



Customer Case Study

Priority Health

“Thanks to ArcSight, it became very easy to look at a series of security events—regardless of which device they came from—and see the real scope of the problem and respond appropriately.”

Tim Maletic, Information Services Security Officer, Priority Health



Industry:
Healthcare

Priority Health's Challenge

The need for Priority Health to monitor its networks, servers and applications—and thereby protect itself, and its customers, from potential threats—has always existed. This need took on greater urgency in the wake of HIPAA (Health Insurance Portability and Accountability Act) and the company's own desire to bolster IT security and further secure patient data. The challenge, however, was that until Priority Health discovered ArcSight, there was simply no available technology that could completely address the company's security goals.

Prior to implementing ArcSight, Priority Health relied on a homegrown security management application that focused primarily on the aggregation and analysis of system log data. But the problem with the application was that it was limited in terms of scope and coverage.

For instance, it did not provide analysis of IDS and firewall logs, which were often subject to inefficient and time-consuming manual reviews.

Moreover, the data generated in the IDS and firewall systems was not integrated with syslog data. This made it difficult for Priority Health to gain true visibility into security events across the entire organization.

“We were using one set of tools to monitor syslog data, another set of tools for firewall data and yet another for IDS data,” says Tim Maletic, information services security officer at Priority Health. “Some systems had reporting capabilities like real-time event notification, while other didn't. The greatest limitation was that we didn't fully understand the true nature of security threats in our environment.”

Customer Brief:

Priority Health is rated one of the top 10 providers of health insurance plans in the nation. Its core purpose is to improve health by providing all people access to affordable and excellent health care. Priority Health serves nearly 450,000 people and 6,300 employers in 31 counties throughout West and Northern Michigan. More than 3,600 health care providers participate in the Priority Health network, including over 1,100 primary care physicians and nearly 1,800 referral specialists.



The ArcSight Solution

The ArcSight deployment immediately addressed the most serious issues at Priority Health. Whereas security systems once operated in silos without any sharing of information, suddenly data from firewalls, syslogs, IDS and even Web servers was integrated into a single console—providing much needed visibility across the organization.

Vulnerability assessment data was also included in the integration mix, which proved to be tremendously beneficial. The company was able to correlate vulnerability assessment data with IDS logs, allowing it to ignore countless security alerts that were simply not applicable to its environment. Security analysts could finally breathe a sigh of relief as they no longer had to spend all their time and energy chasing after false positives.

Just as importantly, ArcSight allowed Priority Health to better manage its vulnerability assessment data, and track that data over time. The bottom line, says Maletic, is that his organization has become much more adept at managing vulnerabilities and measuring the overall performance of the information security platform.

“Thanks to ArcSight, it became very easy to look at a series of security events—regardless of which device they came from—and see the real scope of the problem and what kind of response was needed,” says Maletic. “This is where ArcSight really shines. It is an analysis tool that allows my people to drill into events and understand what is truly going on.”

The openness and flexibility of the ArcSight rules engine has also been very beneficial to Priority Health. “Its ability to use regular expressions in pattern matching, together with the overall logic of the engine, makes writing complex rules relatively simple,” Maletic says.

The ArcSight Impact

Targeted regulatory compliance is also a concern of Priority Health. HIPAA, for instance, mandates that healthcare

companies not only review all their log data for security incidents, but actually respond to those incidents in an effective manner. ArcSight has been instrumental on both those fronts.

Beyond regulatory issues, Maletic is also deeply committed to complying with Priority Health’s own internal security requirements and policies. For example, the company has an acceptable use policy that prohibits employees from using certain software like peer-to-peer applications and instant messaging. Priority Health now uses ArcSight to monitor firewalls and IDS event flows for the use of those unauthorized applications.

With ArcSight, potential threats can be quickly contained because the system automatically recognizes unauthorized activity, creates a security incident ticket in real-time and immediately notifies the appropriate people of the event.

The audit trails and workflow capabilities inherent in ArcSight have also proven highly valuable to Priority Health. The company is currently solidifying its incident response procedures. When certain types of events occur, ArcSight automatically sends an alert to the appropriate security analyst for review. From there, a manager can evaluate and sign off on the analyst’s decision. All this is logged within ArcSight and can be made available for review later by internal or external auditors. Essentially, this audit trail serves as evidence that Priority Health’s incident response procedures are working as required.

Priority Health experiences an overwhelming 2.5 million security events every day. Naturally, it does not have the bandwidth to deal individually with all of them. That’s why it relies on ArcSight to filter these events to a much more manageable and meaningful number. “Now, we are only responding to incidents that truly merit attention,” says Maletic. “We no longer have to devote as much time to incidence response and can spend more time on other important initiatives. I have been very impressed with ArcSight,” concludes Maletic. “It has fulfilled all my expectations.”

Impact Highlights:

- Helps Priority Health comply with HIPAA-related requirements—as well as with its own internal security regulations and policies
- Integrates security data from across the organization on a single console, providing true visibility into the full-range of security events
- Greatly reduces false positives by filtering down 2.5 million security events to a much more manageable and meaningful number

About ArcSight:

ArcSight (NASDAQ: ARST) is a leading global provider of compliance and security management solutions that protect enterprises and government agencies. ArcSight helps customers comply with corporate and regulatory policy, safeguard their assets and processes, and control risk. The ArcSight platform collects and correlates user activity and event data across the enterprise so that businesses can rapidly identify, prioritize, and respond to compliance violations, policy breaches, cybersecurity attacks, and insider threats. For more information, visit www.arcsight.com.



ArcSight, Inc.

5 Results Way, Cupertino, CA 95014, USA
www.arcsight.com info@arcsight.com

Corporate Headquarters: 1-888-415-ARST
EMEA Headquarters: +44 870 351 6510
Asia Pac Headquarters: 852 2166 8302

© 2009 ArcSight, Inc. All rights reserved.
ArcSight and the ArcSight logo are trademarks of ArcSight, Inc. All other product and company names may be trademarks or registered trademarks of their respective owners.
ARST-CS008-031209-01