

# Insider Fever and the Endpoint Vaccine

---

Over the past two years, media reports have followed the development of internal threats to corporate information security as though they were chronicling the spread of a global epidemic of a new and dangerous illness. What once seemed like an exotic insider “virus” has now infected the corporate IT atmosphere. This has caused IT departments from many industries and the public sector to rethink the strategies they have in place to protect the security of their information.

## Network “Immune Systems” Miss Local Leaks

As the modern business environment becomes increasingly dynamic, mobile and distributed, a great deal more confidential information, that can include private client data, is being created, used and stored on employee desktops and laptops. Together with this highly-distributive nature of corporate data, there has been a marked increase in the popularity of removable storage devices like USB flash drives and memory cards. These accessories are now not only more affordable, portable and concealable, they offer storage capacity and download speed sufficient to facilitate the theft or loss of very large, very valuable data files in just a few moments.

Another factor contributing to the rise in insider data breaches is that insiders have mastered a number of simple (and thus potentially dangerous) skills which facilitate the leaking of data from a personal computer’s localports. If they are not equipped to copy data from a computer onto a flash-memory or other standard *plug-and-play* device, they can consider synchronizing data between their PC and a personal mobile device (PDA) or “smartphone”. Then there is the good old-fashioned method of simply printing sensitive documents to paper and carrying them out the door.

Since these local leaks do not use network communications and, conventional network information security mechanisms (such as firewalls, intrusion detection and prevention systems, and email and web content filtering products) are useless in their prevention. This represents a significant gap in the typical information protection system: the network-based Data Leak Prevention (DLP) appliance. Enterprises seeking inoculation from “insider fever” need to understand that, while these much-hyped DLP appliances are effective in filtering the content of network communication applications and services—such as emails, instant messaging, peering networks, etc.— they do little in the fight against these simple local endpoint data breach methods. You can spend hundreds of thousands of dollars on a big DLP console or appliance, yet employees will still be able to slip valuable data in their pocket using a flash drive, smartphone, or with a simple printed hardcopy.

### ***New Vaccine Needed: Endpoint DLP Agents***

It is easy to point out the inefficiency of the network-centric approach to corporate IT security, yet it still dominates the field. This focus is likely to change as studies reveal that breaches via local ports and peripherals (removable memory, smartphone synchronization, document printing) are much more common than those that take place over network channels (email, IM, P2P)...especially as those channels are taken away from the insider due to network level controls. Statistics gathered in multiple market reports that include the recent “2008 Annual Study: Cost of a Data Breach” conducted by Ponemon Institute<sup>1</sup>, confirm this to be the case. In addition, the research makes it clear that the cost of data breaches incurred by organizations across the globe continues to grow.

As a result, more and more IT security professionals and corporate executives have become convinced that without full-featured enforcement agents residing and protecting data directly on endpoint computers, corporate DLP solutions are essentially incomplete and leak-prone.

---

<sup>1</sup> Ponemon Institute, “2008 Annual Survey: Cost of a Data Breach.” (US, UK and Germany reports)

## Vaccine Ingredients – Vital DLP Agent Components

This evidence proves that the 'Wait for the ideal hybrid, network-plus-endpoint DLP solution' approach seems an ill-advised strategy to the already acute 'insider fever' condition. There is no doubt that the functionality and quality of endpoint DLP agents will be of critical importance, and that they will merge the three main technological trends that now dominate any DLP discussion: content filters, contextual access control mechanisms, and encryption. So it is prudent to map a strategy based on the state-of-the-art solutions in each of these areas as evidenced by currently marketed and proven security software.

### **Content Filtering**

Modeled on how humans identify and sort information (typically text documents), content filters are designed to recognize data patterns, to query structured data, and to note the confidentiality status of data and then align block or permit actions with basic per-user privileges established by corporate security policy. Since such mechanisms fit well within the prevailing data-centric model of information security, market theorists claim that content filtering is the most effective and self-sufficient way to protect against data breaches, including those perpetrated at corporate endpoints. However, in practice, even the most advanced content filtering technologies are falling well short of that goal, particularly endpoint agent content filters. These tend to significantly lag behind the functionality and performance of their network-based counterparts, and they share with them the problem of errors such as false negatives and false positives. The accuracy of these systems rarely exceeds 80–85%, and the constant tweaking and remediation time taken by admins and honest users is staggering. To achieve wide market acceptance, endpoint-resident content filtering capabilities will need to improve, beginning with two obvious challenges: They need to better fit the inherently distributed nature of modern endpoint computers and to account for the fundamental difference between data transfer protocols over local ports versus network channels.

### **Context-Aware Device/Port Controls**

It is clear that in order to produce high quality endpoint DLP agents, content filtering technologies are simply not enough. They must be combined with components of a second type of data leak prevention solution on endpoints: port-device control software. There are port-device access control and management solutions that address the 'lion's share' of endpoint vulnerabilities today through context awareness. Certain of these have been field-proven for more than a decade on the market.

According to Forrester Research's definition<sup>2</sup>, endpoint port-device control technologies are a class of context-aware DLP mechanisms that do not use the content of data for analysis and filtering, but rather a set of parameters that define the data's immediate environment, such as "who" (the user or group membership identifier), "the starting point and destination" (interfaces, ports, device classes, device types, and unique device identifiers), "when" (the time), "where" (which endpoint computer, and whether it is currently on or off a protected network), "in which format" (the type of data, i.e., file type), and so on. A viable endpoint leakage protection strategy should start with proven contextual control tools and add endpoint content filtering agents as practical versions become available. The two technologies do not conflict or overlap, but complement each other at different layers to provide "defense in depth".

In the future, endpoint DLP agents will need to provide context-aware control over data flows along *all* possible communications channels. In other words, they will need to cover the three local channels already covered by best-in-class port-device control packages:

- USB memory sticks, flash memory cards, and other memory-enabled standard PnP devices (MP3 players, digital cameras, etc.);
- Data synchronizations between endpoints and locally connected smartphones and PDAs (e.g. Windows Mobile, iPhone, Palm, Blackberry);
- Document printing channels (local/network print spooler control, virtual printers);

And they will need to deliver context-aware control over network communications.

- Data exchanged through popular network applications —email, IM, FTP, Web, social networks, P2P file sharing, , etc.

---

<sup>2</sup> The Forrester Wave: Data Leak Prevention, Q2 2008  
([http://www.forrester.com/rb/Research/wave%26trade%3B\\_data\\_leak\\_prevention%2C\\_q2\\_2008/q/id/45542/t/2](http://www.forrester.com/rb/Research/wave%26trade%3B_data_leak_prevention%2C_q2_2008/q/id/45542/t/2))

In addition to controlling all types of data transmission channels, the port-device control component of a full-featured endpoint DLP solution should be able to control — that is *intercept, analyze, filter, and log* — a computer's data operations at all main context-aware levels: local ports/interfaces, peripheral devices, select data channels, and data types (e.g. file formats). With a high-quality port-device control technology, it should be also possible to control the direction of data flow, , which actions should be logged, and which data should be shadow-copied for deeper analysis.

To quickly respond to customer demand for better leakage protection at endpoints, some network security appliance vendors have attempted to complement their network tools with endpoint DLP agents that offer limited context awareness, that is, cover only one or two leakage channels. They attempt to promote these as “full function” because they incorporate a content filtering module. But this is like protecting a house by putting extra locks on one door, while ignoring other passageways in and out. Data can still be easily lost or stolen, if even one “backdoor” is left open to the user.

### **Encryption**

It is certainly a misconception to believe that encryption technologies alone can constitute a comprehensive data access control solution. Although they are very reliable protection mechanisms for “data at rest” (DAR) and “data in motion” (DIM), encryption solutions cannot protect “data in use” (DIU). The DIU mode requires that data be unencrypted and accessible to users and applications. However, there is no doubt that removable media encryption components — and data object encryption components in the future — should be either embedded into endpoint DLP agents, or complement them by integrating their operations. The purpose of this integration would be to logically correlate encryption, content- and context-aware enforcement actions in the scope of a holistic data protection policy. As a result, the agents will be able to command which types or pieces of data should be encrypted before they are stored to removable media or sent over communications channels.

### **The Ultimate Vaccine**

A harmonious blend of all the above-mentioned technologies -- content filtering, port-device control, and encryption – likely achieved initially by bundling “best of breed” products and then eventually evolving to an integrated endpoint DLP solution -- will enable the creation of a truly effective “vaccine” for the fight against the global “insider fever” epidemic and reduce the damages that companies suffer from data breaches caused by end-user negligence and malicious actions.

In the ultimate paradigm, endpoint DLP agents will be as important to complete DLP solutions as network-based DLP appliances. First, they provide control over local data transmission channels that cannot be controlled from the network (e.g., copying files onto removable media). Second, they can perform traffic content filtering for the endpoint computers they protect, thus substantially improving the performance of network-based DLP appliances. As a result, they increase the scale of the solution while keeping its cost down. In fact, when full-featured endpoint DLP agents are in place, they will become the components that conduct the greater part of DLP processing and control all types of input/output data traffic on corporate endpoints, while network DLP appliances will perform most of the supportive and instrumental functions – which are no less important – of a complete hybrid DLP solution.

However, despite the massive hype and argumentative definition of DLP, this “integrated endpoint + network/endpoint hybrid DLP” scenario just does not exist from any one vendor. To that reality, it is best to move forward today with the most affordable “best of breed” components to protect as much as possible until that “holy grail”, and the IT budget to afford it, arrive.