Roofing and flooring contractor CentiMark uses a Blue Coat ProxySG security appliance to lock down its web traffic and streamline network management.

At a Glance

COMPANY: CentiMark
HEADQUARTERS: Canonsburg, Pa.
EMPLOYEES: 3,000
I.T. STAFF: 6

BUSINESS: Founded in 1968, CentiMark is North America’s largest commercial roofing and flooring contractor, with 80 locations in the United States and Canada. From roof repairs and re-roofing to flooring installations, CentiMark offers a variety of services to its customers. The company prides itself on its top-notch workmanship and use of best-in-class materials. CentiMark’s single-source warranty is backed by its financial strength and a 5A1 Dun & Bradstreet credit rating.
Sometimes, the need for change stares a company right in the face.

CentiMark, a commercial roofing and flooring contractor headquartered in Canonsburg, Pa., faced a significant productivity dilemma when its salespeople were forced to go to a nearby coffee shop to run web conferencing sessions with partners and salespeople outside of its corporate network. The problem could be traced to the company’s old proxy security gateway, which blocked the necessary network protocols to support multimedia transmissions.

The web conferencing issue underscored CentiMark’s critical need for a more flexible solution, says Director of Technology Infrastructure Stephen Rudolph.

That’s when CentiMark turned to CDW for guidance.

“Steve and I had conversations about the web conferencing issue, and they were frustrated with their current proxy,” says Mark Gray, an executive account manager at CDW.

So Gray brought in Jeff Falcon, a senior security solution architect at CDW, to help guide the CentiMark team. After several discussions with the company, Falcon believed that Blue Coat Systems’s ProxySG 900 series proxy security gateway would best fulfill CentiMark’s security and conferencing needs. “The solution aims to accommodate real-time collaboration and video and audio technologies,” Falcon explains. “It’s able to deliver a story that bodes very well for virtualization, voice and video.”

In mid-2012, the CentiMark IT team deployed the Blue Coat proxy appliance to support the approximately 800 users who regularly browse the web via CentiMark’s network.

In addition to the conferencing hiccups, the old device blocked websites in broad categories, such as gambling, keeping at bay large chunks of undesirable web content, Rudolph says. But there was no easy way for the IT department to let sales staff visit a specific site temporarily to do research, and then reblock the site.

“We had a salesperson who needed to provide a quote for one of the casinos in Las Vegas, but the old proxy prevented him from doing the proper research on the casino’s website,” Rudolph explains. “Now, with the Blue Coat proxy, I can very easily open up the site for a few hours so he can do his research, and then lock it back down. I also can do things like block Facebook but allow LinkedIn. The best thing is that all of these tasks take an administrator about 20 seconds to execute.”

“What we like is that the Blue Coat proxy is a stand-alone device that sits between our main servers and the firewall. There’s no need for a physical or virtual server.”

— Stephen Rudolph, Director of Technology Infrastructure
7 Elements of a Proxy Server

According to Blue Coat Systems, an effective web proxy gateway appliance will do the following:

1. **Enforce protocol compliance**: If the protocol transmitted doesn’t comply with standards, by default, it will not pass the proxy. This protects the infrastructure and creates security on the network level. The proxy also can intelligently identify protocols to apply correct security policies.

2. **Conduct significant analysis of applications, far beyond Transport Control Protocol/Internet Protocol headers**: These devices are designed to understand traffic on the Layer 7 application level. When a device manages information at Layer 7, IT managers can apply security protocols that aren’t possible if the packets are simply passing by at the Layer 2 network device or Layer 3 switch level. Threats can be more readily detected because the data are seen as complete objects rather than fragmented packets passing by.

3. **Make intelligent decisions and inform users of exceptions to policies**: A proxy communicates with the user in the event of errors or policy enforcement in more specific language than standard error messages. Blocking a popular malicious website might cause a significant number of calls to the help desk. IT departments can avoid them by giving relevant information to the user directly when an object is blocked.

4. **Cache content and split live content**: Repeated objects can be retrieved once and served to many. For example, it’s possible to download a popular YouTube video once for users to look at thousands of times. This significantly enhances video performance while at the same time releases bandwidth for other critical apps.

5. **Offer the ability to set policies**: A proxy requests data on behalf of a user on the Layer 7 application layer in the OSI model. That means the infrastructure is hidden and protected behind the proxy. Whatever information the IT staff wants to present to the Internet or parts of the Internet can be defined in a policy.

6. **Translate from IPv4 to IPv6**: Because the proxy works at Layer 7, it also can work as a protocol translator between IPv6 and IPv4. The device’s ability to translate in both protocols makes a migration project easier and ensures access between incompatible infrastructures.

7. **Adhere to Quality of Service settings**: A proxy can read, set and follow network QoS settings. It can use more information to set QoS than normal networking devices because it operates at Layer 7 and has more intelligence.

---

**Even More Benefits**

Although the Blue Coat proxy security device cost more than some of the other solutions that Rudolph’s team evaluated, it proved to be the most efficient for their needs. “What we like is that the Blue Coat proxy is a stand-alone device that sits between our main servers and the firewall,” he says. “There’s no need for a physical or virtual server. The Blue Coat proxy has its own internal database for logging and doesn’t require an external database server for logging such as SQL or Oracle.”

Rudolph also appreciates the product’s reporting capabilities. “If there’s a need for an audit, we can get a report with no problem,” he says.

Just as important, the ProxySG 900 allows the IT staff to set up policies for all types of network traffic. “Now, we can handle everything from HTTP for web pages to user datagram protocol for video,” says Systems Administrator Joe Watkins. “It even supports FTP files. Our old proxy gateway didn’t do FTP.”

The ProxySG 900 provides a smoother user experience because it runs transparently. Users can get to the Internet without having to jump through intimidating hoops. For example, they no longer have to enter an IP address in the browser to access the proxy server and surf the web. “The browser now offers a direct connection to the Internet,” Watkins explains. “Users don’t even know they’re going through a proxy. Overall, it’s much more convenient for them.”

**A Holistic Look at Security**

CDW has served as a partner and resource for CentiMark on various projects dating back to the early 1990s, including a virtualization project completed just a few years ago, Gray says. Given that history, CDW was a natural partner to turn to when CentiMark needed a new proxy security solution.

The process began with Falcon helping the CentiMark team take a step back to look at the bigger security picture. In those discussions, “I pointed out that too many companies take the traditional approach to security, where they are always reactive and looking in the rearview mirror,” he says.

Instead, Falcon suggested that the CentiMark team consider a more proactive approach to solving their proxy issues. “I gave them an overview of the current threat landscape,” he explains. “There are so many people at
companies downloading peer-to-peer apps for nonwork purposes, and there also has been an increase in drive-by downloads that often contain malicious code.”

The biggest challenge that companies face with malware is the constant emergence of new threats that existing security systems haven’t yet recognized. “It’s not just about shutting off Facebook or YouTube, or replacing something that’s rusty,” Falcon says, because today’s security threats change hourly.

Falcon encourages companies seeking malware protection to consider the ProxySG 900 gateway because it operates at the Layer 7 application layer, unlike some other solutions on the market, and handles all web filtering updates automatically. Falcon says the appliance is more efficient because it handles many of the web security functions that firewalls once managed, allowing IT workers to focus on other projects instead of standing watch for web-based malware.

“Not having to worry about security issues around web traffic is a huge gain,” Falcon argues. “This shouldn’t — and can’t — be a full-time job for such a small staff.”

CentiMark’s IT team echoes that sentiment. Watkins says the new proxy has made his job much easier because he doesn’t have to manually intervene as often. “Under the Blue Coat proxy, things just work,” he says.

Rudolph, meanwhile, credits CDW with helping the company understand both the current threat landscape and the type of product it needed for its specific network environment. “We’re not a big e-commerce site,” he says. “Our main concern was to find a device that could keep malware from web traffic from infecting our users’ computers.”

According to Rudolph, CDW’s solution architects presented CentiMark’s IT team with three solutions to consider. Rudolph, his staff and CDW personnel then met with each vendor to discuss the advantages and disadvantages of each product.

“CDW steered us to the best possible solution for our needs,” Rudolph says. “They took the time to show us what was out there. We don’t have the time to keep up with the latest developments with proxy security devices, so we really appreciated CDW’s guidance. They really helped us sort out all the networking and security issues.”

“The browser now offers a direct connection to the Internet. Users don’t even know they’re going through a proxy. Overall, it’s much more convenient for them.”

— Joe Watkins, Systems Administrator

Learn more about threat prevention and network security solutions at CDW.com/security.