

White Paper



Financial Services Companies Look
to ArcSight to Gain Greater Security ROI

Financial Services Companies Look to ArcSight to Gain Greater Security ROI

In today's digital economy, Financial Services customers can do everything from access checking and savings accounts to transfer funds, open IRAs and trade stocks on the Internet. But as the Banking and Financial Services industry focuses increasingly on a broad spectrum of online services, IT security becomes critically important. Vigilant protection of account numbers, credit information, passwords and other personal information is not only imperative from a customer service perspective, it is also now required by other interested parties, like insurers, and by privacy provisions in laws like the Gramm-Leach-Bliley Act. Complicating matters are the growing sophistication of network threats and the business, financial and legal issues that result.

The Challenge

With millions of online customers representing more than 20% of its overall account base, one leading financial institution fully realizes the need to make network security a top priority. However, deployment of an array of individual point devices like firewalls, encryption and authentication tools and intrusion detection systems has left security staff overworked and overwhelmed with the vast amount of data generated by these disparate products - data that needs to be tracked, stored, analyzed, and acted on in as close to real time as possible.

Furthermore, a lack of interoperability between point solutions allows no way for security information to be monitored centrally. Says one security manager, "Each device has its own log or console that reports data in a unique format. The problem is that none of these devices can 'talk' to one another to cross correlate the information for a complete view of what's happening across the enterprise. This not only creates an enormous amount of work for the security staff, but it also impedes the timely detection of multi-source, multi-target attacks."

A financial institution's security department typically spends nearly *half* of their hours monitoring and analyzing data. The need for a more comprehensive and centrally managed solution is clear, so that those responsible for security can spend less time tediously reviewing logs and more time dealing with legitimate security incidents *before* any real damage can be done.

The Solution

ArcSight's enterprise software solution for security management offers the data collection, correlation and workflow support critical to a proactive system of defense. By closing the "security gaps" existing in a company's disjointed security infrastructure, ArcSight helps ensure that important information is neither lost nor misinterpreted, and that optimal ROI can be realized from devices deployed throughout the network.

ArcSight can help Banking and Financial Services companies:

- ◆ Greatly reduce the amount of time required for the monitoring of security information, freeing up hours for higher-level activities like proactive interception of legitimate threats. ArcSight's real time data capture and sophisticated cross correlation capability offers users a quick, consolidated view of all security activity in the enterprise.
- ◆ Separate real events from the "white noise" in the environment. False positives arise when data from one device suggests a suspicious incident that may turn out to be a non-event when looked at in the context of the bigger picture. Says another security professional, "With ArcSight, I can easily see whether an alert generated by one of our IDS systems warrants further investigation. This avoids time-consuming wild goose chases and allows me to go home confident that all is well in my sector of the world."
- ◆ Enable even non-security personnel like systems administrators, CIOs, CTOs and employees from auditing and legal departments to monitor and understand what is happening in the security environment. ArcSight's user-friendly console and comprehensive reporting functionality allows fast, simple incident monitoring, rules authoring, and analysis -- regardless of whether to most seasoned security vet or "night watch" systems administrator is at the gate.

Greater ROI on Security Investment

ArcSight's enterprise security management solution has the potential to dramatically improve a company's return on its security investment. By optimizing the value of point devices already in place, ArcSight helps all individuals responsible for security work smarter -- equipped with a centralized, correlated and comprehensive view of security throughout the network. For one financial services company, the initial results are striking: a 50 percent reduction in the time spent collecting and monitoring security data, far fewer false positives, and a more finely tuned ability to quickly handle threats and protect the assets of the organization and its customers.