

Martin, Fletcher



Sanctuary Device Control is Martin, Fletcher's Key to Good Security Health

Background

Martin, Fletcher is one of the largest and fastest-growing healthcare staffing firms in the United States. Based in Irving, Texas, the firm provides permanent placement services for physician, allied and nursing-level professionals throughout 49 states in the U.S. Martin, Fletcher has helped medical facilities in both rural communities and some of the nation's largest metropolitan areas find the most qualified and skilled medical professionals for their organizations. Martin, Fletcher works with medical facilities as diverse as small clinics, private physician practices, nursing homes and large healthcare systems with needs ranging from E.R. nurses to orthopedic surgeons.

The Challenge

Martin, Fletcher prides itself on being one of the industry's most technologically advanced healthcare staffing firms. The company has more than 200 PCs, laptops and tablets connected to its network that enable employees to access databases of information related to doctors, nurses and facilities across the U.S. Security is of the utmost concern to Martin, Fletcher, and one of the new security challenges the Company was facing was the proliferation of removable storage media.

As devices became smaller and smaller - while increasing their storage capacity - locking down USB ports became a priority. Using a device, employees could easily download

sensitive information or inadvertently introduce a virus to the network. USB devices also enabled users to download their own software to the PC, taking up valuable bandwidth and resources.

For years, Martin, Fletcher had been searching for a security solution that would enable them to stop the USB threat. "We tried everything from custom scripts to registry hacks, but nothing was able to prevent users from accessing the USB," said Vice President of Information Systems Fabi Gower.

Gower and the IT staff at Martin, Fletcher turned to systems integrator ProNet Analysis to help them find a solution to permanently eradicate USB access abuse.

The Solution

ProNet Analysis helped Martin, Fletcher choose SecureWave's Sanctuary.

Sanctuary uses a "default, deny" approach to endpoint security that stops security breaches before they can start. All users are denied access by default and administrators authorize access to only the devices that the user needs, eliminating the ability for a user to plug into the network without approval. Granular policy rules enable SecureWave customers to enforce flexible device-use policies rather than simply prohibiting the use of all devices. With Sanctuary, administrators can create and log a complete copy of all data written to authorized devices, enabling them to monitor USB device usage patterns and trends. Since all use is logged, Sanctuary users have an important audit trail that can be used to assure

compliance with corporate and governmental privacy regulations, a critical requirement as HIPAA enforcement nears.

The Benefits

Martin, Fletcher's decision to install SecureWave's Sanctuary across its network has resulted in numerous benefits for the company. Prior to SecureWave, Martin, Fletcher considered moving to a thin client environment to help ease its device access problems. Since implementing Sanctuary, Martin, Fletcher was able to save tens of thousands of dollars by staying with a workstation environment.

"Our Sanctuary deployment was seamless and we've been extremely impressed with the product's ease-of-use," said Gower. "We've been able to save a tremendous amount of our IT administrators' time and resources as they no longer need to deal with USB access problems. Administrators are able to focus their time on solving other IT issues, thereby saving money for the company in IT man hours."

Sanctuary enables administrators to centrally-manage users' access rights all from one console, which has resulted in significant time savings for IT administrators. "Now we don't need to have administrators checking workstations for unauthorized devices all of the time," Gower said. "We only need one administrator to monitor usage, and he can do it all from his desktop at any time of the day."

Sanctuary also enables Martin, Fletcher to safely allow its mobile workforce to use Company laptops and tablet PCs. "Sanctuary is configured so that it will automatically install to

all computers that join our domain,” said Gower. “In the case machines that are used for travel or brought home, the policy enforcement technology remains and restrictions are enforced even when the computer is not connected to our network. This provides us with the peace of mind to allow our account managers and directors to be part of the important

mobile workforce.”

Conclusion

Martin, Fletcher’s SecureWave implementation has resulted in increased administrator productivity and has made the threat of unauthorized USB access non-existent. As Martin, Fletcher continues to grow

and expand its burgeoning network of medical staffing professionals, SecureWave will be there to ensure that all data and systems are safe and secure.



SecureWave
Safeguarding Tomorrow

www.securewave.com
info@securewave.com

North America

13755 Sunrise Valley Drive
Suite 203
Herndon, VA 20171
United States of America
+1 (703) 713 - 3960 Phone
+1 (703) 793 - 7007 Fax

United Kingdom

Midsummer Court
314 Midsummer Boulevard
Milton Keynes MK9 2UB
United Kingdom
+44 (0) 1908 357 897 Phone
+44 (0) 1908 357 600 Fax

Continental Europe and Rest of World

Atrium Business Park
23, rue du Puits Romain
L-8070 Bertrange
Luxembourg
+352 265 364-11 Phone
+352 265 364-12 Fax

© 2007 SecureWave SA. SecureWave and Sanctuary are registered trademarks of SecureWave SA. All third party trademarks are the property of their respective owners.

Martin, Fletcher - Apr. 07 - V2.0