Kriptone

Stop Data Leaks:

Active DLP Systems vs. Passive Monitoring Solutions

WHITE PAPER

Which one is better to combat theft of intellectual property: an active data leak prevention system (DLP) or a passive monitoring solution?

The debate between users of active DLP and passive monitoring approaches goes on for years. In this paper we are publishing a research on the two approaches, analyze their strong points and limitations, and make recommendations as to which approach may better suits your requirements.

Data Leak Protection (DLP)

Data leaks can cause serious damage by exposing sensitive information. **Leaked data can expose information about business operations, trade secrets and intellectual property.** Data leaks in the financial sector can be disastrous, potentially exposing information about customers with long-standing consequences.

Data leak prevention may be required by regulations. Some of the relevant regulations include the International Payment Card Industry Data Security Standard (PCI/DSS), Gramm-Leach-Bliley Act (GLBA) in the United States, SARBANES-OXLEY ACT (SOX) (United States), EURO-SOX (European Union), the US Health Insurance Portability & Accountability Act (HIPAA), California Senate Bill 1386 (SB 1386) (United States), and Data Protection Act (DPA) of 1984 (amended 1998) in the United Kingdom.

> **“75% data breaches come from the inside”**

With as much as 75% data breaches coming from the inside (source, another source), protecting organizations’ IT infrastructure against insider-type of attacks becomes an essential and urgent matter.

Data leak prevention solutions are systems designed to detect and prevent potential data breach coming from the inside.

A typical data leak prevention system (DLP) combines monitoring, detection and prevention functionality, with some systems omitting the prevention part in order to not interfere with the business workflow (more on that later).

In other words, a DLP will normally contain modules monitoring certain types of net traffic and/or user activities, as well as heuristic modules to analyze collected data for possible threats. If a potential threat is detected, a DLP will block suspicious activity, normally sending a security alert.

Let’s have a look at how a typical DLP may work in business environment.

There are two major types of DLPs commonly used in organizations.

- **The first type** is installed as an Internet gateway or proxy server, and has no software installed at client computers. A **network DLP** analyzes network traffic to detect the transmission of sensitive data and blocking the transmission of information that is found to be in violation of the corporate security policy.

While this may sound good in theory, pretty much any encrypted connection (such as those made via the HTTPS protocol) has a great chance to either get unnoticed or blocked entirely. While workarounds exist (such as requiring the use of pass-through HTTPS proxies), this by itself creates additional complications and incompatibilities.

- **The second type** of DLP systems deals with data at the source. **Endpoint DLPs** run client software on end-user workstations, intercepting and analyzing data such as user inputs, Internet connections and application activities at the source. Unlike network-based solutions, endpoint DLP's can analyze both internal activities and external communications of a given workstation.

They have, for example, full access to user inputs and application activities immediately preceding data transmissions, including any text or messages typed but never sent out. Running deeper in the source, they have more factors to analyze. As a result, these types of DLP's are generally more capable than network-only solutions. In turn, this means more possible ways to interfere, and more possible ways to disrupt business activities.

Endpoint DLP's have also another advantage. These systems have full access to computer's hardware, and thus they are able to monitor and control access to physical devices on a low level. Specialized DLP systems exist with a sole purpose of controlling the use of computer's external interfaces such as its USB ports, FireWire (IEEE.1394), built-in card readers and expansion slots. In some cases, these systems will have access to information before it's being encrypted.

Both types of DLP's have the ability to detect and prevent potential violations of corporate security policies.

Network-based DLP's can do this by terminating an outgoing network connection, while endpoint DLP's have many more enforcement tools available ranging from blocking a certain activity with a pop-up to force-closing applications and locking down the computer.

Which type of a DLP to choose between network-based and endpoint systems?

There's no choice between these, as they help accomplish different goals at different points. While endpoint DLP's offer far more control over activities occurring on a certain workstation, they have disadvantages of requiring client software installed, configured and maintained on each workstation being controlled. Every endpoint not running client software (such as the many portable devices, smartphones and laptops, brought in under a BYOD policy) completely slips out of control if some additional MDM/MAM activity is not applied to enforce BYOD security.

On the other hand, network-based DLP's control all traffic going in and out the corporate network. Network-based DLP's do not require installation on every client device, and can effectively control communications occurring from employees' computers, BYOD devices and remote connections.

> **Typical corporate DLP can potentially introduce even more disruptions into business workflow**

As a result, a typical corporate DLP combines the use of network-based and endpoint-based solutions, which, in turn, can potentially introduce even more disruptions into business workflow.

Surveillance and Monitoring

In order to mitigate interruptions to business process introduced by active response systems such as DLP solutions, a different approach is often recommended by security experts.

Instead of deploying a company-wide data leak protection system, experts recommend using passive, non-intrusive monitoring of all employees and network users combined with instant alerts and fast incident response. This approach takes away the guessing of common DLP's and gets rid of intrusive roadblocks intruding into the business process.

> **“ Experts recommend passive, non-intrusive monitoring with instant alerts and fast incident response ”**

The use of monitoring-only solutions allows for uninterrupted workflow combined with fast, situation-based incident response to real threats – as opposed to putting a hard block on normal business activities deemed suspicious by an automated analysis system. By using a monitoring solution instead of a data leak prevention system one puts ones hopes upon qualified security personnel as opposed to betting on the qualities of an automated threat analysis algorithm.

Existing software-based monitoring solutions enable employee monitoring over corporate networks, intercepting network traffic and recording a wide range of user activities.

Commonly recorded activities include:

- Application logs;
- History of Web sites and online resources visited;
- Chats and conversations occurring over a range of instant messaging and social media;
- And so on and so forth.

Collected information is frequently accompanied with **recorded keystrokes and screen captures of the computer's desktop.**

In addition, many of these solutions are not exactly easy to use, generating a set of logs files for various aspects of system use and data access operations. Most are quite resource-intensive, time-consuming to analyze and requiring significant financial investments.

As a result, checking the logs collected for a single employee may take considerable time and effort of a qualified IT security specialist, inevitably causing real security incidents slip through. This was exactly the reason why log-based monitoring solutions still have a lower reputation compared to full-time DLP's.

Building a Monitoring System of Your Dream

While no single existing solution may offer quite the features your IT department may need out of the box, it is still possible to configure a perfect security monitoring system.

Let's see what the main points are.

- First, the system must be as silent and non-intrusive as at all possible. Disruptions to employees' workflow are extremely costly, diminishing productivity and making labor costs skyrocket. Let's settle on a **passive monitoring solution**.

- But then, we want our IT security department to be warned immediately if something's going on that requires immediate attention. Let's add **instant alerts, stop-words and suspicious activity detection** to the list of requirements.

A major point compared to proactive DLP's is the complete **lack of any blocks or obstacles interfering with regular workflow**. Instead, qualified security personnel is notified and allowed to take appropriate actions – or take no action at all if that was a false alarm. This approach allows both sparing existing workflow while enabling immediate incident response when and where required.

- When analyzing an incident, we often don't have the ability to arrive on the spot soon enough. As a result, we'll need the ability to **analyze incident details remotely** by connecting to the remote endpoint, obtaining the relevant information remotely and possibly performing emergency actions (such as locking the endpoint, shutting it down or disabling its network connection).

- Last but not least, we require **the most comprehensive reports delivered in human-readable form**.

The reports must be structured so that they can be quickly reviewed with a single glance or analyzed in deep detail if required. We'll need analytic tools to quickly and thoroughly analyze events and reconstruct the incident for a given timeframe and minimal known details.

Does an Ideal Solution Exist?

We live in an imperfect world. No single solution will offer everything perfectly matching your particular requirements out of the box. However, certain types of monitoring systems are closer to ideal, and can be configured to your exact requirements easier and more completely than others.

In recent years, a new approach to computer monitoring has appeared.

In this type of monitoring systems, **client software intercepts user activities while supplementing raw logs and text-based reports with live video stream captured on the user's workstation**. However, unlike traditional video surveillance systems, these computer monitoring solutions do not make one watch the entire video, even in fast-forward mode.

Instead, they index the video stream with other, text-based information collected from the same workstation, placing searchable markers onto the video stream.

As a result, discovering information relevant to a certain incident becomes easier, while watching the video stream reveals far more detailed information regarding the incident than any text-based log can.

Monitoring Based on Indexed Video Streams

We strongly believe that the future of endpoint workstation monitoring lies in recording on-screen activities of all workstations.

“ The future of endpoint workstation monitoring lies in recording on-screen activities ”

Compared to endpoint monitoring solutions based on collecting raw information and presenting it in the form of static, text, and chart based reports, video-capturing solutions offer the same browsing convenience and searching capabilities while delivering far more valuable information to the expert investigating an incident.

While traditional endpoint monitoring systems can indeed capture every relevant detail related to user activities, reports produced by these systems are static, non-intuitive to review and time-consuming to analyze.

In exchange for all the time and effort spent analyzing text and chart-based reports, these endpoint monitoring solutions give hard evidence and deep insight on what was really happening – again, at exchange for time and effort. This in turn makes them great for post-factum investigations, but hardly suitable for in-time situation-based incident response.

The new-generation systems monitor endpoints by recording on-screen activities with screen capturing software, saving successive screen shots into a chaptered and indexed video file.

“ These video streams are quick and easy to navigate thanks to accompanying text metadata ”

These video streams are quick and easy to navigate thanks to accompanying text metadata. The metadata includes the name of the active application, currently opened Web URL, and any keyboard input entered by the local or remote user including logins and passwords.

All this, combined, creates a perfect system aimed at fast situation-based incident response while offering the same in-depth analytic capabilities as traditional monitoring solutions.

This new-generation approach gains momentum in the area of endpoint monitoring. **But what about remote sessions?**

Monitoring Remote Sessions

Many endpoint monitoring solutions run on workstations and capture low-level hardware-generated events. While this is great to make sure no user input slips through, this approach is irrelevant when monitoring remote terminal sessions.

With **more and more companies relying upon remote workers and independent contractors**, the fact that a certain employee is physically present at their workplace is no longer a given. With no physical mouse movements and key presses, no unencrypted traffic passing through the corporate firewall, no on-screen activity and pretty much nothing visible to physical surveillance cameras, remote sessions become increasingly difficult with network-based or endpoint-based DLP's and traditional computer monitoring solutions.

> **“Monitoring remote sessions is troublesome for endpoint-based workstation monitoring products”**

Indeed, as remote sessions are generally initiated over secure tunnels, any traffic passing through the corporate Internet gateway is (and absolutely must be) securely encrypted. Unless specifically configured within a complex, difficult to set up and maintain solution, encrypted tunneled traffic may carry a lot of sensitive information without the system even noticing.

Monitoring remote sessions is troublesome for endpoint-based workstation monitoring products, too. With no physical activities and no on-screen activities appearing on the computer's display, capturing information occurring in terminal sessions is cryptic.

Fortunately, solutions exist that offer endpoint monitoring of both physical workstations and remote terminal sessions. Ekran System is one of such products.

To sum it up, an endpoint monitoring solution using indexed video streams offers the following benefits:

- ➢ Records all activities performed by regular and privileged users during local, remote, and terminal sessions (full endpoint monitoring*)

- Delivers the required level of security
- Helps mitigate risks imposed by a third party accessing corporate network
- Enables fast incident response by providing fully indexed, searchable video records and instant alerts on pre-defined events
- Allows easy reviewing and analysis of indexed video records
- Provides remote access for security officers to connect to the live video stream of a certain endpoint. Typically, this sort of remote access helps retrieving the current incident state
- Does not require any specific technical skills other than those possessed by a qualified security officer

* For the purpose of endpoint monitoring, there can be three types of sessions: a local session at a workstation, a remote session at a workstation (a single user is active at any time), and terminal sessions at a terminal server (a number of users working in their own sessions simultaneously).

Ekran System: Endpoint Monitoring for Local Workstations and Remote Terminal Sessions

Ekran System is a modern solution for corporate networks to enable monitoring and auditing of independent service providers, employees, and other insiders. **This innovative computer surveillance system is based on capturing on-screen user activities of regular and privileged users, and creating fully indexed and easily searchable video streams.**

Ekran System can monitor all workstations and servers on the corporate network including local, remote, and terminal sessions.

Installed on a server or workstation, Ekran Client records video streams of each session belonging to each regular and privileged computer user, and captures accompanying metadata such as the current application name, window title, URL, keystrokes, and so on. This metadata is tied closely to the video stream, enabling full-text search through the recorded video.

Ekran enables easy playback for all recorded sessions. Coupled with full-text search, the system enables administrators to quickly find key episodes to investigate incidents and analyze productivity and compliance of internal and remote employees, administrators, or third-party service providers.

Thanks to the easily accessible video records, security response personnel will be able to discover all instances of internal data misuse, competitor contacts, issues of fraud and theft of intellectual property.

Ekran System offers the following benefits:

- Non-disruptive monitoring with no disturbance to normal business workflow
- Fast situation-based incident response thanks to instant alerts and easily accessible indexed video recordings*
- Recordings can be reviewed and analyzed by ordinary security officers; no special training required
- Full endpoint monitoring: records all activities performed by regular and privileged users during local and terminal sessions
- Helps mitigate risks imposed by third-party contractors accessing corporate network
- Delivers the required level of security at reasonable cost

* An instant alert can be easily defined for any number of situations. For example, a security officer (Ekran System administrator) can set up a rule to detect an incident such as “<main client name> appears in keystrokes” or “skype appears in application title”. Once the rule triggers, the security officer will receive an instant on-screen notification pop-up and/or an email sent to a predefined address or multiple addresses.

Conclusion

We reviewed the most common types of Data Leak Protection (DLP) and workstation monitoring systems, identified the benefits and downsides of network-based and endpoint-based solutions, and defined their scope of use.

We came up with the list of requirements for a “perfect” workstation monitoring solution allowing for fast incident response without costly interruptions to business routine.

“ We came up with the list of requirements for a “perfect” monitoring solution ”

We found existing solutions corresponding to the listed requirements to be costly and, for many purposed uses, overly complicated.

For this reason, we developed a solution of our own. While the product offers immediate cost savings compared to competition, Ekran System combines all the powerful features required to secure the organization’s corporate network while enabling fast situation-based incident response without intruding into or otherwise interrupting the usual workflow.