White Paper

Best Practices for Securing Remote Access with Multi-Factor Authentication

Identity Essentials

ENTRUST

SECURING A WORLD IN MOTION

CITRIX READY

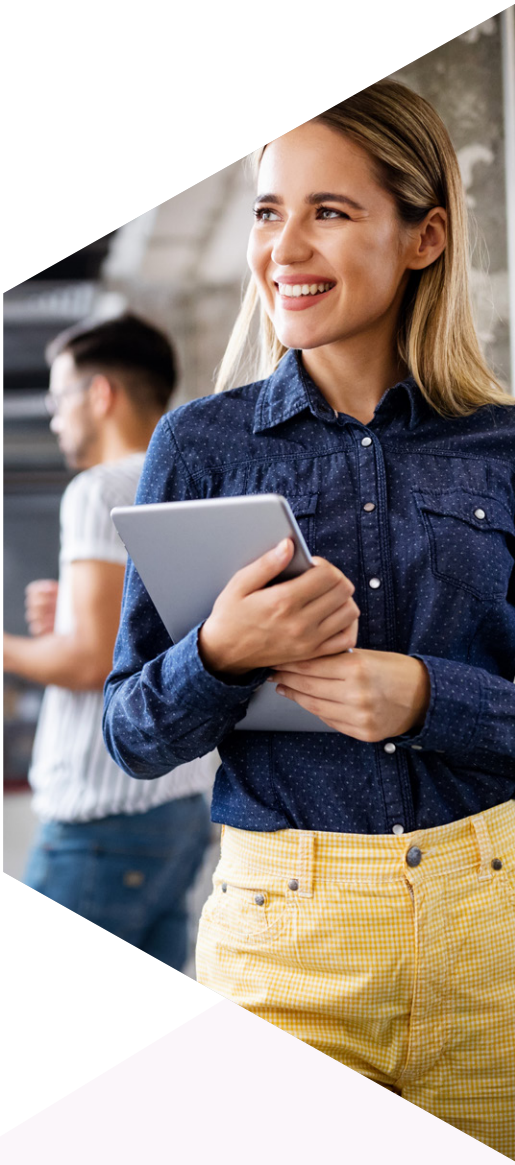
It has been said that there are only two kinds of companies: those who know that they've been hacked, and those who don't.

Cybersecurity is a concern for every company on the planet, and bad things are likely to befall any enterprise where cybersecuity isn't top-of-mind for executive leadership.

To this day, many enterprises rely on the timeworn defense of password protection. In a world where 80 percent of breaches result from weak or stolen credentials (Verizon), relying on such a waning buffer is risky. Internationally recognized corporations have lost resources, prestige, and public goodwill due to simple password hacks. With this substantial susceptibility, more strategic security is necessary for properly protecting enterprise systems and information.

Fortunately, companies using Citrix have a way forward. Entrust Identity Essentials is a Citrix-Ready-certified product. It is a purpose-built authentication system uniquely suited to meet the security demands of modern enterprises while providing an excellent user experience.

This paper discusses the importance of deploying a multi-factor authentication system as an effective defense against modern cybercriminals. It also describes the effectiveness of teaming Citrix NetScaler with Entrust Identity Essentials to meet the growing need for a secure remote access solution for enterprises worldwide.



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.

As the information age dawned, it was perfectly logical to deploy the ancient tradition of the password in protecting access to computer systems. It is thought that the first password-protected computer system was MIT's Compatible Time-Sharing System (CTSS) in the early 1960s. The CTSS pioneered many tools of the modern age, including file sharing, instant messaging and email. Ironically — but not coincidentally — the CTSS may also have been the very first computer system to have been hacked, resulting in a data breach, according to Wired.

Much has changed since those days. Organizations are now able to select differing levels of authentication:

1. **One-factor:** Typically something the user knows, like a password.
2. **Two-factor:** Typically, something the user knows and something the user has (a token, card, fingerprint, phone).
3. **Multi-factor:** Multi-factor authentication uses multiple factors to validate the user's identity. Authentication factors may include items such as location, network, time of day, session ID, device, or even biometric factors such as fingerprints and retinal scans.

citrix™ NetScaler

Though one-factor authentication vehicles such as passwords and PINs have dominated computer system security for decades, the faults of one-factor authentication are becoming better known — and more costly. According to the Verizon 2020 Data Breach Investigations Report, "80 percent of confirmed data breaches involved weak, default, or stolen passwords."

One-factor authentication solutions are limited in their capabilities. Cybercriminals are constantly improving and devising inventive ways to foil them — such as keylogging malware for snaring passwords from unsuspecting users, or skimming data from point-of-sale devices.

The burgeoning threat of phishing attacks continues to result in the widespread theft of user credentials. According to the Verizon 2020 Data Breach Investigations Report, phishing is the #1 form of attack, up from #3 in 2018. Ninety-six percent of the time, these phishing attempts leverage email, and over 60 percent of attempts target credentials.

Two-factor authentication solutions have certainly provided a more effective defense than one-factor solutions against the many and varied modern security threats. But commonly deployed two-factor authentication solutions — such as adding the requirement to produce a hardware or software token in addition to providing a password — have likely frustrated users more than they've foiled cybercriminals. The inherent inconvenience of two-factor methodologies — often clunky and slow — sends user frustration rates soaring and adoption rates plummeting.

The need for an authentication solution that can counter cybercriminals without frustrating users has never been more urgent — particularly in conjunction with the growing trend toward remote accessibility. Accordingly, more and more organizations are moving to the logical next step in tightening their defenses against cybercriminals: multi-factor authentication.

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:

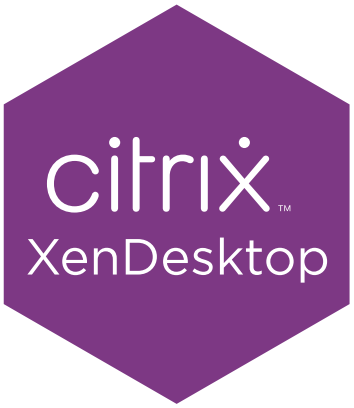
1. **Security:** The chief benefit that any multi-factor authentication solution must offer is effective security against a range of modern, continuously escalating security threats. The capabilities of a multi-factor system should provide a quantum leap beyond the defensive capabilities offered by one- 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 offer easy implementation, easy administration, and an improved user experience will work to leverage the productivity potential of staff 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 offer 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 offer 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 effectiveness 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 offering 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:

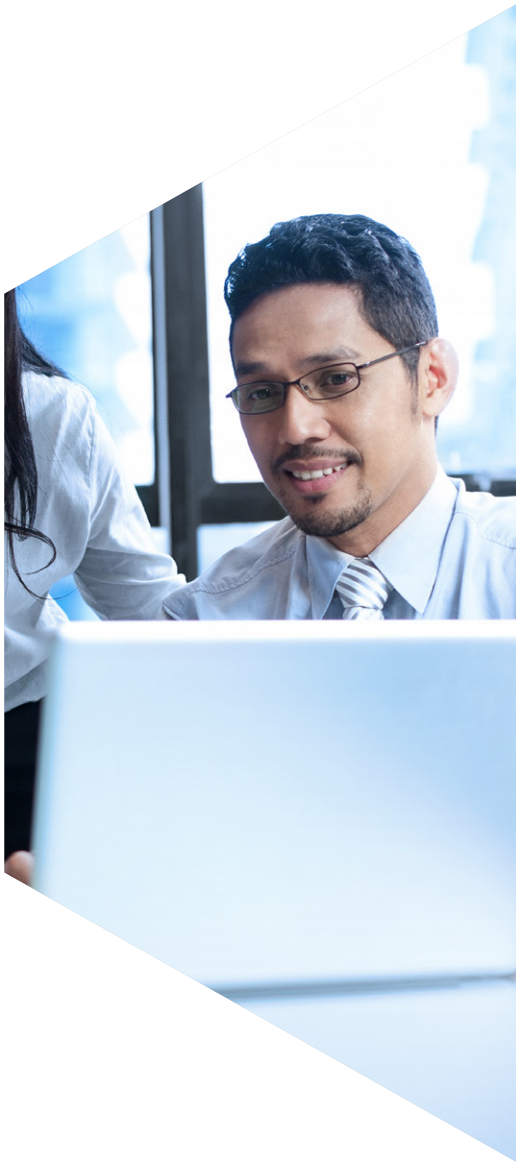
1. **Identity and access:** Administrators must be able to identify users requesting access to a system and limit the degree of access granted. In comparison to simple password-based systems, multi-factor authentication offers a vast improvement in the ability to properly identify requests for access. 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 differentiated access to different 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 traffic 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 tablets, smartphones, and other devices has transformed many enterprise roles into an any place, any time proposition. Workers have benefited from schedules that offer more flexibility, helping to enhance both work- and home-life. Companies have benefited from the leaps of productivity that remote access enables.

But this ongoing paradigm shift has required that enterprises find ways to balance the protection of sensitive data with the impact of remote access upon user flexibility — the widespread use of virtual private networks (VPNs) over unsecured networks, for example.

While remote access does increase the burden of safeguarding enterprise systems and data, the benefits of remote access justify the need for an increased focus upon security. The Citrix Ready Secure Remote Access program is designed to help enterprises conform to the five security pillars listed above while meeting the skyrocketing demand for more remote access capabilities.

Entrust Identity Essentials has been selected to participate in the Citrix Ready Secure Remote Access program. Entrust Identity Essentials has demonstrated the ability to consistently conform with, and support, the five security pillars of the Secure Remote Access program.

Key features of Entrust Identity Essentials include:

- **Easy administration:** Entrust Identity Essentials provides incomparable ease of administration, beginning with quick and easy installation. Flexible and policy-driven administration requirements serve to protect multiple platforms deployed on a mobile scale. Automated routine administrative chores, such as password resets, foster dramatically easier administration along with enhanced usability and adaptability. All of this eliminates the need for special skill sets for administrators. The same skills required to administer Citrix NetScaler are sufficient.
- **Alerts:** Entrust Identity Essentials offers customizable alerts, providing administrators with instantaneous notifications of in-progress attacks or breaches.
- **Adaptive user authentication:** Entrust Identity Essentials leverages contextual information to heighten security while simultaneously enhancing usability and transparency. Contextual factors such as login location, time of login, and many others are used to customize the level of security required. In some cases contextualization altogether eliminates the need for the user to enter additional layers of information.
- **Contextual message dispatching:** Entrust Identity Essentials can be configured to automatically select the most appropriate passcode delivery method based on the login context of the user, such as the geographical location. So for example, if a user is on a business trip to India, the solution can be set up to deliver the OTP via a local service provider, to keep the reliability of delivery higher. And in the event that a user is in an area with poor cellular coverage the solution will deliver the OTP via the Entrust Identity Essentials App or any of the available secondary delivery methods.
- **Geolocation:** The solution's context-based capabilities include comparing a user's geographical location to known trusted or non-trusted locations, and adjusting authentication requirements accordingly.

Entrust Overview

Entrust is privately held and employs more than 2,500 people globally — and the sales and service network covers more than 150 countries worldwide. Entrust solutions are used to safeguard billions of transactions annually and issue 10M+ highly secure identity and payment credentials every day.

Unique offerings of Entrust multi-factor authentication solution, include:

- **Real-time, session-specific security:** Traditional two-factor authentication typically relies on pre-issued token codes — meaning they are vulnerable to theft and simple phishing attacks. Entrust's solution, however, works in real time and generates codes that are only good at the point of login. This means that any codes intercepted by the hacker will not grant the hacker access.
- **No pre-issued token codes:** Entrust Identity Essentials does not rely upon pre-issued token codes. Entrust Identity Essentials sends users a one-time passcode, generated at the time of the user login request. This methodology enables session-specific identification and authentication, denying cybercriminals the opportunity to steal codes over a longer timeframe.
- **Geofencing:** Entrust Identity Essentials allows admins to whitelist and blacklist based on systems and locations. That is, they may limit access through Citrix NetScaler from certain countries, organizations, IP addresses, etc.

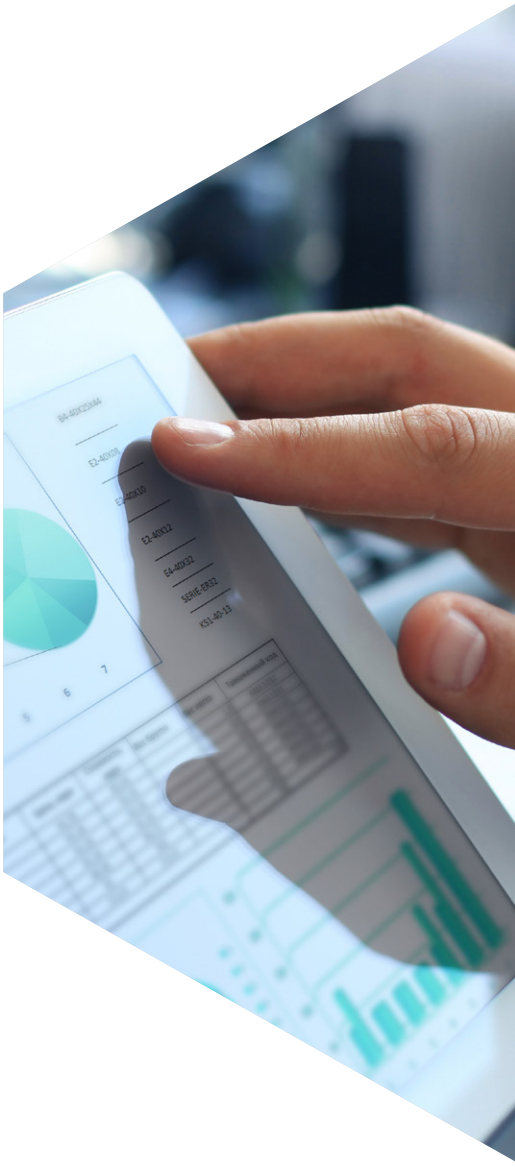
Ultimately, Entrust Identity Essentials offers a perfect fit for organizations that have a need for Secure Remote Access capabilities. The solution integrates seamlessly with a variety of third-party systems, catering to the requirements of today's mobile and digital workforce.

Entrust Identity Essentials also integrates with Citrix NetScaler, enabling Secure Remote Access to applications, networks, and desktops. While Entrust Identity Essentials was originally designed to integrate only with Citrix, many additional system integrations are now supported.

The result is a multi-factor solution that fits Citrix NetScaler, and the benefits accrue to both administrators and users. Installation, the management of routine administrative duties such as resetting passwords, and everyday usability are all easier and more user-friendly than with competing multi-factor authorization solutions. Every day, thousands of Citrix customers worldwide enjoy an easier-to-use, more secure, remote access solution thanks to the teaming of NetScaler and Entrust Identity Essentials.

Choosing the appropriate level of security authentication requires evaluating a number of variables, including the cost of potential worst-case security breaches. But in today's world, one-factor authentication will be insufficient for most organizations. More often than not, the level of risk faced by an organization or department will more than justify the deployment of a form of multi-factor authentication.

Entrust Identity Essentials



Entrust Identity Essentials incorporates a number of innovative features that are not available with other multi-factor solutions. Entrust Identity Essential's adaptive, contextual solution provides a much sought-after balance between strong security and user experience.

One example is the solution's ability to track the location of Citrix XenDesktop locations. An access request from a location known to be safe may enable the bypassing of a onetime passcode submission. For example a user logging in from the corporate HQ, a branch office, or even their home office is not prompted for a one-time-passcode. This simplifies user compliance with security requirements and enhances the user experience leading to increased productivity.

Entrust Identity Essentials also provides token codes that are unique to individual Citrix NetScaler sessions. The token code is sent to the user's mobile phone and will only work on the device that initiated the login request. The solution integrates easily with NetScaler, requiring an authentication server set up with RADIUS Authentication, or potentially several RADIUS servers for failover, load balancing, and high-availability.

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 offering 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 partnership of Citrix and Entrust Identity Essentials offers a win win across the board.

For more information about Entrust Identity Essentials, please visit: www.entrust.com/go/IdentityEssentials

For more information about Citrix NetScaler, please visit: https://www.citrix.com/products/citrix-adc/

APPENDIX:

Learn more about the enterprise security advantages provided by Citrix NetScaler Unified Gateway.

Learn more about the threats and challenges facing organizations worldwide in the Verizon 2020 Data Breach Investigations Report.

To learn more about multi-factor security solutions, contact Citrix and Entrust.

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 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.

Citrix XenDesktop and Citrix Ready are trademarks of Citrix Systems, Inc. and/or one of its subsidiaries, and may be registered in the U.S. and other countries. Other product and company names mentioned herein may be trademarks of their respective companies.
Copyright © 2020 Citrix Systems, Inc. All rights reserved. IA21Q3-iam-best-practices-securing-remote-access-multifactor-authentication-wp