Multifactor Authentication and Identity Management for Secure Remote Access

CITRIX Ready

Symantec™ | CITRIX®

Mobile technologies give people the power to work wherever and whenever they choose. Remote access drives astonishing gains in productivity and employee satisfaction, but enterprises who use simple passwords to protect that access risk financial loss, data theft, and worse.

Passwords are to blame for some of the most infamous recent data breaches. At Anthem Blue Cross, attackers gained access to sensitive medical data using credentials stolen from a handful of database admins. Target, the retail giant, lost credit card information to cybercriminals who used credentials taken from contractors. The Democratic National Committee's most sensitive email messages were downloaded and published despite repeated warnings from the FBI.

Why is the venerable password such a spectacular security failure? The problem, unsurprisingly, is us: we are too trusting and too lazy. Successful cybercriminals are expert social engineers who design attacks that capitalize on these all-too-human weaknesses.

"Phishing" is one such attack. Cybercriminals lure credulous users with "password reset" or "account maintenance" requests that appear to be from a trusted entity (like a bank or an email provider). Once hooked, users willingly share their credentials, thinking they are simply completing a routine task.

"Credential stuffing" or "brute force" attacks target users who cut corners by reusing credentials across online accounts or by choosing easy-to-guess passwords. Attackers use automated attack tools to make millions of login attempts on dozens of sites in just a few hours, making it possible to efficiently find and take over poorly-protected accounts. Reuse is a big problem: research from Experian shows the average Internet user protects 26 online accounts with just five passwords.

Two-factor authentication is the answer to the password problem. By validating a second factor — such as a user's fingerprint or their possession of a trusted device – remote access security becomes far more robust. This paper discusses Symantec's intelligent two-factor authentication solutions that combine unprecedented ease of use with industry-leading effectiveness. Also described are the benefits of teaming Citrix with Symantec's two-factor solutions in meeting the growing need for a remote access security solution for enterprises worldwide.

Business Challenge Summary

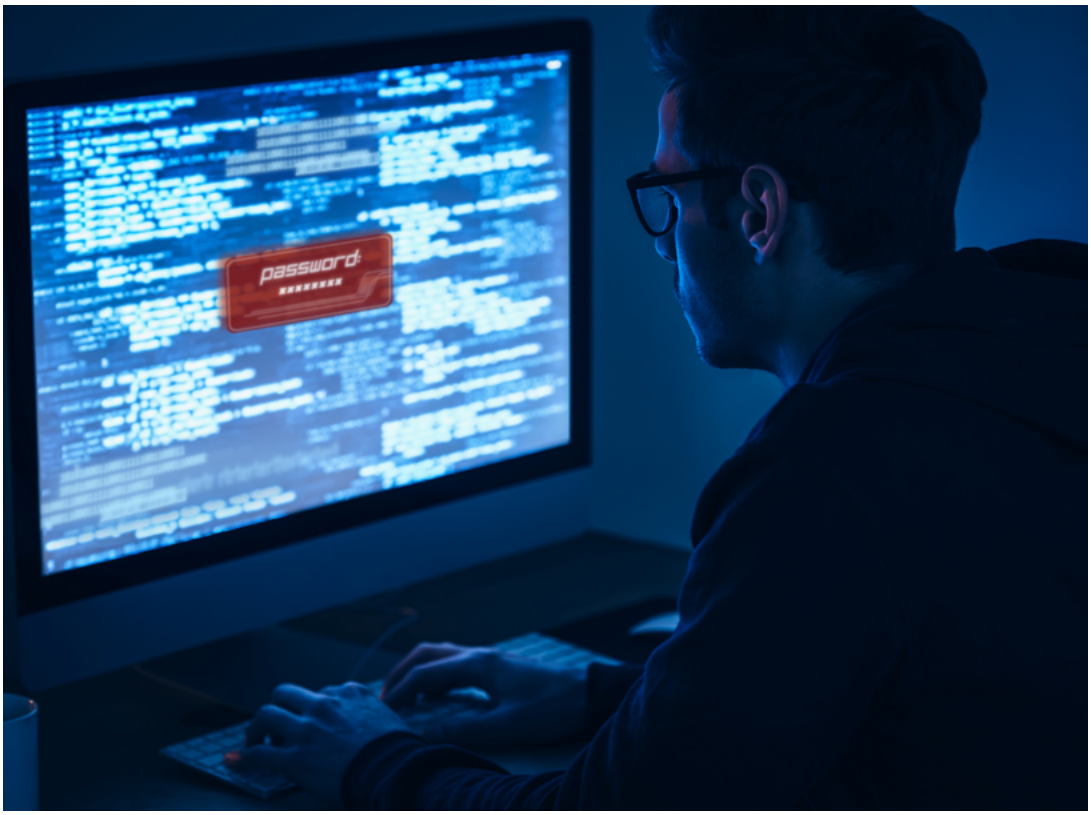
"The world is getting smaller." That is an observation people frequently make these days in reference to the seemingly globe-shrinking impact of advances in technology. But though the world may indeed seem much smaller than it once was, there is an interesting dichotomy to the globe-shrinking effect of recent technological advances: people have grown more remote. More specifically, workforces have grown more remote.

As technology has enabled ever-increasing degrees of mobility, workforces have become less centralized and more scattered. While "going to work" once referred to traveling to a physical location to perform a job, the meaning of that phrase is now much more ambiguous. For many workers, going to work involves simply connecting to their company's systems from wherever in the world they might happen to be. The trend toward remote work is growing at an explosive rate. The leadership of many companies anticipates that at least half of their fulltime staff will be working remotely within just a few years, according to a survey taken at the 2015 Global Leadership Summit in London.

The advent of mobility and remote access offers a rich array of benefits for both workers and companies, including substantial increases in productivity and reductions in costs. But it isn't all good news. The growing remote workforce has created some very serious security challenges for companies both large and small. There is a growing need to authenticate and manage the identities of users attempting to acquire access to companies' proprietary data and systems.

For many organizations, a simple query-password system remains the primary means of user authentication. But it is an unfortunate irony that the most effective passwords are the most difficult to remember.

As a result, many users resort to an easy-to-remember, easy-to-hack password. According to *Computerworld Magazine*, "123456" was the world's most used password in 2015. And more complex passwords are far more likely to be written down somewhere instead of trusted to memory, rendering them more susceptible to theft.



But even the most complex password stored only in a user's memory provides no more than a very primitive level of security, easily foiled by today's technologically sophisticated cybercriminals. Advanced password theft techniques such as phishing provide cybercriminals with the means to snatch passwords away from unsuspecting users. According to the *Verizon 2016 Data Breach Investigations Report*, approximately one out of every seven users will click on an email attachment during a phishing attack — and with very little hesitation.

Adding an extra layer of security in the form of two-factor authentication certainly helps to slow cybercriminals. But the additional protection provided by two-factor authentication varies greatly from one solution to the next. The most effective — and no less importantly, the most user-friendly — two-factor solutions are simple to use, and yet highly sophisticated in the behind-the-scenes workings and algorithms that drive the authentication process.

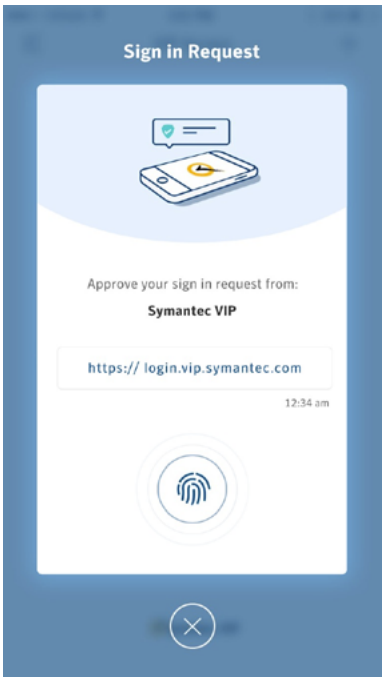
Intelligent two-factor authentication must accurately evaluate a variety of factors during the authentication process, such as the machine through which the request is occurring, its location and user behavior. Perhaps most importantly, effective two-factor solutions should be capable of identifying behavioral deviations in incoming authorization requests through comparisons with a matrix of established past behavioral patterns for that specific user. Incorporating this capability into a solution works to strengthen security while simultaneously enhancing usability.

The need for a two-factor authentication solution that can foil cybercriminals without frustrating users to distraction has never been more obvious or urgent — particularly in conjunction with the growing trend toward remote accessibility. Accordingly, more and more organizations are seeking a two-factor authentication methodology that combines intelligent, effective security with usability and dependability.

Top Three Features to Consider in a Two-Factor Authentication Solution

Maximizing the potential of a two-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 two-factor solutions undergoing evaluation for deployment in any organization:

1. **One-Time Password (OTP) Deployment:** Passwords that reside in a user's memory (or on a sticky note attached to their desk or computer monitor) and are used over and over with each login attempt are constantly exposed to theft. But one-time passwords are another matter. Generated randomly, specifically and uniquely for each login attempt, OTPs are used only one time and then never again. So even if somehow intercepted by a cybercriminal, an OTP will be useless in later attempting an illicit login attempt.



2. **Biometric and Push Authentication:** Biometric authentication offers an unbeatable combo of security and convenience. Many biometric applications, for example, require only that the user press a fingertip to a scanner. Biometric verification is typically very easy and convenient for users, and yet provides a very effective defense against illicit login attempts. Similarly, push authentication also offers an extra layer of security with minimal inconvenience to the user. Response to a push authentication requires no more than a tap of the fingertip to the user's phone. A multifactor authentication solution should offer either biometric or push authentication, with the best solutions offering a choice of one or the other to accommodate the user's preference.

3. **Risk-Based Authentication and User Behavior Analytics:** The ultimate goal of any security solution should be to maximize protection while minimizing user inconvenience. While second-factor authentication provides a substantial boost in security, that extra factor of authentication isn't always needed. The best two-factor solutions have the ability to determine when and if an explicit second factor of authentication is required. The solution might determine, for example, that a login attempt from a registered device perfectly mirrors that user's behavioral history, making it safe to drop the second-

factor requirement. The ability to intelligently apply the security policy assures that the protection potential of a two-factor solution is fully realized, and yet customizes each login experience to minimize inconvenience to the user.

CITRIX® XenDesktop

CITRIX® XenApp

CITRIX® XenMobile

CITRIX® ShareFile

CITRIX® NetScaler

Citrix Ready Secure Remote Access Program Overview

Citrix solutions deliver a complete portfolio of products supporting the 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 smoothly integrate with Citrix products, and that work to 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 confirm the identity of users requesting access to a system and limit the degree of access granted. In comparison to simple password-based systems, two-factor authentication offers a vast improvement in the ability to properly confirm user identity in 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.
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 multifactor 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

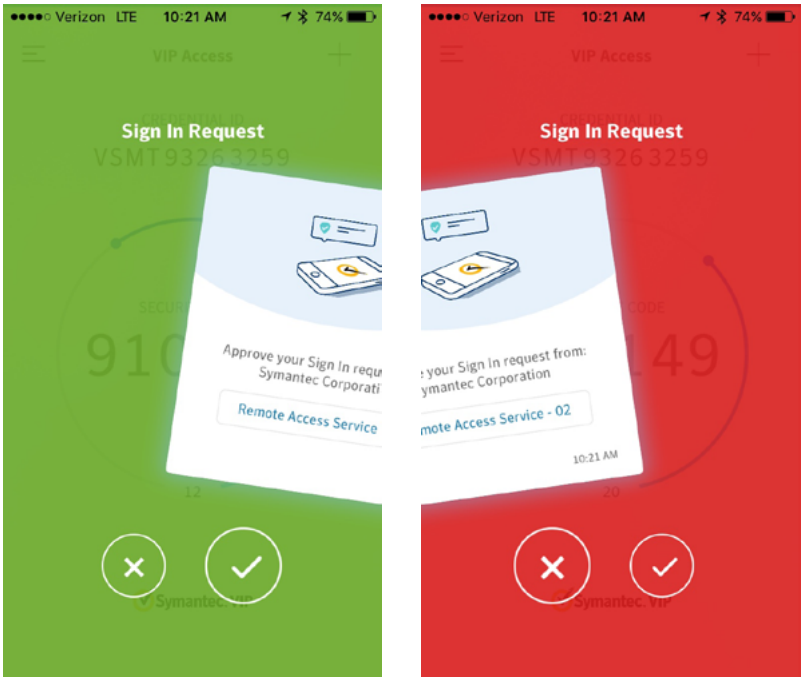
Remote access has enabled an entirely new paradigm of workplace flexibility and productivity. Indeed, the very meaning of the word "workplace" must be redefined to be less location-specific, and more worker-specific. The adoption of mobility enhancing tools such as tablets, smartphones and other devices 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 public 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 justifies 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.

Symantec has been selected to participate in the Citrix Ready Secure Remote Access program. Symantec's intelligent two-factor authentication solution has demonstrated the ability to consistently conform with, and support, the five security pillars of the Secure Remote Access program.

Notably, Citrix — an early adopter of two-factor authentication — has selected Symantec VIP as its current two-factor authentication solution. Since implementing Symantec VIP, Citrix has experienced a 60 percent reduction in total cost of ownership, with an eightfold reduction in administration time. And global deployment of the solution was accomplished in less than 48 hours.



Key features of Symantec's authentication solutions include:

- **Broad Range of Two-Factor Options:** Push verification, biometric fingerprint, intelligent authentication, software or hardware one-time password, out-of-band, SMS and voice-based credentials, and more. Symantec simplifies security with a broad range of two-factor authentication options for customers to pick.
- **Single Sign-On:** VIP Access Manager integrates Single Sign-On (SSO) capability with strong authentication, access control and user management, providing outstanding flexibility and convenience for both users and administrators. SSO capability also enhances workforce mobility by improving cloud application usability.
- **Straightforward, Established Installation Process:** Symantec provides clear and accessible documentation for integration with Citrix NetScaler (more information here). The installation process is straightforward and can be completed quickly. As noted above, Citrix deployed Symantec VIP globally in less than 48 hours.

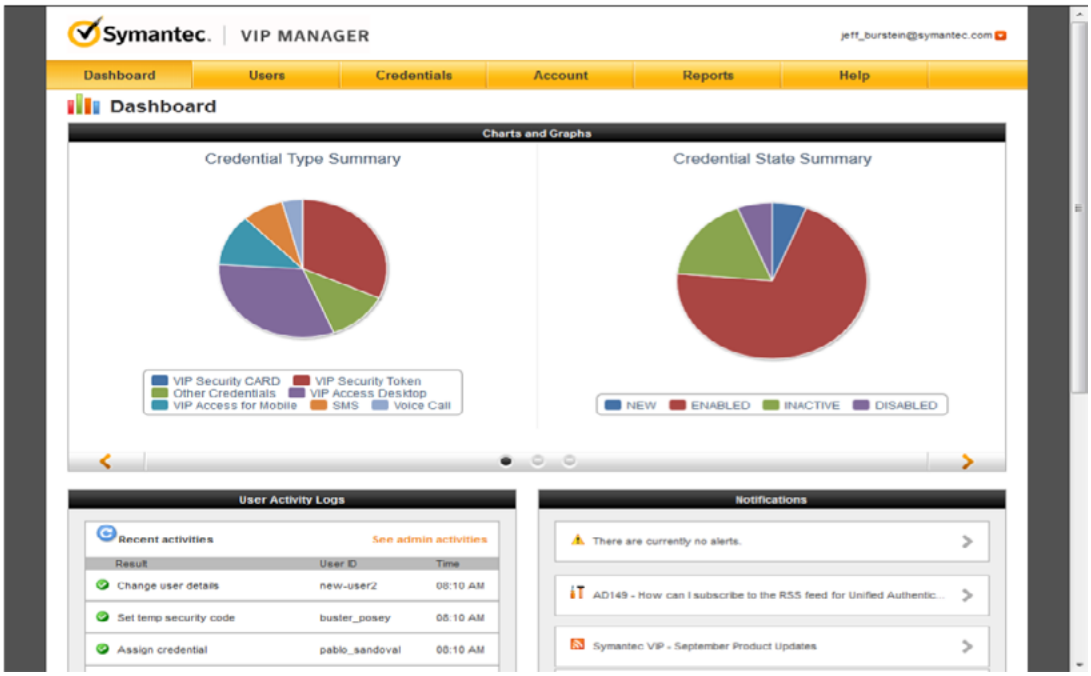
Overview of Symantec

Symantec is a global leader in providing security and information management solutions to customers ranging from consumers and small businesses to the largest global organizations. Symantec's security solutions help to secure and manage customers' information against more risks at more points, more effectively and efficiently than any other company. The company's unique focus is the elimination of risks to information, technology and processes, independent of the device, platform, interaction or location.

Symantec's flagship authentication solutions include Symantec VIP and Symantec VIP Access Manager.

Symantec VIP and Access Manager provide secure access that is cost effective, easy to manage, and user friendly. VIP can help businesses control costs and reduce IT burdens, while simultaneously increasing user adoption rates and satisfaction. The product's unique ease-of-use also helps to slash user errors while boosting productivity.

The flexibility of VIP enables the securing of organizations' comprehensive user bases — including fixed-location employees, remote workers, partners, contractors, vendors, customers and more. The use of VIP is not limited to Virtual Public Networks, but is adaptable to nearly all network, cloud, or mobile/web applications



Symantec Solution Detail

Symantec VIP provides a user-friendly, cloud-based multifactor authentication solution that enables businesses to secure access to networks and applications without impacting productivity. VIP enhances user-friendly two-factor authentication by offering a choice of second-factor authentication methodologies: one-time passwords, remembered devices, one-touch push verification, biometric fingerprints, and risk-based intelligent authentication. VIP intelligent authentication incorporates a risk analysis engine that triggers two-factor authentication based on user, device, and location factors, maximizing protection while minimizing user inconveniences.

Symantec VIP Access Manager provides a single access point for protecting cloud and on-premise web applications via Single Sign-On (SSO). Access Manager utilizes Symantec VIP in providing the security of two-factor authentication. The solution integrates the convenience of SSO with strong authentication, access control and user management for both public and private cloud-based applications.

Both VIP and VIP Access Manager can:

- Protect against unauthorized access and data theft anytime, anywhere, and from any device
- Ensure secure access that is cost-effective and easy to manage
- Solve password management frustration while enhancing user friendliness
- Work for all use case scenarios, including:
    - o Business-to-employee
    - o Business-to-business
    - o Business-to-consumer

VIP and Access Manager integrate perfectly with Citrix products. Symantec's solutions support second-factor authentication factors delivered on users' mobile phones (push notification, biometric fingerprint, etc.). For users, complying with two-factor authentication can be as simple as pressing a fingertip to the phone. Browser-based authentication capability ensures that VPNs can be safely accessed via browsers over unsecured networks.

Unique features of Symantec's two-factor authentication solutions include:

- **Unparalleled Expertise and Experience:** Symantec is the industry leader in two-factor authentication solutions. Symantec was the very first company to offer two-factor authentication as a service. The company boasts a 20-year proven track record, and currently secures more than 3 billion validations per year for 13 million users worldwide.
- **Easy Integration with Citrix:** Symantec's solutions are designed for easy installment and integration with Citrix products, including NetScaler, XenApp and XenDesktop.
- **Admin- and User-Friendly:** Many two-factor solutions offer enhanced security, but only at the cost of nightmarish complications for both users and administrators. Ease-of-use of Symantec's solutions is enhanced through password-less two-factor authentication methodologies such as push-access requests and biometric fingerprint authorization. Intelligent authentication, using a behind-the-scenes risk analysis engine, constantly works to minimize user inconvenience without compromising security. And features such as support for administrator-defined policies make Symantec's solutions among the most admin-friendly on the market — reflected in the eightfold reduction in admin time experienced by Citrix after installing Symantec VIP.
- **Scalability:** VIP security is delivered in the cloud, mitigating the need for underlying hardware and software resources. As a result, the solution can be scaled to large user bases without deploying additional security-dedicated resources. Millions of users can be supported easily and cost-effectively.
- **Supports All Use Case Scenarios:** Symantec two-factor security solutions can support enterprise-to-employee, business-to-business and consumer use cases (such as banking, payment and e-commerce).

- **Trial Account Offer:** Enterprises can try Symantec's security solutions without an upfront commitment by deploying the product on a free trial basis. Once the decision is made to continue with the product long-term, trial accounts may conveniently be converted to paid accounts. And would-be buyers are vetted to assure that the product will be used only for legitimate business purposes, and not as a tool for devising workarounds to existing security protocols.

A Proven Partnership that Minimizes the Cost and Complexity of Two-Factor Authentication

Many companies are scrambling to find better bulwarks of defense against the current explosion of cybercrime. They are searching for solutions that keep systems and data more secure. But they are also seeking solutions that enhance security without associated incurred costs that blow budgets out of the water, or complications that slow the productivity of users. Symantec VIP and Symantec VIP Access Manager offer the extra layer of security that companies seek with two-factor authentication that is affordable to implement, easy to use and extremely effective.

Symantec's solutions are proven to integrate seamlessly and easily with Citrix network security systems to provide an unbeatable enterprise two-factor authentication platform. Symantec'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 security needs of the modern business environment. For companies seeking to protect themselves against the modern-day scourge of cybercrime, the partnership of Citrix and Symantec offers an affordable, proven resource for enhanced security.

To learn more about the Citrix Ready Program partnership with Symantec VIP, please visit: https://citrixready.citrix.com/symantec/symantec-validation-and-id-protection-vip-service.html

For more information about Symantec VIP, please visit: https://www.symantec.com/vip.

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

Appendix

Learn more about the enterprise security advantages provided by Citrix NetScaler Unified Gateway at: https://www.citrix.com/content/dam/citrix/en_us/documents/products-solutions/best-practices-for-enterprise-security.pdf

To learn more about the Citrix Ready Program partnership with Symantec, please visit: https://citrixready.citrix.com/symantec.html

To learn more about security solutions for business enterprises, contact Citrix and Symantec.

About Citrix Ready

Citrix Ready identifies recommended solutions that are trusted to enhance the Citrix Delivery Center infrastructure. All products featured in Citrix Ready have completed verification testing, thereby providing confidence in joint solution compatibility. Leveraging its industry-leading alliances and partner ecosystem, Citrix Ready showcases select trusted solutions designed to meet a variety of business needs. Through the online catalog and Citrix Ready branding program, you can easily find and build a trusted infrastructure. Citrix Ready not only demonstrates current mutual product compatibility, but through continued industry relationships also ensures future interoperability. Learn more at citrixready.citrix.com.

About Symantec

Symantec Corporation (NASDAQ: SYMC), the world's leading cyber security company, helps organizations, governments and people secure their most important data wherever it lives. Organizations across the world look to Symantec for strategic, integrated solutions to defend against sophisticated attacks across endpoints, cloud and infrastructure. Likewise, a global community of more than 50 million people and families rely on Symantec's Norton suite of products for protection at home and across all of their devices. Symantec operates one of the world's largest civilian cyber intelligence networks, allowing it to see and protect against the most advanced threats. For additional information, please visit www.symantec.com or connect with us on Facebook, Twitter, and LinkedIn.