totalsecurity™

Check Point®
SOFTWARE TECHNOLOGIES LTD.

"Inside the corporate network, everything is a known commodity. We needed to make sure this was the case when our people logged on to the network remotely as well."

Brendan Kilcoyne
Network Manager
Osmose

CUSTOMER NAME
Osmose

INDUSTRY
Specialty Chemicals and Services

CHECK POINT PRODUCTS
- Check Point Endpoint Security™

CUSTOMER NEEDS MET
- Secured remote endpoints, regardless of where in the world they were located
- Minimized help desk calls by automating configuration policies
- Centralized management to facilitate updates and ensure compliance

Osmose

www.osmose.com/home.asp

Osmose Protects its Desktops and Laptops with Check Point Endpoint Security

ABOUT OSMOSE

Osmose has long been a leader in the research and development of new products and services in all areas of wood preservation technology as well as Utility and Railroad asset management. With a commitment to quality, technical support, and service, Osmose has built an impressive network of suppliers throughout the United States and in more then 70 countries around the world.

THE OSMOSE CHALLENGE

Osmose was faced with having to support the needs of all the 800 users in their corporate headquarters as well as 200 remote users. The remote users posed a particular challenge in that they would travel frequently and bring their laptops with them, plugging in at various hotels across the country and around the world.

On the surface, this setup has maximized convenience—the technology has enabled remote workers to do their jobs wherever they may be. Deeper down, however, the situation has presented a familiar risk: with so many potentially unsecured endpoints logging in from all over the world, the company's sensitive and proprietary information was in danger of being compromised.

Brendan Kilcoyne certainly has been no stranger to this dilemma; as network manager at Osmose, he has grappled with the issue for years. "Inside the corporate network, everything is a known commodity," he says. "We needed to make sure this was the case when our people logged on to the network remotely as well."

Providing their users the connectivity they need without sacrificing security was a challenge for Osmose with their limited IT resources. "We just don't have the people to deal with it, so we always caution on the side of safety, which led to user frustration," Kilcoyne says. There was no way to ensure these endpoints were secure before they accessed the corporate network, so Osmose instituted a closed Internet access policy that prohibited remote users from accessing the network without whitelisting the hotel's network first.

"Some of the larger hotel chains have a single web site to authenticate customers, but with other chains, each franchise is independently owned and have different polices and configurations at each location," he says. Kilcoyne describes the situation as "frustrating."

This policy and its process were not well received by their users. Even those users who did keep their endpoint security up to date ended up having trouble logging on. In many cases, the only way for users to log on from afar was to call Osmose headquarters in Buffalo, New York and have Kilcoyne or another IT staffer update the white list and walk them through the process. It became so frustrating for their users that many of them stopped trying to use the Internet access available in hotels.

Another challenge was the problem of basic Microsoft Security updates. Because there was no way to force employees to download the latest improvements, many employees neglected to do so.

It was evident that Osmose needed a better endpoint security solution with integrated management so they evaluated other vendors including their existing AV vendor, Symantec. Kilcoyne found their solution "aged" and the new product line did not fit the bill. "We looked at Symantec, Check Point, and McAfee but really Check Point was the only one with an integrated VPN solution," says Kilcoyne. "And I don't know anybody else who can really provide the type of integrated solution that Check Point can provide."

THE CHECK POINT SOLUTION

Everything changed for Osmose with Check Point Endpoint Security™. The solution provided them with a single agent for endpoint security that combines firewall, Network Access Control (NAC), program control, antivirus, anti-spyware, data security, and remote access, offering comprehensive protection that is part of Check Point's renowned Unified Security Architecture. Endpoint Security also forces endpoint compliance with predetermined security policies—a feature that ensures the very same security protections across the board.

Osmose took advantage of these protections immediately. First, Kilcoyne was able to ensure the ability to sign on from any hotel utilized by company employees even with a restricted internet access policy in place. Secondly, by centralizing management to facilitate updates, Kilcoyne pushed the same protections to all endpoints as they logged onto the network, standardizing all machines on the same platform.

In addition, Osmose was able to enforce security policies and patch levels on the endpoints. "With this product, I can look for registry keys, tell when they're out of date and force a GPO update on their systems," says Kilcoyne.

THE BENEFITS OF CHECK POINT SECURITY

With this new technology, Osmose has experienced improved security across the board. For the first time ever, all Osmose endpoints have the same security protection, and Kilcoyne can administer updates from one central spot. Not surprisingly, virus and spyware outbreaks have dropped considerably.

Osmose also has experienced a significant decrease in the number of phone calls from remote workers in hotel rooms, struggling to log on. Kilcoyne says that under the old system, he'd be "lucky" if 50 percent of remote users could successfully connect to the network. Now, with Check Point Endpoint Security, nearly 99 percent of remote users connect successfully the first time. "From an administrative standpoint, it definitely has saved time and money," he says.

THE FUTURE OF OSMOSE

Down the road, Kilcoyne says he hopes to utilize other features of Check Point Endpoint Security, including the product's full media encryption. He adds that the company has just recently deployed filters in Endpoint Security program control—filters which prevent remote users from installing and utilizing software programs that are not on the company's approved list. "It's all part of our effort to make our endpoints more secure," says Kilcoyne.

CONTACT CHECK POINT

Worldwide Headquarters
5 Ha'Solelim Street, Tel Aviv 67897, Israel | Tel: 972-3-753-4555 | Fax: 972-3-624-1100 | Email: info@checkpoint.com

U.S. Headquarters
800 Bridge Parkway, Redwood City, CA 94065 | Tel: 800-429-4391; 650-628-2000 | Fax: 650-654-4233 | www.checkpoint.com

September 4, 2008