CUSTOMERONE

Symantec

Protecting Our Crown Jewels with Data Center Security

In 2012, a security professional in France developed an open source tool called Mimikatz "to play with Windows security."[1] In spite of its lighthearted name, Mimikatz had a dark side: It could be used to extract plaintext passwords and other critical security information from Windows servers.[2] In the hands of bad actors, Mimikatz became an implement of destruction—one that's still effective today: In 2015, The Register (UK) dubbed it "one of the best vacuumers of Windows credentials."[3]

Although Mimikatz is one of countless zero-day threats in the world, it isn't a threat to Symantec because we use Symantec Data Center Security. DCS monitors our servers' integrity and keeps them doing exactly what they're supposed to do—and nothing else. It utterly thwarts Mimikatz's methods for scraping usernames and credentials from servers' memory. Because DCS protection is based on what the servers do—and not on the nature of the attack—we're safe even when hackers alter Mimikatz' source code (as they often do) to evade signature-based detection.[4]

"DCS is great for protecting any server, wherever it is," says security analyst Chuck Edson, our DCS administrator. "It's really powerful, lightweight, and gives us incredible control."

That's why we guard all of our servers with DCS, and why we fine-tune DCS protection on the most important ones, including domain controllers, source-code repositories, and systems that handle certificates, encryption keys, credit-card information, and personally identifiable information. Safeguarding these "crown jewels" in our environment with DCS keeps our employees safe and productive, saves money, and allows our security teams to focus on important tasks rather than log monitoring. DCS is a highly effective component of our data center protection strategy today, and positions us for the future because it protects servers and critical applications from zero-day threats wherever they run—on legacy infrastructure, in the cloud, in hybrid environments, and in our new Next Generation Secure Data Center.

This paper explains how we use DCS now, and tells how our protection has evolved and will grow. We'll tell you which servers we fully harden with DCS and why, and can share even more in an Executive Briefing.

Servers house our most valuable digital assets—our "crown jewels." Symantec protects its critical systems from zero-day threats with Data Center Security: Server Advanced.

Symantec Data Center Security protects the most important resources a company has: the business-critical servers and applications that house priceless data and enable employees to be productive every day. This paper explains to CIOs, CTOs, CISOs, and senior managers how Symantec uses DCS in its own IT environment, and includes some lessons we've learned by organizing and prioritizing our systems for better protection.

How Symantec Data Center Security Protects Critical Systems

The Data Center Security product family is a tiered offering. It starts with **DCS: Server**, which provides signature-based agentless anti-malware and network threat protection and other features. The next tier, **DCS: Monitoring Edition**, adds real-time file integrity monitoring for regulatory purposes and other capabilities. **DCS: Server Advanced** is the most powerful, full-featured tier, and the version we run internally at Symantec. We'll use "DCS" from here on to describe our implementation. (A detailed Product Matrix showing the capabilities of each DCS tier is available.)

"DCS: Server Advanced provides both application control and application isolation," says product manager Kevin Stultz. "It gives you the ability to say what is allowed to run in the data center and what privileges you give people. It's made for companies that want to take a proactive stance and lock down their most critical resources to protect from zero-day threats."

It's helpful to understand some terminology related to DCS. **Integrity monitoring** means watching critical files and processes on servers—things like registries, events, and switches—in great detail in real time; this is sometimes called **intrusion detection**. DCS integrity monitoring logs changes and forwards those logs for analysis. **Application control** discovers applications running on a system and says whether they should be allowed, blocked, or isolated. **Application isolation** uses data from integrity monitoring to wrap a protective shield around the kernel of the server's operating system; sometimes that's called **tamper prevention**. It watches for system calls to the OS kernel and allows or disallows behavior based on finely detailed policies. Application isolation can block entire processes, or be tuned to block specific arguments within those processes—including kernel calls that the operating system does not typically log.

That's a long way of saying this: Data Center Security keeps servers doing what they're supposed to do, and doesn't let them do anything else. This is valuable because, Chuck says, "A great way to hack into a machine is to find a process that's running as a service and inject something into it, or convince it to run something it shouldn't." DCS won't let a service run unless we explicitly allow it—and when it does allow a service to run, it only allows that service to do what it is supposed to do. DCS also alerts us when someone or something tries to change something important—and therefore empowers us to respond quickly and take additional protective action.

This flexibility and granular control is ideal for modern applications and the heterogeneous environments that most companies run. A single application today may be integrated with several others, and components of an application might reside in several places. Fortunately, DCS has tools that profile complex applications and servers, help determine which behaviors are legitimate, and tune the protection accordingly. (We'll tell you more about how we tune DCS on page 4.)

At Symantec, DCS is installed on systems and platforms ranging from legacy servers to virtual and software-defined infrastructures. In virtual environments, we apply DCS protection first at the host level; specially tuned protection is then automatically applied to many guest servers on the host as they spin up. (This enforces consistency and helps with virtual server performance.)

"The host has only one job to do in a virtual environment, and that's to make sure all of its guests keep running," explains Symantec senior information security manager Craig Morea. "We lock the host down with DCS so it can't do anything else. And then we go onto each guest and say, 'Your job is not to be a host; it's to run email, or run SQL, or serve a webpage.' So each guest is locked down, as well, in different ways."

To Tim Fitzgerald, Symantec's chief security officer, the ability to secure all data center resources, regardless of their environments, with a single tool results in better, more consistent security management overall. "Consistency leads to controllability," Tim says. "As we look to more modern data centers, we won't necessarily control all of our servers directly. Servers are coming up and down in the blink of an eye, whether in a software-defined data center or a cloud-based infrastructure. You need a prescribed set of controls that come up and down with them, and DCS helps us do that."

We feel safe with DCS protecting Symantec, because the best hackers and penetration testers in the world have tested it. Since 2011, nobody has been able to crack DCS: Server Advanced in "capture the flag" tests at the annual Black Hat Conference. If you'd like to learn more about those tests or how DCS fits into our overall security strategy, consider visiting one of our two Executive Briefing Centers. We'll walk you through our own blueprint for corporate security, and help you understand how to adapt our model to keep your own critical systems safe.

Data Center Security keeps servers doing what they're supposed to do, and doesn't let them do anything else.

Where We Are Today on Our DCS Journey

More than 7,600 of the servers in Symantec data centers—a mix of internally facing machines and ones connected directly to the Internet, representing a variety of operating systems—are guarded by DCS today. We protect all of them first with a foundational level of DCS integrity monitoring based on the OS.

Application isolation and control protects a subset of our systems, and a sub-subset is fully locked down, or hardened. Why not harden all of them? We prioritize our most important systems for the strongest protection based on what's most important to run Symantec.

Our base policies, which were refined from DCS' out-of-the-box policies, cover about 85 percent of the protection the servers need. To nudge that number higher for select systems, we organize and tag our servers in groups, refine group-level policies, and, as noted earlier, fine-tune protection on some individual servers and applications even further.

The lesson for you: Before you set up DCS, take time to understand which servers and applications are most important for your operations. This is time well spent—and a good fundamental IT practice—because the work will also help with your data center rationalization, budgeting, and business continuity activities.

Tuning DCS results in fewer false positive alerts, which in turn helps our security operations center and incident-response team (IRT) work more effectively. Well-tuned DCS protection also supports change control and change management goals, and adds a layer of protection against insider threats.

That's because DCS notifies our IRT whenever suspicious changes are attempted on a server. The team correlates DCS alerts with tickets in our configuration management database. "If there isn't a ticket open for service on a particular box, then a security incident can be generated and the IRT can follow up," Chuck says. "It's extra help for the people who run change control, because DCS gives them a really detailed view of not only *who's* doing something on a machine, but *what* they're doing on that machine."

How We Got Here

Symantec has run DCS (and its predecessor, Critical System Protection) for many years, but we didn't always use it optimally. Fortunately, that's changed. How we got to our current state offers some lessons for our customers, whether they're already running DCS or just kicking the tires.

Some background: For several years Symantec outsourced our IT function—including DCS operation—to a third party. During this period, the DCS server hardware became unreliable and unable to handle its workload. At the same time, we were occasionally slow to leverage new DCS capabilities that could have delivered great benefits. It didn't help that the contract with our IT vendor sometimes made it hard to change some simple DCS settings.

For those reasons, DCS limped along in monitoring-only mode for years at Symantec. Critical systems were monitored for compliance purposes, but DCS logs were simply filed away for forensic investigations. We wanted to be more proactive about securing our data centers.

So when Symantec repatriated IT operations in 2014, we brought DCS in-house, migrated to reliable, dedicated hardware, and brought on Chuck to administer it. A former technical account manager providing high-touch support to a small number of Symantec's enterprise-class DCS customers, he knew the product cold. We teamed him with Coen Bakkers, a veteran security analyst on our incident-response team who knew our environment in great detail.

The lesson for you: The right people are just as important as the right technology when you're guarding your most critical systems. Most customers need to engage with Symantec professional services or a specialized partner for training to get DCS running and develop the necessary skills.

How To Protect a Next-Generation Endpoint

Every cybersecurity company is talking about next-generation endpoint protection, but trying to nail down exactly what that those four words mean can be tough. Within Symantec IT, we think next-generation endpoint protection should:

- block threats before they get to endpoints
- prevent the takeover and exploitation of endpoint operating systems
- block threats based on file attributes, attack behavior, and relationships (including URLs, machines, users, and historical patterns)
- block threats based on policy-based detection and orchestration
- prioritize threats using global intelligence
- offer tools for discovery, correlation, and remediation of threats
- do it all with few false positives and low performance drag.

Data Center Security is part of our internal strategy for delivering this protection to our most critical systems today and in the future.

With DCS in-house today, protection of our most critical systems is both stronger and more responsive. And when we want to adjust DCS protection, we don't need to consult a contract. We simply call Chuck. "And his response is usually, 'I can have that done later today,'" Craig says.

What is Tuning?

Our calls to Chuck often result in tuning of DCS policies. At its most basic level, tuning is a five-step process:

1. Create a new DCS policy (such as one to allow DFS traffic to flow only between known good domain controllers).
2. Turn on that policy in monitor-only mode. This is the essence of *integrity monitoring*.
3. Collect and study the alerts generated by the policy for a period of time, looking for patterns. This is called *profiling* a server.
4. Adjust the policy until the vast majority of alerts generated by DCS are true *indicators of compromise*.
5. Enable protection of the system, blocking unwanted actions and allowing only normal, expected behavior.

Profiling a known good server or application lets you determine exactly how it is supposed to behave. "The more you know what normal behavior is, the easier it is for you to understand the particular alertings in DCS that you may want to turn on, turn off, or tune," Coen says. Tuning seems straightforward, but while doing it we encountered—and overcame—several challenges that are possible in many IT environments.

"The more you know what normal behavior is, the easier it is for you to understand the particular alertings in DCS that you may want to turn on, turn off, or tune."

— Coen Bakkers, Senior Principal Information Security Analyst

One of those challenges was the sheer number of events DCS can alert on. Consider: In a recent six-month period, DCS generated 120 million alerts in our environment. We whittle this data down, and make sense of it, using tools built into DCS, third-party tools like Splunk, and some homegrown scripts, but evaluating them all takes time and expertise. It's tempting in the face of a mountain of alerts to simply turn an alert off, but resist that temptation. After all, the volume of alerts reflects the granularity of events that DCS can monitor. The better way to stop them is to create good base policies, focus your efforts, and tune your protection until only true indicators of compromise generate alerts.

When sorting through DCS alerts, it helps to have expertise on the inner workings of servers and the applications that run on them. It also helps to be patient and have a penchant for organization. "I know way too much about every DLL [dynamic link library] that Windows has, and all the processes," Chuck says with a grin. "I learn everything that a process does, and then I have a choice: Do we allow this behavior or not?"

Application lifecycles present a different challenge when tuning DCS. Consider a financial application that performs specific activities only during quarterly or annual closing. If we profile that application in the middle of the month, we might miss critical operations—and if we block those operations, the application breaks. To avoid this, we sometimes speed up profiling in a lab setting. "But with financial reporting in particular, you can never be too careful," Chuck says. "If you can bring in the developers of custom applications, you'll be more successful because they know what behavior to expect."

What Lies Ahead

We have more work to do with DCS. We continually fine-tune our protection and harden servers, and we tag and group systems in ever-greater detail to further reduce false positives. We're also leveraging the DCS application-discovery tool, which can scan new Windows and Unix servers for every piece of installed software. Most important, we will be automating and orchestrating more processes using the Operations Director capabilities in DCS.

Increased automation enables our people to focus on higher-value, more complex projects rather than on repetitive tasks. For example, Coen is working on new DCS use cases that extend monitoring to command-line actions, an increasingly common avenue of exploit. "If somebody's doing PowerShell [a Microsoft task-automation framework] on a server, we will log the commands he or she is using," Coen says. "We'll determine what normal PowerShell usage is within Symantec, and what could potentially be malicious usage, and block it."

That's the tactical view. On the strategic level, we intend to use DCS to increase protection and simplify management even further as our applications migrate to next-generation endpoints such as software-defined networks, cloud environments, and application-centric infrastructure like our Next Generation Secure Data Center.

For example, a DCS base agent is built into every new server spun up in the NGSDC. Just as important, as applications are migrated to the new data center, the tuning that Chuck has already done migrates

with them. "Occasionally there are some networking changes, but I can usually tune for them in a matter of minutes," Chuck says. "The safety benefits of that time investment are incalculable."

"DCS gives [the change management team] a really detailed view of not only who's doing something on a machine, but what they're doing on that machine."

– Chuck Edson, Principal Information Security Analyst

Learn More With an Executive Briefing

This brief is intended to give you a broad look at how we use Data Center Security to protect our most valuable systems. 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.

Contact Symantec today.

SYMANTEC SOLUTIONS AND PRODUCTS IN THIS PAPER

Data Center Security: Server Advanced is the tier of the DCS product we run at Symantec. It hardens physical and virtual servers in software defined data centers.

1 GitHub entry for Mimikatz: https://github.com/gentilkiwi/mimikatz
2 Symantec security response article, June 5, 2012: https://www.symantec.com/security_response/writeup.jsp?docid=2012-042615-3731-99
3 "Thanks for open sourcing .NET say Point of Sale villains," The Register, July 17, 2015: http://www.theregister.co.uk/2015/07/17/andromeda_new_pos_malware/
4 "Many attackers lurk undetected for months, then pounce, study finds," CSO Online, Feb. 24, 2015: http://www.csoonline.com/article/2887947/data-protection/many-attackers-lurk-undetected-for-months-then-pounce-study-finds.html

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.