SOLUTION BRIEF:
USER-FRIENDLY STRONG AUTHENTICATION

Top 5 Reasons to Choose User-Friendly Strong Authentication

Who should read this paper

This executive brief asserts that easy *and* secure authentication is possible, and offers five reasons an organization should adopt such a solution. Insights are provided into how to choose the *right* two-factor authentication (2FA) solution, including integration with complimentary solutions like single sign-on, to ensure you are prepared for the challenges of today and tomorrow.

Symantec

Content

Executive Summary

Enterprise security gets more difficult by the day; it's a moving target. Mobile workers and business partners access your network from a vast array of devices and locations. Regulatory compliance imposes additional challenges—as a long list of industry and government regulations require the protection of sensitive data. And then there's the threat of cyber attack by increasingly sophisticated hackers.

Many organizations believe easy *and* secure authentication is impossible. This executive brief illustrates how the right choice is one that combines convenience and security in a strong two-factor authentication (2FA) solution delivered in the cloud to address the challenges of today and tomorrow.

Consider cloud-based authentication

The consequences of inadequate security are well-understood. Repercussions include penalties for regulatory noncompliance, loss of confidential data, theft of intellectual property, damage to brand reputation—the list goes on. But most current 2FA solutions don't adequately address today's more complex, more strictly regulated enterprise environments. To do so, a solution must not only provide a high level of protection, it must be smart, flexible, and easy to implement, manage, and use.

The ideal solution combines the flexibility of the cloud to support mobile workers on a variety of devices; the intelligence to adapt the authentication method to the situation and identify users accurately (including when using a single sign-on (SSO) portal); and the security to guarantee a high level of protection without a cumbersome user experience.

Strong 2FA solutions are designed to provide the necessary protection against unauthorized access to corporate applications and data—within the corporate network and in the cloud. Cloud-based 2FA solutions that are designed with a focus on the user experience not only realize the security benefits of 2FA, but also the flexibility to better support mobile workers and provide a reduction in costs. On-premise solutions demand considerable up-front investment and put a continuing strain on staff resources. An on-premise solution requires budget to train—and retain—people to manage the system in-house. A large part of that management is maintaining availability and, by extension, security for the authentication server. That's not an issue with a cloud-based service because a trusted partner maintains and secures the system for you.

As a benchmark for an effective 2FA solution for the new enterprise, consider a cloud-based solution, but ensure it is both user-friendly and secure - below are five key reasons why you should demand this in your authentication solution.

Reason #1: Better protection for confidential data

Applications and data must be protected from unauthorized access. In the past, organizations addressed the problem solely by requiring user IDs and passwords. Many still do.

But user IDs and passwords are not enough. They can still play a role in access protection, but they also create new openings for security breaches. Complex password schemes drive users to find dangerous workarounds—such as using the same password for every account or posting sticky notes around the cubicle. And even the most elaborate passwords are now easily cracked.

That's why leading organizations are thinking beyond passwords. They're implementing 2FA solutions in which neither of the two authentication factors is a password but, instead, a combination of factors, such as device and behavior verification.

Security-sophisticated organizations are also casting aside the old-school approach of hardware tokens, such as a smartcard or a key fob, for authentication. Hardware tokens are easily lost and inconvenient to use. Look for strong cloud-based 2FA authentication that can eliminate the need for hardware tokens and streamlines access for users.

The future of authentication is stronger security and, at the same time, easier access for employees. For example, if a worker in the field is on a mobile device and her two authentication factors are a thumbprint on her touch screen and her GPS location or device ID, she's got strong security at her fingertips—and the organization is safe from prying eyes.

Reason #2: Enabling easier and more secure access for mobile workers

Mobile devices pose a unique challenge for authentication solutions. The solution must provide secure access from mobile devices while not being so cumbersome that users will try to circumvent it. The best security system in the world is worthless if it's so complex that users find workarounds that weaken it, such as emailing or dropping confidential documents into an unsecure location for easier access later.

Cloud-based architecture better accommodates mobile users while supporting a wide variety of personal devices, from smartphones to tablets. And these days, with the growing prevalence of BYOD, or "bring your own device" policies, that's a vital consideration.

Choose cloud-based 2FA that is functional and flexible, enabling authentication through options such as device and behavior profiling, geolocation, and biometrics - or utilize digital certificates, all of which can be used to provide authentication that's completely transparent to the user. Stick to 2FA that allows simple, safe sign-on for users who, for example, can't type a 15-digit password on a touch screen, such as the salesperson behind the wheel or the executive rushing to his next meeting. Couple that with an SSO solution to provide access to a host of cloud-based applications - making secure mobile access even easier.

In short, easy and secure strong cloud-based 2FA and SSO enables organizations to speed access and enhance the productivity of mobile workers without sacrificing the safety of business-critical applications and data.

Reason #3: Better ability to prove regulatory compliance

Passing a compliance audit means proving control over critical systems, data, and key operational and financial processes. Companies that fail an audit face severe financial penalties, not to mention the brand damage and loss of business that come with noncompliance.

More regulatory bodies are now calling for strong authentication. The rules of HIPAA, the Health Insurance Portability and Accountability Act, require strong authentication to protect health data:

- The Payment Card Industry (PCI) has information security standards to help organizations process card payments and prevent credit card fraud. The standard applies to all organizations which hold, process, or pass cardholder information from a card branded with the logo of one of the card brands.
- The DEA (Drug Enforcement Agency) has strict guidelines for prescribing controlled substances. As per DEA mandated e-Prescribing requirements, physicians must obtain two-factor authentication from a federally approved Credential Service Provider (CSP) - following the strict guidelines set by NIST SP 800-63 Assurance level 3. Broad Government initiatives like NSTIC and public sector compliance mandates like Criminal Justice Information Services for local law enforcement have been in place for some time.
- In 2011, the Federal Financial Institutions Examination Council (FFIEC), which prescribes principles and standards in the financial industry, issued guidance on the need for strong authentication in online banking and is now prepping similar guidance for mobile banking.

"Guidance" from oversight bodies such as these is no longer optional. Therefore, for compliance purposes, only a solution that can provide a thorough audit trail is acceptable; and by extension so is the availability and reliability of the solution. A lapse in the audit trail raises undesirable questions about an organization's processes and procedures.

Choosing a secure user-friendly solution that makes authentication easy will reduce the likelihood of users attempting to circumvent the solution, thereby providing a more complete audit trail. The best solution is one that has a proven track record, a comprehensive audit trail, and is certified by key regulatory bodies (for example, PCI, SAS-70 Type II and Kantara) and complies with NIST SP 800-63.

Reason #4: Lightening the load of IT staff and end users

IT staff have a lot in their inboxes. They are expected to address the needs of a rapidly changing enterprise environment, be innovative, and be responsive to users. Above all, IT is expected to provide impenetrable security to the corporate network and critical applications—and often without additional resources. The authentication solution should not add to the burden.

Cloud-based authentication lightens the load of IT personnel because most maintenance and management for a 2FA service is done by the vendor. On-premises solutions require IT personnel to secure the environment and manage and maintain the authentication server. The burden increases if the authentication method requires hardware tokens or if software tokens are managed like their hardware brethren. Deploying and managing tokens (hard and soft) and scrambling to deal with lost or broken hardware tokens is one of the biggest security time sinks for IT staff.

Look to a single sign-on solution to reduce the burden associated with passwords and extend the layer of security to all cloud-based applications used by the organization. To further lighten the IT burden, choose a cloud-based 2FA solution that offers a self-service portal making it easy for users to download and register their own credentials (software tokens should be free so as not to require management). They should be able to rename, test, and remove their credentials on their own. That means no more waiting to talk to the help desk—and fewer help desk calls. Some organizations that have moved to cloud-based 2FA have cut their IT workload by 60 percent or more. That frees IT experts to focus on other initiatives, while the cloud-based 2FA provider handles system management with the best security people in the world.

Reason #5: Easier planning in a constantly changing environment

The threat landscape is constantly changing. Cyber attacks on businesses and employees are escalating rapidly. As one hole is plugged by an organization another is uncovered. Data leakage, intellectual property theft, fraud, and malicious activities cost businesses millions of dollars every year. A future-proof, strong authentication solution plays a strategic part in addressing these evolving threats.

However, the threat landscape is only one variable that must be considered. Another is the organization's changing needs. The number of users, devices, platforms, initiatives, and organizational mandates change over time. To meet these changing needs, the solution must be flexible, scalable, and capable of instant feature updates. With cloud and mobile taking center stage, being user-friendly must be added to this list. In general, cloud-based 2FA solutions meet those requirements well.

When choosing a strong 2FA solution, look to the cloud, but ensure your solution of choice is both easy to use and secure - this is no longer an impossible combination to expect the *right* authentication solution to deliver. In addition demand scalability, tight integrating with an SSO solution, and the ability to receive instant updates so you can quickly address threats in an increasingly risky business environment; in addition to being able to evolve with you.

Embracing easy and secure cloud-based 2FA

Organizations that have not yet implemented strong 2FA or looked into SSO solutions should start investigating these options now. Every organization has sensitive data that should be secured and therefore has a need for 2FA; and most have a host of cloud-based apps to manage and would benefit from an SSO solution. The question is what you should be looking for in a solution to address the rapidly changing security needs of the new enterprise.

Whether it's an analyst report or a blog post, virtually all sources agree that the move to strong cloud-based authentication is not a question of if, but when. And those organizations that make the move will be at a competitive advantage. They're empowering their mobile workforce by shifting critical data and applications to the cloud. They're taking advantage of the cost savings, flexibility, and scalability available in the cloud. They're guarding against threats from attacks and complying with industry regulations.

Furthermore, organizations should demand a user-friendly *and* secure cloud-based 2FA solution coupled with SSO capabilities to accommodate employees who are increasingly frustrated with complex and ever-changing password regimes.

Easy, secure, and cost-effective authentication is available today in the cloud. Your challenge is to embrace it.

About Symantec

Symantec Corporation (NASDAQ: SYMC) is an information protection expert that helps people, businesses and governments seeking the freedom to unlock the opportunities technology brings – anytime, anywhere. Founded in April 1982, Symantec, a Fortune 500 company, operating one of the largest global data-intelligence networks, has provided leading security, backup and availability solutions for where vital information is stored, accessed and shared. The company's more than 19,000 employees reside in more than 50 countries. Ninety-nine percent of Fortune 500 companies are Symantec customers. In fiscal 2015, it recorded revenues of $6.5 billion. To learn more go to www.symantec.com or connect with Symantec at: go.symantec.com/socialmedia.

For specific country offices and contact numbers, please visit our website.

Symantec World Headquarters
350 Ellis St.
Mountain View, CA 94043 USA
+1 (650) 527 8000
1 (800) 721 3934
www.symantec.com