




## ArcSight ESM

Enterprise Security Management (ESM)  
for Security, Compliance and Insider Threat



**“Thanks to ArcSight, it is very easy to look at a series of security events—regardless of which device they come from—and see the real scope of the problem and what kind of response is needed. ArcSight is an analysis tool that allows my people to drill into events and understand what is truly going on.”**

**Tim Maletic, Information Services Security Officer, Priority Health**

## **We Live in Challenging Times.**

Corporate computer networks are continuously under siege by hackers and malicious insiders eager to exploit any and every vulnerability. The number of attacks on systems continues to rise exponentially. In 1988, the CERT Coordination Center recorded only six attacks against Internet-connected systems. By 2005, that number skyrocketed to an estimated 200,000 attacks.

These attacks are not only increasing in frequency, but in complexity and severity as well. The time to exploitation of today's most sophisticated worms and viruses has shrunk from years to months to days, and in some cases, to a matter of hours. Defending against these attacks is becoming more difficult by the minute.

It is not just external attacks we must defend against, but malicious insiders who aim to steal confidential customer and business data and sell it for financial gain. Some 35% of the top 100 financial institutions were victims of insider attacks in 2004, compared to only 14% the year before, according to a study from Deloitte Touche.

Meanwhile, government regulations like Sarbanes-Oxley, HIPAA, Gramm-Leach-Bliley and FISMA have raised the stakes when it comes to protecting confidential data. Businesses are often compelled to report weaknesses in financial controls, database breaches and information loss. Failure to protect sensitive data and meet regulatory requirements can destroy customer trust, damage stock prices, invite class-action lawsuits and spur government and industry fines. The detrimental consequences of a security breach are extremely far reaching.

### **Crippling Complexity**

Organizations have attempted to protect themselves by implementing best-of-breed security solutions like antivirus gateways, firewalls and intrusion prevention systems. These technologies are valuable, but this has led to a new problem: crippling complexity.

Today, companies are overwhelmed by scores of security devices and systems from many different vendors. These disparate devices generate a huge flood of data. Whereas three years ago, the typical organization had hundreds of security devices generating 50,000 events per day, enterprises today have tens of thousands of security devices emitting billions of events that need to be monitored, logged, analyzed and correlated every day.

Some of these events are false alarms that can overwhelm operations and waste countless hours by leading security analysts on a fruitless hunt for random incidents. Effectively managing and auditing these security events has become a Herculean task.

What is required is a single, integrated solution that enables enterprises to collect, correlate and manage massive amounts of security data from heterogeneous sources for real-time monitoring and response. What is required is a solution that can easily adapt to growing and changing environments. What is required is ArcSight ESM™.

### **ArcSight ESM Solution for Compliance**

Audit, compliance and IT governance are major requirements for all enterprises. The need to centrally collect, monitor, respond and report on security event data is more important than ever. ArcSight automates time-consuming processes related to proving compliance to regulations such as Sarbanes-Oxley, GLBA, FISMA, HIPAA and PCI.

Our multi-award winning security information management solution delivers cost-effective, flexible and intelligent aggregation, correlation, monitoring and reporting to immediately fulfill and enable many important compliance requirements.

### **ArcSight ESM allows you to:**

- Centrally collect, store and monitor security event data
- Easily deliver one-click compliance reporting that provides relevant data in a relevant format
- Demonstrate the ability to monitor, respond and mitigate risk
- Separately monitor and report on events that involve regulated systems
- Easily increase protection while eliminating manual processes
- Save valuable security analyst resources from tedious, manual audit tasks
- Drive accountability and awareness for all stakeholders

## **A True Understanding of Security Threats.**

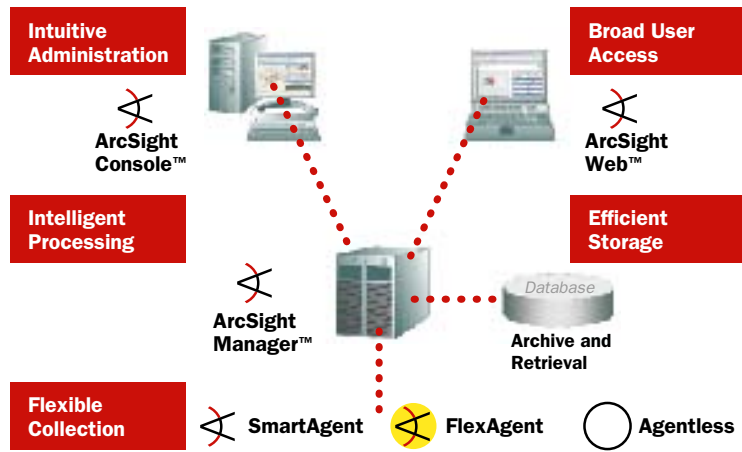
With ArcSight ESM, you don't have to limit the information you collect. You don't have to decide up front what is important and what is not. And you no longer have to miss potential threats due to data overload.

ArcSight ESM ties all security data together in an intelligent system that allows security teams to manage regulatory compliance requirements, communicate the status of security to a broader audience and gain visibility into insider threats, all while ensuring protection at the perimeter. For the very first time, organizations can see the true nature of security threats in their environments.

**“ ArcSight’s SmartAgents and FlexAgents are a tremendous asset. They allow us to collect and normalize data from more than 100 security—and non-security—products in our environment.”**

IT Director at a major health insurance provider





ArcSight ESM delivers flexible collection, intelligent processing, efficient storage with easy and intuitive access for security analysts, operators and management.

## ArcSight ESM: Protecting Your Business

ArcSight ESM was designed to work in concert with security analysts, operators and managers as they strive to protect your business. The system includes a host of tools, features and functions to:

- Seamlessly collect information from any log source
- Intelligently correlate information to derive meaningful information from a sea of data
- Monitor relevance to organizational risk
- Drastically reduce response time, minimizing damage
- Efficiently store and retrieve information leveraging enterprise database capabilities
- Quickly investigate and determine root cause of security issues and breaches
- Flexibly and automatically derive role relevant reports for every security and compliance stakeholder in the enterprise
- Obtain a high-availability, scalable architecture for this mission critical application
- Efficiently manage and customize the system to maintain high performance

## Key Components

At the heart of the system is the ArcSight Manager. This component drives ArcSight's analyses and workflow. The ArcSight Manager is portable across a wide variety of operating systems and hardware platforms, and intelligently correlates output from a wide variety of security and security-relevant systems.

*ArcSight SmartAgents* intelligently collect, pre-process and manage the transmission of event data to ensure high performance and complete information processing. Data is intelligently filtered and aggregated, allowing the agents to boil down millions of security events to the meaningful few that need to be investigated.

*The ArcSight Console* is designed specifically for security analysts, and provides the utmost in flexibility for intuitive administration, rich graphical views and in-depth investigation capabilities.

*ArcSight Web* brings role-relevant security situational awareness to every level in the organization. This secure web-based interface provides dashboard viewing, customized and configurable information views and investigation capability to securely deliver broad user access throughout the distributed enterprise.

*ArcSight Database* is the enterprise, relational database repository used to capture events and store all security management configuration information such as users, groups, permissions, rules, zones, assets, reports, displays and preferences.

Together, these components deliver the most complete and flexible enterprise security management solution on the market.

## ArcSight ESM: A Comprehensive Solution

“We run millions of security events per day through ArcSight and are automatically presented with the critical items that require attention. When responding to incidents, instead of the phone, excel and email madness, we centrally track all progress using ArcSight ESM.”

CIO of a major financial institution

### ArcSight Data Collection: Complete, Intelligent Collection for a Strong Security and Compliance Management Foundation

The ability to capture and normalize all relevant information is essential for a security management solution to deliver true value. ArcSight SmartAgents offer the most advanced collection capabilities available, as well as the broadest device support on the market to ensure all data is effectively collected. ArcSight SmartAgents currently provide out-of-the-box support for over 120 products, more than any other vendor.

You can also create agents unique to your environment with ArcSight FlexAgents. ArcSight's intuitive and proven FlexAgent kit allows for easily customized, high performance integration with non-traditional devices such as physical security systems and proprietary applications.

ArcSight's ability to collect and normalize 100% of event data ensures that rich, process-ready information is securely and efficiently captured and made available for real-time and historical analysis.

### Key SmartAgent Features Include:

- Flexible agent placement delivers multiple deployment options
- Continuous connectivity and integrity checks combined with customizable caching capability ensure that all data is received by the ArcSight Manager and that chain of custody is preserved
- Configurable filtering and aggregation at the agent eliminate irrelevant data and combine duplicate device logs
- Strong data compression at the agent saves valuable bandwidth
- Customizable transmission options based on time-of-day, priority of event and available bandwidth
- Automatic population of vulnerability assessment data to asset profiles

## ArcSight Correlation: Identifying and Prioritizing True Threats

ArcSight ESM delivers the most intelligent and flexible correlation capabilities available to fulfill use cases for security log data, including insider threat, perimeter threat and regulatory compliance. ArcSight correlation allows for accurate and automated prioritization and identification of true threats and compliance issues in a business relevant context. Leveraging intelligently collected data and ArcSight's multi-analytic functions, enterprises gain a long lifetime of value.

### ArcSight Correlation Capabilities Include:

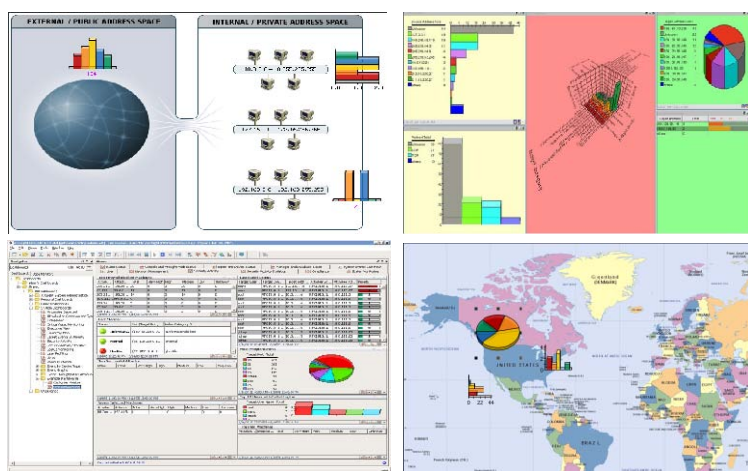
- Elimination of false positives through proven vulnerability to event correlation
- Automatic, accurate prioritization based on asset criticality, event severity and vulnerability status allow analysts to respond to the most pressing issues
- Extensible asset categorization provides the ability to associate correlation rules with organizational policy and risk management objectives
- Over 100 accurate and enterprise proven standard correlation rules provide immediate out-of-the box value
- Real-time, in-memory correlation ensures high-performance processing
- Intuitive authoring system allows users to leverage robust host of analytics for maximum flexibility
- Device independent correlation rules based on the ArcSight extensible categorization language

## ArcSight ESM Solution Streamlines Security

Protecting security at the perimeter is critical to controlling access to the largely unprotected internal network. The protective measures that have been implemented to accomplish this important task emit millions of events. ArcSight ESM focuses its powerful analytic capability to eliminate false positives, validate and prioritize security threats and deliver additional context through providing a central point of information for all related security data.

### With ArcSight, businesses have found:

- Greater rate of true threat identification
- Vastly increased communication and efficiency
- Response times reduced from hours to minutes
- The ability to address 10x threats with no additional headcount



ArcSight ESM provides immediate situational awareness through dynamic reports and customizable dashboards.

### ArcSight Monitoring: Immediate Situational Awareness for a Broad User Base

ArcSight ESM allows organizations to continuously maintain a state of situational awareness via real-time consolidated, risk-relevant views. Effective, efficient and graphically rich monitoring capabilities provide flexible displays to satisfy every role in the organization.

Whether the enterprise has a 24x7 security operations center, or leverages ArcSight ESM as an automated virtual SOC, the system's flexible access, automation and customization capabilities ensure that security status is continually evaluated and critical issues get the attention they require.

### Key Monitoring Capabilities Include:

- Simultaneous access to real-time and historical views via the ArcSight Console or secure anytime, anywhere access via ArcSight Web
- Strong leverage of ArcSight standard content through automated business and technical filtering
- Customizable graphical dashboards with drill down capabilities deliver business, geographic and technical role based views
- Over 40 ready-to-use and customizable graphical dashboards leverage over 150 task specific data monitors
- Threat radar provides a single view of organizational security status based on validated attacks and business risk
- Event graphs draw a concrete and intuitive picture of organizational security
- Geographic and network map views allow users to maintain awareness of high risk areas
- Centralized asset and network modeling allows administrators to push a complete asset and network model to ArcSight SmartAgents



## ArcSight Investigation and Response: Dramatically Shrinking the Window of Vulnerability

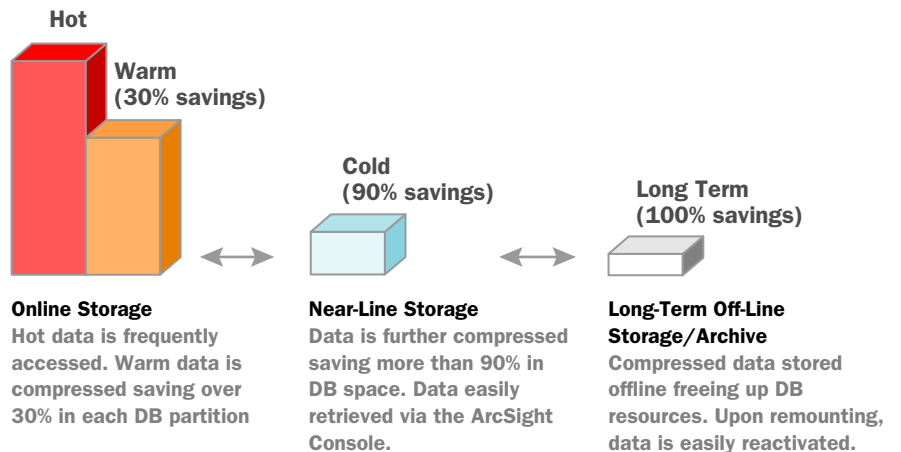
When seconds mean the difference between a successful or thwarted attack, obtaining the data analysts require for decision support is critical. After an incident, the ability to quickly perform forensics allows the organization to prevent a similar attack from recurring.

ArcSight further shrinks the window of vulnerability through key capabilities in workflow, investigation and incident response, including:

- Native case management system provides improved auditability of case management and the ability to launch investigation tools directly from the case
- Available integration with third party trouble-ticketing systems
- Integrated knowledgebase to consolidate and extend organizational security practices and experience
- Real-time collaboration to quickly address the most pressing threats
- Risk relevant notification levels ensure the most critical threats are addressed
- Right click execution of investigation tools including Ping, TraceRoute and customizable scripts
- Simultaneous operation for both real-time monitoring and historical investigations
- Multiple focal levels available using the ArcSight filtering system
- Instant drill down into base events provides immediate context
- Full system search features immediately deliver information that is relevant to the task at hand
- CounterAct technology allows users to send commands to CounterAct supported third party devices, either automatically or on-demand
- Roll-up and individual user case resolution metrics allow organizations to demonstrate processes for compliance and analyze operational effectiveness
- Outbound integration with payload analysis tools provides users with one-click export of payload for fast analysis

## ArcSight SmartStorage: Cost-Effective, Long-Term Security Storage

Retaining pertinent event data enables enterprises to identify long-term trends, investigate attack patterns and manage the increasing pressures created by legal and regulatory requirements. For all these reasons, today's companies must capture and store significantly larger volumes of security information. To reduce the high costs of both online and long-term storage while maintaining necessary access to the data, ArcSight offers ArcSight SmartStorage™ a compression and archiving solution that combines the inherent reliability and performance of enterprise databases with innovative archiving and retrieval management capabilities.



ArcSight SmartStorage drastically reduces storage requirements by automatically managing massive amounts of security data.

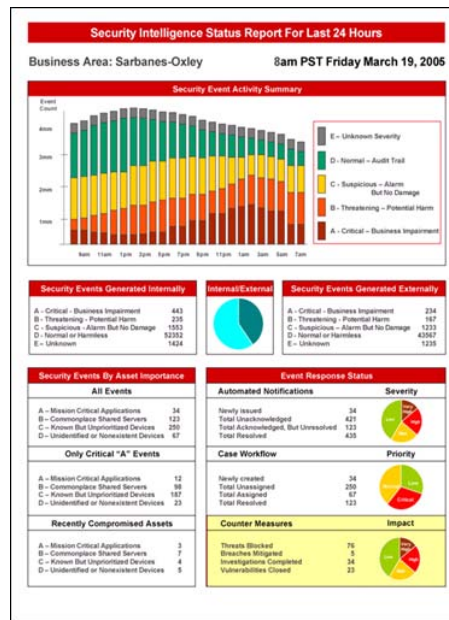
## ArcSight ESM Solution for Insider Threat

ArcSight ESM serves as a central point of truth for user activity. Through the collection of operating system, application, database and other logs, ArcSight can monitor for violations and behaviors that indicate suspicious activity or a breach to acceptable use policy.

ArcSight features an enhanced ability to detect malicious insiders and inappropriate system usage through new data models and analytic functionality such as Operational Time Analysis. This feature allows organizations to define normal times of use for activity for applications and systems based on business roles. ArcSight leverages this operational time profile to automatically pinpoint suspicious behavior based on activity levels, the business role of the application and the time of day of the activity relative to normal operations.

## ArcSight ESM allows you to:

- Integrate application usage to trend employee interaction with sensitive data and immediately alert the security team to anomalies
- Track system changes and portable storage device plug-ins within ArcSight
- Identify and profile at-risk employee behavior
- Create an audit trail for privilege changes on their critical servers



ArcSight ESM delivers automated comprehensive security and compliance reporting to effectively communicate with both business and technical levels.

## ArcSight Reporting: Effectively Communicate with Every Stakeholder

ArcSight ESM delivers automated comprehensive security and compliance reporting to effectively communicate both business and technical level security status and satisfy regulatory reporting requirements. ArcSight Reporting melds the richly collected and correlated information into comprehensive views that enable stakeholders to identify areas of risk, communicate the value and effectiveness of security operations, and easily answer key audit points for security log management, monitoring, systems activity review and incident response.

### ArcSight Reporting Features Include:

- 350+ standard report templates immediately address reporting requirements
- Additional rule, report and dashboard templates to increase out-of-the box capabilities
- Easy-to-author business-level reports for compliance status, business risk and user profiling
- Automated report scheduling and distribution
- Intuitive and flexible report authoring system
- Multiple charts and views provide role-relevant information to every security stakeholder
- Business context reports apprise executives of security status across the enterprise
- Automated filtering of reports provides multiple focal levels to address enterprise reporting needs

## ArcSight Management and Administration: Self-Monitoring for 24x7 Operations

Enterprise security teams have more important things to worry about than the state of their security information management solution. Self-monitoring and self-tuning capabilities help ensure seamless, high performance, 24x7 operations of ArcSight ESM and lightens the SIM management burden with:

- Strong self-monitoring and troubleshooting capabilities, system level alerts, dashboards and performance reporting
- Centralized SmartAgent management and configuration
- Intuitive, easy to use authoring system for rules, reports and dashboards
- Granular access controls to distribute information on a need-to-know basis
- The ability to create and assign role-based views

## Seamless Support for the ArcSight Discovery Family of Analytics

ArcSight Discovery is a family of optional, add-on solutions that further enhances the capabilities of ArcSight ESM. ArcSight Discovery provides businesses with a means of discovering unknown threats and delivering that intelligence directly back into the ArcSight ESM system for continuous monitoring. The Discovery family includes:

### **ArcSight™ Interactive Discovery**

A powerful visual analytics application that accelerates discovery of hard to find, suspicious events and presents compelling visual summaries.

### **ArcSight™ Pattern Discovery**

Advanced statistical algorithms are used to mine behaviors from billions of data points, allowing users to find emerging worms, root-kits and other malicious code and automatically author rules for future detection in real time.

## ArcSight Architecture: Scaling to the Largest, Most Security-Conscious Networks in the World

More than ever, ArcSight ESM is the nerve center for 24x7 enterprise-wide security operations. The system is designed for high performance and scalability and has been battle tested in the most demanding customer environments.

ArcSight ESM not only scales in monolithic deployments, but also in hierarchical and peer-to-peer deployments. As a result, you can deploy the technology in the way that best suits your security organization, whether you operate one security operations center (SOC) or you have numerous SOCs spread across multiple geographical locations that must constantly share information with each other.

ArcSight ESM also offers high availability features to ensure seamless continuous operation. The system's multi-threaded architecture is optimized for highly efficient performance. ArcSight ESM automatically collects and transforms a sea of random security data into prioritized, meaningful security and compliance information.

## Supported Platforms and Browsers

ArcSight provides the broadest array of supported platforms to ensure that enterprises can adhere to their corporate standards and easily manage the ArcSight ESM solution.

Component	Supported Platforms
ArcSight Console	Microsoft Windows Server 2003, Microsoft Windows 2000 Advanced Server, Microsoft Windows 2000 Professional, Microsoft Windows XP Professional, Red Hat Enterprise Linux 3.0, Sun Solaris 9, Macintosh OSX 10.3
ArcSight Manager	Red Hat Advanced Server 2.1, Red Hat Enterprise Linux 3.0, Microsoft Windows 2000 Advanced Server, Microsoft Windows Server 2003, Sun Solaris 8, Sun Solaris 9, IBM AIX 5L

Supported Database	Supported Platforms
Oracle 9i	Red Hat Enterprise Linux 3.0, Microsoft Windows 2000 Advanced Server, Microsoft Windows Server 2003, Sun Solaris 8, Sun Solaris 9, IBM AIX 5L

Component	Supported Browsers
ArcSight Web	Internet Explorer, Mozilla, Safari, Netscape, Firefox

## 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 worldwide 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).

© 2005 ArcSight, Inc. All rights reserved. ArcSight, ArcSight ESM and ArcSight Pattern Discovery are trademarks of ArcSight, Inc. All other product and company names may be trademarks or registered trademarks of their respective owners. 10/05