

REPRINTED from

COMPUTERWORLD®

THE VOICE OF IT MANAGEMENT ■ WWW.COMPUTERWORLD.COM

NOVEMBER 8, 2005

FAA turns to ArcSight for security event management

The new tool is designed to help it sift through a torrent of security data

BY JAIKUMAR VIJAYAN

The Federal Aviation Administration has just finished putting in place a new security event management system designed to help the agency detect and respond to external and internal threats more efficiently.

The new tool is based on a product from ArcSight Inc. called Enterprise Security Management (ESM) that allows the FAA to centrally monitor, collect and analyze information from multiple network security devices such as firewalls and intrusion-detection systems.

The tool is part of a broader FAA bid to bolster its network defenses and incident-response capabilities after the 9/11 terrorist attacks, according to Michael Brown, director of the Office of Information Systems Security at the FAA.

"We were looking for a way to manage the large volume of information coming from multiple [network] sources [and] do a lot of correlation and data reduction," he said. The goal is to help the

agency better manage the large amount of information generated by security systems, Brown said.

ArcSight's ESM, like other products in its class from vendors such as netForensics Inc., NetIQ Corp., and Intellitactics Inc., is designed to help organizations quickly sift through the torrent of data generated by multiple security devices, allowing them to focus on the ones that are most important.

At the FAA, for instance, firewalls, system log files, vulnerability scanners and intrusion-detection systems together generate more than a million alerts a day — only a very small fraction of which really merit any follow-up, Brown said.

"At the end of the day, after all the analysis has been done, we are looking at roughly 15 to 20 alerts" that really matter, he said.

Apart from transforming raw event data into actionable intelligence for security and network administrators, tools such as those from Cupertino, Calif.-based ArcSight can also be useful for

The new tool is based on a product from ArcSight Inc. called Enterprise Security Management (ESM) that allows the FAA to centrally monitor, collect and analyze information from multiple network security devices such as firewalls and intrusion-detection systems.

forensic analysis after an attack, he said.

Like other agencies, the FAA — which is a part of the U.S. Department of Transportation — is also subject to audits by the Government Accountability Office and is required to implement strong incident-response capabilities under the Federal Information Security Management Act.

The new event management capability will allow the FAA to create an auditable security infrastructure to demonstrate compliance with such requirements, Brown said.



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.