WHITE PAPER:
STRONG, SMARTER USER AUTHENTICATION

Effective, User-Friendly Solution Addresses Security Challenges of Today's Mobile Business

Reaping the Benefits of Strong, Smarter User Authentication

Who should read this paper

For business leaders. Passwords and traditional two-factor authentication (2FA) solutions are not enough to meet today's evolving security threats and regulatory requirements, while providing the greater ease-of-use demanded by users. What's needed is strong, smarter authentication.

Symantec

Content

Executive Summary

Many factors are contributing to the growth of the mobile workforce, not the least of which is the rise of cloud-based applications and the mobile device explosion including bring your own device (BYOD) programs. The greater flexibility that mobility offers means more opportunity, but also new challenges.

Information technology (IT) staff are still tasked with meeting the traditional challenges they have always faced: protecting against breaches when data and applications are accessed (remotely or locally) and complying with regulations that ensure protection. But they now face a host of new challenges, such as providing mobile employees with simple, yet secure, access to app that could reside anywhere.

This paper discusses ways that organizations can meet these challenges: by implementing strong, smarter authentication to secure their corporate data and applications, while offering greater ease-of-use.

Security challenges

The working environment has changed. Remote access to data and applications is now commonplace. According to a 2014 Gartner study in the United States, approximately 40 percent of U.S. consumers who work for large enterprises said they use their personally owned smartphone, desktop or laptop daily for some form of work purpose.[1] But this trend poses obvious security risks to organizations, which now must secure access from a wide variety of mobile devices.

Another security challenge for organizations is the popularity of the Software-as-a-Service (SaaS) model for critical business applications, including customer relationship management, human resources, recruiting, performance management, and travel. SaaS applications provide software flexibility and functionality via the Internet, but they also come with a higher security risk than exists when data and applications are locked safely behind a corporate firewall.

Security is further threatened by the use of cloud-based applications such as Dropbox™, Google Drive™, and Adobe Creative Cloud™. Data flows freely on these networks, with security depending solely on the vendor in most cases. A recent report from the Ponemon Institute showed that 69 percent of IT and IT Security respondents were not likely to know whether employees were using unapproved and risky file sharing tools.[2]

That's risky business. But it gets riskier. The use of new social extranets and other tools for business collaboration means more non-employees (customers, suppliers, and business partners) now have access to corporate applications and data.

Every IT executive understands the consequences of inadequate security—including data theft, penalties for noncompliance with regulations, loss of intellectual property, and damage to brand reputation—but many are still developing best practices to deal with the security risks that accompany the mobile workforce and the array of cloud technologies they use.

The exponential growth in the use of mobile devices has led to the acceptance of BYOD policies in many enterprises. According to Tech Pro Research's survey conducted in November 2014, 74% of organizations are either already using or planning to allow employees to bring their own devices to work.[3] As IT struggles to find new ways to address the changes in working style and support initiatives such as BYOD, users of these programs want more changes that will further improve productivity and the user experience.

1- User Survey Analysis: Gartner Consumer Insights — People at Work and Play in 2014
2- Ponemon, Achieving Security in Workplace File Sharing, January 2014
3- Tech Pro Research: Wearable, BYOD, and IoT - Current and Future Plans in the Enterprise Nov 2014

The ideal solution to meet the evolving needs of IT departments and users is two-factor authentication (2FA), using both token and tokenless methods. 2FA authentication is a proven tool to protect against unauthorized access to corporate applications and data—both in the corporate network and in the cloud. Passwordless using biometrics and tokenless authentication deliver a high level of security without burdening users, leading to a smooth user experience. For optimum scalability, flexibility, and ease of deployment, a cloud-based model should be considered. Cloud-based authentication also greatly reduces IT financial and administrative overhead. And when combined with passwordless or tokenless options, savings are increased.

How Two-factor Authentication Works

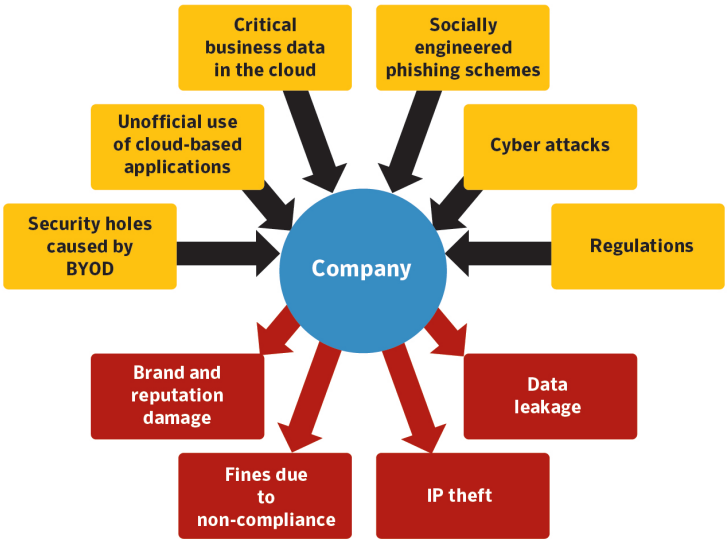
Two-factor authentication (2FA) demands two of the folowing: something a user knows (such as a user name and password), something a user has (a hardware credential such as a token, a smartcard, a cell phone, or in a tokenless implementation, a device or a behavioral profile), or something a user is (such as a biometric fingerprint). For enterprises, this dual mechanism delivers a higher level of security to protect confidential data and applications while meeting compliance requirements.

Security risks and requirements on the rise

Cyber attacks on businesses and employees are escalating rapidly. According to the 2015 Symantec Internet Security Threat Report, advanced attackers targeted five out of six large companies in 2014, which is a 40% increase from the previous year. That means damaged reputations and dollars lost. Data leakage, intellectual property theft, fraud, and malicious activities cost businesses millions of dollars every year. In fact, cyber crime costs an estimated $9 million in damages to organizations. Most of these losses are not incidental. In 2014, 49 percent, making up the majority of breaches, were caused by attackers, up from 34 percent in 2013.[4]

And reported events are just the tip of the cyber-iceberg. Individual employees are targeted every day by socially engineered phishing schemes and other attacks. And when they fall victim to attack, everything from intellectual property to sensitive customer information is in danger.

The consequences of inadequate security and non-compliance



4- Symantec Internet Security Threat Report 2015

These intrusion risks are one driver influencing organizations to seek better security. Another is the growing number of government and industry regulations that mandate tight security. Control of access to data and applications is required by many of these regulations, and information security is a common failure point in compliance audits.

But control is hard, especially at the individual user level. Passwords and user IDs are ineffective security measures. As any corporate IT department well knows, there are numerous flaws in user ID/password systems. Passwords are only as reliable as the humans who use them—and human error is common everywhere, from the cubicle to the executive suite.

The average user has 26 password-protected accounts[5] and only five different passwords, which means a cracked social-network password could equal a cracked corporate account password. It is not uncommon for people to write down their passwords on sticky notes and paste them around their desks or keep them in unprotected files on their hard drives. Even passwords that are protected are crackable—or just plain guessable—for hackers.

Not too long ago, the Institute of Electrical and Electronics Engineers (IEEE) inadvertently left 100,000 user passwords publicly exposed on one of its servers. Bloggers who looked at them discovered the most common passwords among the tech-savvy members of IEEE were "123456,""ieee2012," and "12345678."

Add to these threats the user's desire for convenience (sometimes over security): the enterprise embrace of BYOD policies and even BYOE (bring your own everything). Yes, enterprises realize cost savings with these initiatives. But administrators lose a lot of sleep worrying how to enforce security measures for the bewildering array of devices employees bring and the apps they run.

All of these factors add up to an inescapable conclusion: Enterprises need new, more flexible, more powerful tools to protect sensitive data and infrastructure. They need to move beyond traditional user ID/ password security policies to more robust, reliable, and smarter systems that do away with the password entirely; or at a minimum combine traditional 2FA and contextual or tokenless authentication. Enterprise must offer an easier, less cumbersome experience for their employees.

Managed service

Two-factor authentication is not new. It's a mature and proven way to protect corporate data. But most conventional 2FA solutions focus primarily on the traditional approach to security, that is, hardware or software tokens. Additionally, many are still on-premises and they demand high prices, significant integration efforts, and considerable administrative support.

What organizations need today is a managed service that combines strong 2FA, industry-leading integration, and authentication options to meet diverse needs. The right managed service delivers all the advantages of a SaaS solution, including lower hardware and software costs, fewer software maintenance and labor fees, built-in scalability, reliability backed by industry-leading service-level agreements, and out-of-the-box integration with existing infrastructure.

Authentication options, whether they conform to the traditional 2FA model of dynamic security codes or ease the user experience through new models such as biometrics or profiling, must enable enterprises to select what is right for each user, device, and application. One option that many IT organizations are choosing is contextual or tokenless authentication. Gartner estimates that by year-end of 2017, over 30% of organizations will use contextual, adaptive techniques for workforce remote access.[6]

5- Lazy Password Reuse Opens Brits to Crooks' Penetration, The Register
6- Gartner Magic Quadrant for User Authentication Dec 2014

Contextual tokenless authentication

An increasing number of enterprises are now looking at tokenless authentication as a way to simplify the user experience and reduce costs. They understand that not all authentication requires the dynamic security code that comes with hardware tokens and mobile credentials.

Symantec™ Validation and ID Protection Service tokenless authentication options include device fingerprinting, hardware-based identifiers, and user-behavior risk analysis. The appeal of tokenless authentication is that it greatly simplifies the user experience by hiding the validation of the second factor from the user. As far as users are concerned, all they need is a simple user name/password to access the network. Behind the scenes, Validation and ID Protection Service does all the work of tagging computers, logging behavior patterns, and analyzing login profiles. All of these tokenless options combine user name/password with complex device analysis or a combination of device and behavioral analysis, delivering proven logon security.

Symantec™ Validation and ID Protection Intelligent Authentication (risk-based authentication), performs a full risk analysis based on the device, possible threats, and user behavior profiles. It works by establishing a baseline for a user's normal behavior upon logon. For example, it records the device or location from which a particular user normally gains access. A threat analysis, which can gather data from other Symantec solutions such as the Global Intelligence Network detects recent attacks to ascertain device reputation and health.

When logon behavior is normal, a simple password may be acceptable. When logon is attempted via an unknown device, unusual location, or under suspicious circumstances, the user is prompted via text, email, or voice to respond to a challenge. Because there are no tokens, smartcards, or biometrics, the cost is lower and the user experience for legitimate users is identical to a traditional user name/password model.

Tokenless authentication is a popular option for busy executives who don't want to be slowed down by accessing the network. The tokenless option is also gaining the attention of organizations in vertical markets that before would have seemed unusual, such as education. Attracted by the low cost and ease of use, tokenless authentication is being considered as a viable option for educators to secure access to their district's network

Success Story: Flexibility and Speed

A global consulting firm wanted to boost user experience by eliminating hardware tokens and improving support for PCs and mobile devices. And it wanted to reduce infrastructure costs. It chose Symantec™ Validation and ID Protection Service for two primary reasons: flexibility and rapid deployment. Validation and ID Protection Service offers broad credential support and integrated support for Symantec™ Validation and ID Protection Intelligent Authentication and Symantec™ Registered Computer. And Validation and ID Protection Service comes with a self-service portal for downloading and registering credentials that makes for easy uptake and quick scaling. The consulting firm is now rolling out Validation and ID Protection Service to 325,000 users and is providing Validation and ID Protection Intelligent Authentication for remote access.

Strong, smarter user authentication

Most organizations now have a significant portion of their workforce accessing their network from outside the office via mobile devices. Yet user names and passwords are not enough to adequately protect devices against unauthorized access.

Many enterprises have deployed 2FA but often it is rolled out to only a limited number of users, such as the few individuals who require remote access to the most sensitive corporate data. Why is this? Because users typically resist the added burden of conventional 2FA solutions. What's more, IT teams often oppose these types of solutions, which are primarily on-premises and considered too expensive because they require additional infrastructure investments to deliver the needed scalability and reliability.

Validation and ID Protection Service solves the challenge of securing a mobile workforce and does so without the drawbacks of conventional on-premises 2FA systems. In short, Validation and ID Protection Service offers all the features an effective cloud-based security system must have to provide strong, smarter user authentication.

The managed service comes with the lower cost and better scalability that make all cloud-based solutions attractive. Because there's no infrastructure installed onsite, Validation and ID Protection offers the flexibility of strong authentication that can be updated as needed and tailored to a variety of risk models and policies at an affordable cost. And it's adaptable. Validation and ID Protection Service supports all major platforms and integrates with popular virtual private networks (VPNs), data stores, Web mail programs, and more.

It also reduces the burden on IT staff with the use of self-service options and passwordless authentication. Validation and ID Protection Service features a portal where users can download and register their own credentials. They can also 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. Companies have been able to reduce IT touches by up to 75 percent by implementing Validation and ID Protection Service. In fact, when Citrix Systems implemented it, IT touches were reduced by 60 percent. Eliminating the password further reduces touches with the help desk. An estimated 30% of help desk calls are password related according to Gartner.

Validation and ID Protection Service is flexible, allowing the enterprise to select the type of credentials that best suit the user, device, and use case. Because of the mobility of today's workers and the ubiquity of mobile devices, most employees prefer mobile credentials, with many of those attracted to the option of passwordless authentication to their online apps. Others opt for alternative software credentials or, if there is a policy mandate, a hardware token. Still others chose one of the tokenless options of Validation and ID Protection Service. Because Validation and ID Protection Service supports up to five different credentials, an enterprise can accommodate many different preferences.

Success Story: Improved Uptime, Decreased Resources

At Citrix Systems, most employees use mobile credentials to remotely access the company's VPN. Citrix achieved a number of benefits when it implemented Symantec™ Validation and ID Protection Service. The large and diverse organization was able to simplify by eliminating one-size-fits-all tokens and instituting a BYOD policy. This, along with the self-service portal of Validation and ID Protection Service, improved the user experience and boosted adoption among employees. The company reduced administrative headaches, improved uptime, and decreased the resources it once dedicated to supporting security. Citrix did all this while rolling out Validation and ID Protection Service to 10,000 users.

Symantec Validation and ID Protection Service

Today's enterprise needs an effective, user-friendly solution to address the many security challenges that exist in today's mobile business. Validation and ID Protection Service delivers cloud-based 2FA authentication that offers a smarter, more flexible alternative to meet the unique needs of business today, including all the economic and business benefits of a hosted solution:

Protection: Validation and ID Protection Service cuts the risk of unauthorized access, data breaches, and other security problems. 2FA is the industry-leading solution for enhancing the security of data and applications that reside on a corporate network and in the cloud. By implementing Symantec Validation and ID Protection Service (2FA with risk-based analysis); businesses get the best of both worlds: an enterprise-class security solution and a cloud-based application that meets their cost and reliability needs.

Scalability: Because Validation and ID Protection Service security is delivered in the cloud, mitigating the need for underlying hardware and software resources, enterprises can dial up or dial down their use of the service as their needs change. They'll never have to overbuy capacity—or risk running out of it—as they do with a conventional on-premise solution.

Speed: Many times success is defined by being able to move as swiftly as business requires. With Validation and ID Protection Service, there's no lag time while new servers, operating systems, and applications are provisioned and installed. Everything is ready to go on demand. And because it is a cloud-based service all updates are available immediately - ahead of the competition.

Flexibility: Although the Validation and ID Protection Service offers the ultimate in convenience by using the biometrics in mobile devices to eliminate the password, the wide range of available authentication options allows enterprises to choose the method that works best for them. Choses range from using one-time security codes, tokenless device IDs, passwordless biometric fingerprint, or risk-based authentication. The traditional method that utilizes one-time security codes for mobile credentials, hardware tokens, cards, out-of-band authentication, or other form factors is fully supported. The most popular and user friendly of these credentials is Validation and ID Protection Access for Mobile (now supporting more than 900 mobile devices), which provides a downloadable mobile credential that offers the option of using the 6-digit security code, one-tap Push verification, or passwordless authentication via biometrics. Whichever you choose the mobile credential makes strong authentication more convenient for users, while making 2FA more cost effective for the enterprise.

Intelligence: Validation and ID Protection Service keeps getting smarter and more user friendly. Its tokenless authentication utilizes sophisticated device analysis and Validation and ID Protection Intelligent Authentication behavior profiling to simplify user experiences and offer enterprises the strength of Symantec protection. By making risk-based authentication transparent to the user, risky logon attempts can be identified and blocked without changing the legitimate user's logon experience

Availability: Validation and ID Protection Service offers carrier-class reliability within the highly secure Symantec global infrastructure, featuring military-grade tier-4 data centers. The Symantec Internet infrastructure enables and protects up to 30 billion interactions a day, with unmatched scale, interoperability, and security.

Future proof: Attackers are constantly changing tactics. Enterprises require authentication solutions that can address these challenges, both now and in the future. The Validation and ID Protection Service cloud-based approach enables integration with the Global Intelligence Network allowing you to stay ahead of emerging threats.

Conclusion

As more of their users go mobile and they move critical data and applications into the cloud to achieve cost savings, flexibility, and scalability, enterprises must emphasize security more than ever. The stakes keep getting higher. Data breaches and malware are on the rise, and the cost of a single breach can run into the millions, not to mention the cost in brand damage. At the same time, there is a growing desire for a simpler, smarter user experience when it comes to authentication.

Symantec™ Validation and ID Protection Service is the answer. It's an industry-leading cloud-based 2FA solution that provides all the cost and scalability benefits of a managed service, delivers robust security, and offers the right options for a user-friendly experience. It provides a proven way to prevent unauthorized access to critical data and applications that's easy to implement, cost-effective, and smart.

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