ArcSight™

Whitepaper

Handling Modern Security Issues

Using ArcSight to Monitor Enterprise Threats and Risk

Research 015-061909-01

ArcSight, Inc.
5 Results Way, Cupertino, CA 95014, USA
www.arcsight.com info@arcsight.com

Corporate Headquarters: 1-888-415-ARST
EMEA Headquarters: +44 870 351 6510
Asia Pac Headquarters: 852 2166 8302

Overview

A call center rep has received an offer from a competitor. A week before she leaves, she stays late, accesses the client database, pulls the top 1,000 client records, saves these to a file on her USB key, copies several product planning docs from the engineering server, and mails these to her personal email account.

A major bank suffers a data breach and exposes millions of customer records. The CIO at a competing bank directs his staff to produce reports for internal auditors demonstrating that the firm's access controls are working and customer data is secure. After a week of all-nighters, the staff reluctantly admits it cannot verify that all servers and files are secured.

A database administrator gives two weeks' notice before leaving his employer. On his last day, the Human Resources department asks IT for a report on all databases and files accessed by the DBA during the past two weeks. HR is concerned that the DBA may have copied sensitive data or changed user privileges in key databases. IT unfortunately is not able to produce a definitive report.

Each of these is a fairly common example. In each case, the organization is concerned about protecting its key business information. Perhaps it suspects a breach. Perhaps it is simply being cautious. Or perhaps it is actually losing data and doesn't know. The result is increased risk of loss and penalty. Many organizations are seeking solutions to these and other similar problems.

New Business Challenges

Organizations of almost all sizes and industries now struggle with these business changes:

- **More Transactions Online:** Electronic banking, payment services such as PayPal, self-service wire transfer and self-service stock trading are just a few of the electronic transaction services now widely used by consumers. As a result, more transactions are electronic than ever before, which creates more payment and financial information at risk of a breach.

- **More Mergers and Acquisitions:** Mergers bring new systems, new users, and more points where information can fall through the cracks, and therefore open up new threats. For example, when two large organizations are integrated, it takes time to rationalize the user communities, and existing systems may not recognize the merged users. In the confusion, it is much easier for a malicious insider to take sensitive data without detection.

- **More Layoffs:** In a recent survey, nearly 50% of IT administrators responded that they would take sensitive information from the customer database, if they knew they would be laid off. Though this figure seems shockingly high, it highlights the risk of key users retaliating to loss of employment by stealing data. As economic conditions worsen, this risk only rises.

- **More Outsourcing:** As more business functions are outsourced to partner organizations, the "trusted outsider," i.e., a non-employee who has access to a company's internal systems, becomes more common. CIOs must balance the need to grant access with the risk of doing so.

Increasing Security Trends

These business challenges mean most organizations must manage four increasing security trends:

- **More Account Fraud:** Customers execute more transactions online, including banking, wire transfers, and stock trades. Early adopters may have been more sophisticated, but as the mass market adopts online banking and payments, user accounts become more susceptible to fraud. Phishing, card cloning, social engineering, keyloggers, and other methods all enable fraudulent activity in client accounts.

- **More Data Theft:** With increasing layoffs and mergers, disgruntled employees and contractors often take sensitive data from corporate systems. DBAs, network administrators, and finance analysts are some common types of users with privileged access to data. With data theft on the rise, firms are increasingly wary of activities by privileged users.

- **More External Threats:** Traditional threats such as hackers and malware continue to rise, as well. These external threats have become more subtle, and continue to outwit traditional methods of detection. Hackers sneak through perimeter defenses via new technologies, and zero-day malware outbreaks continue to cause damage to corporate systems.

- **More Regulations:** In the face of the above trends, plus new financial bad news, regulations are likely to increase in the coming years. Reporting requirements and penalties for failure will demand more attention from corporate officers.

Taken together, these trends represent increased pain, cost, and risk for corporate management.

The Big Security Problem

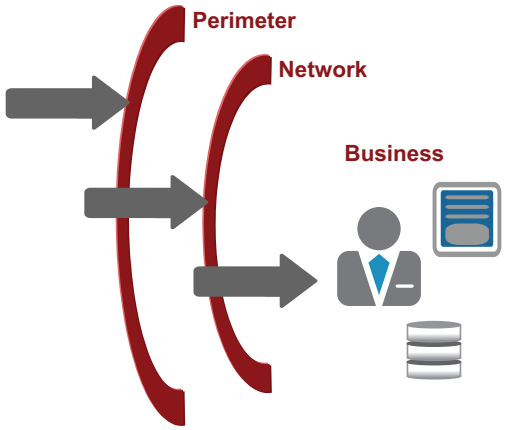
As a result of more data online, more breaches, more threats and more regulations, organizations face more business risk. This risk is very difficult to manage due to lack of visibility. Each information area such as Oracle or Microsoft databases, Microsoft Windows file systems, SAP applications, website, etc., is a source of risk and a challenge to monitor. More importantly, the real challenge is to gain visibility across each of these areas.

An executive at a large global bank recently summarized the problem this way: "We can see various activities that our employees do, various transactions that our customers execute, or various security events on the network. But we can't relate them to each other, so everything looks like a "one-off' and we never really understand what's going on. And so we are exposed."

These concerns are driven by internal security initiatives as well as external regulatory initiatives such as Sarbanes-Oxley in the U.S., BaFin in Germany (MaRisk, MiFID), and international industry standards like Basel II and PCI.

Evolution of Enterprise Threats and Risks

In recent years, the threats and risks faced by most organizations have evolved, moving further and further "inward." Four or five years ago, organizations were most concerned with external threats at the perimeter of their networks. Hackers, phishers, and worms coming through the corporate firewalls were seen as the significant cyberthreats to business operations.



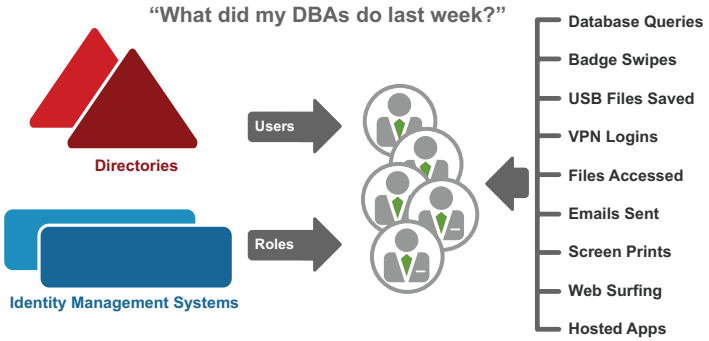
In recent years, as organizations have linked with suppliers, customers, and business partners, the network perimeter has dissolved and the notion of external versus internal threats has blurred. As this happened, organizations became increasingly focused on network activity caused by internal systems, as well as those outside the firewall. Botnets, viruses, keyloggers and other malware became an increasing threat to operations.

In recent years, organizations have better understood that the primary risk to the business comes from the confidential information, the critical applications, and the privileged users that manage to these applications and data. As a result, today's CIO is as concerned about internal breaches, theft, and fraud as well as malware and hackers.

Some Common Examples

The ArcSight SIEM platform is used by the largest, most demanding organizations and government agencies in the world to monitor business activities. Here are some of the most common, high-value example applications:

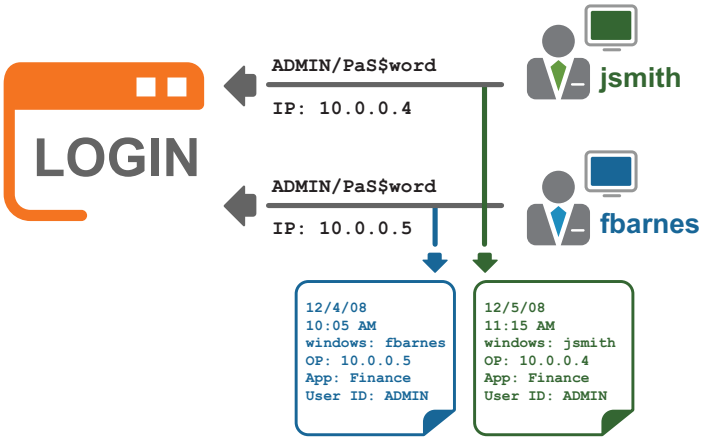
- **Privileged User Monitoring:** By combining user and role information in the corporate directory or identity management system with database activity, file activity, and all other activity, ArcSight can provide actionable answers to questions such as "what did my DBAs do last week?" As a result, organizations can ensure that internal controls are working and information is protected.



- **Terminated Contractor Activity Detection:** As organizations rely on the use of contractors to increase flexibility of costs and operations, they naturally see an increase in turnover, as contracts expire and contractors are terminated. While contractors (or other system users) may be de-provisioned in the corporate HR systems, these same users often have live accounts left active on local servers. For example, an IT contractor might have his

account disabled in the PeopleSoft system, but may still have multiple local accounts active on various Linux file servers, which are not managed by the PeopleSoft processes. As a result, the organization has back-door entry points for terminated users, exposing the firm to risk and theft. The ability to connect local system activity to user status in HR and identity management systems ensures that access controls are applied across the enterprise.

- **Shared User Accounts:** By correlating identity data, IP addresses, and application usage, ArcSight can detect shared use of administrative accounts in legacy applications. Customers can then remediate this use and demonstrate effective controls, without rewriting legacy applications. As a result, ArcSight customers improve compliance while reducing current capital expenditure (CapEx) needs. One financial institution estimated a cost of $8 million and a year of development time to remediate key applications with embedded shared accounts. Instead, the firm was able to implement compensating controls with ArcSight in a few months and at 1/10th the cost.



- **Sensitive Data Monitoring:** By integrating with database activity monitoring and data leakage prevention products and correlating activity across them and web and email systems, ArcSight can monitor risks to confidential data and ensure that it remains private. As a result, organizations can comply with privacy regulations and retain customer loyalty.

- **Account Takeover Detection:** By combining output from fraud detection products with activity within the web servers and databases, ArcSight can detect fraudulent activity from account takeovers. A recent customer in the U.S. discovered nearly $1 million of wire transfer fraud within the first week of installing ArcSight.

- **Continuous Compliance Monitoring:** Using the ability in ArcSight to monitor data and automatically apply rules enables customers to monitor compliance in a continuous and automated manner. Controls can be applied across multiple regulations, saving time, money, and effort. The information is presented in a series of auditor-friendly dashboards that present up-to-the-minute control status and results, as well as real time notifications of violations to all appropriate parties. As a result, organizations get better compliance with less effort, increasing the likelihood of passing audits.

In all of these examples, a key point is that ArcSight leverages the investment companies have already made in different technologies. By connecting the dots across these products, ArcSight delivers significant value and improves the ROI of each.

ArcSight Connects the Dots to Monitor Threat and Risk

While there are multiple useful technologies to monitor specific information risk areas, the real goal is to tie these together and provide a single, comprehensive view of current risk level, security threats and operational activity. The ArcSight SIEM platform provides this single “pane of glass” by aggregating, analyzing, and visualizing activity data across the organization.

This comprehensive real-time view notifies administrators when risky activities exceed a certain level (e.g., a DBA has five failed logins in five minutes to the customer payment card database). In addition, ArcSight correlation capabilities highlight multiple activities that may each be fine on their own, but together represent a risk. For example, a DBA may be running queries against the customer payment card database, doing so outside of normal hours and accessing tables that contain customer PIN codes. Each of these activities is fine, but together may indicate that the DBA’s credentials have been stolen and his account is being used to steal customer data.

ArcSight delivers several key functions that enable visibility across all organizational activity.

- **Collect Broadly:** The ArcSight architecture is designed to collect data from every source of information in an organization, from firewalls, to badge readers to laptops to VOIP phones, to databases and directories. As a result, ArcSight can “see everything.”

- **Normalize and Categorize:** This broad set of data is in a variety of formats and would be impossible to make sense of in native formats. ArcSight normalizes everything to a single common format and then categorizes it for easy analysis by humans as well as machines.

- **Analyze Using Business-Specific Rules:** ArcSight correlates business activities using both built-in rules as well as rules customizable to each individual organization. For example, a bank might want to apply risk metrics such as MCC code, payment location, account location, and payment trends to determine whether transactions are fraudulent. However, a hospital might want to analyze patient status, the nurse department, and previous accesses to warn of a potential personal health information breach. As a result, ArcSight can find the "needle in the haystack" that represents a business risk, as defined by each organization.

- **Investigate:** By storing terabytes of data, ArcSight enables forensics analysis when those risks are found. With ArcSight, it is simple to discover how long a risky activity has been going on and who else was involved. Conversely, when the problem is remediated, ArcSight enables easy reporting to internal and external auditors.

- **Alert, Report, and Visualize:** Finally, real-time dashboards and on-demand or scheduled reports ensure that the right parties receive the information they need, at the right time. ArcSight presents information as each stakeholder requires, so that security administrators can react to problems quickly, while auditors can sign off on results, and management can steer the business with useful metrics.

The ArcSight SIEM platform is designed to help organizations understand who is on the network, what information they are seeing, and which actions they are taking with the information. With this level of visibility, ArcSight customers can protect the business while reducing operating costs. The products are used today across the globe, preventing threats and securing information.

Why ArcSight

ArcSight is unique in its ability to solve enterprise-wide risk and threat monitoring. The ArcSight SIEM platform provides three primary benefits:

- **ArcSight Makes it Easier for Companies to Pass Audits:** Continuous compliance monitoring information, presented in auditor-friendly dashboards, increases the chance of passing audits. Automated collection and reporting cuts the burden on the staff and budget.

- **ArcSight Helps Companies Protect Processes and Data:** Real-time analysis and alerting notifies the department of threats early enough to prevent them and minimize loss.

- **ArcSight Increases Control Over an Organization's Networks as it Becomes Open to Partners and Customers:** Understand at all times who is on the systems, what data is being viewed, and which actions are being taken, whether the users are employees, contractors, customers, or anyone else.

In conclusion to the concepts described in this paper, consider three reasons why ArcSight is best positioned to deliver enterprise threat and risk monitoring:

- **Market Leadership:** As the SIEM market share leader, ArcSight protects the IT infrastructure of the most demanding organizations in the world, including global banks, civilian and military government organizations, and many of the largest retailers in the world.

- **Future Proof:** The job of a CIO is to ensure that an organization's information strategy evolves with the business strategy. The unique ArcSight architecture ensures that as your technology changes, you will be able to continuously monitor the business for risk.

- **Platform Neutral:** Unlike large security enforcement vendors, ArcSight is well-suited to monitor technologies from a variety of providers. ArcSight focuses on risk and threat monitoring, across any third party platform.

ArcSight

To learn more, contact ArcSight at: info@arcsight.com or 1-888-415-ARST