

Briggs and Morgan, P.A. Case Study

Briggs and Morgan Relies on VASCO DIGIPASS to Secure Remote Access to Critical Information.

MISSION CRITICAL

The core business of a law firm has always revolved around the possession of confidential and proprietary information. VPN and web access have made it possible for employees and partners to gain access to such critical data from anywhere at any time. However, with added convenience comes additional risk. In the times of public scandals associated with corporate security breaches, the pioneers in the legal community are leveraging two-factor authentication to fortify security.

Briggs and Morgan, a prominent Midwest law firm serving clients across the United States, has a long history of representing organizations and individuals in civil law matters.

Today the firm has more than 375 employees and 170 attorneys who serve a range of clients including multinational corporations, business start-ups, commercial enterprises, nonprofit educational and charitable institutions, utilities, governmental agencies, public bodies and individuals.

The firm is headquartered in Minneapolis, MN, and maintains its original office in St. Paul. It has recently been honored as a "Go To" law firm by Corporate Counsel Magazine.

- prominent Midwest law firm
- more than 375 employees
- 170 attorneys
- range of clients including multinational corporations, business start-ups, commercial enterprises, nonprofit educational and charitable institutions, utilities, governmental agencies, public bodies and individuals





“Our goal was to prevent exposure to possible data theft, online fraud and other risks involved in opening the network to remote users.”

Jeff Barnes - Network Systems Administrator for Briggs and Morgan

CHALLENGE

Like many legal firms, Briggs and Morgan takes advantage of a variety of technologies such as VPN and web access. When the nature of a case sends an attorney out on the road, the firm provides remote access to email, legal documents, Microsoft Office applications, as well as specialty applications used in the legal industry like Legal Macpac, Delta View, Metadata Assistant and others.

One of Briggs and Morgan's challenges was to make remote access secure and ensure the confidentiality of their clients. Essentially, the firm needed a solution that was secure, portable, proven, and easy to use, and at the same time allowed them to control the Total Cost of Ownership.

OBJECTIVE

“Our goal was to prevent exposure to possible data theft, online fraud and other risks involved in opening the network to remote users. We needed to protect financial transactions, customer agreements, documents related to litigations, IPOs, and other highly confidential information stored on our corporate network”, says Jeff Barnes of Briggs and Morgan. Therefore, the firm's management decided to look into strong user authentication in 2002.

The project was initiated by the firm's IT department. Jeff Barnes, Network Systems Administrator for Briggs and Morgan notes, “It was the fear of the unknown. We just couldn't afford an attack on our network because all our information and data are 100% confidential. We wanted to secure the front end of Microsoft Web Servers and not expose them to the Internet, at the same time making sure that our Citrix and other web enabled applications are properly protected.”

The company also wanted to integrate the user authentication solution with Novell iChain.

SOLUTION

After partnering with a local IT company to evaluate the risks and potential preventive solutions, Briggs and Morgan decided to move forward with VASCO's DIGIPASS strong authentication. The firm chose Digiapss GO1 to securely authenticate their end users to the firm's network resources.

In addition to a static password when accessing the firm's network or webmail server, the user would enter a one-time password randomly generated by VASCO's DIGIPASS GO1, along with the user name. One-Time Passwords change every 32 seconds and are virtually impossible to hack or break. One-Time Passwords enable Briggs and Morgan to safely identify employees that need to access firm's network resources.

APPROACH

The initial phase included deployment of GO1 tokens to a small “volunteer” group, who received user guidelines and the training manual. After several months, all attorneys requesting remote access, received a DIGIPASS GO1.



Briggs and Morgan’s “soft” approach proved to be a very smart one. The technology is not pushed on to the end users, but rather emphasized through training and strict IT security policy: remote access is only granted to users who possess a VASCO DIGIPASS.

The process does not work automatically; employees need to request a DIGIPASS token from the IT department. This ensures a high level of internal buy-in and, at the end, a more secure environment.

RESULTS

Currently, over 275 employees including attorneys, legal assistants, administrative assistants and staff utilize VASCO’s DIGIPASS two-factor authentication to gain access to email, document management and specialty applications from home, while traveling, from a hotel room or a remote business office.

Briggs and Morgan chose VASCO’s DIGIPASS strong authentication because of its flexibility, interoperability, hassle-free deployment and ease of use. Native integration with Novell NMAS and iChain also played a tremendous role in the vendor selection process. “We were very pleased with the way VASCO’s DIGIPASS authentication is integrated with Novell. iChain integration, creating user IDs for remote access, assigning groups, setting privileges. Now we can set up new user in less than five minutes”, says Jeff Barnes of Briggs and Morgan.

Total Cost of Ownership was also an important factor in the decision making process, allowing the firm to take advantage of advanced, yet affordable authentication solution.



“We were very pleased with the way VASCO’s DIGIPASS authentication is integrated with Novell. Now we can set up new user in less than five minutes”

Jeff Barnes - Network Systems Administrator for
Briggs and Morgan

CONTINUED EVOLUTION OF SECURITY

The company plans to take full advantage of VASCO's DIGIPASS Family "mix and match" option that allows customers to pick hardware and software DIGIPASS that best fit their needs. Recently, Briggs and Morgan deployed VASCO's DIGIPASS for Java Phone.

This product allows users to safely connect to remote networks and applications using their cellular phone as a token. It integrates perfectly with any existing VASCO product, without the need to change existing architecture.

Also, a disaster operation plan is being discussed. This would include deploying a mix of hard and soft DIGIPASS to all employees and partners of Briggs and Morgan. In cases of employees' inability to get to the workplace, the firm's daily operation can continue without interruption.

By partnering with VASCO, Briggs and Morgan acquired a solution that allows employees and partners to conduct business securely and benefit from the innovative technology and flexibility that the Internet and remote access offer. The firm's clients continue to recognize Briggs and Morgan for their client service and successful results.

Minneapolis
2200 IDS Center
80 South Eighth Street
Minneapolis, MN 55402
612.977.8400
612.977.8650 fax

St. Paul
W2200 First National Bank Building
332 Minnesota Street
St. Paul, MN 55101
651.808.6600
651.808.6450 fax

Email: briggs@briggs.com

About VASCO

VASCO is the number one supplier of strong authentication and e-signature solutions and services.

VASCO has established itself as the world's leading software company specialized in Internet Security, with a customer base in the financial sector, enterprise security, e-commerce and e-government.

www.vasco.com

BRUSSELS (Europe)

phone: +32.2.609.97.00
email: info-europe@vasco.com

BOSTON (North America)

phone: +1.508.366.3400
email: info-usa@vasco.com

SYDNEY (Pacific)

phone: +61.2.8920.9666
email: info-australia@vasco.com

SINGAPORE (Asia)

phone: +65.6323.0906
email: info-asia@vasco.com