

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 and details the top features to look for in an authentication solution.

"DIGITAL IS THE MAIN REASON JUST OVER HALF OF THE COMPANIES ON THE FORTUNE 500 HAVE DISAPPEARED SINCE THE YEAR 2000." PIERRE NANTERME, CEO OF ACCENTURE

Market trends

Today's enterprises are dynamic and evolving. According to IDC, 72% of the world's employees will be mobile by 2020, and more than 20B devices will be connected to the internet of things. This digital evolution has also 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 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 identity solution that is agile and secure, enabling trusted identities and transactions for business continuity.

7.6B

connected people

75B

connected devices

24B

Connected mobile devices by 2020

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

Questions to ask when considering multi-factor authentication

How will multi-factor authentication affect your customers?

- There is a perception that authentication can cause friction for your customers, so you need to ensure your identity solution of choice is secure and frictionless. To exceed customer expectations, look for a transparent, contextual authentication solution that opens up new services to the end user while ensuring security.

What types of users do you 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.

What applications and resources fit into your immediate authentication plans? Future authentication plans?

- A majority of companies will look for a solution that meets their immediate authentication needs. It's important to be aware of 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 the hassle of switching vendors, which will ultimately reduce your costs.

What is your 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. Your IT department may not be ready to move to the cloud, preferring an on-premises solution. The key is to ensure you have a solution today that will protect your investment – allowing you to transition to the cloud when you are ready.

How do you rate cost, security, and UX priorities?

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

How important is enterprise mobility to your organization?

- As your mobile workforce continues to increase, consider providing 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 provider to provide an even more secure, frictionless experience for you and your employees.

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 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 cost, security, and interoperability.

Key Cloud Considerations

Cost **Security** **Interoperability**

Cost

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

- 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?

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?

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:

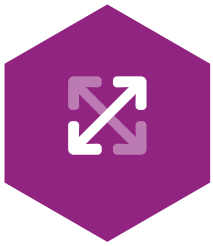
- What applications and services need to interface with the authentication solution?
- Are these applications and services on-premises or cloud-based?
- Do they require specific software versions?
- What upgrade cycles are they on?

Top features to look for in a cloud multi-factor identity 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 criteria you should look for in a cloud-based multi-factor authentication solution are:

Top Criteria



IT agility and flexibility

User experience

Business impact

"78% OF IT SECURITY TEAMS ARE LOOKING TO EMBRACE ZERO TRUST NETWORK ACCESS IN THE FUTURE."
- 2019 ZERO TRUST ADOPTION REPORT, CYBERSECURITY INSIDERS

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 adapt 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. Identity solutions should be able to discern which assets and applications require multifactor authentication depending on real time risk and provide configurable policies to secure access.

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 technical ability of the user accessing the device, you may want to choose different methods of authentication. Various options include:

- **SMS/Email one-time passwords (OTP)**
- **Grid cards**
- **QR codes**
- **Device authentication**
- **Soft tokens**
- **Hard tokens**
- **Mutual authentication**
- **Push notifications**
- **Biometrics**
- **Mobile smart credentials**
- **Digital certificates**

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. Users should not be blocked if they forget to carry their default authenticator.

Modern, multi-level authentication approaches

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

- **Device reputation:** Recognizing and detecting fraud across internet devices based on patterns to stop fraud and abuse in real time, prior to login. Can review the integrity of a device before a trusted identity is provisioned to a user, e.g., bring your own device (BYOD) and mobile precheck.
- **Transactional analytics and behavioral biometrics:** Analyzing points of user interaction such as number of login times, adding an abnormal number of payees, or different touch/swipe motion on a mobile device to gain a complete picture of potentially fraudulent behavior.
- **Adaptive risk-based authentication:** If risk is elevated for a user, it's important to enable step up authentication that is still frictionless for the end user. Examples include mobile push authentication, touchID, and Bluetooth wireless login.

Configurable and adaptive risk-based policies

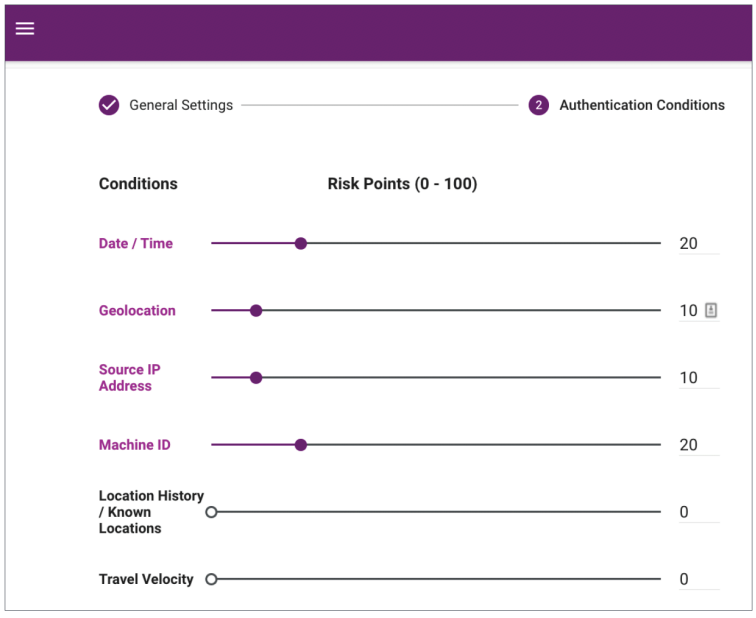
Identity solutions are not one size fits all, especially when it comes to security. Effective authentication solutions provide easy-to-configure, adaptive risk-based policies that allow administrators to define access control policies on a per application, per user group basis using:

- **Weighted risk factors:** Risk factors could be weighted differently within the same application or asset depending on user group.
  - E.g., 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.

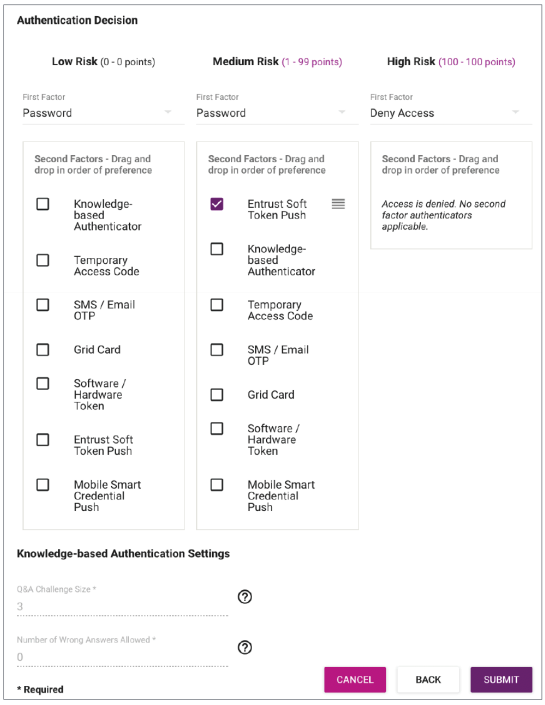
With a flexible authentication solution, you are able to assign varying levels of authentication based on real-time user access in accordance with configured policies.

Entrust Identity as a Service — 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)

Availability

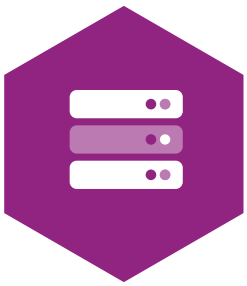
Managing authentication threats is a critical aspect of digital business. The speed of digital business, as well as the anytime-anywhere demands of users increase risk and put more pressure on the authentication solution to be constantly available, as any moment of unavailability is experienced by a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

"THROUGH 2023, ORGANIZATIONS THAT CAN INSTILL DIGITAL TRUST WILL BE ABLE TO PARTICIPATE IN 50% MORE ECOSYSTEMS TO EXPAND REVENUE GENERATION OPPORTUNITIES."

DIGITAL TRUST DRIVES CUSTOMER SATISFACTION AND BUSINESS RESULTS, GARTNER, AUGUST 2020

A good security solution is highly available and resilient against security incidents and downtime. If you select a cloud-based authentication solution, ensure 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 percent, backed by the provider's SLA (service level agreement.)

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



Highly available (at least 99.9% 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

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 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.

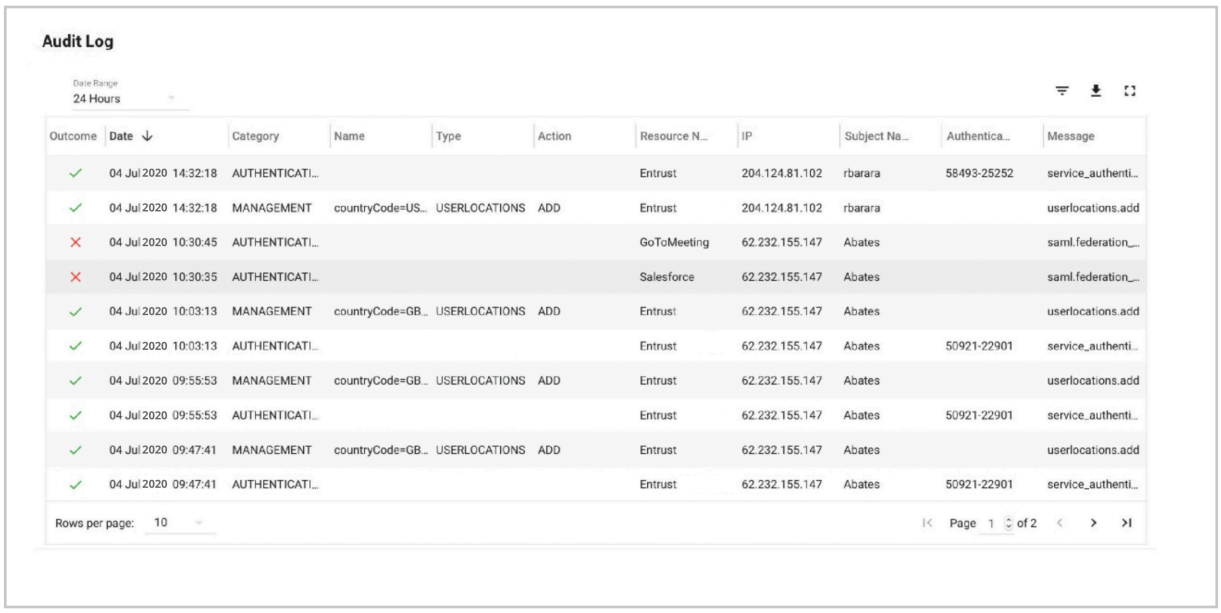
Ensure that your provider is able to integrate with all your applications through configuration and also provides RESTful APIs for automation of workflows.

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.



User Experience

Striking the right balance between security and user experience

Above all, an identity solution should keep your organization and users secure. But the most secure authentication isn't necessarily the best authentication solution. Good security solutions instead weigh the risk of the 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.

Mobility in the workplace

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

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 require a click or swipe of a button to verify access/transactions**
- **Biometric authentication (fingerprint, facial biometrics etc.), enable a transparent experience for your users**
- **Seamless integration with EMM solutions (VMWare, MobileIron etc.) provide a comprehensive solution for you and a better user experience for your users**
- **Mobile smart credentials act as a virtual smart card, increasing security and streamling user endpoints such as physical and logical access**
- **Ensures a user's device has not been compromised, to protect the user's credentials and company's assets**

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 any time, anywhere – when it's most convenient for them.

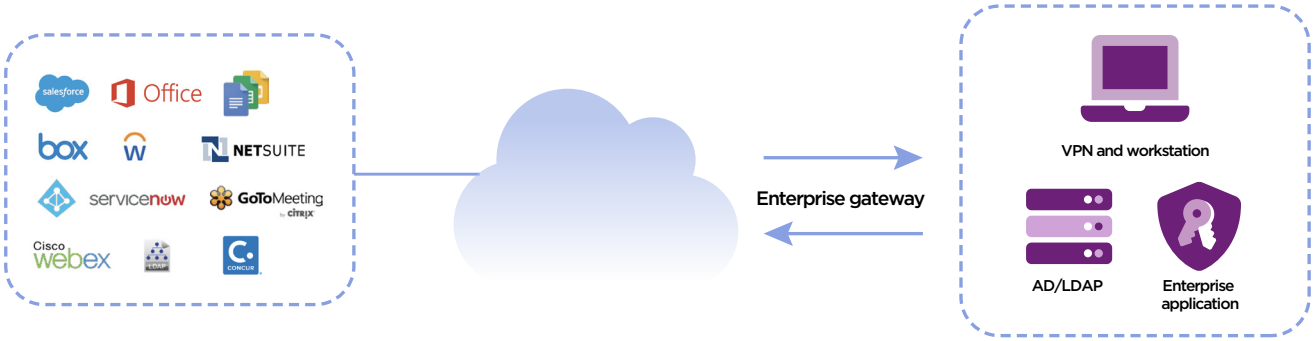
50% OF HELP DESK COSTS ARE MADE UP OF PASSWORD RESETS. - WORLD ECONOMIC FORUM PASSWORDLESS AUTHENTICATION WHITEPAPER, JANUARY 2020

Business Impact

You need an authentication solution that not only meets your current device and user needs, but can also 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.

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 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. Seventy to eighty 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.

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 provides the compliance you require and may include:

Total Cost of Ownership

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

- **Has a solution that scales 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**

CONCLUSION

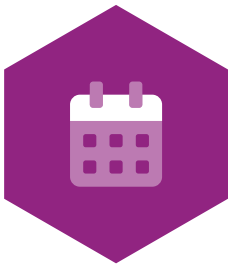
A vendor you can trust

The key to your organization's digital transformation is choosing the right authentication solution partner, and Entrust has been a leader in trusted identity for more than 25 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.

Leader in Trusted Identity



Over 25 years of trusted identity solution experiences

Serving global organizations from world governments to digital business innovators

With an innovative, end-to-end solution

Entrust has protected 95M+ workforce and consumer identities.

For more information

888.690.2424
+1 952 933 1223
info@entrust.com

entrust.com

ABOUT ENTRUST CORPORATION

About Entrust Corporation: Entrust secures a rapidly changing world by enabling trusted identities, payments, and data protection. Today more than ever, people demand seamless, secure experiences, whether they're crossing borders, making a purchase, accessing e-government services, or logging into corporate networks. Entrust offers an unmatched breadth of digital security and credential issuance solutions at the very heart of all these interactions. With more than 2,500 colleagues, a network of global partners, and customers in over 150 countries, it's no wonder the world's most entrusted organizations trust us.

Learn more at
entrust.com

ENTRUST

U.S. Toll-Free Phone: 888 690 2424
International Phone: +1 952 933 1223
info@entrust.com