

Case Study: Sentry Metrics

“ArcSight can keep pace with any amount of data that is being generated — and just as importantly it can make sense of all that data.”

Dave Millier
CEO, Sentry Metrics

Impact Highlights

- Provides Sentry Metrics with a cost-effective alternative to building its own security management engine
- Consolidates disparate security logs in one central location, allowing for greater visibility into threats and vulnerabilities
- Saves time and money by delivering a more manageable and meaningful number of security alerts

About Sentry Metrics

Sentry Metrics addresses the growing need for comprehensive Managed Security Services for enterprise network environments. The company’s philosophy is simple: build a talented team of certified security professionals, select the best tools the industry has to offer, and combine these resources into a centralized holistic environment to provide non-stop security services to its clients.

Sentry Metrics’ Challenge

Sentry Metrics manages everything from firewalls to intrusion detection systems for a growing number of clients. The problem, however, was that these systems operated in silos, without any sharing of information. As a result, it had become increasingly difficult for Sentry Metrics to piece together actual security threats. “We simply didn’t have an easy way to gain visibility into our customer sites and see what was really happening,” said David Millier, CEO of Sentry Metrics.

Anytime there was a blip on the radar at a customer site, Sentry Metrics security experts had to scramble to figure out the true nature of the incident. First, they would examine

firewall logs. Then they would inspect the intrusion detection logs. Next they would scour the server logs. Sifting through all these individual log sources was a manually intensive, time consuming process.

“What we wanted was the ability to bring these logs together in one central repository and normalize the data,” said Dave Millier, CEO of Sentry Metrics. “ArcSight gave us the kind of visibility we required to better serve our clients. For the first time, we are able to see the big picture and quickly put security events in their proper context. Moreover, ArcSight allows us to be proactive rather than reactive by providing a faster time to resolution. This saves hugely in terms of time and effort.”

The ArcSight Solution

Before selecting ArcSight, Sentry Metrics tried to build its own security management engine from scratch. But nearly \$100,000 later, with little to show for the effort, the company began looking for existing enterprise security management tools on the marketplace. What separated ArcSight from the pack was its broad functionality and native support for scores of operating devices. “We put ArcSight



through its paces and it did exactly we wanted it to do,” says Millier. “The product had a lot more to offer than anything else.”

As a provider of managed security services, Sentry Metrics required a solution that could easily interoperate with almost any security product and fit the existing infrastructures of its many customers. That’s why Millier was so impressed with ArcSight’s SmartAgents, which are specifically developed to gather and interpret data from a wide range of devices.

“With SmartAgents, the barriers to getting data back to a central location were eliminated,” says Millier. “We can now talk to many, many sources. Moreover, ArcSight can keep pace with any amount of data that is being generated—and just as importantly it can make sense of all that data.”

At the core of the Sentry Metrics service is an executive dashboard that allows customers to see, via a visually rich interface, exactly what is happening within their own security environments. This dashboard, called The Sentry, is intrinsically linked to ArcSight and allows Sentry Metrics’ clients to experience the entire security lifecycle through customized views that meet their individual needs.

An executive, for instance, can log onto the dashboard and get a high-level snapshot of how well the security environment is performing. An internal security specialist, meanwhile, might see a vulnerability alert that needs to be investigated. Thanks to ArcSight, the analyst can then drill down with precision, perform a forensic investigation and quickly get to the heart of the problem.

The ArcSight Impact

Sentry Metrics has seen tangible results since implementing ArcSight. One Sentry Metrics customer, for instance, has 10 firewalls that generate as many as 35 million events each day. It was nearly impossible to make sense of such an overwhelming amount of data. With ArcSight, Sentry Metrics was able to cut through the noise so that it was focusing on only 2 million events. “ArcSight helps us find the gold that previously was impossible to discover,” says Millier.

Sentry Metrics is also able to leverage ArcSight’s rules engine to create customized rules for any security environment. For example, a typical security tool can generate a list of all failed log-in attempts, but it cannot tell you in precise detail where those failed log-ins came from and who was responsible.

But, for one particular customer, Sentry Metrics was able to customize the ArcSight rules engine so that it only reported log-ins from a few particular IP addresses that were under scrutiny. Suddenly, from an administrative point of view, Sentry Metrics was delivering just four high-priority events to the customer – a much more manageable and meaningful number than the more than one thousand daily events it was previously delivering.

“Our customers have come to realize that flexibility and visibility across the enterprise are vital for making the right business decisions and responding to security threats in a timely fashion,” says Millier. “Not only does ArcSight provide this ability to all our customers, it also enables us to take our own business in new directions.”

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.

For More Information

To find out how ArcSight can help you with your enterprise security management needs, contact ArcSight at info@arcsight.com, call (408) 864 2600 or visit us online at www.arcsight.com.

ArcSight, Inc.

5 Results Way, Cupertino, CA 95014, USA

Email: info@arcsight.com

Phone: 408 864 2600

© 2005 ArcSight, Inc. All rights reserved. ArcSight and ArcSight ESM are trademarks of ArcSight, Inc. All other product and company names may be trademarks or registered trademarks of their respective owners. 06/05

