CUSTOMERONE

Symantec

Source Code Security the Symantec Way

When companies think about their source code it's generally with a single conern: Does it work? But they often overlook an equally crucial question: Are we doing enough to protect it from hackers and thieves?

At Symantec, we've been asking the second question for years. Our earlier security measures were adequate, but in today's world, adequate is no longer good enough. That's why we created a robust strategy to keep our source code secure.

Since 2012 we consolidated hundreds of repositories where we used to keep source code, and then we secured that code in a virtual vault surrounded by five layers of protection. We also subjected the code to the full power of Symantec's monitoring solutions. Finally, we changed internal policies to prevent the sort of employee behaviors that tended to put our code at risk.

The results have been promising. We've been able to protect our source code with an elite level of security, without impeding the developers who need access to the code.

Our strategy works just as well for any company looking to protect its source code or other confidential data. In this paper we'll explain what we did, how we did it, and how you can get the same results. After that, if you'd like to learn more about how our model can work for you we'll be happy to arrange an executive briefing and demonstration.

As one of the world's leading cybersecurity companies, Symantec has developed best-in-class strategies to keep our own source code safe. In **Source Code Security The Symantec Way**, we share our best practices with you.

This paper is intended for CIOs, CTOs , CISOs, and other senior managers exploring how to safeguard their intellectual property. We'll give you a transparent look into how we locked down our own source code, from consolidating our repositories to securing the code in multiple layers of protection. We'll tell you what worked–and what didn't.

Our goal, as always: to help you model your own security after the best we have to offer.

Background

Tim Fitzgerald, our chief security officer since June 2014, remembers the two events that shaped his view of cybersecurity. The first was news of a state-sponsored attack on more than 30 companies in late 2009. The other was the realization in 2012 that Symantec's PCAnywhere code had been stolen six years earlier, which reinforced our need to constantly improve our security.

Google revealed the first event in 2010 when it accused hackers in China of breaking into its systems to gain access to specific email accounts and steal some of its intellectual property. The announcement came on Tim's third day at Symantec, back when he was a manager of information security. He recalls how deflated the news left him, and he wondered whether his team was fighting a war it couldn't win.

Then, in 2012, a group of hackers released a segment of confidential Symantec source code that had been stolen in 2006. The source code was already obsolete by that point, but the incident still caused us to take a hard look at how to protect Symantec holistically and our intellectual property specifically.

"When I became the CSO that was my first priority: We couldn't have a theft of our source code on a massive scale." Tim says. "Our goal was to avoid a catastrophic loss."

In the years since then, we've accomplished that thanks to an ambitious four-step plan to secure our source code: consolidate, protect, monitor and manage. Here's a quick recap of our journey, starting with a summary of our solution and followed by a discussion of how we achieved it.

The Solution, Summarized

In the summer of 2015 we finished consolidating our source code repositories into duplicate environments in Arizona and Virginia. The code now sits in what we call our "bank vault," secured by several "locks" and five additional levels of protection.

The solution takes advantage of a number of Symantec products that alert us when the source code is moved in ways that violate corporate policy (for example, if it's emailed or saved to a thumb drive):

- **Data Loss Prevention** monitors our network and endpoint layers, scanning for the exfiltration of highly confidential data
- **Control Compliance Suite** manages "risk thresholds" of IT infrastructure and provides remediation recommendations
- **Validation and ID Protection Service** provides two-factor authentication to limit unauthorized access
- **Symantec Endpoint Protection (SEP)** secures our endpoints with firewall, intrusion protection, antivirus and more to protect against targeted attacks

We also developed a policy to thwart social-engineering efforts. Specifically, we trained our engineers to be extra-vigilant when they receive requests for access to source code. For example, even when the request comes from a colleague, the engineer is required to verify the inquiry with the requester's manager.

Getting to this point wasn't easy—it took several years of strategizing, implementing and fine-tuning. But ask our executive staff if the effort was worth it and the answer is clear.

"Compared to where we were when we started, I feel a lot better now," Tim says. "We're making solid progress toward a steady protection scheme, so it'll be exponentially harder for someone to get in and do something catastrophic."

How We Got Here

As we mentioned, our four-step plan to secure our source code was to consolidate, protect, monitor and manage.

Specifically we:

1. Consolidated our repositories and migrated them to two centrally managed systems;
2. Blanketed our source-code environment in our strongest level of security technology;
3. Tracked suspicious source-code movement with security policies that were fine-tuned enough to give us the alerts we wanted, but not so broad as to overwhelm us with false positives; and
4. Managed the whole system with a dedicated staff that has granular control over the entire process.

STEP 1: CONSOLIDATE THE REPOSITORIES

The first phase was to consolidate our source-code repositories—all 750 of them, and all dispersed across the globe—into two approved, secured platforms.

One reason we had so many repositories was, whenever we acquired companies, we just kept using whatever they'd been using. Our developers liked it that way—it meant they had convenient access to their code. But the setup wasn't nearly so comforting for our Global Security Organization, which needed to keep close tabs on every single line of code to make sure it was properly secured from unauthorized access.

We'd been wanting to consolidate our repositories for years to simplify

our processes and eliminate legacy systems with known vulnerabilities. We'd delayed consolidating so as not to disrupt our development efforts, but the more sophisticated the hacker community became, the more we realized we had to act.

The consolidation process turned out to be relatively straightforward. However, we ran into some internal resistance as we began evaluating third-party vendors to provide our repository solution. Most of our developers were already using a solution by Perforce, but some insisted on being allowed to use an open-source product called Git.

At the time we dismissed Git because the open-source version wasn't robust enough for our purposes. But in the two years it took us to transition to Perforce, at least one Git-based solution—an Atlassian product called Stash (later renamed BitBucket)—became mature enough that we were able to approve it as a second option for employees. That helped quell the dissent.

STEP 2: PROTECT THE SOURCE CODE

While the consolidation project was underway, other Symantec teams were developing an ambitious strategy to encase our source code within five layers of protection: application security controls; host-based security; network security; physical security; and on the outermost level, a set of tight policies and standards.

(Some of the elements are proprietary, but we can go into greater detail at an executive briefing.)

Our developers expressed concern that the additional layers of security would slow them down. So we made sure that every new measure would allow them to work at least as efficiently as before.

"That was a very important aspect," says Suresh Sinha, who led our source-code protection program. "We were protecting Symantec's credibility in the marketplace but we also wanted to provide developers a platform to do what they do best: product development."

STEP 3: MONITOR THE MOVEMENT OF SOURCE CODE

Once we locked up our source code, we needed to make sure it was accessed only in compliance with Symantec policy. We had the perfect product to do that: Symantec Data Loss Prevention. It works by monitoring the network and endpoint layers, always scanning for the exfiltration of highly confidential data.

Our security staff programmed Symantec DLP to scan for the secret watermarks we've embedded in our code that allow us to track how the code is used.

We also set up Symantec DLP to track how other confidential data moved around our network. That turned out to be a good learning experience. The product can be set up to look for things like digits matching the pattern of a Social Security or credit-card number, or it can track certain customer information. The rules are simple, but the issue is in fine-tuning them to give you sufficient—but not excessive—information.

For example, we set up a rule to look for Columbus, a code name for an acquisition. We were flooded with alerts (everything from innocuous mentions to false positives), way too many for our team to investigate. Multiply that by scores of other rules, each producing its own avalanche of hits, and what we got was a nightmare: 10,000 alerts per day, with a staff of just six to vet them all. Needless to say, plenty of alerts went uninvestigated.

"Our initial efforts with DLP were not well thought out," Tim acknowledges. "We went through several iterations of using and misusing the solution before we figured out just how powerful it can be when it's used strategically rather than as a catch-all solution."

Here's the lesson for you: Think through your DLP tracking strategy ahead of time, before you start implementing. Know what data you want to track, and at what level of granularity. Then develop rules to get there, but be ready for a bit of trial and error. And if your rules deliver too many alerts, don't get discouraged and discontinue the rules—instead, tweak and refine them so the results are actionable. (See the CustomerONE story, "Symantec Data Loss Prevention: From Adoption to Maturity" for more about how we did this.)

STEP 4: MANAGE THE PROCESS INTELLIGENTLY

In the past, we had repositories being run variously by IT, engineering and infrastructure teams. That led to redundancies and duplication of effort, as well as inconsistency in how we responded to alerts.

We solved that by ceding all control to our Security Operations Center. Our SOC staffers know which alerts are serious and which are lesser priorities. They also know how to handle various concerns themselves and when to elevate them to other departments.

We advise customers to do something similar. By having a single point of contact, users will know their alerts are being managed consistently, by people specifically trained for the role.

We also enlisted our IT staff to help keep source code safe. Like the rest of us, our engineers are apt to let their guard down in a safe environment. They might be too trusting when someone who identifies herself as a colleague asks for access to code. Or they might take risky shortcuts as they move code from one site to another.

So in our Global Symantec Labs in Southern California, we've developed specific policies to thwart such efforts. For example, we ask engineers to be vigilant and skeptical of requests for code. We ask them to avoid giving out confidential information until they've

successfully identified the person on the other side of the phone call or email. They must document the person's request and then confirm with both the person's manager and our global security team before granting approval.

We were concerned that engineers would be reluctant to comply with vetting policies that took them away from their primary engineering roles. As it turns out, that wasn't a problem.

"They know they're working for a security company," says Thomas Teller, a senior manager with Global Symantec Labs. "They want us to have high standards everywhere. They don't want to be the weak link in the chain when it comes to maintaining the confidentiality of our source code."

Challenges

As you develop your own source-code protection strategy, be ready for two possible challenges: overcoming the technical challenge of reinventing legacy infrastructure, and finding the right staff to run your program.

For us, rebuilding our legacy infrastructure involved complicated changes to how our systems communicate with each other. We also had to figure out how to strengthen our security controls without forcing our engineers to jump through too many hoops.

These were formidable challenges, but our employees had the technical skills to succeed. But what if your staff doesn't have that same level of technical know-how?

Here's some advice from Danny Graves, the Symantec manager who helped run our source-code protection project. The key, he says, is to start with a smart strategy that's developed in collaboration with the best technical minds in your company. Then make sure you predict and plan for the sort of obstacles we've outlined, well before you encounter them.

"A task this complex comes down to project management," he says. "Involve the key members of your development community, security and IT—not just the leadership but the actual 'doers' who use these environments every day. Then sit down and agree on the best strategy to implement best practices wherever you can."

Best practices include patch management, encryption, strong authentication, endpoint protection and centralized management.

While you're working through the technical issue, prepare for a second challenge: staffing.

To do the job right you'll need a wide variety of skills—engineering leaders, project managers, Data Loss Prevention engineers, and more. All tend to be in short supply, but finding the right ones will save you time in the long run.

"We went through several iterations of using and misusing [DLP] before we figured out just how powerful it can be."

— Tim Fitzgerald, Symantec Chief Security Officer

Learn More with an Executive Briefing

This brief was intended to give you a broad look at how we keep our source code secure. Your Symantec representative can show you how to adapt our blueprint to protect your own confidential information.

For a 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

Control Compliance Suite: CCS enables risk-prioritized data center security operations and compliance through automated continuous assessments and a unified view of security controls and vulnerabilities

Validation and ID Protection: VIP delivers user-friendly authentication to protect networks, applications, and data through standards-based two-factor and risk-based token-less authentication

Symantec Endpoint Protection: SEP provides layered protection and intelligent security to guard against targeted attacks and advanced persistent threats on all endpoints

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.