

Marc Appelbaum from Vonage Discusses Their Use of the Imperva SecureSphere Web Application Firewall (WAF)

Listen to Podcast [here](#).

Brian Contos: Welcome to the Imperva Security podcast. I'm Brian Contos, chief security strategist for Imperva. If you would like to learn more about this subject and Imperva, visit Imperva.com, check out our [blog](#), follow us on [Twitter](#), or send us an e-mail at blog@imperva.com.

Joining me today is Marc Appelbaum. Marc is a manager of information security for Vonage, a leading provider of broadband telephone services. Marc is responsible for all information security functions for Vonage worldwide. Under Marc's leadership, Vonage has deployed several security initiatives, including a global vulnerability management program, a global security information management system, and security awareness programs.

Marc has developed policies and procedures that now involve the security team in all technology projects. Marc also maintains the responsibility for ensuring IT compliance with all government and industry regulations, such as SOX, PCI, CPNI, and others.

Vonage is an Imperva customer, and part of Marc's responsibilities is managing the Imperva SecureSphere Web Application Firewall.

Welcome to the show, Marc.

Marc Appelbaum: Great. Thank you very much for having me, Brian.

Brian Contos: So Marc, before we get going, it's been a few months since we were together on the east coast. What's new? What are you working on these days?

Marc Appelbaum: We finished up some compliance audits, and now we're kind of taking a look and see how we improve upon things and kind of optimize. We put a lot of infrastructure in place last year, so we want to build on that and improve things. Some of the things we're going to look to improve is, really, with the web app, creating more functionality out of it, looking at our vulnerability scanning and expanding what we're doing, just not for compliance but looking at other areas in the infrastructure.

Brian Contos: So your infrastructure is a global one, is that correct?

Marc Appelbaum: That's correct. We have collocation facilities across the US, Canada, one in Mexico, actually, and a few in the United Kingdom.

Brian Contos: So it's no small feat when you're going after these projects.

Marc Appelbaum: No, we take into account, pretty much, we deal with several thousand servers in our devices. Again, not including the customers' devices, which reach about 2.6 million homes.

Marc Appelbaum from Vonage Discusses WAF

Brian Contos: 2.6 million homes. Wow. So Marc, I've got to ask: how critical is application security for you now, and has that changed in the last couple years?

Marc Appelbaum: I think it's incredibly critical now, and I think it's risen to the forefront in the past several years, with the data breaches, and things like SQL injection and cross-site scripting have really brought things to the forefront, especially with the advent of Web 2.0 web services extending XML out to the edge and making our applications more available.

Brian Contos: Yeah. Web 2.0 certainly adds so much usability from sort of a user-experience perspective, but it does open up a Pandora's Box, if you will, of security concerns if you don't think about it early on, doesn't it?

Marc Appelbaum: Absolutely. That's why several of those things we put in place last year actually include ensuring that a security team's involved in projects in the beginning so we can do an analysis prior to things rolling into production, because the last thing we would want to do is, say, open up some new product and find flaws after it rolls out into production. So we're trying to cut things off in the early stages of development.

Brian Contos: So Marc, I know that you're a proponent of WAF, and of course, you leverage Imperva's SecureSphere Web Application Firewall. What are some of the key value points you see?

Marc Appelbaum: I think the first key, Brian, is the fact that it's always there. It's always on. It's constant application security, whereas other things, such as code reviews, or even vulnerability scans, are point-in-time snapshots of an environment. The WAF is always looking at the traffic that's traversing it. It's always monitoring for vulnerabilities. It's constantly being updated through your application defense center. And in our case, we could add custom rules as we need, or if we're looking for certain, specific items or safe entries, we could look at that. But I think the key is that it's always there. It's not a point-in-time snapshot. It's constant protection.

Brian Contos: I've said this on some shows before, but this whole notion of defense in depth and code reviews and black-boxing and white-boxing and security development life cycles, I think it's all critical. It's all important. But at the end of the day, that's all stuff you do before you flip the switch on and it's facing your customers. At that point, you have to have other mitigating controls to audit, to monitor, to block, when you're in the middle of the game, right? And hopefully all that prep has helped, but it's certainly nice to have the WAF augment that, isn't it?

Marc Appelbaum: Exactly. The augmentation, I think it complements the other practices that you do in development and QA. You can only catch so much. And the fact is, new threats come out every day, so having that defense at the edge, to be able to write custom rules, or just to be updated on a routine basis of new signatures, gives an added layer of security. There's no silver bullet, so I think bringing all this stuff together, they complement each other.

Brian Contos: So you've been using WAF for some time now. I'm wondering, do you have any interesting use cases that you might be able to share with us of how you're leveraging it or things you've seen or been able to prevent or protect?

Marc Appelbaum: Some things we've seen and we're looking at to go further is, obviously, the standard SQL injections, cross-site scripting that we're all getting hit with. But we're just trying to take it to a different level and look at patterns from various IPs that

Marc Appelbaum from Vonage Discusses WAF

will help not so much prevent but detect phishing attempts and other attempts to defraud customers. We're trying to look at certain patterns from various IP addresses to see if they fit a profile that we're developing, to say, "You know what? This looks like it may not be legitimate customer traffic." Other uses that we've talked with other colleagues as well as law-enforcement partners are the ability to look for specific patterns that may be of interest to law enforcement. Not that we're doing that today, but that's always something that we could leverage.

Brian Contos: Interesting. So you're taking the analytics that you're getting from the WAF, and of course you're using them from an organizational perspective, to protect your assets, but at the same time you're seeing if there's some value-add that you can then deliver outward to your customers and maybe partners that, of course, you don't control the security for.

Marc Appelbaum: Correct. It's great that we protect ourselves, but how can we help everybody else? We all need to kind of form a little community and try to help each other, at the end of the day.

Brian Contos: What are some of the other complementary technologies that you used with web application firewalls? I know there's a myriad of things that various organizations will connect to their WAFs. What are some of the things that you've looked at or you're currently using today with your WAF?

Marc Appelbaum: We're sending, actually, data from the WAF to our security management system so it can be correlated with other events from our standard intrusion detection centers and our vulnerability scanners. So that way we bring all the data into one place and we can normalize it, still use the WAF for the analytics that it does, but then be able to take that day and correlate it with, say, a Snort signature, or if we note that a web server has a particular vulnerability, we can raise the score of an alert to send out to our operations center. So that's kind of how we're trying to tie it in today. Some things I could see in the future is leveraging database monitoring. We have database monitors in place today. It would be really nice if we could trace that whole transaction so that we could follow user A through the entire flow of a process. So I think that's something that we're going to be looking at in the future. But today, the fact that we can correlate data and we can bring it to a central repository is critical, not just for the compliance; it helps us in understanding the environment a little bit better.

Brian Contos: Now, Marc, for those folks that are listening who might be new to application security or web application firewalls, if they're working for an organization and they're looking at some steps they can take to increase their security around their web application environment, what are some suggestions that you'd give them? What's some of the low-hanging fruit that they can address first?

Marc Appelbaum: I would really get a vulnerability scan of that application, and not just a vulnerability scan but an application-layer scan, whether you use WebInspect or an nCircle or a Qualys, but look at that application. Operating systems, we all understand. People have gotten pretty used to patching operating systems by now. The sheer fact is many people don't look at how their applications are getting configured. If you're running a web server, start looking at that Apache server: how is that built? Or that IIS: how are you building that? And then move out from there. What applications are you laying on top of that? How are you building them? Are you building them with security in mind?

Marc Appelbaum from Vonage Discusses WAF

If I put a house up and I just put security in the roof or the walls and the foundations aren't strong enough, it'd kind of collapse at the end of the day. So if I start with a solid foundation of the operating system's secure, the middleware, the application server's secure, and now I build my application and I scan it and I test it, I have a better chance of having a stronger application, at the end of the day. Then you could add the web application firewalls.

I mean, all that just comes together. If I just have a web app firewall, but I have the ability to root the operating system or root through Apache on a Linux box, I'm not really doing anybody a service. I need to look at all of that. So the core application security is really, if we focus on the application and we think of the things that add extra layers and don't rely solely on the network to provide security, I think we have a better posture, as an entity.

Brian Contos: Yeah. I've been hearing a lot about the integration of WAF with application-level vulnerability scanners more and more. And it seems like many organizations are now saying, "Look, we're going to do the code review and the scanning and all that upfront, but we're going to run the web application firewall as well to ensure that we're monitoring and protecting while we're in production." But at the same time, they want to connect these two so it's a closed loop. So maybe you scanned it last month. Maybe you're scanning it again this month and you discover something new. So that information can be fed back into the web application firewall, perhaps while code fixes are being put in place, while things are being patched, et cetera. It seems like a real nice marriage of vulnerability assessment and web application firewall.

Marc Appelbaum: Absolutely. It gives you the best of both worlds. Let's say I put up a new web server. And maybe it wasn't fully patched, or the Apache's not exactly up to standard. But if I add that vulnerability scanner, I can now augment the rules to say, "You know what? This version of Apache has vulnerabilities X, Y, and Z, " I've written rules to at least alert on that and stop the attack, like I said, I bought myself some time to go back and fix that code. And as we both know, every day there's new vulnerabilities coming out, and so you can't keep up with it on a day-to-day basis. There's a development cycle involved in that. So, again, you just buy that buffer. And I think the key is you have to buffer. It's not this silver bullet pegged to the solution.

Brian Contos: Well, Marc, it's always great getting real, live web application security practitioners and managers on this show to talk about their life experiences. Thanks so much for joining us today.

Marc Appelbaum: It was my pleasure, and thank you for having me.

Brian Contos: If you would like to learn more about this subject, and Imperva, please visit imperva.com. For questions or comments about this podcast, please send an email to blog@imperva.com, and follow us on Twitter for the latest Imperva news.



North America Headquarters
3400 Bridge Parkway
Suite 101
Redwood Shores, CA 94065
Tel: +1-650-345-9000
Fax: +1-650-345-9004

International Headquarters
125 Menachem Begin Street
Tel Aviv 67010
Israel
Tel: +972-3-684-0100
Fax: +972-3-684-0200