Krueger Wholesale Florist, Inc.

Location:

Rothschild, WI

Industry:

Distribution

Solution:

iPrism Web Security

Deployment:

Hybrid Remote Filtering

Results:

In addition to helping him secure his network against threats, Troemel reports that deploying iPrism Web Security has had a very positive effect on Krueger Wholesale's bottom line.

Kruegar Gains Improved Employee Productivity with EdgeWave iPrism

Overview

Krueger Wholesale Florist, located in Rothschild, WI, is a distributor of fresh cut flowers, green plants and supplies to customers across a seven state area. They have over 200 employees at their corporate headquarters and at three other locations.

The Challenge

When IT Manager, John Troemel, joined Krueger, there was no Web security solution in place at all. Krueger had been relying on a Windows firewall and Symantec antivirus software to protect their network. Because employees were accessing the network from a variety of endpoints including onsite and remote work stations, as well as via mobile and roaming devices, Troemel knew he needed a more robust security strategy. He was also concerned that bandwidth was being exploited since employee Internet usage was virtually unrestricted. This was compromising network efficiency and threatening to impede critical business processes. Troemel explained, "As we performed some system upgrades we found that two-thirds of the employees were streaming internet radio, and I thought – no wonder our hosted email at the time didn't work! Clearly, I needed to take control."

Troemel reports that he uses Power over Ethernet (POE), which combines power and data on one cable with a centralized wireless system to enable their VOIP, business secure, and guest networks. They also had all their iPhones, windows mobile devices, and PCs connected through their wireless system.

Troemel researched Web security solutions for several weeks, considering different options, including a software-based Websense solution. He decided, however, that a software-only solution would be too complex to deploy and maintain, and the operational requirements of adding a dedicated server and additional bandwidth was less than appealing.. He explained, "A big challenge was to administer a solution without putting a load on existing aging computers because we didn't have the budget to upgrade. I decided we would not have a software-based solution, it would be hardware for me all the way."

The Solution

Ultimately, Troemel chose EdgeWave's iPrism Web Security solution because it was the most costeffective choice, and offered all the features he required. Troemel initially deployed an iPrism 10h appliance but subsequently upgraded to the 30h appliance to better accommodate his bandwidth needs and to accommodate company growth. He liked that as a self-contained solution, iPrism requires no additional hardware or software and virtually zero maintenance. As he describes it, "Large IT departments can consider bigger software-based solutions because they have the manpower to manage them, but why hire an IT guy to maintain and monitor a software-based

"We have three remote locations that I can now filter just as if they were on the network with no loss in bandwidth. And, as we try to prevent access to inappropriate material on work computers, this was a big advantage. I don't have to worry about the company being liable for content since iPrism monitors and blocks bad content and other threats"

John Troemel
IT Manager
Krueger Wholesale Florist

solution when iPrism allows you to set-it and forget-it?" Also, the iPrism Hybrid Remote Filtering service was an important factor in securing his remote and roaming users. Troemel found the most efficient configuration for his wireless network was to have one Internet gateway connected to VOIP and one connected to the iPrism.

Ease-of-Evaluation and Deployment:

As a self-contained appliance with its own hardened and optimized OS, iPrism was extremely appealing to Troemel as it provided complete interoperability with his existing network and systems. He also appreciated the ease with which he was able to deploy iPrism for evaluation, and then switch it into production mode. iPrism's streamlined integration with directory services made authenticating all his users hassle-free. "We were able to implement iPrism on our network and link to Active Directory with no effect on users. We used the proxy setting for testing in IT and on several work stations before implementation. Once we were ready, we simply unplugged our network from our Adaptive Security Appliance (ASA), plugged it into the external port on the iPrism, and ran the provided cord back to our network. We were done in minutes and filtering had begun."

Bandwidth Issues Resolved:

Implementing iPrism immediately solved the bandwidth degradation Kreuger was experiencing. The ability to control Web access meant that users were no longer able to visit bandwidth intensive sites and download offending files and applications. Troemel reports, "We have a 35 Mbps pipe and we were using as much as 89% of it before iPrism. Since deploying iPrism, daily usage ranges between 10- 30%. This has really improved network speed and availability, which has made employees happier."

iPrism Override Resolved:

Troemel feels that iPrism's unique, granular override feature, which allows im to delegate override privileges to a secondary administrator or even provide self-override roles to some end-users, saves him precious IT management time. He explained, "The override option, based on grouping, means that if I'm surfing for some software and it is blocked I can just click on the override button, put in my credentials, and get what I need. At the same time, my users, who don't have override privileges, can request the access option and I can easily accommodate them."

Hybrid Remote Filtering:

iPrism's unique hybrid remote filtering was another feature that was important to Troemel. The iPrism remote filtering service employs proprietary technology that allows companies to filter all their remote users without using a VPN, deploying anything in their DMZ or requiring any PAC file implementations. Troemel also liked the fact that iPrism's cloud based technology does not cause browser latency and allows him to filter all of his users no matter where they are located, ensuring the enforcement of company acceptable use and security policies. He explained, "We have three remote locations that I can now filter just as if they were on the network with no loss in bandwidth. And, as we try to prevent access to inappropriate material on work computers, this was a big advantage. I don't have to worry about the company being liable for content since iPrism monitors and blocks bad content and other threats."

Blocking Virus, Malware and Spyware:

Troemel discovered that the company's high bandwidth consumption was due in part to infected computers on the network. "Since iPrism was able to block machines from misusing the Internet, we were able to quickly isolate several PCs that were

using a lot of bandwidth due to malware and spyware and get them cleaned up. I never have to worry again because I know the iPrism will keep the machines clean." Troemel was also pleased with the performance of the iPrism anti-virus commenting, "An added benefit that was the elimination of virus issues. If you can't get to a virus on the Internet, your company can't get infected!"

iPrism Outbound Botnet Protection:

When Troemel learned that iPrism now features additional botnet protection leveraging proprietary ThreatSTOP technology, he checked the botnet category in his URL database to see if bots had been detected in his network. Bots are autonomous applications that infect networks via Internet access or email. They can hide in a network and remain harmless until they contact control and command centers outside the network, where they are joined together to form huge botnets. These zombie networks, designed solely for financial gain, are under the control of cyber criminals, often huge crime syndicates. iPrism blocks bots from "phoning home", alerts administrators of their presence, and allows time to remediate before any damage is done. When Troemel enabled the botnet detection feature on his iPrism, he discovered some problems he did not know he had, "Good thing is, I have no incursions because I keep a really clean network and iPrism helps things stay secure. It did show me some desktops that are trying to connect with Skype that should not be, so I was able to fix that problem."

Comprehensive On-Box Reporting and Real-Time Monitor:

iPrism's on-box reporting provides a significant benefit in supporting Troemel's efforts to keep his network secure from Web-based threats and automatically generate reports for Krueger management. "I have set up custom reports, based on iPrism templates, which get sent off at midnight to each department manager for a review of the employees in their departments. We even send auto reports to each remote location manager for that particular location." He also finds reporting an effective way to keep tabs on employee activity, "IT gets an all-inclusive daily report, along with my boss, on user activity. If I see a spike, that tells me there is either some abuse taking place, or someone brought in a thumb drive or disk." Troemel also finds the iPrism Real-Time Monitor to be useful in detecting issues as they arise. "I also use the live monitor when I'm trying to troubleshoot bandwidth issues. People think it is for big brother purposes, but it's really a great tool to for identifying internet issues as they happen."

iPrism ProCare Technical Services:

iPrism technical support also earned high marks from Troemel for responsiveness. "iPrism Technical Support is awesome! There haven't been too many issues, but if you were to ever have an issue, the EdgeWave support team remotes right into the device and gets it taken care of!".

The Result

In addition to helping him secure his network against threats, Troemel reports that deploying iPrism Web Security has had a very positive effect on Krueger Wholesale's bottom line.

iPrism's Low TCO:

iPrism's low total cost of ownership has saved Krueger time and money on IT expenditures. According to Troemel, iPrism's easy management features and its near

zero-maintenance requirement not only help conserve resources, but also save many IT hours that can now be focused on business-critical tasks. "Once implementation was done, iPrism required no interaction from IT. For a one-man IT department, time is BIG money." He also notes that the person he replaced in IT used to spend weeks cleaning PC's that were infected with spyware and malware. "That is no longer needed because iPrism has solved that problem."

Improved Employee Productivity:

Now able to efficiently manage Krueger's Internet access, Troemel cites iPrism as the catalyst behind the company's measurable improvements in employee productivity. "Prior to iPrism, several users had been abusing their Internet privileges with non-work related activities throughout the day. With iPrism, we can now open up the internet for personal use around scheduled timeslots, such as 30 min before work, one hour at lunch, and 30 min after work. Managing employee internet access has allowed us to maintain employee morale and increase productivity, while enforcing the company's acceptable use policies."

EdgeWave

4225 Executive Sq, Ste 1600
La Jolla, CA 92037

Phone: 858-676-2277
Fax: 858-676-2299
Toll Free: 800-782-3762
Email: info@edgewave.com

About EdgeWave

EdgeWave is a leader in the cyber security industry, delivering innovative, effective and efficient email and web security protection for thousands of business and government organizations. Our mission is to mitigate the risks you face in the real world, and support you in reducing the cost and complexity of protecting your organization in today's fast-changing security and risk environment.

For more information about EdgeWave, visit www.edgewave.com