



BENELOGIC: A CASE STUDY IN SECURITY AND CENTRALIZED MANAGEMENT

MARCH 2006

THE STORY

To meet the ever-evolving demands of managing employee benefits, free up HR departments and offer a more complete solution to employees, several enterprises have begun to employ benefit management technologies. A leader in this space is Benelogic, a Maryland-based company that designs intuitive software applications to streamline and simplify employee benefits management. An efficient, cost-effective alternative to time-consuming and expensive paper-based benefits enrollment and administration processes, Benelogic's solutions provide a flexible, secure environment that is easily implemented and managed over the Internet.

Benelogic's service is the trusted source for online benefits management for more than one million employees and users, spread across 150 enterprises. On average, Benelogic's service receives 15,000 hits a day, a number that continues to double each year. In addition to supporting its customer base, Benelogic's network also supports the company's 100 employees across several different US locations.

As an Application Service Provider (ASP), Benelogic has the dual challenge of securing and optimizing its online environment while also providing a flexible, useful internal network for its employees. With its customer base rapidly increasing each year, it needed to upgrade its network to support current and future growth. The first step in this process was to upgrade its security.

"With more than 100 employees, remote locations, and the need to scale our network as our company expands, we have all the business and security challenges of a growing enterprise. However, our challenges are augmented and complicated by the fact that our technology and business model is very much like an ASP," said Kendall Miller, CIO of Benelogic. "Not only do we have to secure our

resources and internal network but we have to create, host and protect a feature-rich, online environment for our customers. Security is paramount in both accounts and an absolute necessity for running our business.”

BUSINESS CHALLENGE

In addition to protecting its network from viruses and keeping customer information safe from hackers while still offering the best user experience, Benelogic had several other requirements of a new security appliance.

Multiple locations and zones within Benelogic’s network heightened the need for a group of appliances that could be easily and successfully managed from one central location. Due to the fact that its network was growing increasingly complex as more locations and customers were added, the company needed a solution capable of reaching gigabit throughput speeds between several of its networks. Additionally, due to the fact that the traffic on its network experiences seasonal spikes (about 70% of its total network transactions occur over two months of the year), Benelogic needed a highly redundant solution that could scale to accommodate periodic network strains.

“In our business there is an immediate connection between user experience and security. Our challenge was improving and maintaining both simultaneously, without limiting or adversely affecting either,” Miller added. “With that being said, in addition to improving the reliability and breadth of our external and internal networks, we also wanted to make them easier to manage and more efficient.”

THE WATCHGUARD SOLUTION

Benelogic investigated solutions from SonicWall, Nokia, Microsoft and Cisco before ultimately deciding on the WatchGuard Firebox X Peak Unified Threat Management appliance.

In addition to deploying a pair of redundant WatchGuard Firebox X Peak 8000 appliances and a Firebox X Peak 5000 (for active failover and recovery purposes) at its headquarters, Benelogic also deployed a Firebox X Core 700 at a remote office and five Firebox X Edge 5 appliances throughout its network. Almost half of Benelogic’s employees also have the ability to VPN into the internal network to remote access their desktop systems via a software VPN client.

Ultimately, Benelogic selected WatchGuard for three specific reasons:

1. The multi-box, central management functionality enabled Benelogic to easily and effectively monitor and administer each WatchGuard appliance from headquarters. “This was one of the most important decision factors for us. We wanted to implement solutions from a single vendor throughout our network, but struggled to find one that came with the management capabilities we were looking for,” Miller noted. “Not only was WatchGuard able to secure our headquarters, remote sites and mobile users with its appliance line, but the WatchGuard System Manager allowed us to conduct changes, administer updates and make settings edits from our headquarters. Additionally, WatchGuard’s UI is so intuitive and easy to use that our entire IT staff can manage the system - we didn’t have to train one particular person to manage the system, which saves an unbelievable amount of time.”
2. Due to the rapid adoption of its technology and the subsequent need to increase bandwidth on a regular basis to support escalating levels of traffic, Benelogic’s network continues to grow increasingly complex with each day. Therefore, it needed an appliance that could scale to support this kind of network complexity, or more specifically, a solution capable of supporting gigabit throughput speeds. “Gigabit-capable firewalls aren’t rare anymore, but, as we found, easy to manage, affordable, scalable gigabit firewalls certainly are. The WatchGuard appliance was the only one we found that met our specific needs and requirements.”

3. Another goal of Benelogic's implementation was to further aggregate its network by increasing the number of available security zones. To do this, Benelogic needed an appliance that was capable of supporting independent ports, dynamic routing and a high number of multiple VPN tunnels. "One of the more important long term goals of our implementation was to increase the segmentation of our network. Most notably, we wanted to firewall off our development team from the rest of our network and double our security zones from three to six. The port independence and redundancy of the WatchGuard appliance made these transitions seamless and painless, and the fact that the appliance can support up to 10 distinct security zones gives us the flexibility to further aggregate our network moving forward," Miller noted.

RESULTS

In addition to securing and improving the performance of Benelogic's online benefits platform and internal network, the company has seen other positive results from its WatchGuard implementation. Among them:

- The gigabit-throughput capabilities of the appliance have increased the performance of Benelogic's Benefits Admin application.
- The aggregation of the network from three to six security zones has greatly increased the amount of available bandwidth throughout the network.
- The managing and monitoring tools have greatly decreased the man power and time necessitated for troubleshooting.

"We've been very impressed and satisfied with our relationship with WatchGuard thus far," Miller added. "The ASP nature of our business makes it that almost every aspect of our business is visible to the public eye. It's imperative then that any kind of technical upgrade or overhaul is done seamlessly without any interruption of any kind to the end-user. The knowledge of WatchGuard's technical teams and the overall ease-of-use of the appliance have assured this. Those facts, in addition to the security and performance benefits have absolutely validated the selection."

For more information about WatchGuard security solutions, visit us at www.watchguard.com, or contact your reseller.

ADDRESS:
505 Fifth Avenue South
Suite 500
Seattle, WA 98104

WEB:
www.watchguard.com

U.S. SALES:
1.800.734.9905

INTERNATIONAL SALES:
+1.206.613.0895

ABOUT WATCHGUARD

Since 1996, WatchGuard Technologies has provided reliable, easy to manage security appliances to hundreds of thousands of businesses worldwide. Our Firebox X family of unified threat management (UTM) solutions provides the best combination of strong, reliable, multi-layered security with the best ease of use in its class. All products are backed by LiveSecurity® Service, a ground-breaking support and maintenance program. WatchGuard is a privately owned company, headquartered in Seattle, Washington, with offices throughout North America, Europe, Asia Pacific, and Latin America. For more information, please visit www.watchguard.com.

No express or implied warranties are provided for herein. All specifications are subject to change and any expected future products, features, or functionality will be provided on an if and when available basis. ©2007 WatchGuard Technologies, Inc. All rights reserved. WatchGuard, the WatchGuard logo, Firebox, Core, Peak, and Stronger Security, Simply Done are either trademarks or registered trademarks of WatchGuard Technologies, Inc. in the United States and/or other countries. All other trademarks and tradenames are the property of their respective owners. Part No. WGCE66359_082007