Advantages of Integrated Central Management and Control of Data Protection Elements

What is the most effective way to easily and effectively deploy a comprehensive data protection solution?

Data protection has added a completely new layer of requirements for effective security operations. Only a very few organizations have not already deployed multiple layers of defense against attack and infection including Firewalls, Intrusion Prevention, Content URL Filtering, and Anti-virus at the gateway, and endpoint firewalls, AV, and white listing on servers, desktops, and mobile devices. But data protection (or Data Leak Prevention) provides another layer of defense against attacks that either bypass traditional defenses or for which there is no defense at all: accidental or malicious leakage of critical data. These trusted insiders, usually employees, but also contractors, temporary help, even persistent hackers who gain an insider's privileges, might accidentally or maliciously transfer data via ftp, email, or webmail. They may engage in backing up critical files and data to USB thumb drives which are easy to smuggle out. The easy transportability of an organization's critical data has opened the door for data loss and theft. To address this newly exposed level of vulnerability (which has always existed) a new product category has begun to gain popularity, especially at large organizations with security operations teams.

Specialized DLP products have several components. First there is the data discovery and tagging component. Software agents, or network crawlers, are deployed to find all of an organization's data, perhaps classify it, and tag it several ways so that it can be identified as it moves across a network. Often algorithms are used to fingerprint data and documents in such a way that even a cut and paste of a portion of document can be identified, alerted, or potentially blocked. Enforcement agents need to be deployed on every endpoint, server, and gateway. In addition those agents give the enterprise the ability to control what types of devices (iPhones, thumb drives, portable hard drives) can be attached to each endpoint and enforce strict policies on what data can be transferred to them.

Another element of data protection is encrypting data at rest and is rapidly being deployed to laptops, smartphones, and tablets. On top of that Mobile Device Management solutions control those devices remotely and can wipe them or lock them down if they are lost or stolen.

This paper is sponsored by Trend Micro.

A separate data protection console from an overlay DLP product requires separate personnel, separate training, separate reporting and compliance regimes, and separate trouble ticketing and SIEM (Security Information and Event Management) integration. As a result, many overlay DLP deployments take over a year and even then are left in monitor and alert mode — which offers no additional security, just another source of alerts to be monitored and added to the IT staff's daily list of tasks to address, or in many cases, ignored.

Trend Micro integrates Data Loss Prevention into their products at each layer of defense, unified by central policy management and visibility through Trend Micro Control Manager 6. For Trend Micro customers with DLP-ready products already deployed, a deployment scenario involves simply licensing and activating the integrated DLP capability.

Trend Micro products that support integrated DLP modules are:

- **Trend Micro OfficeScan**
- **Trend Micro ScanMail**
- **Trend Micro Portal Protect**
- **Trend Micro InterScan Messaging Security**
- **Trend Micro InterScan Web Security**

Central policy management, monitoring, and reporting are provided by the Trend Micro Control Manager.

There are many more organizations with little or no full time security staff and lacking the time or expertise to deploy an overlay DLP product. They also suffer data loss, yet often they are not even aware it has occurred. But a law firm may find itself facing an opponent with an uncanny knowledge of their client's business. Or a manufacturer may discover they are competing against their own designs in the marketplace — designs that were exfiltrated and reproduced offshore. Data protection is a critical layer of security for all businesses, research institutes, health care providers, and State and local governments. Organizations would do well to look for a solution that leverages existing infrastructure, is easy to deploy, and easy to manage.

As with all segments of the security industry, as the threats rise the once-complex overlay products evolve into easy–to-integrate and manage solutions that can be deployed in those organizations that do not have the IT resources to purchase and use large and cumbersome special purpose products.

Integration with an existing security console, especially the endpoint security management solution is trending upwards, driven by the need for efficiency and visibility. Data Protection tools that are built to seamlessly integrate with the existing layers of security are best positioned for easy deployment and low-impact management.

Through deploying integrated Data Protection within your existing deployed layers you do not add a new layer to monitor and manage, you increase the depth of your defense.

This paper is sponsored by Trend Micro.