



## Customer Case Study

# Priority Health

“ArcSight has become our primary partner in security. With ArcSight ESM and ArcSight Logger, we have effectively shifted from a reactive security stance to one that is very proactive and forward-thinking – and the value to our company is huge.”

Paul Melson, Manager of Information Security, Priority Health



**Industry:**  
Healthcare

**Products:**  
ArcSight ESM  
ArcSight Logger

### The Priority Health 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 the Health Insurance Portability and Accountability Act (HIPAA) and the company's own desire to bolster IT security and further secure patient data. The challenge, however, was that until Priority Health discovered the ArcSight SIEM platform, there was simply no available technology that could completely address their security goals.

Prior to implementing ArcSight ESM, 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 Paul Melson, Manager of Information Security at Priority Health. “Some systems had reporting capabilities like real-time event notification, while others didn't. The greatest limitation was that we didn't fully understand the true nature of security threats in our environment.”

Additionally, Priority Health needed a better way to collect all log events, and a faster and more effective way to search log data, whether it was structured or unstructured.

### The ArcSight Solution

The ArcSight ESM 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 ESM allowed Priority Health to better manage its vulnerability assessment data, and track that data over time. The bottom line, says Melson, 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 Melson. “This is where ArcSight ESM 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 ESM 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,” Melson says.

Priority Health also implemented ArcSight Logger, a leading-edge log management solution that integrates seamlessly with ArcSight ESM and can quickly search across both structured and unstructured log data. “We are so excited about the integration,” says Melson. “The ability to tap into ArcSight Logger right from the ArcSight ESM console and search long-term historical data is such a huge benefit.”

### **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, Melson is also deeply committed to complying with their 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 ESM to monitor firewalls and IDS event flows for the use of those unauthorized applications.

With ArcSight ESM, 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 ESM have also proven highly valuable to Priority Health. The company is currently solidifying its incident response procedures. When certain types of events occur, the system 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 ESM and can be made available for review later by internal or external auditors. Essentially, this audit trail serves as evidence that Priority Health incident response procedures are working as required.

The implementation of ArcSight Logger has also enhanced the organization’s ability to troubleshoot and perform top-to-bottom security investigations. “Prior to ArcSight Logger, it would take us hours and hours to research our logs, but now we have cut that down to a matter seconds,” says Melson. “ArcSight Logger is unbelievable. We are able to search months and even years worth of data – and the performance is just screaming fast.”

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 ESM to filter these events to a much more manageable and meaningful number. “Now, we are only responding to incidents that truly merit attention,” says Melson. “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 Melson. “The company and its solutions have fulfilled all my expectations.”

### **Customer Brief:**

Priority Health is an award-winning health benefits company recognized for its innovative solutions that improve health, lower costs and increase patient satisfaction. It serves more than half million people with a broad portfolio of products, including commercial and government health plans. As a nonprofit corporation, Priority Health provides all people access to affordable health care. It continues to be rated as one of America’s Best Health Plans by *U.S. News & World Report* and the National Committee for Quality Assurance.

### **Impact Highlights:**

- ArcSight ESM helps Priority Health comply with HIPAA-related requirements – as well as with its own internal security regulations and policies
- The solution integrates security data from across the organization on a single console, providing true visibility into the full-range of security events
- ArcSight ESM greatly reduces false positives by filtering down 2.5 million security events to a much more and meaningful number
- ArcSight Logger enables Priority Health to improve its security posture by searching months and even years’ worth of log data in a matter of seconds



**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

© 2010 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-CS009-0609-03

### **About ArcSight:**

ArcSight (NASDAQ: ARST) is a leading global provider of security and compliance management solutions that protect businesses and government agencies. ArcSight identifies, assesses, and mitigates both internal and external cyberthreats and risks across the organization for activities associated with critical assets and processes. With the market-leading ArcSight SIEM platform, organizations can proactively safeguard their assets, comply with corporate and regulatory policy and control the risks associated with cybertheft, cyberfraud, cyberwarfare and cyberespionage. For more information, visit [www.arcsight.com](http://www.arcsight.com).