Symantec Data Loss Prevention: From Adoption to Maturity

In the summer of 2015, a Symantec employee unintentionally violated policy when he configured his work email to auto-forward to his personal account. A coworker later emailed him a snippet of source code—another policy violation, compounded by the fact that the code was being diverted outside the company.

Neither employee had malicious intent, their shortcuts could have exposed our most valuable asset—our source code—to any number of bad actors around the world.

Fortunately, Symantec Data Loss Prevention (DLP) was on the job. It alerted our Security Operations Center that someone was emailing source code. An incident-response team sprang into action, investigating the activity and shutting it down before any damage was done.

If we hadn't been using Symantec DLP we may not have learned of the violations for months, if ever. That's why we've made it a major part of our protection strategy. It alerts our security team whenever sensitive information is emailed, saved to a thumb drive, or otherwise moved around the network in a suspicious way, thus enabling us to take immediate action and make sure no policies are being violated.

Symantec Data Loss Prevention: From Adoption to Maturity is written to inform CIOs, CTOs, CISOs, and other senior managers about our journey to help secure our data. In this paper we explain the challenges we faced, how we solved them, and the lessons we learned that might be of value to you. We also describe our best practices and the experiences of our IT staffers as they developed and installed one of the most robust solutions for data loss prevention in the industry.

Data Loss Prevention—Getting It Right

Every company has information it needs to keep secure. Whether that's source code, customer data, or personally identifying information, there's a heavy price to pay if confidential files escape your network. Part of the answer involves keeping bad actors out, but if hackers do sneak into your network (maybe by stealing an employee's logon credentials) you need to be sure they can't slip any information out.

We need to be sure too. That's where we rely on Symantec DLP.

"Our key priority is to safeguard Symantec's most critical assets: source code, customer data, and our employees' personally identifiable information," says Tim Fitzgerald, our chief security officer. "A broad and creative deployment of Symantec DLP is one of the most powerful tools we have to help us achieve this."

The product is highly customizable, so you'll want to fine-tune it to meet your own company's specific needs. That step can take some time—we worked for two years to get our own strategy just right—but as you'll see, our results have been well worth the effort.

Strategic Overview

Tracking your information involves five steps:

1. Decide what information you want to track
2. Tag it with a watermark or other secret identifier
3. Create rules so you're alerted when someone moves watermarked information under unusual circumstances
4. Ensure the alerts are evaluated and acted upon immediately
5. Refine the rules to minimize false positives

History

Symantec acquired its Data Loss Prevention product in 2007. Because the company's primary goal was to strengthen our product portfolio, the idea of implementing it internally was only a secondary priority.

At the time our IT staff was outsourcing some of its infrastructure efforts to a third party. When we asked the vendor to set up Symantec DLP for us, our initial focus was to use it to protect our network and endpoints, and not so much to keep tabs on our source code.

We re-evaluated in 2012. That's when we brought our IT operations in-house to be managed internally. At that point we decided to make full use of Symantec DLP's capabilities by installing it as a key part of our source-code protection strategy.

Navigating the Learning Curve

When we implemented Symantec DLP we had the right idea, but we discovered there was a bit of a learning curve. We as a company had extensive knowledge about how to fine-tune Symantec DLP, but our IT teams, who were new to the product, created rules that were overly broad and not as well thought out.

"We treated it like antivirus software—just turn it on and let it work," Tim says. "In hindsight, that's not what Data Loss Prevention is. It's a very sophisticated hunting tool, but if you don't tell it what to hunt for it finds everything and becomes unusable."

That's also the top complaint we get from customers. They'll set up broad rules for everything from credit-card numbers to Social Security numbers, and end up with such an avalanche of alerts that they give up and turn off the rules entirely.

Here's how to avoid that: Before you begin, your executive staff and security practitioners need to have an in-depth conversation about risk management. Figure out what data you need to protect and what you think the threats are, and then bring in your engineers to craft the appropriate policies.

We did it backward. We had our engineers create policies, and when we got too many alerts we'd dial the rules back and try again, a method of trial and error that played out for more than a year. If we had strategized first, we could have gotten up to speed in a matter of months.

In parallel with creating and testing our policies, we developed a way to secretly mark our source code so Symantec DLP could track how it was being moved around. The process involved overcoming a few technical challenges.

First, we had tens of millions of lines of code to watermark. We also had to track down where all of our code was; we hadn't given our developers great tools to store their code in a single area, so a lot of them saved their work on laptops and other unsecured devices.

So we undertook an ambitious effort. First we consolidated about 750 source-code repositories around the world and migrated their contents to two centrally managed systems. Then we used proprietary technology to watermark our code. (For more information read our companion CustomerONE story: "Source Code Security the Symantec Way.")

Fine-Tuning Our Alerts

Once our code was watermarked and secured, we created rules for the DLP software to use to detect suspicious activity.

Customers seem surprised when we tell them how time-consuming this step is. Tim Deese, a Symantec engineer who helped run our DLP effort, explains it this way: "Suppose you want to track activity around Social Security numbers," he says. "If you just create a policy to detect nine-digit numbers, then every nine-digit number—product numbers, ZIP codes, even some phone numbers—will trigger an alert."

In this case, you'd have to analyze every alert, determine which were false positives and tweak your rule to keep them from getting flagged. Then you'd have to let the new rule run for a period of time and then spend another week or so re-examining the results, continuing the cycle until you've gotten it just right. In the meantime you have to do the same for all of your other rules.

"It's a fair amount of work," Tim Deese says. "The process is simple but it's just a large volume of data. And you have to analyze it in great detail to make sure you're not excluding genuine threats."

You may also have to deal with conflicting corporate demands. One business unit might want a rule loosened, even if it creates more alerts, and another unit might want the same rule more focused. That can lead to administrative back-and-forth that slows the process down.

So what's the lesson for you? Two things: First, set up rules only for your more critical information; and second, have a clear hierarchy for approving policies, so the process of tweaking rules and policies doesn't get hung up in bureaucratic wrangling.

Responding Appropriately to Alerts

There's no point receiving an alert if the alert is never acted upon. We had that problem when we were outsourcing our DLP monitoring to the third party. Since we hadn't developed clear policies, there were times when alerts got ignored because we and the vendor each thought the other would investigate.

We solved that by assigning all monitoring responsibilities to our Security Operations Center in Virginia. Today when staffers there receive an alert they know they're the ones responsible for investigating. If they think a particular activity could be malicious they escalate the matter along a clearly defined hierarchy. And if an alert doesn't rise to that level, as with our employee who was forwarding work emails to a personal account, they handle it according to internal policy.

You'll need a similar process. Know who in your company should receive the data alerts, and then have a clear process that outlines when they escalate those alerts and to whom.

We'll be happy to help you strategize.

Staffing Challenges

Tim Deese joined our support department in 2006. When we acquired the Data Loss Prevention product the following year he volunteered to get trained on it, a decision that he jokes gave him job security for life.

"It's the truth. It's a hot market, even two to three years after DLP exploded in the market," he says. "When customers buy our software and look around for help setting it up, there aren't many people. It's definitely a challenge."

Symantec used to offer professional services to help with installations, but we've moved away from that business model. We do offer training, which Tim strongly recommends.

"In order for a customer to develop expertise in-house, I'd say take a couple of people and put them through our training and give them the resources we have," he says. "In three to six months they could become pretty proficient at managing their own deployment."

Best Practices

Keep in mind that Data Loss Prevention is just one piece of your overall data-protection strategy. Danny Graves, a senior Symantec information-security analyst, recommends the following best practices as well:

- Impose strong authentication and password controls
- Manage all policies centrally to ensure consistency
- If you have engineering labs, make sure developers use secure centralized repositories, not their own individual solutions
- Use strong encryption
- Maintain an agile patch-management system
- Make sure endpoint protection is updated and turned on for everyone on the network

"Most of these are no-brainers," Danny says, "but they're easy to forget or overlook."

Our Next Steps

In 2016, we'll be going to market with a new cloud-based Data Loss Prevention service. We'll provide the hardware, maintenance and service, freeing customers from having to manage infrastructure and physical security.

"That's a big step forward for us," says Linda Park, a Symantec product-marketing manager. "This is where the industry and market are headed."

Even with cloud services, however, customers would still need their own staffers to respond to incidents.

Also in the works: a solution to provide what CSO Tim Fitzgerald describes as the holy grail of source-code protection: prevention. It's one thing to detect when source code is being moved inappropriately— the next step is disallow the movement.

That's exactly where we're headed.

The biggest challenge in prevention is finding a balance between blocking suspicious actions and impeding our staff's legitimate work. Symantec is close to a solution, which we expect to roll out in 2016. Stay tuned.

Learn More with an Executive Briefing

This brief was intended to give you a broad look at how we use Symantec Data Loss Prevention internally. Your Symantec representative can show you how to adapt our blueprint to make your own DLP journey even smoother.

If you'd like even more in-depth experience, visit our Executive Briefing Centers at our U.S. headquarters in Mountain View, California, or in Reading, U.K.

Executive briefings provide you an exclusive opportunity to learn how Symantec solutions can protect your business and network environments. We'll customize the briefing to meet your specific goals, and we'll also give you a sneak peek at new technologies and challenges on the horizon.

SYMANTEC SOLUTIONS AND PRODUCTS IN THIS PAPER

Data Loss Prevention: DLP discovers where data is stored across your cloud, mobile, and on-premises environments; monitors how it's being used on and off your corporate network; and protects it from being leaked or stolen

customer_one@symantec.com

CustomerONE Team
350 Ellis Street
Mountain View, CA 94043
800-745-6054

Symantec's CustomerONE team can facilitate discussions between you and our IT security practitioners to help you address your security questions and concerns. Please contact us directly or through your Symantec sales team.

This document is provided for informational purposes only and is not intended as advertising. All warranties relating to the information in this document, either express or implied, are disclaimed to the maximum extent allowed by law. The information in this document is subject to change without notice.