HYPERSECU®

Remote Access

Securing Your Employees Out of the Office

01/26/2017

HSTE-NB0011-RV 1.1

HYPERSECU INFORMATION SYSTEMS INC

#200-6191 Westminster Hwy | Richmond BC | V7C 4V4 | Canada
604-279-2000 | www.hypersecu.com

Introduction

With technology growing and many employees working out of office, remote access is rapidly becoming required at many corporations. Remote access offers the convenience of accessing company servers, documents, CRM, and other critical information when employees are working off-site, thus building higher productivity and increasing employee retention.

It's also causing huge vulnerability concerns. Remote access poses a threat to company security by opening up the opportunity for hackers to access servers and make away with crucial company records, including sensitive data, confidential client information, and other company secrets.

Many of these security breaches are occurring at the authentication level. That means access points must be kept secure: static usernames and passwords are no longer safe. Companies need the protection of strong mutlti-factor authentication.

Understanding the Statistics

Hacking remains one of the biggest threats to data security and the numbers are only growing over the years. According to Symantec's 2014 Internet Security Threat Report, the number of total breaches grew by more than 60% in 2013 compared to the year before. At the same time, the number of exposed identities went from 93 million in 2012 **to 552 million in 2013**.

A total of

62%

more data breaches occured in 2013 compared to 2012.

Symantec Report, 2014

A total of

552 million

identities were exposed over 8 hacking incidents in 2013.

Symantec Report, 2014

More significantly, these millions of identities weren't exposed or stolen over hundreds of small attacks. In 2013, a total of eight attacks occurred. In just one single hack, as many as 150 million identities were breached, exposing information such as social security numbers, medical records, user names and passwords, and birth dates.

What does this mean for companies? For starters, it means that corporations need to protect themselves at all costs. It only takes one successful attack for a hacker to expose millions of sensitive identity information. With each incident, organizations aren't just losing critical data—they're also losing the trust of customers and potential business partners, which can be a huge blow to a company's reputation and finances.

"In just one single hack, as many as 150 million identities were breached."

Facing the Risks

It's also important to look at how organizations are facing these increased risks, especially in light of the growing use of remote access among employees. A Webroot survey reports that 64% of companies allow remote access to servers for 25% of their employees. While the increased productivity and convenience is valuable, the security risks are far from negligible—and many security professionals find it a serious challenge to manage remote users, even with advanced encryption through Virtual Private Networks (VPNs).

90% **agree that security management for remote users is highly challenging**

50% **of U.S. firms with remote users estimate that Web-borne attacks cost $25,000 to $10 million**

25% **of employees who have remote access experience higher rates of Web-borne attacks**

Webroot Survey, 2013

The Challenge of VPN

Virtual Private Networks are commonly used to secure remote access. They provide state-of-the-art security measures to connect remote uses to company servers through an encrypted channel.

While the channel itself is highly secure, the challenge lies in the login phase: end users are often required to only have a static username and password in order to gain access. Also known as single-factor authentication (as opposed to the more secure multi-factor authentication), static usernames and passwords are extremely vulnerable, putting companies at risk of major data breaches.

Common methods to steal passwords include:

- Brute force attacks
- Key loggers
- Phishing
- Malware
- Wi-Fi traffic monitoring
- Tabnabbing, a form of phishing that convinces users to submit login details by impersonating popular websites

Attacks aren't limited to strangers, either. Insider threats can also be a potential problem, where internal employees may steal credentials in order to sell them to other hackers.

The bottom line is, secure encryption can only protect users so far. Securing the gate at the authentication stage is equally important and that means addressing the password problem.

The Password Challenge

While a simple solution might seem to be just getting employees using remote access to change their passwords and even usernames on a regular basis, implementing such regulations is easier said than done.

Many employees already have trouble trying to recall just one set of passwords, which can lead to lowered productivity. It affects not just large enterprises, but small businesses, as well. A recent study by Centrify discovered that an average company of 100 employees can lose as much as $42, 000 per year due to people struggling to remember their passwords. Combine this with a policy of frequently changing your password and the loss in productivity could be even higher.

Use two-factor authentication (2FA) to increase login security without needing to juggle multiple changing passwords.

Since one of the major advantages of remote access is the ability for employees to increase their productivity, that increased productivity shouldn't be hindered by password struggles and IT administrators needing to enforce rules and regulations about updating passwords.

Instead, the key is to make using, remembering, and changing authentication credentials on a regular basis an easy process for both employees and companies. This is the clear advantage of using two-factor authentication for remote access.

Two-factor authentication comes in many forms, two of the most popular being dynamic one-time passwords (OTP) and digital certificates through a Public Key Infrastructure (PKI). These solutions offer companies the ability to allow remote employees secure access to company servers and other sensitive data without the need to manually change passwords every few months. In fact, with an OTP for example, users don't need to remember their password at all: the device offers a single-use password they can read and enter when needed. This is both convenient for the employee and can help save the company thousands of dollars annually.

A company of 100 employees can lose as much as

$42,000

per year in productivity due to people struggling to remember their passwords.

Centrify Survey, 2014

Solve Challenges with 2FA

Hypersecu offers multiple two-factor authentication (2FA) solutions in order to keep remote access secure without the difficult process of implementing frequent password changes and the challenge that comes with employees forgetting their access passwords.

2FA is a concept built upon **something you know**, such as a password, and **something you have**, such as a hardware token. Because one of the two factors required (something you have) is the hardware device itself, which is then kept securely in possession of the employee, hackers have no way of accessing that device even if they were to obtain the correct information (something you know).

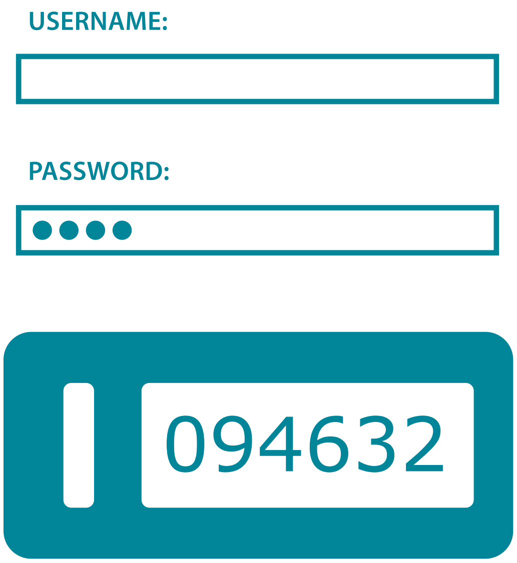
There are two popular forms of 2FA available, both of which are simple to integrate and cost-effective to maintain: one-time passwords (OTP) and a digital certificate-based Public Key Infrastructure (PKI).

HyperOTP™ for Remote Access

HyperOTP™ solutions are designed with simplicity, convenience, and security in mind. They work especially well for remote users. Each token generates a new 6-8 digit password every 30 or 60 seconds, based on your security needs. By simply pressing a button, a user can see the generated password, enter that number into the password field, and gain access to the company server.

Some benefits of using OTP include:

- **Simple integration.** There's no need to overhaul your existing IT infrastructure: HyperOTP uses algorithm standards outlined by the Open Authentication Organization (OATH) and allows for seamless integration with all RADIUS-enabled servers across all devices.
- **Cost-efficient.** Since there's little disruption to the existing IT infrastructure, OTP can be added to your company without a huge amount of investment. The cost to maintain it is also competitively low.
- **Time-efficient**. OTP setup is quick and requires minimal installation. Many OTP servers can be set up in just a matter of days and OTP is designed for plug-and-play usability. For end users, no installation is required.
- **Flexibility.** Whether you're a large enterprise or a small business of under a hundred employees, and regardless of your industry, HyperOTP can be customized for your precise security needs.



HyperPKI™ for Remote Access

Hypersecu's HyperPKI™ HYP2003 tokens operate using Public Key Infrastructure technology. PKI technology involves a private key and a public key, and is based on the use of digital certificates. A digital certificate, issued by a trusted Certificate Authority, provides proof that the user is really who they say they are, while the public and private key pairs are used to encrypt data and ensure that the encrypted data can only be read by the right person.

As a result, companies using PKI for remote access are highly protected. It's difficult to fake an employee's identity even if a hacker were to obtain the employee's password. Vital authentication information, including the private key, is stored directly on the HYP2003 that the employee keeps, and each token is further protected by a PIN. Hackers are effectively locked out. Even if the token were to fall in the wrong hands, only the employee knows the PIN. Digital certificates can also be revoked as soon as a token is reported stolen or missing

Use HyperPKI to:

- **Secure VPN access.** PKI adds a second layer of authentication to remote access. A user must insert the HYP2003 and enter their PIN in order to gain access to the VPN login page. While it's an extra step for the login phase, this keeps hackers from using any passwords they might've gleaned to gain access.
- **Digitally sign emails and documents.** Prevent malicious hackers from hijacking an employee's identity and sending unauthorized messages or documents. Remote workers communicate often by email and because they aren't on-site, it can be difficult to tell if the employee is behind their computer or not. As a result, someone posing as an employee can easily get their hands on sensitive company correspondence. Digital signing assures the identity of the person behind every email and document sent.
- **Encrypt emails and documents.** In addition to identity assurance, PKI also allows you to encrypt any sensitive messages or documents. Only authorized users with the correct private and public key can view encrypted emails. Emails also stay encrypted—remove the PKI token and the message becomes blank. This means anyone who gains unauthorized access to the company's servers won't be able to read what they find.

1. Insert your HYP2003 into a USB port to identify yourself as a valid user.
2. Input your PIN to gain access to the company authentication page.
3. Input your username and password to access the company server.
4. Log out and remove your token when finished, ensuring that no else has access.

Adapting to Mobile

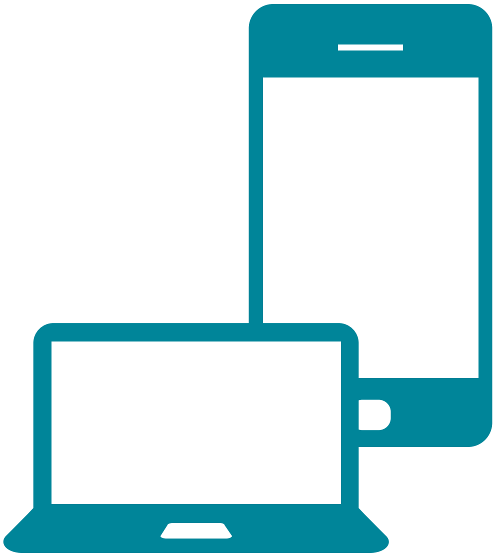
Remote access isn't limited to employees working out of a home office station. Also known as Bring Your Own Device (BYOD), many employees are turning more and more to mobile devices in order to do their work, making even on-site employees into remote workers from time to time. For those who are frequently on the go such as field government workers and traveling business employees, the ability to use mobile devices for work is invaluable.

The more advanced mobile technology grows, however, the more opportunities hackers have to gain access. As a result, it's more important than ever to make sure that personal devices are as secure as company equipment.

2FA is a simple, flexible option that can be adapted to mobile devices such as tablets, phones, and laptops.

Integrating two-factor authentication with mobile devices is quick and painless. Depending on your employees' needs and the IT infrastructure you've chosen for your company, you can use either HyperOTP™ or HyperPKI™. Both solutions are highly flexible and designed to adapt for mobile use.

With HyperOTP, it's as easy as inputting the OTP password when accessing company emails and servers through your mobile device. Meanwhile, digital certificates are transferable so there's no need to set up another user in order to access company information on another device with PKI. Although the HYP2003 is designed for USB ports, HyperPKI also comes in mobile-friendly forms including AudioPass, which allows you to use your digital certificates by plugging the token into your device's audio jack port.



Personal mobile devices are becoming increasingly common in the workplace, with a predicted 38% of employers no longer providing company mobile devices by 2016.

Gartner Study, 2013

Get Started with Hypersecu

Hypersecu offers a wide line of multi-factor authentication solutions to secure your business, including OTP, PKI, and smart card readers. Our flexible products are designed to suit your needs no matter the size of your business or the industry you're in. If you're not sure what's right for you, we're happy to provide consultation to work out a customized solution that covers all of your information security challenges.

Learn More

We provide demos of our products upon request and our expert consultants are ready to answer your questions. Contact us or visit our website at www.hypersecu.com to learn more.

Hypersecu Information Systems Inc
#200-6191 Westminster Hwy
Richmond, BC V7C 4V4 Canada

Email: sales@hypersecu.com | Phone: 604-279-2000