



## Case Study: Capital BlueCross

**“ArcSight has been with us every step of the way—they listened to our needs and are invested in our success. ArcSight proved to us they aren’t just a technology vendor, they are a partner.”**

Kent Podvin, Director of IT, Capital BlueCross

### Impact Highlights

- Allows Capital BlueCross to quickly demonstrate compliance with regulatory requirements like HIPAA
- Collects, correlates, and analyzes log data from more than a hundred sources, both traditional and non-traditional
- A complete view of the security environment; create meaningful reports on network, system and physical security events

### About Capital BlueCross

Capital BlueCross, headquartered in Harrisburg, PA, is the leading health insurance company in Central Pennsylvania and the Lehigh Valley. It is committed to making health insurance simple, offering easy to use health care and personal service at competitive prices. The company has been serving its customers for more than 67 years and employs more than 2,300 people. Capital BlueCross is an independent licensee of the Blue Cross and Blue Shield Association.

### Capital BlueCross’ Challenge

Everyday, customers entrust Capital BlueCross not just with their personal health data, but their very identities. To make healthcare as easy and accessible as possible, the company allows customers to view personal claim information over the Web and access a variety of online forms. Protecting data, and keeping customers safe and secure, is vital to the company’s success. That’s why Capital BlueCross is deeply committed to building a world-class security program.

As a central part of this program, Capital BlueCross required a security management solution that would allow it to take a comprehensive approach to logging, monitoring and incident response—as well as demonstrate compliance with regulatory requirements like HIPAA and those mandated by the Blue Cross and Blue Shield Association.

To begin with, Capital BlueCross needed a way to automatically review all its log data for security incidents, and respond to those incidents in an effective manner. The challenge, however, was that it had to collect logs from both traditional and non-traditional data sources. The company demanded a solution that could integrate not only with firewalls, intrusion detection systems, network devices and operating systems, but also with its physical security system, mainframes, applications, printers and other security relevant devices.

“We required a truly flexible solution that could meld into our environment,” said Kent Podvin, director of IT at Capital BlueCross. “ArcSight not only addressed our needs today, but they are capable of growing with us into the future as we add even more data sources and continually improve our security program.”





## The ArcSight Solution

Capital BlueCross evaluated a dozen vendors using a number of high-level criteria—including architecture, implementation and maintenance as well as general product capabilities such as correlation, centralized administration, scalability, anomaly detection and technical support expertise—before selecting ArcSight Enterprise Security Management (ESM).

ArcSight ESM™ received the highest scores in all these categories. But it was the system's FlexAgents that most impressed Capital BlueCross. ArcSight FlexAgents are specifically developed to collect data from and interoperate with scores of security—and non-security—products. This was especially important to Capital BlueCross, which needed to intelligently aggregate data from more than 100 sources.

ArcSight ESM didn't just collect and organize the data; it helped Capital BlueCross make sense of it all by combining these disparate data sets into a single intelligent system. For the first time, Capital BlueCross gained a comprehensive view of its security environment and was able to quickly create meaningful reports based on network, system and physical security events.

"ArcSight's FlexAgents are a tremendous asset," says Podvin. "But we are also very pleased with the completeness of ArcSight's capabilities from a correlation, risk management and reporting standpoint."

## The ArcSight Impact

Prior to implementing ArcSight, Capital BlueCross was challenged with finding the most efficient use of its disparate logs and generate reports. For instance, it took longer than necessary for a security analyst to manually piece together relevant data in a spreadsheet.

With ArcSight, however, Capital BlueCross is now able to automatically collect the data, place it in a central repository and intelligently transform millions of random log events into a meaningful picture of real security incidents, all in a reasonable amount of time. This automation is critical because it enables the company to keep the price of healthcare insurance as low as possible for its customers while still building a secure and HIPAA compliant security operation.

"Our investment in ArcSight gives us the power to quickly discover security threats and better protect our customers," says Podvin. "But just as important, it allows us to do this with fewer internal resources and with minimal impact on staffing."

When it came to determining what data should be logged, Capital BlueCross started from the recommended data list that the Blue Cross and Blue Shield Association workgroup had developed for logging best practices. For reporting, Capital BlueCross leveraged ArcSight's ISO-17799 reporting module created for the healthcare industry.

This module features out-of-the-box rules mapped directly to the HIPAA standard. For instance, the system knows which rules support which compliance issues, whether it's a configuration change on a critical server that requires an activity review or a successful attack that necessitates an instant response. The end result is that Capital BlueCross is better able to maintain the confidentiality, integrity, and availability of patient health data that the law requires—and that the company demands of itself.

Thanks to ArcSight, Capital BlueCross is also ahead of the game in terms of pending Sarbanes-Oxley-like legislation for non-profits. The company expects that the hard work it has put into its security initiative will provide better protection and ensure it is ready for any additional IT Security related legislations.

"ArcSight has been with us every step of the way," says Podvin. "We really feel like they listened to our needs and are invested in our success. ArcSight proved to us they aren't just a technology vendor, they are a partner."

## About ArcSight

ArcSight, the recognized leader in Enterprise Security Management (ESM), provides real-time threat management and compliance reporting yielding actionable insights into your security data. By comprehensively collecting, analyzing and managing security data, ArcSight ESM enables enterprises, government organizations and managed security service providers to centrally manage information risk more efficiently. ArcSight's customer base includes leading global companies across all verticals—and more than 20 of the top 30 U.S. federal agencies.



### ArcSight, Inc.

5 Results Way, Cupertino, CA 95014, USA  
[www.arcsight.com](http://www.arcsight.com)  
email: [info@arcsight.com](mailto:info@arcsight.com)

Corporate Headquarters: 408 864 2600  
EMEA Headquarters: +44 870 351 6510  
Asia Pac Headquarters: 852 2166 8302

© 2005 ArcSight, Inc. All rights reserved.  
ArcSight and ArcSight ESM are trademarks  
of ArcSight, Inc. 11/05