

A background image showing a person in a security operations center (SOC) working at a desk with multiple computer monitors displaying data and charts. The scene is dimly lit with blue and green tones.

## Case Study: Unisys

**“ArcSight gave us a richer and more customizable set of capabilities that allows us to tailor our security service to each customer’s unique environment.”**

John Summers

Global Director of Managed Security Services, Unisys

### Impact Highlights

- Enables Unisys to quickly identify and respond to threats and attacks on customer networks around the world
- Provides the scalability, flexibility and configurability to grow the Unisys business
- Allows Unisys security analysts to greatly reduce the number of hours they spend chasing false positives

### About Unisys

Unisys’ Security Services practice employs a global team of more than 300 security consultants. The Managed Security Services Provider (MSSP) portion of the business has customers around the world that benefit from a highly integrated security environment that provides proactive, real-time monitoring and management, configuration management, and response and remediation services. Unisys delivers these capabilities from Security Operations Centers (SOC) in the Americas, Europe and Australasia. By out-tasking the security of their networks and data centers to Unisys, customers benefit from an improved security posture, reduced staffing challenges and potentially lower costs.

### Unisys’ Challenge

Unisys monitors more than 150 million security events every day in support of more than 200 customers. The challenge is that each customer has different security environments and vendor devices. In addition, many of these devices, such as intrusion detection systems, are notorious for generating an enormous amount of security events—the vast majority of which are false alarms.

Unisys needed to find a way to absorb millions of security events from scores of heterogeneous devices, and then synthesize and aggregate the data in such a way that it could help customers quickly identify and respond to true security risks and attacks.

Unisys realized that it had to implement a best-in-class event monitoring and management infrastructure at the core of its business. Unisys pulled together a top team of internal security experts and conducted a major review of all the top enterprise security management vendors in the market.

In the end, the selection came down to ArcSight and one other vendor. Unisys held a product review between the two vendors, placing them side by side and running real production feeds from its customers. “ArcSight really proved to us that it was the superior product,” says John Summers, global director of managed security services at Unisys.



## The ArcSight Solution

Where ArcSight really eclipsed the competition was event-per-second processing, which speaks directly to the scalability of the product. As an MSSP serving an ever-growing roster of clients, Unisys believes that this scalability is critically important to its success—and the security of its customers.

Unisys was also deeply impressed with the flexibility and range of configurability of the ArcSight solution. “The primary strategic reason for deploying ArcSight on a global basis was to deliver superior business value that our competitors could not match, and that our customers could not provide for themselves,” says Summers. “ArcSight gave us a richer and more customizable set of capabilities that allows us to tailor our security service to each specific customer environment.”

One customer, for instance, was installing a new device just as an unrecognized worm emerged in the network. The signatures of this fast-spreading worm were not available from the vendor. But with the help of ArcSight, Unisys was able to determine the characteristics of the worm’s propagation pattern.

Once Unisys plugged those new characteristics into ArcSight, it was able to pick up signs of infection in this customer’s network. Unisys then immediately contacted the customer with the news. As a result, the customer was able to begin the remediation process well in advance of the worm posing any substantial impact to its network. “ArcSight gives us the ability to get ahead of the curve and keep up with new security threats in the wild,” says Summers.

## The ArcSight Impact

ArcSight has delivered tremendous business value to both Unisys and its customers. Unisys has experienced significant efficiency improvements in terms of resources and human capital since it began using ArcSight. In particular, the tool has allowed Unisys security analysts to greatly reduce the number of hours they spend chasing false positives in customer events. In the case of one customer, the number of security events being processed actually declined by a factor of ten.

Unisys is also very impressed with the support it has received from the ArcSight development team. Summers admits he had some concerns on the support front because Unisys is a big company and ArcSight is a growing startup in a new technology space.

“ArcSight has consistently stepped up and done the right thing to support Unisys,” he says. “We have been able to successfully align our respective visions for enterprise security management,”

The relationship has evolved to the point where Unisys is now working with ArcSight product managers on feature requirements for future versions. “This alignment has been key to the joint delivery of business value to our mutual customers,” says Summers.

As the person ultimately responsible for placing ArcSight at the core of the Unisys infrastructure, Summers is always asking his engineering team if he picked the right product, did the right thing and if ArcSight is really delivering all the value we hoped it would? The answer, concludes Summers, has been a resounding yes on all accounts.

## 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](mailto:info@arcsight.com), call (408) 864 2600 or visit us online at [www.arcsight.com](http://www.arcsight.com).

### ArcSight, Inc.

5 Results Way, Cupertino, CA 95014, USA

Email: [info@arcsight.com](mailto: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. 11/05

