Look Before You Leap

DON’T JUMP INTO THE CLOUD WITHOUT ADJUSTING YOUR NETWORK DESIGN AND SECURITY CONTROLS

also

PREPARING FOR A BREACH
APPLICATION WHITELISTING
FEATURES

Are You Ready?
22 CLOUD SECURITY Migrating to the cloud requires careful retooling of network design and security controls. BY DAVID NEWMAN

Prepare for the Inevitable
31 INCIDENT RESPONSE Security breaches are going to happen. Don’t get caught flat footed. BY RAVILA HELEN WHITE

Extra Layer of Defense
39 ANTIMALWARE Use application whitelisting as another weapon in the battle against malware. BY ERIC OGREN

DEPARTMENTS

Be the Next Security Rock Star
5 EDITOR’S DESK Grab your newfound visibility by the horns and figure out how to bring oversight and direction to cybersecurity. BY MICHAEL S. MIMOSO

Signature-based Antivirus Gets a Tune-up
12 SCAN Security vendors are adding new capabilities into their products to keep up with the surge in malware. BY ROBERT WESTERVELT

Web Hazards
14 SNAPSHOT

A Chat With Marcus Ranum and Gary McGraw
16 DISCUSSION Security expert and columnist Marcus Ranum talks to software security specialist Gary McGraw. BY MARCUS RANUM

ALSO

Time to Kill the Kill Switch
8 PERSPECTIVES Giving the president power to shut off the Internet would have devastating consequences. BY PAUL ROHMEYER

48 SPONSOR RESOURCES
The new network is secure.

Of course, if government-grade network security seems excessive, feel free to ignore this message.
Be the Next Security Rock Star

Grab your newfound visibility by the horns and figure out how to bring oversight and direction to cybersecurity.

BY MICHAEL S. MIMOSO

IF YOU WANT to be the next best thing in information security, put aside all those cloud security manuals you’re brushing up on. Clear your desk of all those pesky, nasty regulations and forget trying to interpret compensating controls and whether they’ll fill a compliance checkbox for you. Forget firewall rules, encryption key management and APT. If you wanna be a rock star, figure out how to bring oversight and direction to your profession.

Figure out how to weed through the various and sundry definitions of cybercrime, cyberwar and cyberespionage and stop the confusing juxtapositioning of those three very different notions. Tell us how to reduce the signal-to-noise ration for that trio, and more importantly, clue us in as to who should respond to each, and how.

These are indeed interesting times.

Things are happening in information security… er, check that, things are becoming public knowledge in information security that indicate a seriously rapid maturation and recognition of the importance of what you do to every day life. We’re starting to see what focused, organized groups of criminal, political and military organizations can do with cyberweapons. We are understanding that the same cyberweapon used to take down a banking website could be the basis for a much more powerful tool that could inflict damage on critical infrastructure. My zero-day vulnerability that is open to a SQL injection could be your zero-day that spins a uranium-enrichment centrifuge into oblivion.

My zero-day vulnerability that is open to a SQL injection could be your zero-day that spins a uranium-enrichment centrifuge into oblivion. No other industry works this way; faulty Toyota gas pedals won’t shut off electricity to the West Coast of the United States.

You wanna be the next security rock star? Figure out how to respond in a big-boy voice to this dynamic. Realize that criminals are opportunists and will move on to the next target if your security is too strong. Realize that a state-sponsored intelligence operator probably won’t move on, and instead will jab and poke and probe until he ruptures your defenses (that’s what money and patience will do for ya). Realize that while yes the attacks might be the same, the risk aversion and ultimate response might
be totally different. For years you wanted to be heard, well this is your time to shout.

This is a turning point, an inflection point—and the point is that this opportunity for security professionals, practitioners and experts that cannot be wasted. Since the start of 2010, we’ve had Operation Aurora, Stuxnet, HB Gary, the further development and sophistication of the Zeus Trojan, and several countries on the brink of revolution taken off the grid. The Internet is a platform not only for economy, but it can be used anything society can dream up; even crime and warfare. And it’s been done at a speed few dreamed possible a decade ago. Today is the time for legislative and executive guidance. Serious discussion has to be held on ground rules of incident detection, response and reporting beyond the four walls of your corporation.

Maybe you knew that, for example as in the case of Stuxnet, an infected USB stick could derail a country’s nuclear program for a half-decade. Maybe you knew that the cat-and-mouse game between the U.S., China, and Russia over intellectual property and strategic national documents has been going on for years. Maybe you knew that security companies were running clandestine operations for the U.S. government.

The bubble on your self-contained world of network security and compliance reporting has burst. Information security is going to go mainstream; hell, even Stephen Colbert riffed on HB Gary. And funny thing, this is what you wanted all along. It used to be you wanted a regular sit-down with the CEO to explain why what you do matters. Data breaches and the resulting compliance made that scenario real. Don’t wait for another incident get out in front of this. It’s time for the security industry to turn its visibility into a positive, flex some muscle, and make sure the right people have the right information to make the right call.

Michael S. Mimoso is Editorial Director of the Security Media Group at TechTarget. Send comments on this column to feedback@infosecuritymag.com.
We’re paranoid as well. We just call it prudence. Backed by every major security certification, we can help design and install the right security solutions for you.

Trust no one except us at CDW.com/security
Time to Kill the Kill Switch

Giving the president power to shut down the Internet would have devastating consequences. 

BY PAUL ROHMeyer

Among the most intriguing storylines to emerge from the crisis in Egypt related to attempts by the Egyptian government to tightly control the flow of information in and out of the country. The reaction of the Egyptian government to the social unrest included the intentional disruption of voice and data communications, resulting in what appears to be the first intentional deployment of a “kill switch”—the shutdown of Internet access—by a central government as a political tool. Simultaneously, there has been continued debate over the merits of the so-called “Internet kill switch” within the U.S., described by proponents as an important tool to blunt widespread cyber-attacks.

Despite recent reassurances by policymakers such as Sen. Joseph Lieberman that an Internet kill switch is not in the nation’s best interests or immediate future, political winds change quickly. Therefore, the information security industry would be well served by explaining some of the many reasons why the concept should be mercifully euthanized and eliminated from discussion about cybersecurity guidance, regulation, and policy.

First off, enabling the shutdown of even a piece of the U.S. Internet architecture would be an overly broad technical control that is unmatched to any observable technical threat. Public statements asserting the need for such capabilities have relied on vague descriptions of the risks the kill switch is intended to mitigate. Supporters are similarly unable to point to actual past events to demonstrate any need for such high-impact capabilities; they haven’t clarified what sort of attacks that would achieve a threshold to require a shutdown of Internet capabilities by government.

The nature of the distributed Internet architecture, the availability of multiple Internet...
access mechanisms, inexpensive peer-to-peer capabilities, and the subjective nature of technical threats and vulnerabilities, among other factors, make the implementation of kill switch capabilities practically impossible. Supporters of the concept seem to ignore, or disregard, the depth of integration of U.S. business, government, and general public resources with the Internet.

The U.S. Senate Committee on Homeland Security and Governmental Affairs last June asserted the president already was granted kill switch powers under the Communications Act of 1934, and suggested that a proposed law, S. 3480, Protecting Cyberspace as a National Asset Act of 2010, would establish limits on broad presidential powers. Intended to quell “myths” about S. 3480, the committee’s memo raised more questions than it answered. For example, it didn’t explain the characteristics of a bona fide “cyber emergency,” yet asserted that the threat of a catastrophic cyberattack is not a matter of “if” it will happen but rather a matter of when. The document failed to present any examples or scenarios where disconnecting service would actually protect assets or aid recovery.

Another important consideration is that the legal, business, and political landscapes have certainly evolved quite a bit since 1934, and a law intended to control a first-generation, centrally managed, land-line telephone system may not be applicable to the present context. The degree of reliance on telephone service in 1934 did not at all approach the level of dependency business, governments, and citizens have on the Internet today. Early telephone systems provided support for voice communications, whereas the Internet is arguably the single most important business resource for many organizations. The phone system of 1934 was also the product of a closely regulated monopoly that enjoyed true ownership and control over all architectural assets.

The Internet, on the other hand, is largely a system of standards and interface rules that enable communication between diverse information resources which are owned by numerous private entities that rely on it to offer services in a competitive, global private sector. Therefore, any federally-directed shutdown would disrupt intrastate and interstate commerce, as well as international businesses. The global economy includes U.S. companies that provide contracted services to foreign customers; the capability of government to halt Internet communications would threaten the ability of private enterprises to deliver global services. Likewise, a shutdown would technically cripple organizations that have embedded cloud computing and other virtualized resources into their architectures as they would be unable to function without appropriate connectivity.

The mantra of “just shut it off” is not a particularly well-designed technical control and its inclusion in any regulation suggests either a lack of understanding of the architecture and our reliance on it, or the existence of other non-stated goals. Kill switch capabilities would provide very little in the way of protection against genuine cyberthreats, but would certainly succeed in delivering even more power to the federal bureaucracy and potentially severe and unnecessary
disruption to businesses. It may not be much of a stretch to conclude the kill switch could be a formidable political tool, although it may not be a very effective one, as seen when Egyptian citizens applied technical innovation to overcome the shutdown, such as using voice-to-text services to maintain a social media presence.

Ours is government of checks and balances, and the separation of powers is codified in our system of governance on the federal and state levels. Overstepping the U.S. Constitution in the name of theorized cyberthreats would be harmful, disruptive, and of little genuine cybersecurity benefit. A kill switch ignores the property rights of the private sector owners of the systems and resources the Internet relies on. It’s a poorly conceived control that reflects a fundamental lack of understanding of Internet architectures and risks on the part of its proponents. And that seems to suggest cybersecurity is perhaps not the primary objective.

Paul Rohmeyer is a faculty member in the graduate school at Stevens Institute of Technology. He provides technology risk management guidance to firms in the financial services industry, and previously held management positions in the financial services, telecommunications and pharmaceutical industries. Send comments on this column to feedback@infosecuritymag.com.
Penetration Testing Software for:
- Web Applications
- Network Systems
- Endpoint Systems
- Wireless Networks

Find the gaps in your vulnerability management program...
Click here to download a free gap analysis tool.

CORE IMPACT® Pro provides the missing link in your vulnerability management program.
- Identify exploitable vulnerabilities
- Prioritize critical exposures and risks
- Map attack paths across IT layers
- Eliminate false positives
- Assess end users against phishing attacks
- Comply with PCI, FISMA/NIST, HIPAA and other mandates

Learn more:
Visit www.coresecurity.com
or call us at (617) 399-6980
Signature-based Antivirus Gets a Tune-up

Security vendors are adding new capabilities into their products to keep up with the surge in malware. 

By Robert Westervelt

SECURITY EXPERTS and now executives at security vendors are in agreement that signature-based antivirus isn’t able to keep up with the explosion of malware. For example, in 2009, Symantec says it wrote about 15,000 antivirus signatures a day. The number has increased to 25,000 antivirus signatures every day.

“Signatures have been dying for quite a while,” says Mikko H. Hypponen, chief research officer of Finnish-based antivirus vendor, F-Secure. “The sheer number of malware samples we see every day completely overwhelms our ability to keep up with them.”

Security vendors have responded by updating their products with additional capabilities, such as file reputation and heuristics-based engines. They’re also making upgrades to keep up with the latest technology trends such as virtualization and cloud computing.

New and constantly changing malware variants have forced antivirus vendors to respond, says Chris Christiansen, an industry analyst and program vice president for security products and services at IDC. He says reputation technologies provide a far more predictable way of enhancing security.

“Users we’ve been talking to have been complaining endlessly about how a variety of the signature-based technologies have been failing them,” Christiansen says.

Hypponen says F-Secure takes the layered approach, using different scanning engines, including file reputation and heuristics engines, to attempt to detect nefarious activity, but he adds that “no solution is 100 percent effective and no one claims to protect against everything.” Application whitelisting, which was once seen as the answer to antivirus’ failure to keep up, also is not the panacea, Hypponen says. The technology isn’t effective against document exploits, including those that target Microsoft Word or Adobe Reader. “You can’t whitelist all known good documents,” he says.
Just prior to RSA Conference 2011, Symantec announced planned updates to its endpoint protection suites, which include support for VMware's API for virtualization. Like F-Secure, the security giant also added heuristics and reputation-based engines to monitor potentially malicious file behavior. Piero DePaoli, director of product marketing, calls the company’s SONAR technology “advanced,” and says the behavioral reputation engine (acquired by Symantec in 2005) can detect whether a file is acting suspicious. The feature helps block new exploits targeting zero-day flaws, he says.

The system is being tested on more than 100 machines at Temple University. Seth Shestack, associate director of information security at Temple, says the latest version seems to be detecting malware before any malware signatures are developed. The machines on average get a 12- to 36-hour lead time on detecting new malware variants over traditional detection methods, Shestack says.

Trend Micro CEO Eva Chen says signatures are going to continue to be needed to protect computer users, but new technologies can help bolster the effectiveness of signatures. “It needs to be a cocktail solution,” she says.

Chen says Trend has long used reputation technology, offering a threat detection appliance she developed that supports antivirus by monitoring files on the network for anomalies and tracking the destination of the files to detect problems. The goal is to provide technology that is “content aware, context aware and location aware,” Chen says.

“There’s monitoring and risk management that you should put in place,” Chen says. “If you get infected, we can tell you early that you’ve got strange activity going on in your network.”

Trend Micro also is tackling the issue of what Chen calls “antivirus storm” with its newly configured protection of virtualization hypervisors. Traditional antivirus doesn’t work in virtual environments, she says, because if one virtual machine performs a scan, all the other machines stop working.

“This scanning is very I/O intensive, because all the virtual machines are sharing the same I/O bus and the same memory ports,” Chen says. “This is a big headache for the security and the virtualization people.”

About six months ago, Trend added support for VMware’s virtualization hypervisor API so the company doesn’t have to load its agents on all the virtual machines. A smart agent embedded into the VMware API can do the scanning of all the machines, greatly reducing performance issues, Chen says.

“There’s monitoring and risk management that you should put in place. If you get infected, we can tell you early that you’ve got strange activity going on in your network.”

—EVA CHEN, CEO, Trend Micro
Web Hazards by Information Security staff

Web surfing is seemingly becoming more treacherous than ever. According to researchers at Web security firm Dasient the number of websites infected with malware nearly doubled in the last quarter of 2010 compared to the last quarter of 2009. They estimate that more than 1 million websites were infected in Q4 2010. After three months of Web browsing, the probability that an average Internet user will hit an infected page is approximately 95%, assuming that user views 100 pages a day, according to Dasient.

Source: Dasient
Teaching you security...one video at a time.

Traditional learning methods have always been about flooding students with as much information as possible within a given time frame -- often referred to as 'drinking from a firehose'.

The Academy Pro allows information security professionals to learn about today's most important technologies on demand and at their own pace.

Check out The Academy Pro at www.theacademypro.com

Sponsored by:

www.theacademypro.com

The Academy Pro © Owned by Black Omega Media Group Incorporated
Marcus Ranum: Do you think the emphasis on mega-frameworks like Google Toolkit or Ruby or (insert favorite Web2.0 technology here) is going to improve the state of software security, make it worse, or be neutral? I’m really torn between writhing with discomfort at the idea of these large code-masses that are being used in lots of important places—it’s just too complicated to get it all right!

Gary McGraw: Both. The gigantic frameworks themselves can make analysis of a system that includes them a lot harder. If you think about automated static analysis for code review, the frameworks lead to a big ‘whack-a-mole’ game: the data flow goes in and it pops back out again in any number of surprising places. On the other hand, if you do the right thing from a static analysis perspective, you can sometimes pre-compute where the mole is going to pop back out and use that to your advantage. Frameworks can help with security too—enterprises that create frameworks of their own, and apply those consistently for their developers have been having pretty good luck. That’s because the notion of standardization within a business is a good way of getting away from the bespoke (build it by hand slightly different each time) nature of software within an enterprise.

Marcus: So you think we’re getting the main value out of code re-use? That’s pretty much what the software engineering guys were saying would happen, back in the 1980s. Is it paying off?

Gary: I think in the case of code and particular bugs, yes. That’s because the frameworks, in my mind, have more to do with code than with architecture.

Marcus: Can you elaborate on that a bit? It seems like architecture is always going to be fairly purpose-specific—so, short of having a “framework for a Web banking app” that’s basically COTS plus some tweaking required, programmers are pretty much doomed to
have to build their code upward from basic building blocks. The building blocks get bigger and more powerful so now they’re fully rendered graphical interfaces, or a database for storing formatted objects, but the innovation has to always happen at the level of architecture or you’re just producing “me too” applications. I don’t see any way that you can make a framework that will prevent you from making business logic mistakes.

**Gary:** One of the other problems, which is one that Ross Anderson and others have pointed out for years, is the notion of trying to program “Satan’s Computer.” You can have all sorts of perfectly constructed components and put them together into a disaster of an insecure system. That’s why we joke that the best software security in the world would involve taking away somebody’s keyboard.

**Marcus:** You winced when I said “business logic mistakes” — did I misspeak?

**Gary:** There are two kinds of defects in software that lead to security problems. One kind is bugs: did something stupid with `printf()` or made an ‘off by one’ error. Such bugs are localized in code and can be analyzed pretty easily: “Marcus needs to learn how to wield `printf()`” or even “let’s search our entire code-base for uses of `printf()`.” Then there are flaws: architectural problems that are not found in the code—they’re design issues.

Over the years we’ve gotten quite good at finding bugs but we’re still not so good at finding flaws. Making the flaw-finding process automatable or at least cheap enough that it doesn’t take really experienced guys to find them is our current challenge. We’ve gotten so good at finding bugs that we forgot that the split is about 50/50 between bugs and flaws. So, when we get excited because we’ve found and fixed a lot of bugs, what we’ve really done is gotten a better measure of how bad things really are. Let me give you a really good example of a flaw that I’ve seen in real code that we couldn’t detect using bug-hunting techniques: forgot to authenticate user. You can do code reviews all day and you’ll never catch that one.

**Marcus:** I know this is one of those “grey-bearded old programmer” questions, but what about the availability of code quality tools? It seems that the newer stuff doesn’t have much in the way of CASE (Computer Assisted Software Engineering — remember that?) tools. Back in the ’80s, we had these things called “debuggers” that don’t appear to even exist for Web apps. I’ve written about some of my experiences working with SABER-C, a C language interpreter that used to do fantastic error-checking—I used it as a checker, bug-squasher, and regression-testing tool. In fact, I still have an old SPARC with a copy of SABER-C that I keep in case I ever need to do any more C coding. These were tools some of us learned that we couldn’t live without—but the Web2.0 generation seems comfortable with “hit reload and if it looks like it works, put it into production!” That’s got to have an impact on security.

**Gary:** I agree, but it sort of depends on your environment. Some of the IDEs have some beautiful stuff built in, but usually you have to know that the capabilities are there and to turn them on. But I agree with you, there’s a whole bunch of stuff that we built for understanding software long ago and ironically, the attackers are using it to greater advantage than the people
who should using it to understand the software they are building! A case in point that you brought up: debuggers. My favorite example, though, is coverage tools. If you talk to most QA people and say “Hey, do you guys use coverage tools?” and they look at you like a cow at a new gate, “Whuut? Huh?” A coverage tool helps you determine which parts of code you’re running during a test. So it gives you some insight into how good your tests are. Coverage also turns out to be very helpful for attackers. Suppose you know that there’s a certain potentially vulnerable system call way down there in the code (something like lstrcpy( ) in win32), your next job is to figure out how to create a control flow that will tickle that bug—a coverage tool is super for doing that.

Marcus: What do you think about “fuzzing”? I was just at the RSA conference and there were products there that do Web application testing using that technique. I guess you point the box at a target and it tries to inject stuff into every Web form and see what happens, and so forth. Is this just another ‘badness-o-meter’ or does it tell you something useful about your security?

Gary: Fuzzing is a very interesting technology. You may not recall that I wrote this tome on software engineering back in 1998 called Software Fault Injection—it was all about providing some inputs and tweaking the input, then having observable conditions in your code, and seeing what happens. Fuzzing is kind of a subset of that. It’s easier in some conditions than in others—for example, it’s pretty simple to fuzz the UNIX command line, because of how they’re invoked. You can just vary command options and pipe unexpected stuff into the command’s input or just send bits. It’s also pretty easy to fuzz protocols, especially stateless network protocols of the HTTP variety. What’s harder and way, way more interesting is applying fuzzing technology at the APIs of components or the APIs of big classes in your object-oriented code-pile. The thing is it takes some real knowledge to be able to build fuzzing capability at that level because you need to understand what the system will accept and build a sort of grammar to fuzz the API. That is an incredibly powerful technique and it turns out that there are many product security organizations in enterprises that use that technique as part of their software security regimen.

Marcus: That reminds me of a wonderful talk at a USENIX back in the 1980s on errors in processors’ math libraries. It turned out that the errors predictably come in close to edge-cases—if you’re in a 32-bit architecture you can guess that the mistakes will come around +/- 2^32 and 2/31. It’s just like assuming that if you’re collecting data from a network connection, you should probably be prepared to handle more than BUFSIZ worth of data in a single line, etc. Knowing where you make your mistakes and knowing
how to avoid them is what separates the programmers you want working on your applications from the ones whose keyboards you want to take away.

**Gary:** In some sense that’s related to fuzzing but what you’re really talking about is boundary condition testing and limit testing. If wielded properly, such testing brings an enlightened tester as close to a “security testing guy” as he or she can get.

**Marcus:** I think you’ve talked me around about the point of fuzzing, because I was feeling a little bit dismissive of those products when I first saw them.

**Gary:** Some kinds of fuzzing I share your skepticism about. If your Web application is falling prey to tests that are really stupid, then you’ve got a bigger problem. If we automate a bunch of security tests and we run them against a piece of software and it finds problems, then we know one thing about that software—it really sucks. That’s a great thing to know, if you discover it in time before you ship! The problem is if you treat that same set of canned tests as a “security-meter” and, if you find no results of interest, saying, “well it must be secure.” Then you’re crazy. That’s why I coined the term “badness-o-meter.”

**Marcus:** What’s the current status of your work with The Building Security In Maturity Model (BSIMM)?

**Gary:** There are a whole bunch of large corporations in many different verticals that are trying to tackle the software security problem from an institutional perspective. The way they’re trying to do that is by creating software security groups that have the authority, responsibility, and budget to solve the software security problem. They’re taking a multi-year run at it, and the BSIMM is a study of 33 of those large enterprises’ initiatives. We’re not trying to make a prescriptive model of software security or a methodology like the Touchpoints; we’re just describing what we see — so there’s a big difference between BSIMM and something like Microsoft’s Security Development Lifecycle (SDL). The SDL purports to tell you how to do software security—it’s prescriptive. The BSIMM is just a descriptive measurement tool; it says, “everybody does this — do you?” It’s just about observable facts.

**Marcus:** The implication, though, is that there’s going to be some kind of recommendation. Isn’t that what people are going to take away? People will jump from “everybody does this” to “well, these guys are doing this, and their software’s pretty good, so maybe that’s what we should do, too!”

**Gary:** Maybe so. A lot of companies, like Microsoft, have learned a lot about doing software security at the enterprise level in the last 10 years, and it’s worth seeing who’s doing what and providing those data for you to use as you see fit. Sometimes very confused application security “experts” out there say “well you don’t really need a software security group, you know” but the
BSIMM reveals that though maybe you don’t need one, everybody who is doing this seriously has one. It’s sort of a pile of facts for you to weigh against your possibly stupid opinions.

**Marcus:** Let’s switch topics to something a bit more consumer-oriented. What about the “app stores” that are proliferating everywhere? I bought an iPad the other day because I like the idea of changing the software installation/purchase lifecycle from “here’s a computer with everything pre-installed” to picking and choosing (and paying) for the code I want and having it more or less automatically maintained. It seems like a potentially big win with the “walled garden” model but there’s a great looming question about keeping malware out of the walled garden. That seems to be a serious software security issue as well, no?

**Gary:** The problem with many of the app stores nowadays is that they do relatively little to identify “who wrote that stuff” and whether they were supposed to write it or if it’s malicious. There’s very little testing going on. In fact I’ve heard some stories recently, including this one: there was an app in the Google Android app store that claimed to be a “Bank of America” online banking app, and it was not even written by or distributed by Bank of America. Of course it still asked for your credentials…!

**Marcus:** I guess it also raises the issue of your software supply chain. Some of these apps are being contracted out by companies and aren’t being developed in-house. So I suppose you’ve got the potential that a business could push an app into an app store under its own name, and later discover that they had fed malware to all their customers. It seems to me that app stores are pushing some businesses into being software publishers and they haven’t yet realized that. There’s a big difference between having a website with possible security problems, and pushing possibly insecure or malicious code to your entire customer base.

**Gary:** I don’t think that this notion of “little apps in an app store” is going to miraculously solve the software quality problem or the software security problem.

**Marcus:** Darn. Isn’t there some chance that the app store will be able to disable or revoke software that’s determined to be bad? Perhaps there’s some ‘safety in numbers’ we can still take advantage of.

**Gary:** I think that in return for whatever slender advantage you might get that way, you’re giving up a great deal of freedom to run what you like. I feel like the iPad device is a sort of castrated computer: It’s good for displaying content, but it’s not full-featured enough if you want to create content. So what you will find emerging is the people who these lightweight systems appeal to tend to be consumers and/or PowerPoint watching executives rather than content creators. That has implications for security, as well, since a creator is a more serious target than a consumer.

**Marcus:** Gary, as always, a pleasure!
Find the cybercriminal.
(Never mind. ArcSight Logger already did.)

Stop cybercriminals, enforce compliance and protect your company’s data with ArcSight Logger.

Just downloaded the customer database onto a thumb drive.

Learn more at www.arcsight.com/logger.
CLOUD COMPUTING PROMISES many benefits: It can reduce IT costs and downtime while vastly increasing storage, mobility, and provisioning options. It’s also a potential security nightmare: perimeters disappear; clients and servers move around at will; and old models of access control, authentication, and auditing no longer apply.

All these challenges can be met, but any migration to the cloud requires careful planning. Cloud computing fundamentally changes long-standing best practices in network design, encryption and data loss prevention, access control, authentication, and auditing and regulatory compliance. To prepare their network for the cloud, organizations need to take stock of their infrastructure and adjust their practices and processes accordingly.
START WITH THE PLUMBING

A common misperception about cloud computing is that moving services to an off-site provider will reduce bandwidth requirements. In fact, the reverse is often true: Cloud computing can increase bandwidth requirements due to increased Internet connectivity. A move to cloud computing also has implications for virtualization and the suitability of existing security infrastructure and security policies.

To understand how cloud computing can radically shift network and security requirements, consider a common hub-and-spoke network design (see Figure 1). Here, branch offices connect with one or more enterprise data centers where key applications reside. There’s a well-defined perimeter to the public Internet, and the bandwidth, latency, and packet loss characteristics between sites are easy to measure.

In contrast, cloud computing involves Internet connectivity for every site in the enterprise (see Figure 2). Here, given that applications now reside in the cloud, there is no clearly defined perimeter. Further, the traffic characteristics of every site’s Internet connection may affect application performance. As a result, some organizations find a move to the cloud results in increased requirements for bandwidth and security monitoring.

Beyond basic network characteristics, there’s also the question of what kind of traffic leaves the enterprise as it moves to cloud computing. Understanding what kind of traffic you have is just as important as knowing how much traffic you have. If net-
work flow analysis—which uses existing flow-reporting tools in routers and some switches to provide an in-depth view of application traffic—isn’t already deployed, this would be an excellent time to consider implementing it.

To be fair, this is an extreme, strawman example of cloud network design. Hybrid designs are more likely, with branch-office Internet connectivity still channeled through one or more internal data centers. Even so, cloud computing means key applications are reached via new connections outside the enterprise. Testing the network characteristics of these new connections is critical.

**NETWORKING AND VIRTUALIZATION**

Virtualization is a key enabling technology for cloud computing and data center consolidation. Well before moving to the cloud, many enterprises have adopted virtual servers as a means of saving on hardware, increasing uptime, or both. For these organizations, migrating a virtual infrastructure to the cloud can have a significant impact on application performance.

Consider vMotion from VMware, which moves virtual machines (VMs) between host servers with virtually no downtime perceived by users or applications. This is truly the “killer app” for virtualization; network managers like vMotion because it’s such an easy, hitless way to move VMs around.

For all its benefits, though, implementing vMotion into the cloud can affect application performance. First, there’s the issue of bandwidth: vMotion requires lots of it, and assumes a high-throughput, low-latency network. It’s possible to use vMotion to move VMs across slower wide-area network links, but not with its zero-downtime benefit. This could be an issue when using vMotion between an enterprise staging site and the cloud provider, or even within the cloud provider’s network if that encompasses multiple physical sites. Either way, if network managers want to avoid VM downtime, ensuring close proximity of VMware hosts is a must.

Second, vMotion generally requires source and destination VMware host servers to reside within the same layer-2 network (that is, within the same broadcast domain). This isn’t a problem even in large data centers, which deliberately create very large broadcast domains to accommodate virtualization. However, it could be an issue in moving VMs across different IP subnets, for example between an enterprise and the cloud provider. Suitability for vMotion should be a part of any network design review. The same caveats apply for vApps, which does for applications what vMotion does for VMs.

**IMPACT ON SECURITY DEVICES**

If Internet traffic increases with cloud computing, then so too will the load on security devices such as firewalls, VPN concentrators, and IDS/IPS appliances. This has implications both for
pure performance and for security policy. The performance piece is simple: Increased Internet connectivity means a heavier workload for security devices. It’s great to upgrade to, say, a 100-Mbit/s Internet connection as part of the move to cloud computing, but if existing security devices are rated only to 10 Mbit/s, they will quickly become a bottleneck.

Depending on security policy, a move to the cloud may require enabling additional IDS/IPS signatures, and this too can have a negative performance impact. Network Test has conducted multiple performance assessments of multifunction security devices where forwarding rates drop by a factor of 20x or more when IDS/IPS signatures are enabled. VPN devices such as IPSec or SSL concentrators also can degrade throughput and increase latency.

Other policy issues to consider include interoperability and changes to existing firewall rule sets. Cloud providers have their own security devices, but long experience with IPSec and SSL VPN troubleshooting suggests interoperability isn’t a given. Even though both IPSec and SSL are based on open standards and may work flawlessly inside a multivendor enterprise network, there’s no guarantee of interoperability with a cloud provider’s equipment. Similarly, firewall and IDS/IPS rule sets will change as enterprises move more applications into the cloud, possibly affecting other parts of the firewall rule set in unexpected ways.

Testing can help validate a move to the cloud, provided it’s done with a meaningful workload. When it comes to performance measurement, some security appliance vendors perform tests using overly simple workloads. It’s possible, for example, to test a firewall the same way as an Ethernet switch, and then only with large packets. However, this isn’t a very stressful load; it will produce impressive numbers for a data sheet, but it’s not representative of enterprise traffic.

A better practice is to model the particular mix of applications that will reside in the cloud, paying particular attention to transaction sizes, transaction durations, concurrent connection counts, overall bandwidth utilization, and network characteristics such as latency, jitter, and packet loss. With these key metrics in hand, it’s possible to craft a synthetic workload that will yield meaningful predictions about security device performance for a given enterprise.

**ENCRYPTION AND DLP IMPLICATIONS**

As noted, cloud computing changes or eliminates the concept of a perimeter, and that has profound implications for encryption and data loss prevention (DLP).

Prior to cloud computing, network managers were mainly concerned with a single set of encryption endpoints between customers and Internet-facing servers (see Figure 3). That changes with cloud computing, where there are now three sets of encryption endpoints to consider: from customer to Internet; within the cloud; and from cloud to enterprise (see Figure 4). Encryption within the cloud may be necessary for regulatory compliance, or because a cloud
The provider’s network may span multiple physical locations.

There’s no one right approach to where to apply encryption in the cloud model. The simplest approach of encrypting everything from end to end sounds appealing, but also has the unintended consequence of “blinding” some key security and network management tools such as application-aware firewalls and deep-packet inspection devices. Encryption everywhere also can complicate DLP, where the imperative is to maintain visibility of where data is sent and stored.

As usual, policy is the right place to begin in redesigning encryption and DLP for the cloud. At a minimum, a cloud-aware security policy should specify that traffic never leaves the enterprise unencrypted. Security policies should be revised to add requirements for detection of any breach of the encryption policy, including within the cloud provider’s network.

Similarly, a cloud migration is an ideal time to review policy as to permitted protocols. A revised policy should banish, once and for all, insecure protocols such as FTP that allow cleartext transmission of passwords and other sensitive data. At the same time, policy also should specify which users can employ protocols that might leak data over encrypted protocols such as SSH and Secure Copy (SCP).

A revised policy should banish, once and for all, insecure protocols such as FTP that allow cleartext transmission of passwords and other sensitive data.

A redesigned DLP infrastructure can actually help solve some encryption problems by automating many processes. For example, DLP systems can automatically encrypt files attached to email and monitor traffic for files sent outside the enterprise using email or instant messaging. File-level encryption is also an option.

One final question to consider is whether the existing encryption and DLP infrastructure is adequate for cloud computing. Even if no upgrade to encryption and DLP is deemed necessary, network managers should consider how to implement these services within the cloud: As VM versions of existing appliances, as hardware devices between VMs and the network, or some combination of these.
A DIFFERENT ACCESS CONTROL MODEL

Cloud computing also changes long-standing concepts about access control. Historically, enterprises have used IP-centric access control models, where rules were based on criteria such as source and destination subnet addresses. That doesn’t make much sense in a cloud context, where users can connect from anywhere, on any device, and where servers may be cloned or move around within the cloud.

Cloud computing changes access control from an IP-based to a user-based model. Essentially, cloud computing adopts the network access control (NAC) credo that who you are governs what resources you can reach. Because both clients and servers can be mobile in cloud computing, a dynamic approach to security policy is needed. Access control in the cloud should follow the NAC model of applying rules dynamically, in real time, as endpoints appear on the network. This approach is equally valid for clients and servers.

Of course, user-based access control supplements but does not replace the old IP-centric rules. Any sound migration strategy should include a review of existing access control lists (ACLs) on enterprise routers. It may make sense to rewrite and tighten ACLs so that inbound traffic for key applications comes from, and only from, the cloud provider. Similarly, new rules may be necessary to enable users to reach newly migrated applications in the cloud.

AUTHENTICATION REQUIREMENTS

Cloud computing stretches authentication requirements, both figuratively and literally. Anywhere, anytime client connectivity may require new, stronger forms of authentication. At the same time, the move to place services in the cloud extends the trust domain enterprises need to protect. For both clients and services, strong control over password and key management is a must, as is better break-in detection.

With cloud computing, clients no longer cross a single, well-defined security perimeter before being granted access to enterprise resources. Clients also may connect to these resources from shared public networks such as Wi-Fi hotspots, increasing the risk of password interception. A move to two-factor authentication, for example tokens plus some biometric mechanism, makes sense to ensure clients are properly authenticated. Some well-known public cloud services such as Google Apps also support passwords plus tokens for authentication.

Password synchronization is also important. Maintaining separate sets of user accounts and passwords, one apiece for resources in the cloud and in the enterprise, is not a sound practice. Besides the added administrative overhead, two sets of accounts also inconveniences users and doubles the likelihood they will write down one or both passwords and save them in public view. A single sign-on system covering both enterprise and cloud-based user accounts can help here.
There’s also an imperative to protect authentication mechanisms in the cloud, including both passwords and API keys. Many cloud services make use of representation state transfer (REST) Web services, which in turn use API secret keys for authentication. This raises a couple of potential risks. First, REST security can poorly implemented. For example, a security researcher has demonstrated how a major hosting provider transmits the secret key in plaintext as part of an authentication request. Although the request must be made over SSL, any compromise of either side of the SSL tunnel would also result in loss of the secret key.

Second, even in a well-designed system the API key represents an extremely valuable resource, with serious consequences if it’s lost. For example, enterprises on Google Mail identify themselves to Google’s servers using an API key associated with the entire enterprise, not individual users. If this secret key were stolen, an attacker could impersonate any email account or share any Google document associated with the enterprise. Sound practices to protect the API key include encryption and a software audit to review API usage.

A review of IDS/IPS and DLP configurations also is in order. If signatures to detect cleartext transmission of passwords aren’t already in place—for example, in IMAP and POP email—they should be added.

**COMPLIANCE COMPLICATIONS**

At least initially, cloud computing complicates the security auditor’s job, since the systems and processes to be audited will be much more widely distributed. And there are certain to be regulatory considerations when it comes to moving sensitive data to and from the cloud.

Logging and monitoring is critical in the cloud, but also more complicated, with large cloud providers’ networks spanning multiple continents. While this has the advantage of moving content closer to users, it complicates timestamp synchronization between server logs. Without rigorous time synchronization among servers, troubleshooting becomes very difficult. Setting all system clocks in a single time zone, such as coordinated universal time (UTC), also is essential for taking the guesswork out of distributed log analysis.

A move to the cloud may increase the number of servers involved, especially where virtualization’s cloning features are used, and this in turn increases the volume of logs to be analyzed. Network managers may want to consider implementing a unified log analysis system to collect and synthesize data from all the new sources.

Various regulatory regimes require data sanitizing as data moves to and from the cloud. This is similar to the encryption issues previously discussed, where cleartext transmission might be acceptable within a secure data center, but is never permitted across a public network. The Payment Card Industry Data Security Standard (PCI DSS) specifications for credit card handling offer a well-known example of data sanitizing. Among other things, these specifications require credit card data to be encrypted, obfuscated, or deleted before storage.
Cloud providers must be PCI-compliant to handle such data, and also must have auditing measures in place to maintain that compliance. To mitigate risk, enterprises also should require insurance coverage on the cloud provider’s part in the event of a data breach in the cloud, and build such coverage into any service contract.

In some cases, enterprises may have more rigorous compliance requirements than a cloud provider can meet. This isn’t necessarily a dealbreaker for a given cloud provider, but it may require the enterprise to implement its own compliance framework within the cloud.

Cloud computing’s benefits are real: a lower IT profile, faster provisioning, and global availability of new services. At the same time, network managers need to think carefully before making the transition. Every challenge discussed here can be resolved, but each will require careful planning before and during the move to the cloud.

David Newman is president of Network Test, an independent test lab and engineering services consultancy based in Westlake Village, CA. He is the author of IETF RFCs on firewall performance measurement and many articles on network device performance and security. Send comments on this article to feedback@infosecuritymag.com.
Get Comprehensive Network Protection - including Application Control!

WatchGuard’s new Application Control for XTM appliances allows businesses to control what’s being used on their networks – from Facebook to Skype – for tighter security and increased productivity. With sophisticated behavioral analysis and more than 2,300 signatures, it allows IT to control over 1,500 web 2.0 and business apps with ease.

- Find out how you can take back control of your network with our free white paper at www.watchguard.com/appcontrol.
- See how WatchGuard outperforms every other major UTM brand on the market at www.watchguard.com/utmmarketreview.

For more information, call 1.800.734.9905 or visit www.watchguard.com. Get red. Get secured.
Security breaches are going to happen. Don’t get caught flat footed.

Most IT leaders now know they must align with the business in order to be successful. However, one area where organizations continue to slip up is incident response planning. Enterprises spend copious amounts of time developing security policies and processes in order to secure systems and prevent breaches and data loss. Yet when a security breach occurs, they typically don’t have a process in place to manage a coordinated response, within IT and external to IT.

There are a variety of reasons organizations may not have a coordinated incident response plan. Perhaps the organization has invested in IT security, which is about technology, rather
than information security, which focuses on strategy and business process. Part of that business component is incident handling. While incident handling is tactical in nature, it is driven out of program strategy and is a process to manage tactical responses.

**INCIDENT HANDLING DEFINED**

Information security incident handling is an action plan for dealing with: intrusions (internal/external), cybercrime (copyright violations, hate crimes, child pornography etc), disclosure of sensitive information or denial-of-service attacks.

For those of you who are familiar with the Information Technology Infrastructure Library (ITIL), you may wonder what the difference is between ITIL’s incident management and information security’s incident handling. A fine distinction exists in the fact that ITIL does not prepare an organization to deal with events that may result in litigation. Additionally, where the root cause of an event in IT service management may be shared with customers, events which require infosecurity incident handling are typically confidential and considered “need-to-know.” The final distinction lies in the difference between an event vs. an incident. ITIL defines any event that causes business disruption to customers or end users as an incident. In information security, events that require incident handling are related to security.

If your organization has implemented ITIL, work to integrate the concepts of information security incident handling within your incident management process. Beyond promoting a common response for all events which disrupt services, there is the opportunity to embed security events as a normal part of business operations. In other words, it can act as a diffuser for you and your staff in that you are not the lone purveyors of seemingly bad news to the business. It is accepted that incidents of a security nature will occur and the appropriate rigor is in place for management.

**PREPLANNING CONSIDERATIONS**

Security incidents are unexpected regular events—the computing world’s oxymoron. Any organization with a connection to the Internet or that uses computers can expect to experience unexpected security events on a regular basis. Why? There are always vulnerabilities found and mistakes made; the regularity occurs with each release of software and each action taken by a technology user.

Due to the unexpected and stressful nature of security related events, be prepared to devote your time and attention to the management of the incident. Detailed forms must be completed and descriptive notes taken. Likely, you will identify different types of security incidents resulting
in specific procedures for each type of incident. However, it’s unlikely your employer has the capacity to employ individuals whose primary responsibility is incident handling. Competing responsibilities reduce incident handling at its best to an ad hoc maturity level. Even with training and the right forms and procedures to guide you, it can be challenging to capture information correctly or follow instructions. Cooperation beyond the doors or IT is essential.

TEAMWORK REQUIRED

Incident handling is not an IT process but a business process that must be supported by the legal, human resources, communications and physical security teams of your organization. Relationships must be built with these teams and expectations set in order to avoid conflict. Information security may drive the leadership of incident handling and provide the necessary training, however a governance board of sorts should be assembled to oversee the process. Legal and HR must be involved to validate the legal soundness of your program to ensure non-reputation of evidentiary data, which is a costly process.

Best-of-class technical environments are required to establish non-repudiation of evidentiary data. Dedicated hardware and specialized software is required along with training on the use of the software. Combined with the possibility of infrequent use, your business partners—the legal, HR and other teams—may challenge cost effectiveness. Be prepared to provide transparency around the cost of people, process, and technology. For organizations with regulatory obligations, the long-term investment should be part of the ROI strategy for selling incident handling. If your organization does not have regulatory obligations, brand protection and reputation are legitimate considerations.

Discretion is an important element of information security incident handling. In ITIL’s incident management process, outages and their root causes are shared with customers and business partners openly. In contrast, information security incident handling requires the discretion of all involved parties. Casual bandying of security incidents among employees can reduce the trust of internal business customers. More importantly, should the information find its way to customers or partners external to the organization, damage to brand, reputation and trust will occur. Remember the principle of need-to-know (N2K) when handling incidents. Never talk to the press in response to a security incident unless directed by your legal team and senior leadership. Also, you can mitigate organizational Chatty Cathys by providing ongoing education and training.

Review all policies related to appropriate use and technology. While you may not directly write policy, you should familiarize yourself with your organization’s policies. Suggest additional policies supporting your incident handling plan. For example, work with the IT team to implement standards that will support the process. Some of the most seemingly granular
discrepancies, such as overlooking clock synchronization or log retention policies, can undermine the information you’ve gathered.

**BUILDING OUT YOUR PLAN**

Different types of incidents require different types of handling. Determining the response plan prior to an incident will streamline handling. Identify what types of incidents you may have to handle:

- Malware breach and containment
- Information disclosure
- Employee investigations
- DDOS attacks
- Hostile take-over

This may also be an opportunity to scope communications; knowing who needs to know in advance will help in avoiding unnecessary disclosure. For example, a DDoS attack does not require Need-to-Know (N2K): Most likely, sharing the cause of a network interruption with everyone will not damage brand or reputation.

Determining response plans prior to an incident will also help you pick the appropriate tools for recovering information. Identify what types of technology you may have to handle through technology scoping:

- Client PC technology
- PDA technology
- Cell phones
- Server technology
- Infrastructure technology
- Routers
- Switches
- Firewalls

Develop forms that will help you capture the information that is required for collection during an incident; SANS has a number of sample incident handling forms. Identify what types of documentation you will need to handle an incident through documentation scoping:

- Contact log—names of each point of contact during the incident;
- Evidence log—data points of information collected during the incident;
- Chain-of-custody log—audit trail of collected evidence when it changes hands;
- Communication log—information about incident and contact during initial incident notification;
- Sanitation record—information required for sanitized media;
- Recovery record—steps taken to recover from incident;
- Eradication log—steps taken to remove malware or hostile user;
- Identification record—type of incident and who discovered it.
PREPARE A TOOLKIT
Incidents can occur any time. You need a toolkit that provides access to all documentation required to capture incident information from beginning to end. When network compromises occur, you may not have the luxury of retrieving electronic documentation from the network. Having printed documentation ensures the information you capture is as accurate as possible. You must have the same documentation at home. Incidents are not considerate; they may happen at 3 a.m.

When possible, request dedicated technical resources, such as a spare drive for imaging

Costly Mistakes
Do not allow mistakes to derail your incident handling program. Below are some of the most common and costly errors that undermine incident handling.

- **Disorganization**: Incident handling is useless if you do not have a plan or the appropriate forms for recording incident information. Waiting to develop a plan once an incident has occurred will result in disaster.

- **Rushing incident resolution**: When an incident has occurred, it’s important to dedicate adequate time to understand how the incident occurred in the first place. If the investigation is rushed, it may result in missing critical information or reintroducing a compromised system into your infrastructure.

- **Lone Ranger syndrome**: Relying on your skills and expertise without engaging others. Depending on the maturity of your organization, you may have to champion incident handling, but it’s better to at least have the framework for a team and share that with proposed team members than to mishandle an incident and be left holding the bag.

- **Discounting Johnnie Cochran**: If we assume that we will end up in court, then you should also assume that the court will want to understand how you collected your information. Litigation is all about proving or disproving a person’s information. When you cannot provide documentation that would be expected of our industry, then all your handling may have been useless, along with your legal counsel and public relations.

- **Violation of need-to-know**: Anyone who knows about the incident may have to testify in court. Stories vary in times of stress or through misinformation. Only those directly required to have knowledge of an incident should be briefed. Even then, tell them only what they need to know. Let your legal team determine whom outside of IT should be apprised.

- **Tunnel vision**: Incident handling is more than just a detailed task; it’s a business process. Take a strategic view when approaching incident handling.

—RAVILA HELEN WHITE
and a spare workstation for gathering logs and performing other forensics tasks for incident handling. It is important to establish non-repudiation of the information you’ve gathered. Even if you cannot justify a dedicated server for storing recovered information, request storage that has limited access. Require periodic audits of the storage area controlled by keycard access to establish enforcement of access.

When handling incidents that require physical evidence recovery, store the hardware in a location that is secure, with limited access. You must also consider what collection tools you will use, such as log file analyzers, disk imaging, and forensics software. Select commercial tools for information capture. Open-source tools are cool but organizations should purchase commercial tools to establish non-repudiation. If you do choose to use open-source tools, clearly document them as part of your toolkit.

**NOTE-TAKING BEST PRACTICES**

Take good notes, but keep in mind that lengthy notes containing unnecessary information are not helpful and will only muddy the incident should it result in litigation. Notes must be informative, concise, and contain the facts of what you are handling. For instance, it is not necessary to mention that you are dealing with a suspected embezzler/child pornographer/information thief, etc.; this is where your forms will assist. Complete generic fields prior to handling an incident. Record only those facts related directly to your evidence recovery:

- **Who** — contacted you; performed information recovery
- **What** — was recovered (e.g. log files)
- **When** — date and time of recovery
- **Where** — location of recovered evidence
- **How** — tools and method for evidence recovery

---

**Consider Certification**

Incident response training pays off quickly.

Consider investing in training for at least one person in your organization. The dollars spent are easily returned the first time you must respond to a security breach.

The SANS Institute has a great reputation for providing incident handling training. Certification as a SANS GIAC Certified Incident Handler is certainly a step in the right direction to ensure your organization can recover from a security breach or respond adequately to a litigious event.

There are legal implications related to incident handling. Therefore, remember that whether you are certified or not as an incident handler and receive training, you need to partner with your legal counsel to implement and, if necessary, supplement the organization’s incident handling program.

—RAVILA HELEN WHITE
POINTS TO KEEP IN MIND

Any incident involving the recovery of information or technology associated with employee misconduct should be reported to your resident legal counsel. They will make the call regarding the appropriate actions to take. You should also notify legal should a third party who’s been entrusted with your data experiences a breach resulting in exposure.

Remember, incident handling is a business process that requires a plan. You will need a thorough understanding of your organization to propose and implement a systemic plan. Once a plan is in place, update the process regularly. Just as disaster recovery plans and backups should be tested, so too should incident handling procedures. This will ensure that the kinks are worked out prior to an incident.

Understand your responsibility. Incident handlers get into trouble when they go beyond the bounds of what is appropriate for their role. Only ask questions related to capturing relevant information. Beware of acting as a proxy to HR and legal when it comes to dealing with people. Do not go beyond the role of an incident handler. It’s more trouble than it’s worth.

Ravila Helen White is the director of enterprise security and architecture at a company in the Pacific Northwest. Prior to that, she was the head of information security at The Bill & Melinda Gates Foundation and drugstore.com. Send comments on this article to feedback@infosecuritymag.com.
THE ULTIMATE ENTERPRISE THREAT AND RISK MANAGEMENT PLATFORM.

The ArcSight ETRM Platform is the world’s most advanced system for safeguarding your company against data theft, complying with policies and minimizing internal and external risks. Finely tuned to combat cybertheft and cyberfraud, the ArcSight ETRM Platform gives you better visibility of real-time events and better context for risk assessment, resulting in reduced response time and costs.

Learn more at www.arcsight.com/etrm
APPLICATION WHITELISTING is an idea that makes too much pragmatic sense for it not to have appeal as an anti-malware mechanism. Intuitively, a technology operating in the kernel that detects suspicious changes in an IT controlled software configuration should be a simpler and easier to scale solution than a technology that looks at all files to identify and clean all attacks known to the world.

Application whitelisting (AWL) came into the security scene several years ago with an active approach to combat the relentless success of malware infiltrating endpoints. Signature matching antivirus has been overmatched in keeping pace with the volume of new attacks. While antivirus diligently scans to detect attacks against its blacklist of malware signatures, attacks continue to sneak through, undetected by security software.
In contrast, AWL validates that the program the user requests to run is on the IT-approved software list and analyzes the integrity of the program before making an allow or block decision. The whitelist approach of approved applications and programs has to be considered a valuable, manageable, and effective layer of defense that can complement the attack blacklist approach favored by antivirus vendors.

Unfortunately, application whitelisting followed the path of host intrusion prevention, with vendors positioning the technology as a replacement for antivirus. This has confused enterprise security organizations and created a competitive environment where security vendors are not cooperating effectively to solve a critical business problem for customers.

Fortunately, there has been traction within enterprises for a coordinated defense of application whitelisting and antivirus products in the fight against malware. There are practical ways that companies can use AWL today to improve their endpoint security. And with some improvements, the technology could serve as a significant layer of a larger endpoint management strategy in the future.

**NO ANTIVIRUS KILLER**

The surge in malware creates expensive problems for businesses by placing regulated data at risk and disrupting IT operations to clean infected devices. Application whitelisting tries to tackle the problem based on these premises:

- **Only malware changes programs without IT knowledge.** Malware needs to modify executable programs to launch attacks and survive reboot cycles on the endpoint. A pragmatic alternative to scanning for malware is to simply detect changes to programs that are not associated with patches or software upgrades.

- **Identifying compliant configurations is easier than identifying malware.** Through the first three quarters of 2010, McAfee Labs reports identifying more than 14 million unique pieces of malware, a rate of more than 60,000 new infections per day, continuing the trend of year-over-year growth in malware. Intuitively, checking a list of valid software configurations in real-time is a smaller problem to solve than checking files for traces of malware.

- **The concept of trusted sources, fueled by feeds from software vendors, simplifies management of compliant configurations.** Platform vendors, especially Microsoft, automatically supply application whitelisting vendors with detailed information on the files contained in released software products. This relieves IT of the burden of having to figure out what is legitimate system software enabling IT to focus on defining approved custom applications.

However, the shared belief that there must be a better way to secure endpoints led to the unfortunate positioning of application whitelisting as an antivirus replacement. Every application whitelisting vendor believed that AWL would put AV on the road to obsolescence.
Ultimately, the technology has not been able to supplant the antivirus grip on endpoint security because it does not by itself fundamentally solve the malware problem. AWL has proven to be very effective in the hands of skilled IT, but there are flaws that impact usability and security that have yet to be overcome:

- **Most organizations cannot lock down user endpoints.** The concept of locking down IT policy-compliant endpoint configurations sounds good in theory, but in practice users need the flexibility to install applications and personalize their PC. Too tight a lockdown of the endpoint disrupts user productivity; too light a lockdown weakens the security benefits of application whitelisting.

- **Many threats are delivered as active code through the browser and do not modify whitelisted programs.** Application whitelisting is good at making allow or block decisions when a program is launched, but cannot easily make decisions on active code that is delivered to the browser. The problem will get worse as users become more dependent on browser-driven applications. For example, the number of social networking users actually surpassed email users last July, according to a report by Morgan Stanley. The browser is now the target of choice for malware developers.

- **IT security teams are forced to decide on which user applications should be allowed or blocked.** IT must not only deploy and administer an additional endpoint security product, but it must also make timely allow/block policy decisions on user application requests. Although automatically allowing applications from trusted sources saves time, security teams must be willing to commit extra time for application whitelisting support.

Application whitelisting vendors have been challenged to establish AWL as a vibrant segment of the endpoint security market. Lumension, McAfee, and Microsoft have integrated application whitelisting into next-generation endpoint security and management solutions, while Bit9 and CoreTrace remain as major independent whitelisting suppliers. Thus far, enterprise security teams have spoken via product purchase decisions and the verdict is that application whitelisting is finding broader appeal as a key element of a comprehensive endpoint security strategy rather than an outright replacement for antivirus.

There are important business considerations that application whitelisting has not been able to overcome. The first is that the technology is an incremental product to purchase and administer. Enterprise security budgets for endpoints are committed to antivirus, and that is not going to change with compliance mandates and the absence of reasonable alternatives. In addition, application whitelisting has been unable to overcome resistance from the antivirus industry with its lucrative subscription revenue streams to protect. While antivirus vendors are in the business of protecting endpoints, they must be careful in not de-valuing their solutions by being too quick to embrace innovative approaches. For instance, most AV vendors will tell
sales prospects that they have whitelisting; they’ll also say it’s not application whitelisting that makes allow or block decisions on program launch requests, but rather a performance-enhancing technique indicating that a file has been unchanged since the last scan (so only new signatures need to be checked). It’s hard to imagine many AV vendors admitting that they need application whitelisting when their business depends upon scanning for attacks. This resistance has caused confusion among IT decision makers.

**BEST PRACTICES FOR THE SHORT TERM**

There is no question that application whitelisting works well to protect executables, providing a defense against zero-day attacks and custom attacks that evade antivirus detection. AWL backs up AV and will detect unauthorized modifications to programs and enforce security policy, either allowing the program to run or blocking execution of the program. AWL’s ability to look inward towards compliant software configurations for symptoms of an attack provides a complementary layer to AV’s ability to mitigate damage from identified attacks. In the short term, organizations leveraging the combined strengths of both approaches will significantly enhance their resistance to malware outbreaks.

- **Use application whitelisting to secure system-level components and antivirus to vigorously scan other programs.** Best practices call for locking down critical software against unapproved changes, blocking execution of explicitly unauthorized user-installed programs, and closely monitoring the use of all other programs. Programs delivered from trusted sources that are unmodified copies from the distribution media do not need to be scanned for attacks. Security teams can focus the separation of security powers by coordinating application whitelists with antivirus exclusion lists to reduce functionality overlap and increase performance.

- **Evaluate integrated management of endpoint security technologies.** Vendors are integrating application whitelisting, antivirus, patch management, and application intelligence into single endpoint security management consoles. An integrated approach can save administration time and effort, and also ensure that there are no gaps in security coverage.

- **Prioritize computing assets requiring application whitelisting defenses.** Mission critical command and control stations, IT operations and service desk computers, and sensitive servers are more appropriate for cooperative AWL and AV solutions than devices that require a higher level of user application customization. Start deploying application whitelisting to bolster antivirus defenses on devices that are needed to keep the technical infrastructure operational, even in the face of a new attack.

**AWL’s ROLE IN FUTURE SECURITY STRATEGIES**

The concept of a balanced approach to endpoint security with application whitelisting is compelling, with the technology evolving to support emerging endpoint security strategies. There has to be a significant role for application whitelisting to play as organizations evolve their physical devices, deploy virtualization services for desktops, and shift their infrastructure into the cloud and handheld devices. While it is not clear what direction application
whitelisting will take, these are some areas that demand attention in order for whitelisting to remain viable in the future:

- **Extend the concept of trusted sources to include applications and active code from Web downloads.** While this may sound like a tall order, electronic storefronts such as Apple’s already employ a form of application whitelisting; an iPad or iPhone will not allow an unauthorized program or modified program to run. AWL vendors can federate trusted sources, perhaps with reputation-based services, to provide more protection against browser-based attacks.

- **Automate reporting of application intelligence.** It will take years for organizations to evolve to application-centric firewalls. However, application whitelisting already produces intelligence on actual application usage on a user by user basis. Reporting application intelligence derived from whitelisting through systems such as a SIEM or protocols like the Trusted Computing Group’s IF-MAP would provide organizations the application information they need to streamline network processing without having to refresh their firewalls.

- **Add the ability to transparently replace infected software elements.** Virtualization allows IT teams to automatically replace non-compliant software; as software becomes more disposable, the emphasis will shift from identifying and cleaning attacks to detecting change and replacing software. Whitelisting is a technology that is perfectly suited to provide attestation of infected software.

---

**Taking a Different Tack**

Customers of Cisco’s defunct host intrusion prevention software are turning to application whitelisting.

**Many users of** the now retired Cisco Security Agent are replacing their CSA host intrusion prevention (HIPS) software with application whitelisting. The HIPS promise was to by correlate file, network, and operating system activity to detect the presence of attacks that evade antivirus, and leverage the IT-defined policy rule set to block further execution of the attack. With AWL, the focus shifts to protecting executable software and file, network, and system resources by blocking the ability of zero-day attacks to execute. AWL is a simpler model based on the premise that only malware makes unauthorized changes to programs.

The critical weakness limiting broader deployment of Cisco CSA and HIPS in general is the need for IT to define and maintain a complex rule set to enforce security policy. Since IT owned the rule set, any software upgrades or new software installations would generate trouble tickets to the security service desk for re-calibration. The Cisco CSA administration effort was difficult to scale to large distributed organizations. The AWL administration burden is significantly lighter than CSA since there is no longer a need for IT to define and maintain complex rules defining acceptable file, network, and system activity.

In many ways, the application whitelisting ability to thwart malicious code fulfills the goals for host intrusion prevention. Companies that added a HIPS layer to their endpoint security to complement antivirus now have an opportunity to evolve that strategy to application whitelisting.

—ERIC OGREN
services to ensure the integrity of virtualized software. In addition to enforcing allow/block policy decisions, IT would be able to automate the recovery from attacks with an additional “replace and allow” decision. The ability to replace infected or obsolete elements would fundamentally change endpoint management strategies, and it would be enabled by whitelisting’s ability to detect modifications.

- **Enrich antivirus subscription services.** The winning application whitelisting vendor will find resources that can be added to AV subscription services. AWL and AV vendors have the security of user endpoints as a common interest, even though they take opposite technical approaches. The motivation is there on both sides if application whitelisting vendors can show a plan that protects the antivirus business model. Perhaps AV vendors can stream reputation scoring for AWL to act on active code requests, or AWL can upload application configurations to streamline AV scanning. Enterprises need application whitelisting and antivirus to work together; the sooner that happens the better it will be for everyone.

Application whitelisting vendors are researching ways to add most of these capabilities in their products. Right now, though, AWL solves a hard problem of detecting the presence of unauthorized software before it can execute to launch an attack. It is not—and will never be—a replacement for antivirus. However, application whitelisting approaches will be a critical element in the evolution of endpoint security strategies. With foresight and execution, application whitelisting is well positioned to reduce the impact of malware.

---

Eric Ogren is founder and principal analyst of the Ogren Group, which provides industry analyst services for vendors focusing on virtualization and security. He previously served as a security industry analyst for the Yankee Group and ESG, and has also served as vice president of marketing at security startups Okena, Sequation and Tizor. Send comments on this article to feedback@infosecuritymag.com.
The average organization is now exposed to more than 50 malware incidents per month. And traditional anti-virus software detects less than 20% of all new malware – increasing your endpoint TCO.

Break with the status quo and start securing your data and your dollar with Lumension® Intelligent Whitelisting™.
COMING IN
MAY

Data Protection
If your organization handles, processes and stores credit card information or personally identifiable customer information, then federal and industry regulations play a large role in how your infosecurity team establishes policy and creates processes for data security. This feature will guide you through the policy, process and technology decisions you need to make to build a successful data protection program that addresses PCI-DSS and state privacy laws.

Social Engineering
Today’s targeted attacks start with careful reconnaissance by the attacker in order to infiltrate an organization. This article will look at how attackers are using scamming to their advantage, provide examples of effective social engineering, and explain how security managers can build processes to help fend off these attacks and ultimately keep company assets secure.

International Regulations
With the global economic downturn, many companies have shed their geographic silos in favor of a streamlined centralized data infrastructure to achieve cost synergies. This feature looks at how companies can navigate data security and privacy across international borders.

Don’t miss our monthly columns and commentary.
what drives your approach to IT security?

Balancing business priorities and risks is key to a solid approach.

SystemExperts helps you build a comprehensive and cost-effective information security plan that makes sense for your company. Right now, our ISO 17799/27002 Compliance Program helps you to focus resources on your most important business risks and comply with regulations such as Sarbanes-Oxley, FFIEC, HIPAA, PCI, and Gramm-Leach-Bliley. Best of all, our approach works equally well for “Main Street” businesses and the Fortune 500 clients we’ve proudly served for years.

If you want a practical IT security plan that addresses your real business risks, contact us today at 888.749.9800 or visit our web site at www.systemexperts.com/public.

- ISO 17799/27002 Compliance
- HIPAA and PCI DSS Compliance
- Application Vulnerability Testing
- Security Audits and Assessments
- Security Architecture and Design
- Identity Management
- Penetration Testing
- Security Best Practices and Policy
- Emergency Incident Response
- System Hardening
- Technology Strategy
- ASP Assessments
SPONSOR RESOURCES

See ad pages 21, 28

- ArcSight Customer Success
- First Annual Cost of Cyber Crime Study - Benchmark Study of U.S. Companies
- Integrate Enterprise and Cloud Security for a 360-degree View of User Activity

See ad page 7

- Entrusting Endpoints
- Guarding the Gateway

See ad page 11

- CORE IMPACT Pro V11 Download
- Continuous Enterprise Risk Measurement White Paper
See ad page 4

- Five Best Practices to Protect Your Virtual Environment
- Alternatives for Securing Virtual Networks
- Nielsen Mobile Case Study

See ad page GH

- Think Your Anti-Virus Software is Working? Think Again
- Intelligent Whitelisting: An Introduction to More Effective and Efficient Endpoint Security
- Lumension® Intelligent Whitelisting™ Overview

VERISIGN™

- Webinar: Managed DNS - Using Hybrid Routing to Optimize DNS Performance
- Benchmark your Company's Infrastructure Protection: Take the Executive Threat Assessment
See ad page 30

- **Compare WatchGuard head to head with all other major brands**
- **See how Data Loss Protection can help your business avoid embarrassing situations**