

White Paper



ArcSight Helps Secure Major e-Service Providers

ArcSight Helps Secure Major e-Service Providers

Attacks on Web servers doubled this year over last, and nearly 90% of companies surveyed have been infected with worms or viruses, despite having antivirus software installed, according to the Information Security Industry Survey, performed annually by *Information Security* magazine.

- "Survey: Web attacks doubled in past year" *Computerworld*, October 9, 2001

For any service provider responsible for the information resources of its clients, IT security is not just an afterthought -- its critical to the competitive and legal requirements of doing business. Managed Security Providers are the obvious example, but Application Service Providers are also being asked to write security provisions into their service level agreements and ISP's are increasingly front and center in the battle to protect internal networks from attack. Clients want the assurance that their key business functions are protected from both an infrastructure and individual application perspective. While service providers have invested in sophisticated security technologies such as firewalls and intrusion detection systems, the real opportunity lies in maximizing these technologies in terms of monitoring, investigating, resolving and reporting to specific service level agreements. This requires an advanced security management solution.

The Challenge

The challenge for service providers is two-fold: How can they provide *individualized* (and even customized) security for each client, while also utilizing their economies of scale, expertise and integrated oversight to protect the entire customer complex. It's important for providers to be able to tell the difference between a compromised system or component that threatens only one customer out of many, or a threat that puts the entire infrastructure at risk. In addition, each customer has a different set of objectives and policies when it comes to security.

For example, one organization may require an automatic account cancellation after detecting five failed attempts at a login, while another may simply want to contact the account owner prior to acting. With hundreds or even thousands of customers, the service provider faces a significant challenge in not only detecting these triggering events but also in acting appropriately in each instance.

In the area of reporting, every customer has specific requirements based on their internal policies and procedures, management structure, legal and regulatory requirements and staff expertise. As reports are an important deliverable in the service provider business relationship, they can consume significant amount of resources to prepare and deliver.

Finally, security responsibility is often split between internal staff and the outsourcer. The client staff often requires real time oversight over crucial business processes while relying on the tools and expertise of the service provider to ensure the appropriate level of protection. Supporting this shared security responsibility is completely outside the scope of the typical security point products such as intrusion detection systems. A centrally controlled, enterprise-level, and configurable solution for security management is key.

The Solution

In addition to its core strengths of security information consolidation and analysis, ArcSight provides e-service providers with flexible, fully configurable monitoring, investigation, issue resolution and reporting capabilities for shared security management of outsourced IT resources. As a result, one leading service provider is leveraging ArcSight to more efficiently meet its clients' security needs within the technical and business model that makes outsourcing so attractive. The ArcSight solution customizes the security functions for service providers by:

- ◆ Assigning access privileges to all ArcSight users so that each customer's information is protected and only the specific service provider staff associated with the account can see the data.
- ◆ Grouping security information into Zones that represent any logical view required such as business organization, network topology, trusted and untrusted sources, and organization responsibilities so that each customer has a separate and protected view of their security activities and how they relate to their business.
- ◆ Providing correlation rules that work specifically on the information Zones to detect customer-specific conditions that require attention and follow up. ArcSight Access Control Lists ensure the support staff within the service provider will only see the alerts for the customers they manage.
- ◆ Supporting individualized Knowledge Base pages that reflect not only industry sourced prescriptions for handling security problems (such as CVE and CERT) but also customer-specific policies and procedures that can be accessed instantly when a problem occurs.
- ◆ Case management workflow that groups and manages all the information pertaining to a particular problem so that anyone with the proper access can track the progress of an incident.
- ◆ Providing controlled browser access to the ArcSight system to view alerts, events, cases and the Knowledge Base through myArcSight that enables both the provider and the customer to simultaneously view events and determine appropriate responses in a coordinated manner. In addition, main consoles can be deployed both within the service provider and the client should multiple levels of access be required.
- ◆ Fully customizable reporting functions that will deliver exactly the reports needed based on the data available for only that customer.

A Partnership with Service Providers

Because ArcSight enables any number of properly authorized constituents to share oversight and administration of the security network, service providers and their clients are leveraging the solution to co-manage critical security functions. For a Managed Security Provider, the end user staffs the security function with dedicated professionals during its main business hours and then shifts responsibility to the ArcSight-equipped MSP outsource partner for the remainder of the day. In this way, in-house expertise and responsibility is maintained for a key business function without incurring the duplication and expense of a 24x7 internal operation. Completely scalable for single-user, multi-user and even multi-site environments, ArcSight provides the only enterprise-level platform for comprehensive, centralized security management, no matter how complex the setting.