FIDELIS SECURITY SYSTEMS

The Power to Prevent:
It's the Next Generation

FIDELIS SECURITY SYSTEMS, INC. 4416 EAST WEST HIGHWAY, SUITE 310, BETHESDA, MD 20814

Tech Talk: *Data Discovery Approaches Utilizing Fidelis XPS™*

Fidelis Security Systems
February, 2009

What is Data Discovery?

As organizations look at implementing data security strategies—thus advancing from traditional administration and access control—to controlling the actual information itself, many organizations are making an effort to create an inventory of their digital assets (sensitive or protected information). The process of creating a digital inventory, referred to as **data discovery**, helps an organization understand where their sensitive or protected information is stored—including potentially unprotected or unsupported locations, and business processes that use this sensitive or protected information. To date, most organizations do not have any process to create, let alone, maintain this digital asset inventory.

Before undertaking a data discovery project, it is important to scope what type of information needs to be discovered and where to look for that potential information. Most large organizations have now accumulated petabytes of information, most of which is unclassified and often uncontrolled. It is important to create a specific focus to the project and prioritize the type(s) of sensitive or protected information that have the potential for the highest negative impact in the event of a security breach. Data discovery, like other technology projects, will have a higher likelihood of success when the scope of the project is focused, particularly for the first phase of the implementation.

Data Discovery Evolves

Many "first generation" data leakage prevention (DLP) solutions included discovery products that did not originate as discovery products at all. As these initial DLP solutions required an enterprise to register their protected/sensitive data to have an acceptable degree of accuracy, discovery capabilities were developed to attempt to simplify the enrollment of sensitive information. An organization would be required to use these tools to integrate their DLP solution to their key enterprise data stores where they *knew* sensitive information resided.

During this time, many information lifecycle management (ILM) and search vendors began to include rudimentary discovery capabilities for sensitive information in their products. In response, first generation DLP vendors attempted to morph their data enrollment solutions into these new data discovery technologies that crawl other locations on the network to look for sensitive or protected information, thus creating the digital asset inventory. This initial approach is just one of many approaches to data discovery.
Fidelis Security Systems provides organizations multiple approaches to managing the data discovery process. This paper discusses each of these alternatives, the potential benefits, and issues to think about when implementing each approach.

Discovery Methods Defined

Before discussing each data discovery approach in detail, it is important to define the different methods for data discovery: active, passive, and local.

Passive Discovery—network sensor(s) observe live network traffic for sensitive or protected information, identifying the source and destination systems to identify data stores.

Active Discovery—centralized server(s) that connect(s) to data stores across the network and extract information back to the central solution for analysis.

Local Discovery—agent-based scanning of the system on which the agent is installed.

Fidelis XPS™ Data Discovery Approaches

Built on a patented deep session inspection™ platform, the Fidelis Extrusion Prevention System®, Fidelis XPS, is the industry's only next-generation DLP solution with the power to deliver comprehensive prevention over all ports and all channels, complete visibility and control, and the lowest total cost-of-ownership to stop network data leakage on multi-gigabit-speed networks. Simply deployed as a context-aware network appliance, several of the Fidelis XPS products—and those of our partners—include native data discovery components, allowing organizations to identify systems inside the enterprise that are known to contain sensitive information in the simplest manner for assembling a digital asset inventory with a minimal amount of effort. The various approaches to data discovery utilizing Fidelis XPS include:

1) Passive data discovery utilizing Fidelis XPS Internal;

2) Active data discovery with existing Information Lifecycle Management and Search technologies, in conjunction with Fidelis XPS Internal;

3) Active web data discovery with Fidelis XPS Web Walker;

4) Active data discovery with Fidelis Security Systems' partner, Verdasys Digital Guardian.

Approach #1 – Passive Data Discovery with Fidelis XPS Internal

Fidelis XPS Internal is the only network data leakage prevention solution designed for use deep inside an organizations network as opposed to being deployed at the network perimeter. As both the only network DLP solution to scale to multi-gigabit-speeds and the only network DLP solution to understand protocols seen inside the network (e.g., database access protocols, Microsoft file sharing, web services), Fidelis XPS Internal is able to provide the only Passive Data Discovery function available in any DLP solution—enabled by allowing customers to place sensors inside the network to build an organization's inventory of sensitive or protected information by watching real-life *internal* network traffic and business processes.

Unlike perimeter-based solutions where the information has left the network once observed, Fidelis XPS Internal sensors can be placed deep in the network, thus allowing an organization to see and track the sources and destinations containing protected/sensitive information by observing data transfers of data-in-use *inside the trusted environment*.

Passive Data Discovery with Fidelis XPS Internal is typically accomplished at a fraction of the cost of active scanning because of the simplicity of deploying network appliances compared to the resources required to design, configure, and deploy active discovery. Deployment of Fidelis XPS Internal for Passive Data Discovery is one of the simplest ways to gain a digital asset inventory. Once policy is defined in the Fidelis XPS CommandPost™ management console, an organization just needs to deploy the Fidelis XPS Internal network sensor(s) to key points in their network to observe internal communications and business processes. The policies used are the same policy sets for all other Fidelis XPS sensors, so an organization can take advantage of all pre-built or custom policies in use from their data-in-motion deployments. This deployment is typically measured in hours or days, whereas many active discovery solutions take months of configuration before they can be successfully deployed. Once deployed, Fidelis XPS Internal monitors all systems that send traffic on a network link—there is no need to do a system-wide inventory, a complex and time consuming process, to get started.

Additionally, Passive Data Discovery with Fidelis XPS Internal typically requires no modification to any monitored systems or the network and incurs no negative performance impact on the network (or any system) as the sensor is deployed out-of-band, receiving a "carbon copy" of all network traffic and conducts the analysis on this copy. Because of this no-impact approach, Passive Data Discovery with Fidelis XPS Internal can be run as a continuous operation, whereas active discovery scanning typically must be run during limited maintenance windows to avoid performance impact of production systems—a concern that is not present with the Passive Data Discovery approach.

Benefits	Issues to Consider

• Incredibly fast time-to-value
  o deployed in hours or days
  o does not require a systems inventory or logins to get started
• Uses existing pre-built and custom policies in Fidelis XPS CommandPost
• Simple – does not require modifications or logins to any monitored system
• No production impact, so can be run continuously
  o No additional server load created
  o No additional system load or network traffic created
• Low total cost-of-ownership—does not require definition of new systems, maintenance of logins, and other overhead
	• Information is discovered once it is used in a business process
	• Passive approach, by nature, requires separate remediation process

Approach #2 - Active Discovery with Fidelis XPS Internal and Existing Enterprise Search and/or Data Warehousing

As Fidelis XPS Internal understands more applications and protocols than other network DLP solution and can scale to internal network speeds, organizations can place a Fidelis XPS Internal sensor in front their existing enterprise search and/or data warehousing solutions. All traffic scanned by those existing solutions will be analyzed as it flows through Fidelis XPS Internal, providing the same visibility as our Passive Data Discovery approach, while leveraging all existing installed assets to put the digital assets in motion to be discovered. Since these assets are already deployed and actively scanning information, this approach also is typically delivered at a fraction of the cost of other active scanning solutions.

Benefits	Issues to Consider

• Incredibly fast time to value
  o deployed in hours or days
  o does not require a systems inventory or logins to get started
• Uses existing pre-built and custom policies in Fidelis XPS CommandPost
• Simple – does not require modifications or logins to any monitored system
• No production impact, so can be run continuously
  o No additional server load created
  o No additional system load or network traffic created
• Low total cost-of-ownership—does not require definition of new systems, maintenance of logins, and other overhead
	• Passive approach, by nature, requires separate remediation process
	• Need to map protocol capabilities of search or data warehousing solutions to Fidelis XPS Internal solution

Approach #3 - Active Web Data Discovery with Fidelis XPS Web Walker

Fidelis XPS Web Walker is a turn-key appliance designed to scan systems with HTTP or HTTPs interfaces. It enables an organization to quickly get a risk assessment of the content posted to existing web-based systems, and discover if protected or sensitive information is posted for download. To simplify deployment, and not require a complete systems inventory, Fidelis XPS Web Walker crawls links found in the defined base web site(s), effectively self-discovering any linked system.

As Fidelis XPS Web Walker is based on the same technology as other Fidelis XPS sensors, it uses the same policy set for all other Fidelis XPS sensors, so an organization can take advantage of all pre-built or custom policies in use from their data-in-motion deployments. Additionally, it is very high-performance, where implementations are often gated by the ability of the web servers or network ability to deliver information to the appliance.

Benefits	Issues to Consider
• Uses existing pre-built and custom policies in Fidelis XPS CommandPost • Simple appliance-based configuration • Can "crawl" links from an initial server/server list to discover other servers with a system	• Limited to systems with HTTP or HTTPs interfaces • Passive approach, by nature, requires separate remediation process • Requires logins for password protected sites • Performance limited to throughput of servers and network bandwidth

Approach #4 - Active Data Discovery with Verdasys Digital Guardian

Fidelis Security Systems and Verdasys partner to provide a comprehensive best-of-breed data leakage prevention solution. Verdasys Digital Guardian has robust active discovery capabilities across the platform including laptops, desktops, and server agents. This infrastructure is highly configurable, enabling the flexibility to scan by location, machine, groups, and/or individuals. As Verdasys Digital Guardian uses an agent-based approach, it requires a deployment of agents to most systems. Alternatively, systems with agents can be configured to scan connected systems. This approach requires an upfront inventory and resources to conduct the agent deployment, as well as testing the agent with critical production systems before deployment. However, this approach also gives an organization access to both data-in-use and data-at-rest, and also provides the most robust integrated options for remediation.

Benefits	Issues to Consider
• Agent-level integration provides the most robust options for remediation • Inventory includes both data-in-use and data-at-rest	• Requires agents to be installed on most systems or systems with agents to be configured to scan connected systems • May require scheduling or run in the background to avoid performance impact

Conclusion

Fidelis Security Systems, alone or with other best-of-breed partners, provides the most robust options for enterprise data discovery. Depending on goals and available resources, an organization can decide to use passive, active, local discovery, or a combination of them, to best meet their goals. The ability to choose the right option, as opposed to a "one size fits all" scenario—which actually fits nothing—is critical to ensuring the success of an organization's data discovery project. Additionally, by working with Fidelis XPS for data discovery, the benefits of control, accuracy, and scalability of the only next-generation network DLP solution are attained.

About Fidelis Security Systems

Since 2002, Fidelis Security Systems has given global enterprises the power to prevent data leakage while solving their biggest data leakage challenges—safeguarding intellectual property and identity information, complying with government and industry privacy regulations, and enabling visibility into and control over their networks. Built on a patented deep session inspection™ platform, the Fidelis Extrusion Prevention System®, Fidelis XPS™, is the industry's only next-generation data leakage prevention solution with the power to deliver comprehensive prevention, complete control, and the lowest total cost-of-ownership to stop data leakage on multi gigabit-speed networks. To learn more about why organizations choose Fidelis XPS to protect their brand, intellectual property, and resources, visit www.FidelisSecurity.com.