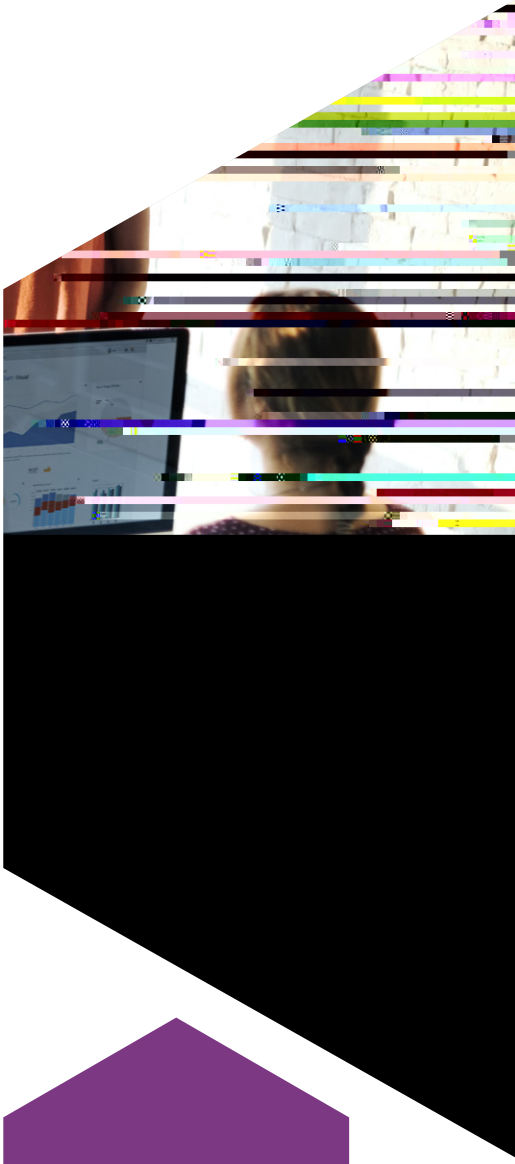
ENTRUST

SECURING A WORLD N

To this day, many enterprises rely on the timeworn defense of password protection. In a world where

Business challenge summary

Protecting access to information, systems, or valuables with passwords is a tired tactic. Perhaps the best known password of all time is the one that restricted access to a cave sheltering great riches in the ancient fable Ali Baba and the Forty Thieves. That password, of course, was “Open Sesame,” and there is no reckoning the countless disappointed children who have tried and failed to gain access to some coveted nook with that timeless phrase.



Six top features to consider in a multi-factor authentication solution

Maximizing the potential of a multi-factor authentication methodology requires the installation of a system that delivers a full range of key capability and usability features. The following, in particular, should be considered must-have features for multi-factor solutions undergoing evaluation for deployment in any organization:

1. **Security:** The chief benefit that any multi-factor authentication solution must o□er is e□ective security against a range of modern, continuously escalating security threats. The capabilities of a multi-factor system should provide a quantum leap beyond the defensive capabilities o□ered by one- and two-factor authentication solutions. And a solution that enables contextual intelligence support provides greater security against evolving cybersecurity threats.
2. **Productivity:** Choosing the right multi-factor authentication solution can enhance user productivity, particularly in comparison to two-factor solutions. Multi-factor solutions that o□er easy implementation, easy administration, and an improved user experience will work to leverage the productivity potential of sta□ members. It will also limit the productivity-stifling occurrences of security breaches.

3. **User experience:** Though it may seem counterintuitive, a multi-factor solution can o□er the potential of a more streamlined and transparent user experience. A multi-factor solution that is designed to be user-centric should be flexible and adaptive, providing a level of convenience that slashes user resistance and spurs widespread organizational adoption. Solutions that o□er contextual intelligence capabilities further enhance the user experience by adjusting the level of authentication needed in response to threat level assessments.

4. **Lower total cost of ownership (TCO):** Choosing the right multi-factor authentication solution can substantially lower TCO while also boosting user productivity and strengthening organizational security. It is quite realistic, in fact, to anticipate a cost reduction of up to 50 percent over traditional two-factor authentication solutions.

5. **Hassle-free administration:** A multi-factor solution should enable faster and easier administration by streamlining — or even eliminating — common administrative chores such as user enrollment and maintenance.

6. **Flexibility and reliability:** Both e□ectiveness and usability are enhanced with multi-factor solutions that provide a range of security token delivery options (SMS, email, app, voice-call, etc.). The best multi-factor solutions also maximize reliability by o□ering features such as automatic failover mechanisms and location-aware dispatching capabilities.

Citrix Ready secure remote access program overview

Citrix solutions deliver a complete portfolio of products supporting secure access of apps and data anytime, at any place, on any device, and on any network. These include:

1. **XenApp and XenDesktop** to manage apps and desktops centrally inside the data center
2. **XenMobile** to secure mobile applications and devices while providing a great user experience
3. **ShareFile** to provide controlled and audited data access, storage, and sharing, both on-premise and in the cloud
4. **NetScaler** to contextualize and control connectivity with end-to-end system and user visibility

Citrix solutions also integrate with third-party security products to provide advanced levels of system management and identity, endpoint, and network protection. The Citrix Ready Secure Remote Access program was launched to identify and showcase partner products that are proven to both smoothly integrate with Citrix products and help enhance Secure Remote Access by adding extra layers of security. The Citrix Ready Secure Remote Access program serves as an aid to IT executives in quickly and easily finding and sourcing solutions for their Secure Remote Access needs, helping to secure organizations' corporate networks from theft of data, DDoS, and other security attacks that may be perpetuated via Remote Access.

Citrix advises that organizations can best defend against security attacks that might occur through Remote Access by following five best practices — pillars of focus that support enterprise security:

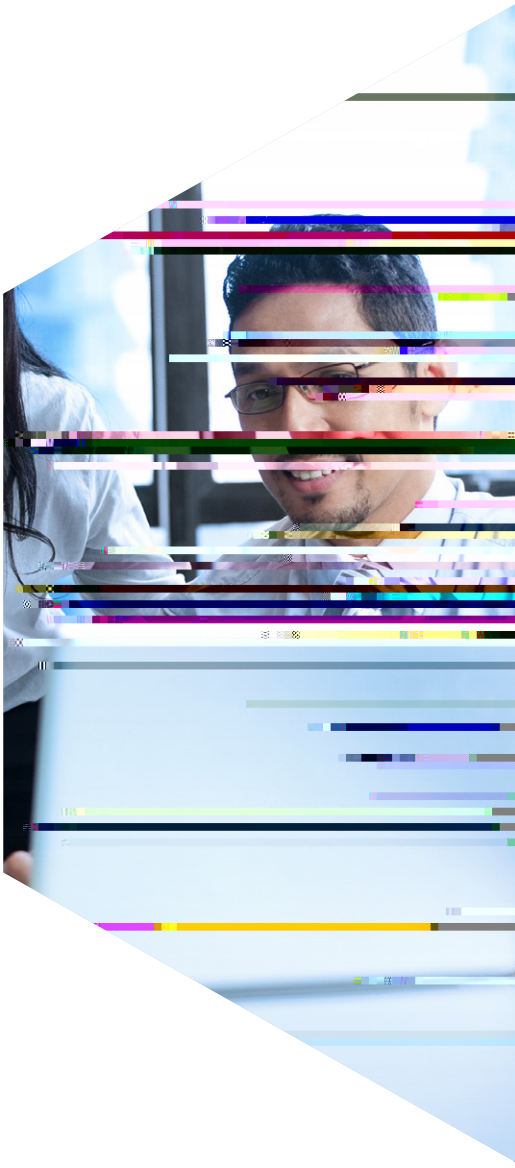
1. **Identity and access:** Administrators must be able to identify users requesting access to a system and limit the degree of access granted. In comparison to simple password-based systems, multi-factor authentication o□ers a vast improvement in the ability to properly identify requests for access. The degree of access granted to each individual user should be based on context. The principle of least privilege helps to ensure that users are granted rights that are limited only to those required in the performance of their jobs. Any authentication solution should meet this key requirement for di□erentiated access to di□erent resources by taking advantage of authorization capabilities in, for example, Citrix NetScaler.

2. **Network security:** The growing demand for remote access complicates the process of securing a network. Yet the integrity of network security must be maintained while supporting remote access for mobile and third-party users. Network and host segmentation can be useful in shrinking surfaces that are vulnerable to attack. And implementing a multi-layer approach helps to boost network security while ensuring availability.

3. **Application security:** All types of applications are potential targets for hackers, but the veritable explosion of apps has created many additional points of vulnerability for most enterprises. Apps on mobile devices are particularly susceptible to exploitation. An important step in reducing risk is enacting centralization and the encrypted delivery of applications. Containerization for mobile apps and inspection of incoming data streams can help to reduce app-related security vulnerabilities.

4. **Data security:** The security of enterprise data can be enhanced by the centralization and hosted delivery of data by enforcing secure file sharing (to reduce data loss) and by the containerization of data (both in-transit and at rest).

5. **Monitoring and response:** Vigilance and fast action are required to successfully counter the attacks that most enterprises face on a daily basis. A rapid response to breaches is also critically important, given that even the most secure systems are not completely invulnerable to successful attacks. Rapid detection and response to successful attacks serve to minimize damage and help to limit susceptibility to imminent additional attacks. End-to-end visibility into application tra□c supports faster identification of security breaches and system anomalies.



The benefits and burdens of remote access

Remote access has enabled an entirely new paradigm of workplace flexibility and productivity. Indeed, the very meaning of the word “workplace” must be redefined to be less location-specific and more worker-specific. The adoption of mobility enhancing tools such as t2.8 (s)-10 ( )]TJ 1 n.-5.1 (c)9.9 (e)-3.8 (/0-1.3 (s5.9 (sr)-24, s(i)10 m.6 (c)46 (i) (e)01 (n)5)19.2)-5.8

A proven partnership that provides increased security with fewer hassles

Entrust Identity Essentials benefits users with enhanced security, keeping the mounting cyberthreats of a dangerous world at bay. Compared to traditional two-factor solutions, Entrust Identity Essentials provides better security while also o□ering an easy to use interface, making life simpler for administrators and users alike. Computer systems and enterprise data are kept safe, while productivity is simultaneously increased. The net result is a substantial decrease in TCO relative to other security solutions.

Entrust Identity Essentials has proven to integrate seamlessly and easily with Citrix network security systems to provide an unbeatable enterprise multi-factor authentication platform. Entrust Identity Essential's selection to the Citrix Ready Secure Remote Access program provides enterprises with a proven, reliable remote access security solution for facing the ever-escalating needs of the modern business environment. For companies seeking to protect themselves against the modern-day scourge of cybercrime, the

ABOUT CITRIX READY

Citrix Ready Program is a technology partner program that helps software and hardware vendors of all types develop and integrate their products with Citrix technology for Digital Workspace, Networking, and Analytics. To become a partner and earn the Citrix Ready designation, partners validate their solutions through a robust testing and verification process that ensures compatibility with Citrix solutions. Technical specialists are available to assist with the integration and testing phases on the way to Citrix Ready verification. Partners can then participate in joint marketing activities to drive awareness and generate demand for their solutions. Partner solutions are also listed in the Citrix Ready Marketplace, a website that customers can use to easily search and find compatible solutions for their Citrix deployments or environment.

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 o□ers 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.