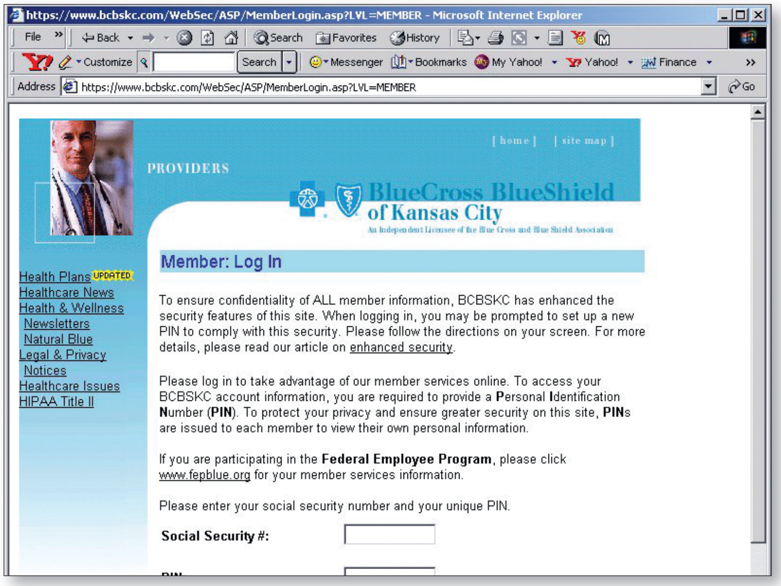
SANCTUM

Blue Cross Blue Shield of Kansas City (BCBSKC)

Highlights

www.bcbskc.com

- ***Industry***
  Healthcare
- ***Application***
  Corporate Web site with secured areas for BCBSKC members, employers, providers and brokers
- ***Business Problem***
  BCBSKC wanted to take proactive steps to ensure that protected health information and other private data on the site would not be illegitimately accessed or compromised.
- ***Security Solution***
  AppShield™ 4.0
- ***Business Benefits***
  BCBSKC management and customers can be confident the confidential data sitting in their Web site applications is fully protected. Additionally, the HTTP logging features provided by AppShield greatly simplify technical support.
- ***ROI***
  Significant development costs saved; one-day deployment; special-purpose intrusion detection software eliminated.



Member: Log In

To ensure confidentiality of ALL member information, BCBSKC has enhanced the security features of this site. When logging in, you may be prompted to set up a new PIN to comply with this security. Please follow the directions on your screen. For more details, please read our article on enhanced security.

Please log in to take advantage of our member services online. To access your BCBSKC account information, you are required to provide a **P**ersonal **I**dentification **N**umber (**PIN**). To protect your privacy and ensure greater security on this site, **PIN**s are issued to each member to view their own personal information.

If you are participating in the **Federal Employee Program**, please click www.fepblue.org for your member services information.

Please enter your social security number and your unique PIN.

Social Security #:

Sanctum AppShield™ secures the sensitive Member, Employer, Provider and Broker data that lies within the Blue Cross Blue Shield Kansas City Web site.

BCBSKC Protects Sensitive Health Information With AppShield™, Uncovering Unexpected Benefits Along the Way

In order to prevent cookie poisoning and query string manipulation on BCBSKC's Web site, Web Architects Jeff Shipley and Dave Whittaker knew that their combination of SSL encryption, authentication and virus detection software just wasn't enough. Highly sensitive healthcare information was at stake.

> *"With its top-notch performance, AppShield has already paid big dividends for us. And I have never been treated as well as I have been by Sanctum customer support."*
>
> --Jeff Shipley, Web Architect,
> Blue Cross Blue Shield,
> Kansas City

AppShield: Automated Web Application Firewall

- Maximum Web application protection with secure proxy architecture
- Ensures HIPAA regulatory compliance and delivers great ROI
- No patches, rule updates or administrative headaches
- Positive security model enforces application logic behavior for signatureless enforcement
- Secure and passive modes for rapid deployment

> *"AppShield was arguably one of the easiest technology investments we have made here at BCBSKC. Web site security is such an important issue for us, and Sanctum's demonstration of AppShield left no doubt in our minds that it would solve our Web application security challenges."*
>
> –Bruce Koster, E-commerce Project Leader, Blue Cross Blue Shield of Kansas City

Within days of the audit, Shipley and Whittaker selected Sanctum's AppShield as their application-level security solution, and just as quickly, BCBSKC management approved it. Today, with minimal administration and virtually no impact on Web application throughput, AppShield protects the BCBSKC Web site not only against known forms of attack, but also against malicious activity that has yet to be conceived.

Blue Cross and Blue Shield of Kansas City (BCBSKC) is the largest provider of health plans in a 32-county area covering greater Kansas City and Northwest Missouri. Through its variety of benefit plans, BCBSKC provides every one of its 805,000 individual and group customers access to the 4,000 physicians and 57 hospitals in its network. BCBSKC's Web site, launched in May of 2000, continues the company's tradition of unencumbered accessibility for members, employers, healthcare providers, brokers and the public at large. However, in providing these legitimate users more convenient access to healthcare-related information, BCBSKC also attracts illegitimate attempts to view, abuse and perhaps corrupt its valuable information assets.

"We have approximately 30 Web applications serving our constituents," explains Whittaker. "And nearly 95 percent of the information these applications provide is considered sensitive." Particularly at risk were members' personal and medical records, as well as the financial information exchanged between BCBSKC and its providers and brokers.

After six months in production, BCBSKC's Web site experienced no breaches of security. Soon after the Web site's six-month milestone, the potential for malicious activity against the site through cookie poisoning and query string manipulation was discovered. That's what drove BCBSKC to AppShield. "We thought we had taken the necessary steps to protect our site," Whittaker recalls. "We reasoned that by encrypting our cookies, we were safe; but during the audit, the ethical 'hackers' found a way around that. At that point, we had two options: either stop using cookies, or put something out there to protect them."

Eliminating the cookies, however, was not an attractive solution. "We have thousands of pages on our Web site that use cookies for navigation and authentication," Shipley explains. "It would have taken three or four developers working full time for at least two months to redevelop the entire site without cookies. With AppShield in place, we could continue using cookies with the confidence that AppShield would prevent their corruption. So, it was clear that the investment in AppShield would justify itself very quickly."

Bruce Koster, E-commerce Project Leader at BCBSKC, concurs, noting, "AppShield was arguably one of the easiest technology investments we have made here at BCBSKC. Web site security is such an important issue for us, and Sanctum's demonstration of AppShield left no doubt in our minds that it would solve our Web application security challenges."

AppShield protects against malice … and inefficiency

Serving as a Web application firewall for a load balanced Web server farm, AppShield protects the BCBSKC Web site by automatically recognizing security policies for each application through an on-the-fly analysis of outbound HTML pages. It then enforces compliance with the policies for each incoming HTTP request. This method of protection makes it nearly impossible for hackers to take advantage of any security loophole that might exist.

The BCBSKC Web site now logs, on average, 30,000 hits per day, and traffic on the site is growing 30 percent annually. With that in mind, it may seem that the dynamic analysis and checks that AppShield performs would create considerable latency, but Whittaker dismisses any such concern. "We've been very pleased with the response time through AppShield," he says. "Even with a significant volume of hits and considerable processing on the application side, AppShield is definitely no bottleneck."

Although it was cookie poisoning that initially drove BCBSKC to search for a better application-level security solution, query-string manipulation was an equally disturbing threat. "We accommodate numerous database queries on our site," Whittaker says. "And all of the HTTP-based attacks, as well as viruses such as Nimda, replicate through query-string manipulation, which most virus detection products aren't designed to recognize. AppShield essentially serves as a filter, stopping the malicious queries before they even reach the virus protection software."

Shipley points out that placing AppShield in front of its Web servers isn't just good for virus protection—it can also prevent an excess load on the servers caused by distributed denial-of-service and other random attacks. "So, not only does AppShield help protect our Web site," he explains, "but it also helps us avoid wasting processor cycles."

BCBSKC has also reaped some unexpected benefits from AppShield. One such benefit is helping the Web architects be more responsive to their customers. "Often customers will call in and say, 'I was doing such and such on the site, and I got an error message,'" Shipley explains. "But we've found that customers aren't always able to retrace their activities on the site accurately. Twice in the last week I've been able to go back to the AppShield logs, find the customer's IP address, and follow through the activity history to find out exactly where the reported error occurred, and why. Consequently, AppShield has been very helpful in debugging problems on the Web site."

A pain-free path to HIPAA compliance

AppShield's logging capability, however, delivers another, more significant benefit to BCBSKC. As a health plan provider, BCBSKC is required to have its policies, procedures and processes meet the requirements of the Health Information Portability and Accountability Act (HIPAA, see www.sanctuminc.com/news/govtregs/index.html). Among HIPAA's mandates for security standards is the protection of all medical records and other individually identifiable health information against any reasonably anticipated threats to their security or integ-

> *"We had nothing that would prevent people from abusing our site through URL attacks, cookie poisoning and other unpredictable activity….before we discovered AppShield, we just didn't know how to prevent them. Now, AppShield has become a vital component of our security infrastructure."*
>
> --Jeff Shipley, Web Architect, Blue Cross Blue Shield of Kansas City

rity. To help ensure compliance, HIPAA requires all healthcare organizations to maintain audit control mechanisms to record and examine system activity.

With AppShield logging all incoming requests, such audit control is built in. "In that sense," Whittaker says, "AppShield has reduced the amount of additional work needed to be HIPAA compliant."

The security standards for HIPAA have not been finalized and BCBSKC prefers to keep its complete security plans confidential. However, the health plan provider has gone so far as to state that it already has in place policies and procedures that secure protected health information, both internally and through its Web site. "With AppShield, we can more confidently stand behind that statement," Shipley says.

The missing security link

AppShield is part of BCBSKC's multi-tiered security strategy, which encompasses virus detection and prevention, encryption, authentication and application-level security. "We were very diligent about implementing all these layers of security," Shipley says. "The one piece we didn't have in place was the application-level protection against malicious activity. We had intrusion detection software in place, which would look for specific, known attacks; but we had nothing that would prevent people from abusing our site through URL attacks, cookie poisoning and other unpredictable activity. We always knew there was a potential for these types of attacks, but before we discovered AppShield, we simply didn't know how to prevent them. Now, AppShield has become a vital component of our security infrastructure."

As BCBSKC continues to bolster its security strategy, it has discussed application-level security with various other vendors. But the company hasn't had any second thoughts about its selection of AppShield software. "From our experience with other vendors, there's no way any other tool would be able to provide the same out-of-the box functionality as AppShield does, without a lot of configuration," Shipley says. "With AppShield 4.0, it takes only about a day to provide application-level protection for a Web server configuration like ours."

And the BCBSKC Web architects are not short on vendor experience. "We have implemented numerous different software packages," Shipley claims. "I have never received such prompt and courteous technical support as I have from Sanctum. Sanctum's customer support, coupled with AppShield's ease of implementation and its top-notch performance, has already paid big dividends for us."

AppShield scales to meet tomorrow's demands

As BCBSKC expands its Web site, its security needs will change as well. By 2003, the company will probably move to the many-to-many AppShield configuration (using multiple AppShield nodes to protect multiple servers). "This will take care of our application-level security needs as we expand our Web server farm," Shipley says.

Looking back on their experience, Whittaker and Shipley have this advice to offer other Web architects: "Have AppShield in place before you put your applications on the Web." With its automated policy generation, AppShield can easily accommodate new applications, the demand for which seems to descend on Web managers almost as quickly and unpredictably as new security threats. But that's another story.

SANCTUM
2901 Tasman Drive, Ste. 205
Santa Clara, CA 95054
Phone: 877-888-3970 (US/Canada)
+972-9-958-6077 (Israel)
+44 7710 939512 (European HQ)
408-352-2000 (International)
Fax: 408-352-2001
www.SanctumInc.com