Securosis, L.L.C.

Best Practices for Endpoint Data Loss Prevention

by Rich Mogull

This Report Sponsored by: symantec.

Author’s Note

The content in this report was developed independently of any sponsors. It is based on material originally posted on the Securosis blog but has been enhanced and professionally edited.

This report is sponsored by Symantec Inc.

Special thanks to Chris Pepper for editing and content support.

Sponsored by Symantec

Symantec’s Vontu Data Loss Prevention Solution is the industry's first integrated suite to prevent the loss of confidential data wherever it is stored or used - across endpoint, network, and storage systems. By reducing the risk of data loss, Vontu DLP helps organizations ensure public confidence, demonstrate compliance, and maintain competitive advantage. Symantec’s Data Loss Prevention customers include many of the world’s largest and most data-driven enterprises and government agencies. Symantec’s DLP products have received numerous awards, including IDG’s InfoWorld 2007 Technology of the Year Award for “Best Data Leak Prevention,“ as well as SC Magazine’s 2006 U.S. Excellence Award for “Best Enterprise Security Solution“ and Global Award for “Best New Security Solution.“ For more information, please visit http://go.symantec.com/vontu.

Copyright

Table of Contents

Introduction

Information Protection for the Modern Workforce

The modern enterprise faces information protection challenges we never could have imagined in the days when mainframes were dominant. The average laptop can carry up to a half-terabyte of storage, while keychain-sized USB storage devices can hold entire customer databases. Our users promiscuously connect to any network within wireless range of their laptops, emailing and exchanging our most sensitive information via a mix of private and public services. Simply locking down users is no longer an option; we need enabling technologies that protect our information while only minimally restricting our users. Rather than broadly blocking activity, we want to only block those actions that can damage us. These information protections needs to be mobile, adaptive, and minimally intrusive.

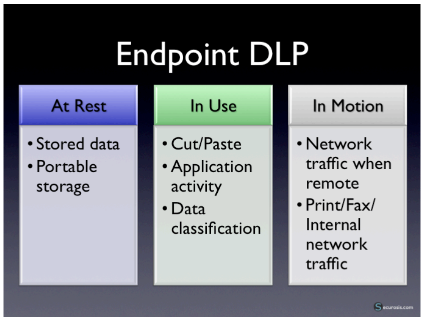
One of the most promising techniques to help reduce this risk is labelled Data Loss Prevention (DLP). While most people think of network monitors when they hear “DLP”, the truth is that DLP tools have evolved to work on the network, in storage, and on the endpoint. Endpoint DLP is particularly well suited for enabling the modern workforce — it enables us to intelligently protect our information based on the content, without completely blocking users from useful tools and services ranging from portable storage to online services.

Defining Endpoint DLP

Consider our definition of DLP:

”Products that, based on central policies, identify, monitor, and protect data at rest, in motion, and in use through deep content analysis”.

Endpoint DLP helps manage all three aspects of this problem. The first is protecting data at rest when it’s on the endpoint — or what we call content discovery. Our primary goal is keeping track of sensitive data as it proliferates out to laptops, desktops, and even portable media. The second part, and the most difficult problem in DLP, is protecting data in use. This is a catch-all term we use to describe DLP monitoring and protection of content as it’s used on a desktop — cut and paste, moving data into and out of applications, and even tying in with encryption and enterprise Document Rights Management (DRM). Finally, endpoint DLP provides data in motion protection for systems outside the purview of network DLP — such as laptops out in the field.



Endpoint DLP

At Rest	In Use	In Motion
• Stored data • Portable storage	• Cut/Paste • Application activity • Data classification	• Network traffic when remote • Print/Fax/ Internal network traffic

Endpoint DLP is a little difficult to discuss since it’s one of the fastest changing areas in a rapidly evolving space. No single product has every little piece of functionality we’re going to talk about, so (at least where functionality is concerned) this report will lay out all the recommended options which you can then prioritize to meet your own needs.

Endpoint DLP Drivers

At the beginning of the DLP market we nearly always recommended organizations start with network DLP. A network tool allows you to protect both managed and unmanaged systems (like contractor laptops), and is typically easier to deploy in an enterprise (since you don't have to touch every desktop and server). It also has advantages in terms of the number and types of content protection policies you can deploy, how it integrates with email for workflow, and the scope of channels covered. During the DLP market's first few years, it was hard to even find a content-aware endpoint agent.

But customer demand for endpoint DLP quickly grew thanks to two major needs — content discovery on the endpoint, and the ability to prevent loss through USB storage devices. We continue to see basic USB blocking tools with absolutely no content awareness brand themselves as DLP. The first batches of endpoint DLP tools focused on exactly these problems — discovery and content-aware portable media/USB device control.

The next major driver for endpoint DLP is supporting network policies when a system is outside the corporate gateway. We all live in an increasingly mobile workforce where we need to support consistent policies no matter where someone is physically located, nor how they connect to the Internet.

Finally, we see some demand for deeper integration of DLP with how a user interacts with their system. In part, this is to support more intensive policies to reduce malicious loss of data. You might, for example, disallow certain content from moving into certain applications, such as encryption tools. Some of these same hooks are used to limit cut/paste, print screen, and fax, or to enable more advanced security such as automatic encryption and application of DRM rights.

The Full Suite Advantage

As we've already hinted, there are some limitations to endpoint only DLP solutions. The first is that they only protect managed systems where you can deploy agents. If you're worried about contractors on your network or you want protection in case someone tries to use a server to send data outside the walls, you're out of luck. Also, because some content analysis policies are processor and memory intensive, it is problematic to get them running on resource-constrained endpoints. Finally, there are many discovery situations where you don't want to deploy a local endpoint agent for your content analysis — *e.g.*, when performing discovery on a large SAN.

Thus our bias towards full-suite solutions. Network DLP reduces losses on the enterprise network from both managed and unmanaged systems, and servers and workstations. Content discovery finds and protects stored data throughout the enterprise, while endpoint DLP protects systems that leave the network, and reduces risks across vectors that circumvent the network. It's the combination of all these layers that provides the best overall risk reduction. All of this is managed through a single policy, workflow, and administration server; rather than forcing you to create different policies; for different channels and products, with different capabilities, workflow, and management.

Technology Overview

Broad Scanning with Deep Content Analysis

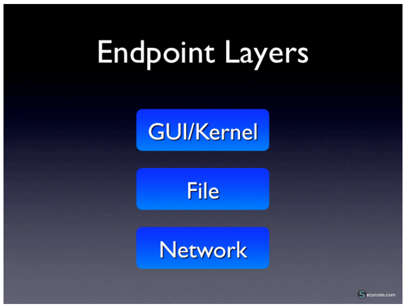
The key distinguishing feature of DLP, endpoint or otherwise, is deep content analysis based on central policies. This contrasts with non-DLP endpoint tools, such as encryption or portable device control (USB blocking). While covering all content analysis techniques is beyond the scope of this report, some of the more common ones include partial document matching, database fingerprinting (or exact data matching), rules-based, conceptual, statistical, predefined categories (like PCI compliance), and combinations of the above. They offer far deeper analysis than just simple keyword and regular expression matching. Ideally, your endpoint DLP tool should also offer preventative controls, not just policy alerts after violations occur. How does all this work?

Base Agent Functions

There is tremendous variation in the capabilities of different endpoint agents. Even for a single given function, there can be a dozen different approaches, all with varying degrees of success. Also, not all agents contain all features; in fact, most agents lack one or more major areas of functionality.

Agents include four generic layers/features:

1. *Content Discovery:* Scanning of stored content for policy violations.
2. *File System Protection:* Monitoring and enforcement of file operations as they occur (as opposed to discovery, which is scanning of content already written to media). Most often, this is used to prevent content from being written to portable media/USB. It's also where tools hook in for automatic encryption or application of DRM rights.
3. *Network Protection:* Monitoring and enforcement of network operations. Provides protection similar to gateway DLP when an endpoint is off the corporate network. Since most endpoints treat printing and faxing as a form of network traffic, this is where most print/fax protection can be enforced (the rest comes from special print/fax hooks).
4. *GUI/Kernel Protection:* A more generic category to cover data in use scenarios, such as cut/paste, application restrictions, and print screen.



Endpoint Layers

GUI/Kernel

File

Network

Between these four categories we cover most of the day to day operations a user might perform that places content at risk. It hits our primary drivers from the last section — protecting data from portable storage, protecting systems off the corporate network, and supporting discovery on the endpoint. Most of the tools on the market start with file and (then) networking features before moving on to some of the more complex GUI/kernel functions.

Agent Content Awareness

Even if you have an endpoint with a quad-core processor and 8 GB of RAM, it would be wasteful to devote all that horsepower to enforcing DLP.

Content analysis may be resource intensive, depending on the types of policies you are trying to enforce. Also, different agents have different enforcement capabilities, which may or may not match up to their gateway counterparts. At a minimum, most endpoint tools support rules/regular expressions, some degree of partial document matching, and a whole lot of contextual analysis. Others support their entire repertoire of content analysis techniques, but you will likely have to tune policies to run on more resource constrained endpoints.

Some tools rely on the central management server for aspects of content analysis, to offload agent overhead. Rather than performing all analysis locally, they ship content back to the server, and act on any results. This obviously isn't ideal, since those policies can't be enforced when the endpoint is off the enterprise network, and it sucks up a bit of bandwidth. But it does allow enforcement of policies that are otherwise totally unrealistic on an endpoint, such as fingerprinting of a large enterprise database.

One emerging option is policies that adapt based on endpoint location. For example, when you're on the enterprise network most policies are enforced at the gateway. Once you access the Internet outside the corporate walls, a different set of policies is enforced. For example, you might use database fingerprinting of the customer database at the gateway when the laptop is in the office or on a (non-split-tunneled) VPN, but drop to a rule/regex for Social Security Numbers (or account numbers) for mobile workers. Sure, you'll get more false positives, but you're still able to protect your sensitive information while meeting performance requirements.

Agent Management

Agent management consists of two main functions — deployment and maintenance. On the deployment side, most tools today are designed to work with whatever workstation management tools your organization already uses. As with other software tools, you create a deployment package and then distribute it along with any other software updates. If you don't already have a software deployment tool, you'll want to look for an endpoint DLP tool that includes basic deployment capabilities. Since all endpoint DLP tools include central policy management, deployment is fairly straightforward. There's little need to customize packages based on user, group, or other variables beyond the location of the central management server.

The rest of the agent's lifecycle, aside from major updates, is controlled through the central management server. Agents should communicate regularly with the central server to receive policy updates and report incidents/activity. When the central management server is accessible, this should happen in near real time. When the endpoint is off the enterprise network (without VPN/remote access), the DLP tool will store violations locally in a secure repository that's encrypted and inaccessible to the user. The tool will then connect with the management server next time it's accessible, receiving policy updates and reporting activity. The management server should produce aging reports to help you identify endpoints which are out of date and need to be refreshed. Under some circumstances, the endpoint may be able to communicate remote violations through encrypted email or another secure mechanism from outside the corporate firewall.

Aside from content policy updates and activity reporting, there are a few other features that require central management. For content discovery, you'll need to control scanning schedule/frequency, as well as bandwidth and performance (*e.g.*, capping CPU usage). For real time monitoring and enforcement you'll also want performance controls, including limits on how much space is used to store policies and the local cache of incident information.

Once you set your base configuration, you shouldn’t need to do much endpoint management directly. Things like enforcement actions are handled implicitly as part of policy, thus integrated into the main DLP policy interface.

Policy Creation and Workflow

Policy creation for endpoints should be fully integrated into your central DLP policy framework for consistent enforcement across data in motion, at rest, and in use. Policies are thus content focused, rather than location focused — another advantage of full suites over individual point products. In the policy management interface you first define the content to protect, then pick channels and enforcement actions (all, of course, tied to users/groups and context). For example, you might want to create a policy to protect customer account numbers. You’d start by creating a database fingerprinting policy, pulling names and account numbers from the customer database — this is the content definition phase. Assuming you want the policy to apply equally to all employees, you then define network protective actions — *e.g.*, blocking unencrypted emails with account numbers, blocking HTTP and FTP traffic, and alerting on other channels where blocking isn’t possible. For content discovery, quarantine any files with more than one account number that are not on a registered and authorized server. Then, for endpoints, restrict account numbers from unencrypted files, portable storage, or network communications when the user is off the corporate network, switching to a rules-based (regular expression) policy when the policy server isn’t available.

Incident management should also be fully integrated into the overall DLP incident handling queue. Incidents appear in a single interface, and can be routed to handlers based on policy violated, user, severity, channel, or other criteria. Remember that DLP is focused on solving the business problem of protecting your information, and thus tends to require a dedicated workflow.

For endpoint DLP you’ll need some additional information beyond network or non-endpoint discovery policies. Since some violations will occur when the system is off the network and unable to communicate with the central management server, “delayed notification“ violations need to be appropriately stamped and prioritized in the management interface. You’d hate to miss the loss of your entire customer database because it showed up as a week-old incident when the sales laptop finally reconnected.

Otherwise, workflow is fully integrated into your main DLP solution, and any endpoint-specific actions are handled through the same mechanisms as discovery and network activity.

Integration

If you’re running an endpoint only solution, an integrated user interface obviously isn’t an issue. For full suite solutions, as we just discussed, policy creation, management, and incident workflow should be completely integrated with network and discovery policies.

Other endpoint management is typically a separate tab in the main interface, alongside management areas for discovery/storage management and network integration/management. While you want an integrated management interface, you don’t want it so integrated that it becomes confusing or unwieldy to use.

In most DLP tools, content discovery is managed separately to define repositories and manage scanning schedules and performance. Endpoint DLP discovery should be included here, and allow you to specify device and user groups instead of having to manage endpoints individually.

Deployment Best Practices

Preparing for Deployment

Before installing a DLP tool and creating any policies, first focus on setting expectations, prioritizing, and defining your internal processes. The greatest barriers to successful deployment aren't technology issues, but rather failure of the enterprise to understand what to protect, decide how to protect it, and recognize what's reasonable in a real-world environment.

Setting Expectations

The single most important requirement for any successful DLP deployment is properly setting expectations at the start of the project. DLP tools are powerful, but far from a magic bullet or black box that makes all data completely secure. When setting expectations you need to pull key stakeholders together in a single room and define what's achievable with your solution. All discussion at this point assumes you've already selected a tool. Some of these practices deliberately overlap steps during the selection process, since at this point you'll have a much clearer understanding of the capabilities of your chosen tool.

In this phase, discuss and define the following:

- What kinds of content you can protect, based on the content analysis capabilities of your endpoint agent.
- How these compare to your network and discovery content analysis capabilities. Which policies can you enforce at the endpoint? When disconnected from the corporate network?
- Expected accuracy rates for those different kinds of content — for example, you'll have a much higher false positive rate with statistical/conceptual techniques than partial document or database matching.
- Protection options: Can you block USB? Move files? Monitor network activity from the endpoint?
- Performance — taking into account differences based on content analysis policies.
- How much of the infrastructure you'd like to cover.
- Scanning frequency (days? hours? near continuous?).
- Reporting and workflow capabilities.
- What enforcement actions you'd like to take on the endpoint, and which are possible with your current agent capabilities.

It's extremely important to start defining a phased implementation. It's completely unrealistic to expect to monitor every last endpoint in your infrastructure with an initial rollout. Nearly every organization finds they are more successful with a controlled, staged rollout that slowly expands breadth of coverage and types of content to protect.

Prioritization

If you haven't already prioritized your information during the selection process, you need to pull all major stakeholders together (business units, legal, compliance, security, IT, HR, etc.) and determine which kinds of information are more important, and which to protect first. I recommend you first rank major information types (*e.g.*, customer PII, employee PII, engineering plans, corporate financials), then re-order them by priority for monitoring/protecting within your DLP content discovery tool.

In an ideal world your prioritization should directly align with the order of protection, but while some data might be more important to the organization (engineering plans) other data may need to be protected first due to exposure or regulatory requirements (PII). You'll also need to tweak the order based on the capabilities of your tool.

After your prioritize information types to protect, run through and determine approximate timelines for deploying content policies for each type. Be realistic, and understand that you'll need to both tune new policies and leave time for the organization to become comfortable with any required business changes. Not all polices work well on endpoints, and you need to determine how you'd like to balance endpoint against network enforcement.

We'll look more closely at how to roll out policies and what to expect in terms of deployment times later in this paper.

Workstation and Infrastructure Integration and Testing

Despite constant processor and memory improvements, our endpoints are always in a delicate balance between maintenance tools and a user's productivity applications. Before beginning the rollout process you need to perform basic testing with the DLP endpoint agent under different circumstances on your standard images. If you don't use standard images, you'll need to perform more in-depth testing with common profiles.

During the first stage, deploy the agent to test systems with no active policies and see if there are any conflicts with other applications or configurations. Then deploy some representative policies, perhaps adapted from existing network policies. You're not testing these policies for actual deployment, but rather profiling a range of potential policies and enforcement actions so you have a better understanding of how future production policies will perform. Your goal in this stage is to test as many options as possible to ensure the endpoint agent is properly integrated, performs satisfactorily, enforces policies effectively, and is compatible with existing images and other workstation applications. Make sure you test any network monitoring/blocking, portable storage control, and local discovery performance. Also test the agent's ability to monitor activity when the endpoint is remote, and to properly report policy violations when it reconnects to the enterprise network.

Next (or concurrently), begin integrating the endpoint DLP into your larger infrastructure. If you've deployed other DLP components you might not need much additional integration, but you'll want to confirm that users, groups, and systems from your directory services match which users are really on which endpoints. While with network DLP we focus on capturing users based on DHCP address, with endpoint DLP we concentrate on identifying the user during authentication. Make sure that, if multiple users are on a system, you properly identify each user so that policies are applied appropriately.

Define Process

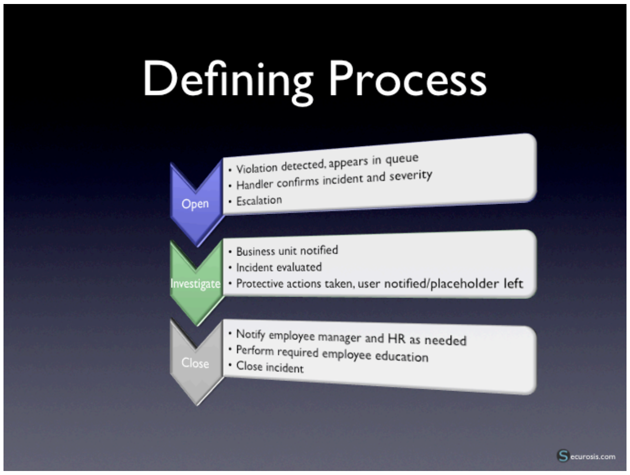
DLP tools are, by their very nature, intrusive. Not in terms of breaking things, but in terms of the depth and breadth of what they find. Organizations are strongly advised to define their business processes for dealing with DLP policy creation and violations before turning on the tools. Here's a sample process for defining new policies:

1. Business unit requests policy from DLP team to protect a particular content type.
2. DLP team meets with business unit to determine goals and protection requirements.
3. DLP team engages with legal/compliance to determine any legal or contractual requirements or limitations.

4. DLP team defines draft policy.
5. Draft policy tested in monitoring (alert only) mode without full workflow, and tuned to acceptable accuracy.
6. DLP team defines workflow for selected policy.
7. DLP team reviews final policy and workflow with business unit to confirm needs have been met.
8. Appropriate business units notified of new policy and any required changes in business processes.
9. Policy deployed in production environment in monitoring mode, but with full workflow enabled.
10. Protection certified as stable.
11. Protection/enforcement actions enabled.

And here’s one for policy violations:

1. Violation detected; appears in incident handling queue.
2. Incident handler confirms incident and severity.
3. If action required, incident handler escalates and opens investigation.
4. Business unit contact for triggered policy notified.
5. Incident evaluated.
6. Protective action taken.
7. User notified if appropriate, based on nature of violation.
8. Notify employee manager and HR if corrective action required.
9. Perform required employee education.
10. Close incident.



Defining Process

- Violation detected, appears in queue
- Handler confirms incident and severity
- Escalation

- Business unit notified
- Incident evaluated
- Protective actions taken, user notified/placeholder left

- Notify employee manager and HR as needed
- Perform required employee education
- Close incident

These are, of course, just basic examples, but they should give you a good idea of where to start. You’ll notice that these depend heavily on knowing who your users are, their job roles, and who they report to. Before deployment, it’s important to evaluate your directory infrastructure to know if it accurately reflects your organizational structure. If not, consider updating your directory services or adjusting your processes to account for the manual identification of users in your incident workflow.

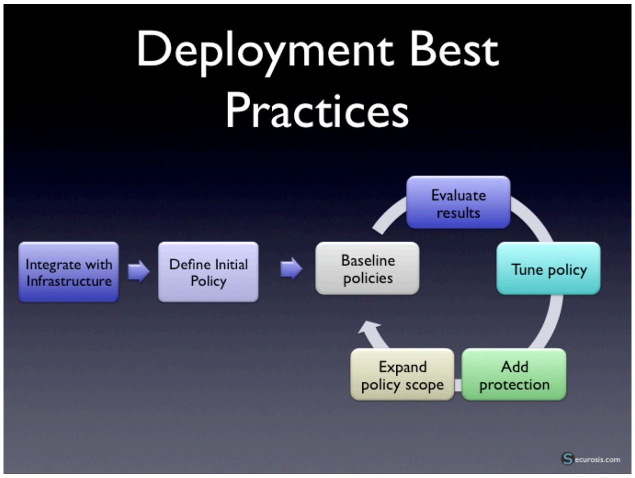
Deployment

By this point you should know what policies you’d like to deploy, what content to start protecting, how you’d like to grow that protection after initial deployment, and your workflow for policy violations.

Now we’re ready to move beyond planning into deployment.

1. *Integrate with your infrastructure:* Endpoint DLP tools require integration with a few different infrastructure elements. First, if you are using a full DLP suite, figure out if you need to perform any extra integration before moving to endpoint deployments. Some suites OEM the endpoint agent and you may need some additional components to get up and running. In other cases, you’ll need to plan capacity and possibly deploy additional servers to handle the endpoint load. Next, integrate with your directory infrastructure if you haven’t already. Determine if you need any additional information to tie users to devices (in most cases, this is built into the tool and its directory integration components).
2. *Integrate on the endpoint:* In your preparatory steps you should have performed testing to be comfortable that the agent is compatible with your standard images and other workstation configurations. Now you need to add the agent to the production images and prepare deployment packages. Don’t forget to configure the agent before deployment, especially the home server location and how much space and resources to use on the endpoint. Depending on your tool, this may be managed after initial deployment by your management server.

3. *Deploy agents to initial workgroups:* You'll want to start with a limited deployment before rolling out to the larger enterprise. Pick a pilot workgroup where you can test your initial policies and get feedback on how the agent functions in production.
4. *Build initial policies:* For your first deployment, you should start with a small subset of policies, or even a single policy, in alert or content classification/discovery mode (where the tool reports on sensitive data, but doesn't generate policy violations).


Deployment Best Practices

5. *Baseline, then expand deployment:* Deploy your initial policies to the pilot workgroup. Try to roll the policies out one monitoring/enforcement mode at a time, *e.g.*, start with endpoint discovery, then move to USB blocking, then add network alerting, then blocking, and so on. Once you have a good feel for the effectiveness of the policies, performance, and enterprise integration, you can expand into a wider deployment, covering more of the enterprise. After the first few you'll have a good understanding of how quickly, and how widely, you can roll out new policies.
6. *Tune policies:* Even stable policies may require tuning over time. In some cases it's to improve effectiveness, in others to reduce false positives, and in still other cases to adapt to evolving business needs. You'll want to initially tune policies during baselining, but continue to tune them as the deployment expands. Most clients report that they don't spend much time tuning policies after baselining, but it's always a good idea to keep your policies current with enterprise needs.
7. *Add enforcement/protection:* By this point you should understand the effectiveness of your policies, and have educated users where you've found policy violations. You can now start switching to enforcement or protective actions, such as blocking, network filtering, or encryption of files. It's important to notify users of enforcement actions as they occur, otherwise you might frustrate them unnecessarily; dealing with false positives and handling exceptions also require users to understand that DLP is in play. If you're making a major change to established business process (*e.g.*, restricting access to a common content type to meet a new compliance need), consider scaling out enforcement options on a business unit by business unit basis.

Deploying endpoint DLP isn't really very difficult; the most common mistake enterprises make is deploying agents and policies too widely, too quickly. When you combine a new endpoint agent with intrusive enforcement actions that interfere (positively or negatively) with people's work habits, you risk grumpy employees and political backlash. Most organizations find that a staged rollout of agents, followed by first deploying monitoring policies before moving into enforcement, then a staged rollout of policies, is the most effective approach.

Use Cases

We’ve finished our review of endpoint DLP best practices, as well as how to deploy and maintain a system. Now we’ll focus on a couple use cases that illustrate how it all works together. These are synthetic case studies, based on interviews with real DLP customers.

Endpoint Discovery and File Monitoring for PCI Compliance Support

BuyMore is a large regional home goods and grocery retailer in the southwest United States. In a previous PCI audit, credit card information was discovered on some employee laptops mixed in with loyalty program data and customer demographics. An expensive, manual audit and cleansing was performed within business units handling this content. To avoid similar issues in the future, BuyMore purchased an endpoint DLP solution with discovery and real time file monitoring support.

BuyMore has a highly distributed infrastructure due to multiple acquisitions and independently managed retail outlets (approximately 150 locations). During initial testing it was determined that database fingerprinting would be the best content analysis technique for the corporate headquarters, regional offices, and retail outlet servers, while rules-based analysis is the best fit for the systems used by store managers. The eventual goal is to transition all locations to database fingerprinting, once a database consolidation and cleansing program is complete.

During Phase 1, endpoint agents were deployed to corporate headquarters laptops for the customer relations and marketing team. An initial content discovery scan was performed, with policy violations reported to managers and the affected employees. For violations, a second scan was performed 30 days later to ensure that the data was removed. In Phase 2, the endpoint agents were switched into real time monitoring mode when the central management server was available (to support the database fingerprinting policy). Systems that leave the corporate network are then scanned monthly when they connect back in, with the tool tuned to only scan files modified since the last scan. All systems are scanned on a rotating quarterly basis, and reports generated and provided to the auditors.

For Phase 3, agents were deployed to the rest of the corporate headquarters team over the course of 6 months, on a business unit by business unit basis.

For the final phase, agents were deployed to retail outlets on a store by store basis. Due to the lower quality of database data in these locations, a rules-based policy for credit cards was used. Policy violations automatically generate an email to the store manager, and are reported to the central policy server for followup by a compliance manager.

At the end of 18 months, corporate headquarters and 78% or retail outlets were covered. BuyMore is planning on adding USB blocking in their next year of deployment, and has already completed deployment of network filtering and content discovery for storage repositories.

Endpoint Enforcement for Intellectual Property Protection

EngineeringCo is a small contract engineering firm with 500 employees in the high tech manufacturing industry. They specialize in designing highly competitive mobile phones for major manufacturers. In 2006 they suffered a major theft of their intellectual property when a contractor transferred product description documents and CAD diagrams for a new design onto a USB device and sold them to a competitor in Asia, which beat their client to market by 3 months.

EngineeringCo purchased a full DLP suite in 2007 and completed deployment of partial document matching policies on the network, followed by network-scanning-based content discovery policies for corporate desktops. After 6 months they added network blocking for email, HTTP, and FTP, and violations are at an acceptable level. In the first half of 2008 they began deployment of endpoint agents for engineering laptops (approximately 150 systems).

Because the information involved is so valuable, EngineeringCo decided to deploy full partial document matching policies on their endpoints. Testing determined performance is acceptable on current systems if the analysis signatures are limited to 500 MB in total size. To accommodate this limit, a special directory was established for each major project where managers drop key documents, rather than all project documents (which are still scanned and protected at the network). Engineers can work with documents, but the endpoint agent blocks network transmission except for internal email and file sharing, and any portable storage. The network gateway prevents engineers from emailing documents externally using their corporate email, but since it’s a gateway solution internal emails aren’t scanned.

Engineering teams are typically 5-25 individuals, and agents were deployed on a team by team basis, taking approximately 6 months total.

Conclusion

These are, of course, fictional best practices examples, but they’re drawn from discussions with dozens of DLP clients. The key takeaways are:

- Start small, with a few simple policies and a limited scanning footprint.
- Grow deployments as you reduce incidents and violations to keep your incident queue under control and educate employees.
- Start with monitoring and alerting and employee education, then move on to enforcement.
- This is risk reduction, not risk elimination. Use the tool to identify and reduce exposure but don’t expect it to magically solve all your data security problems.
- When you add new policies, test first with a limited audience before rolling out to the full scope, even if you are already covering the entire enterprise with other policies.

Endpoint DLP is a powerful tool for reducing the risk of data loss while enabling the mobile workforce, especially when part of a full suite DLP solution with network and stored data capabilities.

About the Author

Rich Mogull has over 17 years experience in information security, physical security, and risk management. Prior to founding Securosis; Rich spent 7 years as a leading security analyst with Gartner; where he advised thousands of clients, authored dozens of reports, and was consistently one of Gartner's top international speakers. He is one of the world's premier authorities on data security technologies and has covered issues ranging from vulnerabilities and threats, to risk management frameworks, to major application security. Rich is the Security Editor of *TidBITS*, a monthly columnist for *Dark Reading*, and a frequent contributor to publications ranging from *Information Security* magazine to *Macworld*.

About Securosis

Securosis, L.L.C. is a security consulting practice dedicated to thought leadership, objectivity, and transparency. Our consultants have all held executive level positions and are dedicated to providing the highest value strategic consulting available.

We provide services in four main areas:

- Publishing and Speaking: including independent, objective white papers; webcasts; and in-person presentations.
- Strategic Consulting for Vendors: including market and product analysis and strategy, technology guidance, product evaluations, and merger and acquisition assessments.
- Strategic Consulting for End Users: including product selection assistance, technology and architecture strategy, education, and security management evaluations, and risk assessments.
- Investor Consulting: including product and market evaluations, available in conjunction with deep product assessments with our research partners.

Our clients range from stealth startups to some of the world's best known technology vendors and end users. Clients include large financial institutions, institutional investors, startups, mid-sized enterprises, and major security vendors.

Securosis has partnered with security testing labs to provide unique product evaluations that combine in-depth technical analysis with high-level product, architecture, and market analysis.