The Next Line of Defense — How Security Leverages Virtualization to Counter Sophisticated Threats

Transcript of a discussion on how adaptive companies are leveraging their virtualization environments to become more secure and reduce cyber risks.

Listen to the podcast. Find it on iTunes. Get the mobile app. Download the transcript.

Dana Gardner: Welcome to the next edition of BriefingsDirect. I'm Dana Gardner, Principal Analyst at Interarbor Solutions, your host and moderator.

When it comes to securing systems and data, the bad guys are constantly upping their games -- finding new ways to infiltrate businesses and users. Those who protect systems from these cascading threats must be ever vigilant for new technical advances in detection and protection. In fact, they must out-innovate their assailants.

Today's BriefingsDirect security insights discussion examines the relationship between security and virtualization. We will now delve into how adaptive companies are finding ways to leverage their virtualization environments to become more resilient, more intelligent, and how they can protect themselves in new ways.

Roemer

To learn how to ensure that virtualized data centers do not pose risks -- but in fact prove more defensible -- we are joined by two security-focused executives.

Please join me now in welcoming Kurt Roemer, Chief Security Strategist at Citrix. Welcome, Kurt.

Kurt Roemer: Thanks, Dana.

Gardner: We're also here with Harish Agastya, Vice President for Enterprise Solutions at Bitdefender. Welcome, Harish.

Harish Agastya: Hello, Dana.

Gardner: Kurt, virtualization has become widespread and dominant within data centers over the past decade. At that same time, security has risen to the very top of IT leadership’s concerns. What is it about the simultaneous rise of virtualization and the rise of security concerns? Is there any intersection? Is there any relationship that most people may miss?

Soup to nuts security

Roemer: The rise of virtualization and security has been concurrent. A lot of original deployments for virtualization technologies were for remote access, but they were also for *secure* remote access. The apps that people needed to get access to remotely were usually very substantial applications for the organization -- things like order processing or partner systems; they might have been employee access to email or internal timecard systems. These were things that you didn’t really want an attacker messing with -- or arbitrary people getting access to.

Security has grown from just providing basic access to virtualization to really meeting a lot of the risks of these virtualized applications being exposed to the Internet in general, as well as now expanding out into the cloud.

Security has grown from just providing basic access to virtualization to really meeting a lot of the risks of these virtualized applications being exposed to the Internet in general, as well as now expanding out into the cloud. So, we have had to grow security capabilities to be able to not only keep up with the threat, but try to keep ahead of it as well.

Gardner: Hasn’t it historically been true that most security prevention technologies have been still focused at the operating system (OS)-level, not so much at the virtualization level? How has that changed over the past several years?

Roemer: That’s a good question. There have been a lot of technologies that are associated with virtualization, and as you go through and secure and harden your virtual environments, you really need to do it from the hardware level, through the hypervisor, through the operating system level, and up into the virtualization system and the applications themselves.

We are now seeing people take a much more rigorous approach at each of those layers, hardening the virtualization system and the OS and integrating in all the familiar security technologies that we’re used to, like antivirus, but also going through and providing for application-specific security.

So if you have a SAP system or something else where you need to protect some very sensitive company data and you don’t want that data to be accessed outside the office arbitrarily, you can provide very set interfaces into that system, being able to control the clipboard or copy and paste, what peripherals the application can interface with; i.e., turn off the camera, turn off the microphone if it’s not needed, and even get down to the level of with the browser, whether things like JavaScript is enabled or Flash is available.

So it helps to harden the overall environment and cut down on a lot of the vulnerabilities that would be inherent by just leaving things completely wide open. One of the benefits of virtualization is that you can get security to be very specific to the application.

Gardner: Harish, now that we are seeing this need for comprehensive security, what else is it that people perhaps don't understand that they can do in the virtualization layer? Why is virtualization still uncharted territory as we seek to get even better security across the board?

Let's get better than physical

Agastya

Agastya: Customers often don't realize when they are dealing with security in physical or virtual environments. The opportunities that virtual environments provide to them are to have the ability to take security to a higher level than physical-only. So *better than physical* is, I think, a key value proposition that they can benefit from -- and the technology innovation of today has enabled that.

There is a wave of innovation among security vendors in this space. How do we run resource-intensive security workloads in a way that does not compromise the service-level agreements (SLAs) that those information technology operations (IT Ops) administrators need to deliver?

There is a lot of work happening to offload security-scanning mechanisms on to dedicated security virtual appliances, for example. Bitdefender has been working with partners like Citrix to enable that.

Now, the huge opportunity is to take that story further in terms of being able to provide higher levels of visibility, detection, and prevention from the attacks of today, which are advanced persistent threats. We seek to detect how they manifest in the data center and -- in a virtual environment -- what you have the opportunity to do, and how you can respond. That game is really changing now.

Gardner: Kurt, is there something about the ability to spin up virtualized environments, and then take them down that provides a risk that the bad guys can target or does that also provide an opportunity to start fresh: To eliminate vulnerabilities, or learn quickly and adapt quickly? Is there something about the rapid change that virtualization enables that is a security plus?

Persistent protection, anywhere, anytime

Roemer: You really hit on the two sides of the coin. On one side, virtualization does oftentimes provide an image of the application or the applications plus OS that could be fairly easy for a hacker to steal and be able to spin up offline and be able to get access to secrets. So you want to be able to protect your images, to make sure that they are not something that can be easily stolen.

On the other side, having the ability to define persistence -- what do you want to have to persist between reboots versus what's non-persistent -- allows you to have a constantly refreshed system. So when you reboot it, it's exactly back to the golden image -- and everything is as it should be. As you patch and update you are working with a known quantity as opposed to the endpoint where somebody might have administrative access and it has installed personal applications and plug-ins to their browser and other things like that that you may or may not want to have in place.

> The nice thing with virtualization is that it's independent of the OS, the applications, the endpoints, and the many environments that we all access our apps and data from.

Layering also comes into play and helps to make sure that you can dynamically layer in applications or components of the OS, depending on what's needed. So if somebody is accessing a certain set of functionality in the office, maybe they have 100% functionality. But when they go home, because they are no longer in a trusted environment or maybe not working on a trusted PC from their home system, they get a degraded experience, seeing fewer applications and having less functionality layered onto the OS. Maybe they can't save to local drives or print to local printers. All of that's defined by policy. The nice thing with virtualization is that it's independent of the OS, the applications, the endpoints, and the varied situations that we all access our apps and data from.

Gardner: Harish, with virtualization that there is a certain level of granularity as to how one can manage their security environment parameters. Can you expand on why having that granular capability to manage parameters is such a strong suit, and why virtualization is a great place to make that happen?

On the move, virtually

Agastya: That is one of the opportunities and challenges that security solutions need to be able to cope with.

As workloads are moving across different subgroups, sub-networks, that virtual machine (VM) needs to have a security policy that moves with it. It depends on what type of application is running, and it is not specific to the region or sub-network that that particular VM is resident on. That is something that security solutions that are designed to operate in virtual environments have the ability to do.

Security moves with the workload, as the workload is spawned off and new VMs are created. The same set of security policies associated with that workload now can protect that workload without needing to have a human step in and determine what security posture needs to belong to that VM.

That is the opportunity that virtualization provides. But it's also a challenge. For example, maybe the previous generations of solutions predated all of this. We now need to try and address that.

We love the fact that virtualization is happening and that it has become a very elastic software-defined mechanism that moves around and gives the IT operations people so much more control. It allows an opportunity to be able to sit very well in that environment and provide security that works tightly integrated with the virtualization layer.

Gardner: I hear this so much these days that IT operations people are looking for more automation, and more control.

Kurt, I think it's important to understand that when we talk about security within a virtualization layer, that doesn't obviate the value of security that other technologies provide at the OS level or network level. So this isn't either-or, this is an augmentation, isn't that correct, when we talk about virtualization and security?

The virtual focus

Roemer: Yes, that's correct. Virtualization provides some very unique assets that help extend security, but there are some other things that we want to be sure to focus on in terms of virtualization. One of them is Bitdfender Hypervisor Introspection (HVI). It's the ability for the hypervisor to provide a set of direct inspect application programming interfaces (APIs) that allow for inspection of guest memory outside of the guest.

When you look at Windows or Linux guests that are running on a hypervisor, typically when you have tried to secure those it's been through technology installed in the guest. So you have the guest that's self-protecting, and they are relying on OS APIs to be able to effect security. Sometimes that works really well and sometimes the attackers get around OS privileges and are successful, even with security solutions in place.

One of the things that HVI does is it looks for the techniques that would be associated with an attack against the memory of the guest from outside the guest. It's not relying on the OS APIs and can therefore catch attacks that otherwise would have slipped past the OS-based security functionality.

Gardner: Harish, maybe you can tell us about how Citrix and Bitdefender are working together?

Step into the breach, together

Agastya: The solution is Bitdefender HVI. It works tightly with Citrix's XenServer hypervisor, and it has been available in a controlled release for the last several months. We have had some great customer traction on it. At Citrix Synergy this year we will be making that solution generally available.

We have been working together for the last four years to bring this groundbreaking technology to the market.

What is the problem we are trying to solve? It is the issue of advanced attacks that hit the data center when, as Kurt mentioned, advanced attackers are able to skirt past endpoint security defense mechanisms by having root access and operating at the same level of privilege as the endpoint security that may be running within the VM.

They can then essentially create a blind spot where the attackers can do anything they want while the endpoint security solution continues to run.

These types of attacks stay in the environment and the customer suffers on average 200 days before a breach is discovered. The marketplace is filled with stories like this and it's something that we have been working together with Citrix to address.

The fundamental solution leverages the power of the hypervisor to be able to monitor attacks that modify memory. It does that by looking for the common attack mechanisms that all these attackers use, whether it's buffer overflows or it's heap spraying, the list goes on.

They all result in memory modification that the endpoint security solution within the VM is blinded to. However, if you are leveraging the direct inspect APIs that Kurt talked about -- available as part of Citrix's XenServer solution – then we have the ability to look into that VM without having a footprint in there. It is a completely agentless solution that runs outside the security virtual appliance. It monitors all of the VMs in the data center against these types of attacks. It allows you to take action immediately, reduces the time to detection and blocks the attack.

Gardner: Kurt, what are some of the major benefits for the end-user organization in deploying something like HVI? What is the payback in business terms?

Performance gains

Roemer: Hypervisor Introspection, which we introduced in XenServer 7.1, allows an organization to deploy virtualization with security technologies behind it at the hypervisor level. What that means for the business is that every guest you bring up has protection associated with it. Even if it's a new version of Linux that you haven't previously tested and you really don't know which antivirus you would have integrated with it; or something that you are working on from an appliance perspective -- anything that can run on XenServer would be protected through these direct inspect APIs, and the Bitdefender HVI solution. That's really exciting.

So for the business, HVI gives you higher security, it gives you better performance, and the assurance that you are covered – no matter what's happening in the guest.

It also has performance benefits because you don't have to run antivirus in every guest at the same level. By knowing what's being protected at the hypervisor level, you can configure for a higher level of performance.

Now, of course, we always recommend having antivirus in guests, as you still have file-based access and so you need to look for malware, and sometimes files get emailed in or out or produced, and so having access to the files from an anti-malware perspective is very valuable. But you may need to cut down some of the scanning functionality and be able to meet much higher performance objectives.

So for the business, HVI gives you higher security, it gives you better performance, and the assurance that you are covered -- no matter what's happening in the guest.

Gardner: Harish, it sounds like this ability to gain introspection into that hypervisor is wonderful for security and does it in such a way that it doesn't degrade performance. But it seems to me that there are also other ancillary benefits in addition to security, when you have that ability to introspect and act quickly. Is there more than just a security benefit, that the value could go quite a bit further?

The benefits of introspection

Agastya: That’s true. The ability to introspect into memory has huge potential in the market. First of all, with this solution right now, we address the ability to detect advanced attacks, which is a very big problem in the industry -- where you have everything from nation-sponsored attacks to deep dark web, malicious components, attack components available to common citizens who can do bad things with them.

The capability to reduce that window to advanced attack detection is huge. But now with the power of introspection, we also have the ability to inject, on the fly, into the VM, additional solutions tools that can do deep forensics, measure network operations and the technology can expand to cover more. The future is bright for where we can take this between our companies.

Gardner: Kurt, anything to add on the potential for this memory introspection capability?

Specific, secure browsers

Roemer: There are a couple things to add. One is taking a look at the technologies and just rolling back through a lot of the exploits that we have seen, even throughout the last three months. There have been exploits against Microsoft Windows, exploits against Internet Explorer and Edge, hypervisors, there’s been EternalBlue and the Server Message Block (SMB) exploits. You can go back and be able to try these out against the solution and be able to see exactly how it would catch them, and what would have happened to your system had those exploits actually taken effect.

If you have a team that is doing forensics and trying to go through and determine whether systems had previously been exploited, you are giving that team additional functionality to be able to look back and see exactly how the exploits would have worked. Then they can understand better how things would have happened within their environment. Because you are doing that outside of the guest, you have a lot of visibility and a lot of information you otherwise wouldn't have had.

One big expanded use-case here is to get the capability for HVI between Citrix and Bitdefender in the hands of your security teams, in the hands of your forensics teams, and in the hands of your auditors -- so that they can see exactly what this tool brings to the table.

Something else you want to look at is the use-case that allows users to expand what they are doing and makes their lives easier -- and that's *secured browsing*.

Today, when people go out and browse the Internet or hit a popular application like Facebook or Outlook Web Access -- or if you have an administrator who is hitting an administrative console for your Domain Name System DNS environment, your routers, your Cisco, Microsoft environments, et cetera, oftentimes they are doing that via a web browser.

Well, if that's the same web browser that they use to do everything else on their PC, it's over-configured, it presents excessive risk, and you now have the opportunity with this solution to publish browsers that are very specific to each use.

For example, you publish one browser specifically for administrative access, and you know that you have advanced malware detection. Even if somebody is trying to target your administrators, you are able to thwart their ability to get in and take over the environments that the administrators are accessing.

As more things move to the browser -- and more very sensitive and critical applications move to the cloud -- it's extremely important to set up secured browsing. We strongly recommend doing this with XenServer and HVI along with Bitdefender providing security.

Agastya: The problem in the market with respect to the human who is sitting in front of the browser being the weakest link in the chain is a very important one. Many, many different technology approaches have been taken to address this problem -- and most of them have struggled to make it work.

The value of XenApp coming in with its secured browser model is this: You can stream your browser and you are just presenting, rendering an interface on the client device, but the browser is actually running in the backend, in the data center, running on XenServer, protected by Bitdefender HVI. This model not only allows you to shift the threat away from the client device, but also kill it completely, because that exploit which previously would have run on the client device is not on the client device anymore. It’s not even on the server anymore because HVI has gotten to it and stopped it.

Roemer: I bring up the browser benefit as an example because when you think of the lonely browser today, it is the interface to some of your most critical applications. A browser, at the same time, is also connected to your file system, your network, your Windows registry, your certificate chain and keys -- it’s basically connected to everything you do and everything you have access to in most OSes.

What we are talking about here is publishing a browser that is very specific to purpose and configured for an individual application.

What we are talking about here is publishing a browser that is very specific to purpose and configured for an individual application. Just put an icon out there, users click on it and everything works for them silently in the background. By being able to redirect hyperlinks over to the new joint XenServer-Bitdefender solution, you are not only protecting against known applications and things that you would utilize --

but you can also redirect arbitrary links.

Even if you tell people, “don’t click on any links”, you know every once in a while it’s going to happen. When that one person clicks on the link and takes down the entire network, it’s awful. Ransomware attacks happen like that all the time. With this solution, that arbitrary link would be redirected over to a one-time use browser. Bitdefender would come up and say, “Hey, yup, there’s definitely a problem here, we are going to shut this down,” and the attack never would have had a chance to get anywhere.

The organization is notified and can take additional remediatative actions. It’s a great opportunity to really change how people are working and take this arbitrary link problem and the ransomware problem and neutralize it.

Gardner: It sounds revolutionary rather than evolutionary when it comes to security. It’s quite impressive. I have learned a lot in just the last week or two in looking into this. Harish, you mentioned earlier that before the general availability being announced in May for Bitdefender HVI on XenServer that you have had this in beta. Do you have any results from that? Can you offer any metrics of what’s happened in the real world when people deploy this? Are the results as revolutionary as it sounds?

Real-world rollout

Agastya: The product was first in beta and then released in controlled availability mode, so the product is actually in production deployment at several companies in both North America and Europe. We have a few financial services companies, and we have some hospitals. We have put the product to use in production deployments for virtual desktop infrastructure (VDI) deployments where the customers are running XenApp and XenDesktop on top of XenServer with Bitdefender HVI.

We have server workloads running straight on XenServer, too. These are typically application workloads that the financial services companies or the hospitals need to run. We have had some great feedback from them. Some of them have become references as well, and we will be talking more about it at Citrix Synergy 2017, so stay tuned. We are very excited about the fact that the product is able to provide value in the real world.

Roemer: We have a very detailed white paper on how to set up the secured browsing solution, the joint solution between Citrix and Bitdefender. Even if you are running other hypervisors in your environment, I would recommend that you set up this solution and try redirecting some arbitrary hyperlinks over to it, to see what value you are going to get in your organization. It’s really straightforward to set up and provides a considerable amount of additional security visibility.

Bitdefender also has some really amazing videos that show exactly how the solution can block some of the more popular exploits from this year. They are really impressive to watch.

Gardner: Kurt, we are about out of time, but I was curious, what’s the low-lying fruit? Harish mentioned government, VDI, healthcare. Is it the usual suspects with compliance issues hanging over their heads that are the low-lying fruit, or are there other organizations that would be ripe to enjoy the benefits?

Roemer: I would say compliance environments and anybody with regulatory requirements would very much be low-lying fruit for this, but anybody who has sensitive applications or very sensitive use-cases, too. Oftentimes, we hear things like outsourcing as being one of the more sensitive use-cases because you have external third parties who are getting in and either developing code for you, administering part of the operating environment, or something else.

We have also seen a pretty big uptick in terms of people being interested in this for administering the cloud. As you move up to cloud environments and you are defining new operating environments in the cloud while putting new applications up in the cloud, you need to make sure that your administrative model is protected.

Oftentimes, you use a browser directly to provide all of the security interfaces for the cloud, and by publishing that browser and putting this solution in front of it, you can make sure that malware is not interrupting your ability to securely administer the cloud environment.

Gardner: Last question to you, Harish. What should organizations do to get ready for this? I hope we have enticed them to learn more about it. For those organizations that actually might want to deploy, what do they need to think about in order to be in the best position to do that?

A new way of life

Agastya: Organizations need to think about secure virtualization as a way of life within organizational behavior. As a result, I think we will start to see more people with titles like Security DevOps (SecDevOps).

As far as specifically using HVI, organizations should be worried about how advanced attacks could enter their data center and potentially result in a very, very dangerous breach and the loss of confidential intellectual property.

If you are worried about that, you are worried about ransomware because an end-user sitting in front of a client browser is potentially putting out your address. You will want to think about a technology like HVI. The first step for that is to talk to us and there is a lot of information on the Bitdefender website as well as on Citrix’s website.

Gardner: I’m afraid we will have to leave it there. You’ve been listening to a sponsored BriefingsDirect discussion that examines the relationship between security and virtualization. We have learned how adaptive companies are finding new ways to leverage their virtualization environments to become more resilient and proactive in how they can thwart threats by putting in distinct browsers for specific uses and reduce their threat exposure.

So please join me now in thanking our guests, Kurt Roemer, Chief Security Strategist at Citrix. Thank you, Kurt.

Roemer: Thank you, Dana. Thanks, Harish.

Agastya: Thank you, Kurt. Thank you, Dana.

Gardner: And we have been here with Harish Agastya, Vice President for Enterprise Solutions at Bitdefender. Thank you, Harish.

I'm Dana Gardner, Principal Analyst at Interarbor Solutions, your host and moderator for this ongoing series of BriefingsDirect Discussions. I want to also thank our sponsor, Bitdefender, for supporting these presentations. And of course, a big thank you as well to our audience. And please come back next time.

Listen to the podcast. Find it on iTunes. Get the mobile app. Download the transcript.

Transcript of a discussion on how adaptive companies are leveraging their virtualization environments to become more secure and reduce cyber risks.

You may also be interested in:

- How IT innovators turn digital disruption into a business productivity force multiplier
- Cybersecurity standards: The Open Group explores security and safer supply chains
- How the Citrix Technology Professional Program Produces User Experience Benefits from Greater Ecosystem Collaboration
- DevOps and Security, a Match Made in Heaven
- Expert Panel Explores the New Reality for Cloud Security and Trusted Mobile Apps Delivery
- Cybersecurity crosses the chasm: How IT now looks to the cloud for best security
- Capgemini and HPE Team Up to Foster Behavioral Change That Brings Better Cyber Security Across Application Lifecycles
- Feedback loops: The confluence of DevOps and big data