Leveraging Your Existing Infrastructure to Achieve Data Protection

Answers the question: How can the various elements of a data protection solution — end point, server, network — be leveraged at each layer to quickly achieve an effective data protection regime?

Effective security is built in layers. Despite oft repeated alerts that the perimeter is dead and the layered model is outdated, layered security remains the most effective means to organize, deploy, and manage an effective defense against the rising tide of attacks.

The layers of protection can be physical or abstract. In physical terms, defenses can be deployed at the gateway, at the server (file server, email, and SharePoint), and on the endpoint itself. The abstract layers are network, endpoint, user, application, and data. These infrastructure solutions often span all of the physical layers.

The drawback of the layered security model is that it is often used to justify purchasing separate security products and layering them as well. Each additional layer of products, along with the resources required to deploy, update, and manage them, entail costs which include licensing, support, maintenance, updates, training, and the risk of misconfiguration. While the increased cost and complexity of a layered security approach are balanced by the improved protection it provides, introducing additional, "overlay" layers into this model further increases overhead and the risk that attacks will slip through due to misconfiguration or excessive complexity.

Data loss prevention is a layer of security that is traditionally deployed as an overlay at each physical layer: gateway, server, and endpoint. If data protection functionality can be incorporated in existing products then those layers of defense have been deepened while minimizing the complexity that results from introducing additional standalone products at each physical layer.

This paper is sponsored by Trend Micro.

Leveraging Existing Infrastructure for Data Protection

May 1, 2012

KEY POINTS

Most organizations already have content inspection on web gateways, email servers, and internal network devices, as well as malware defense on endpoints. An integrated data protection solution that is deployed across these devices would be the ideal means to provide layered deployment of the elements of a data protection solution: discovery, classification, and control of documents and data. If you already have a product deployed that inspects files and executables for malicious content, adding file classification and data protection policy enforcement represents an easy way to implement data loss prevention without increasing overhead and complexity.

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.

- Choosing a low-impact way to achieve data protection on the endpoint is the most critical decision. Deploying a separate agent to each endpoint with a separate management console to manage that deployment and then provide the dashboard view of alerts, file usage, and control of USB attached devices like thumb drives, portable hard drives, and even iPods, is a costly and inefficient way to implement DLP at the endpoint. Instead, a more efficient and effective approach is to integrate with the existing anti-malware agent that is already deployed on all endpoints.

- Leveraging existing content control elements in a comprehensive DP regime delivers effective content control without the expense and implementation issues of “shelf-ware” from separate vendors.

- While turning on license keys for data protection within an existing security agent may incur additional licensing cost, this cost is still far lower than deploying a new overlay product for data protection. The greatest savings comes from not having to deploy, learn, and manage data protection through an unfamiliar command console.

While many large organizations have deployed an overlay standalone data loss prevention solution to control documents, files, and columns in databases, most small organizations have not, and moreover lack the resources and expertise to do so. Yet, data protection is a critical defense against misuse of corporate information and outright theft by attackers or insiders. By quickly leveraging their existing threat protection infrastructure for data protection, the existing layers of defense can be deepened and extended without adding a new layer of complexity to an already complex security environment.

This paper is sponsored by Trend Micro.