Kansas Development Finance Authority Gains Peace of Mind, End-Points Virtual Shield Using Hypervisor-Level Security

Transcript of a discussion on how a Kansas economic development organization gains peace of mind by relying on increased automation and intelligence in how it secures its systems, data, and people.

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

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

For small and medium-sized businesses (SMBs) and government agencies, implementing and managing IT security has leaped in complexity. Once safe products used to thwart invasions now have been exploited. E-mail phishing campaigns are far more sophisticated, leading to damaging ransomware attacks.

What's more, the jack-of-all-trades, IT leaders of these mid-market concerns are striving to protect more data types on and off premises, their workload servers and expanded networks, as well as many essential devices of the mobile workforce.

Security demands have gone up, yet there is a continual need for reduced manual labor and costs, while protecting assets sooner and better. We will now learn how a Kansas economic development organization has been able to gain peace of mind by relying on increased automation and intelligence in how it secures its systems and people.

Kater

To explore how an all-encompassing approach to security has enabled improved results with fewer hours at a smaller enterprise, please join me in welcoming our guest, Jeff Kater, Director of Information Technology and Systems Architect at Kansas Development Finance Authority (KDFA) in Topeka.

Welcome, Jeff.

Jeff Kater: Thank you, Dana.

Gardner: As a director of all of IT at KDFA, security must be a big, big concern, but it can't devour all of your time. How have you been able to balance security demands with all the other IT demands?

Kater: That's a very interesting question, and it has a multi-segmented answer. In years past, leading up to the development of what KDFA is now, we faced the trends that demanded very basic anti-spam solutions and the very basic virus threats that came via the web and e-mail.

What we've seen more recently is the growing trend of enhanced security attacks coming through malware and different exploits -- that were once thought impossible -- are now are the reality.

Therefore in recent times, my percentage of time dedicated to security has grown from probably five to 10 percent all the way up to 50 to 60 percent of my workload during each given week.

Gardner: Before we get to how you've been able to react to that, tell us about KDFA.

Enterprise-ready 24/7

Kater: KDFA promotes economic development and prosperity for the State of Kansas by providing efficient access to capital markets through various tax-exempt and taxable debt obligations.

KDFA works with public and private entities across the board to identify financial options and solutions for those entities. We are a public corporate entity operating in the municipal finance market, and therefore we are a conduit finance authority.

KDFA is a very small organization -- but a very important one. Therefore we run enterprise-ready systems around the clock, enabling our staff to be as nimble and as efficient as possible.

There are about nine or 10 of us that operate here on any given day at KDFA. We run on a completely virtual environment platform via Citrix XenServer. So we run XenApp, XenDesktop, and NetScaler -- almost the full gamut of Citrix products.

We have a few physical endpoints, such as laptops and iPads, and we also have the mobile workforce on iPhones as well. They are all interconnected using the virtual desktop infrastructure (VDI) approach.

Gardner: You've had this swing, where your demands from just security issues have blossomed. What have you been doing to wrench that back? How do you get your day back, to innovate and put in place real productivity improvements?

Kater: We went with virtualization via Citrix. It became our solution of choice due to not being willing to pay the extra tax, if you will, for other solutions that are on the market. We wanted to be able to be nimble, to be adaptive, and to grow our business workload while maintaining our current staff size.

> *We wanted to be able to be nimble, to be adaptive, and to grow our business workload while maintaining our current staff size.*

When we embraced virtualization, the security approaches were very traditional in nature. The old way of doing things worked fantastically for a physical endpoint.

The traditional approaches to security had been on our physical PCs for years. But when that security came over to the virtual realm, they bogged down our systems. They still required updates done manually. They just weren't innovating at the same speed as the virtualization, which was allowing us to create new endpoints.

And so, the maintenance, the updating, the growing threats were no longer being seen by the traditional approaches of security. We had endpoint security in place on our physical stations, but when we went virtual we no longer had endpoint security. We then had to focus on antivirus and anti-spam at the server level.

What we found out very quickly was that this was not going to solve our security issues. We then faced a lot of growing threats again via e-mail, via web, that were coming in through malware, spyware, other activities that were embedding themselves on our file servers – and then trickling down and moving laterally across our network to our endpoints.

Gardner: Just as your organization went virtual and adjusted to those benefits, the malware and the bad guys, so to speak, adjusted as well -- and started taking advantage of what they saw as perhaps vulnerabilities as organizations transitioned to higher virtualization?

Security for all, by all

Kater: They did. One thing that a lot of security analysts, experts, and end-users forget in the grand scheme of things is that this virtual world we live in has grown so rapidly -- and innovated so quickly -- that the same stuff we use to grow our businesses is also being used by the bad actors. So while we are learning what it can do, they are learning how to exploit it at the same speed -- if not a little faster.

Gardner: You recognized that you had to change; you had to think more about your virtualization environment. What prompted you to increase the capability to focus on the hypervisor for security and prevent issues from trickling across your systems and down to your endpoints?

Kater: Security has always been a concern here at KDFA. And there has been more of a security focus recently, with the latest news and trends. We honestly struggled with CryptoLocker, and we struggled with ransomware.

While we never had to pay out any ransom or anything -- and they were stopped in place before data could be exfiltrated outside of KDFA's network -- we still had two or three days of either data loss or data interruption. We had to pull back data from an archive; we had to restore some of our endpoints and some of our computers.

As we battled these things over a very short period of time, they were progressively getting worse and worse. We decided that we needed to have a solution for our virtual environment – one that would be not only be easy to deploy, easy to manage, but it would be centrally managed as well, enabling me to have more time to focus back on my workload -- and not have to worry so much about the security thresholds that had to be updated and maintained via the traditional model.

We needed to have a solution for our virtual environment — one that would be easy to deploy, easy to manage, and it would be centrally managed.

So we went out to the market. We ran very extensive proof of concepts (POCs), and those POCs very quickly illustrated that the underlying architecture was only going to be enterprise-ready via two or three vendors. Once we started running those through the paces, Bitdefender emerged for us.

I had actually been watching the Hypervisor Introspection (HVI) product development for the past four years, since its inception came with a partnership between Citrix, Intel, the Linux community and, of course, Bitdefender. One thing that was continuous throughout all of that was that in order to deploy that solution you would need GravityZone in-house to be able to run the HVI workloads.

And so we became early adopters of Bitdefender GravityZone, and we are able to see what it could do for our endpoints, our servers, and our Microsoft Exchange Servers. Then, Hypervisor Introspection became another security layer that we are able to build upon the security solution that we had already adopted from Bitdefender.

Gardner: And how long have you had these solutions in place?

Kater: We are going on one and a half to two years for GravityZone. And when HVI went to general availability earlier this year, in 2017, and we were one of the first adopters to be able to deploy it across our production environment.

Gardner: Let's elevate our discussion. If you had a "security is easy" button that you could pound on your desk, what are the sorts of things that you look for in a simpler security solution approach?

IT needs brains to battle breaches

Kater: The "security is easy" button would operate much like the human brain. It would need that level of intuitive instinct, that predictive insight ability. The button would generally be easily managed, automated; it would evolve and learn with artificial intelligence (AI) and machine learning what's out there. It would dynamically operate with peaks and valleys depending on the current status of the environment, and provide the security that's needed for that particular environment.

Gardner: Jeff, you really are an early adopter, and I commend you on that. A lot of organizations are not quite as bold. They want to make sure that everything has been in the market for a long time. They are a little hesitant.

But being an early adopter sounds like you have made yourselves ready to adopt more AI and machine learning capabilities. Again, I think that's very forward-looking of you.

But tell us, in real terms, what has being an early adopter gotten for you? We've had some pretty scary incidents just in the recent past, with WannaCry, for example. What has being an early adopter done for you in terms of these contemporary threats?

Kater: The new threats, including the EternalBlue exploit that happened here recently, are very advanced in nature. Oftentimes when these breaches occur, it takes several months before they have even become apparent. And oftentimes they move laterally within our network without us knowing, no matter what you do.

Some of the more advanced and persistent threats don't even have to infect the local host with any type of software. They work in the virtual memory space. It's much different than the older threats, where you could simply reboot or clear your browser cache to resolve them and get back to your normal operations.

Earlier, when KDFA still made use of non-persistent desktops, if the user got any type of corruption on their virtual desktop, they were able to reboot, and get back to a master image and move on. However, with these advanced threats, when they get into your network, and they move laterally -- even if you reboot your non-persistent desktop, the threat will come back up and it still infects your network. So with the growing ransomware techniques out there, we can no longer rely on those definition-based approaches. We have to look at the newer techniques.

As far as why we are early adopters, and why I have chosen some of the principles that I have, I feel strongly that you are really only as strong as your weakest link. I strive to provide my users with the most advanced, nimble, and agnostic solutions possible.

We are able to grow and compute on any device anywhere, anytime, securely, with minimal limitations. It allows us to have discussions about increasing productivity at that point, and to maximize the potential of our smaller number of users -- versus having to worry about the latest news of security breaches that are happening all around us.

We are able to grow and compute on any device, anywhere, anytime, securely, with minimal limitations.

Gardner: You're able to have a more proactive posture, rather than doing the fire drill when things go amiss and you're always reacting to things.

Kater: Absolutely.

Gardner: Going back to making sure that you're getting a fresh image and versions of your tools … We have heard some recent issues around the web browser not always being safe. What is it about being able to get a clean version of that browser that can be very important when you are dealing with cloud services and extensive virtualization?

Virtual awareness, secure browsing

Kater: Virtualization in and of itself has allowed us to remove the physical element of our workstations when desirable and operate truly in that virtual or memory space. And so when you are talking about browsers, you can have a very isolated, a very clean browser. But that browser is still going to hit a website that can exploit your system. It can run in that memory space for exploitation. And, again, it doesn't rely on plug-ins to be downloaded or anything like that anymore, so we really have to look at the techniques that these browsers are using.

What we are able to do with the secure browsing technique is publish, in our case, via XenApp, any browser flavor with isolation out there on the server. We make it available to the users that have access for that particular browser and for that particular need. We are then able to secure it via Bitdefender HVI, making sure that no matter where that browser goes, no matter what interface it's trying to align with, it's secure across the board.

Gardner: In addition to secure browsing, what do you look for in terms of being able to keep all of your endpoints the way you want them? Is there a management approach of being able to verify what works and what doesn't work? How do you try to guarantee 100 percent security on those many and varied endpoints?

Kater: I am a realist, and I realize that nothing will ever be 100 percent secure, but I really strive for that 99.9 percent security and availability for my users. In doing so -- being that we are so small in staff, and being that I am the one that should manage all of the security, architecture, layers, networking and so forth -- I really look for that centralized model. I want one pane of glass to look at for managing, for reporting.

I want that management interface and that central console to really tell me when and if an exploit happens, what happened with that exploit, where did it go, and what did it do to me and how was I protected. I need that so that I can report to my management staff and say, “Hey, honestly, this is what happened, this is what was happening behind the scenes. This is how we remediated and we are okay. We are protected. We are safe.”

We I want that management interface and that central console to really tell me when and if an exploit happens, what happened with that exploit, where did it go, what did it do to me, and how was I protected.

And so I really look for that centralized management. Automation is key. I want something that will automatically update, with the latest virus and malware definitions, but also download the latest techniques that are seen out there via those innovative labs from our security vendors to fully patch our systems behind the scenes. So it takes that piece of management away from me and automates it to make my job more efficient and more effective.

Gardner: And how has Bitdefender HVI, in association with Bitdefender GravityZone, accomplished that? How big of a role does it play in your overall solution?

Kater: It has been a very easy deployment and management, to be honest. Again, entities large and small, we are all facing the same threats. When we looked at ways to attain the best solution for us, we wanted to make sure that all of the main vendors that we make use of here at KDFA were on board.

And it just so happened this was a perfect partnership, again, between Citrix, Bitdefender, Intel, and the Linux community. That close partnership, it really developed into HVI, and it is not an evolutionary product. It did not grow from anything else. It really is a revolutionary approach. It’s a different way of looking at security models. It’s a different way of protecting.

HVI allows for security to be seen outside of the endpoint, and outside of the guest agent. It’s kind of an inside-looking-outward approach. It really provides high levels of visibility, detection and, again, it prevents the attacks of today, with those advanced persistent threats or APTs.

With that said, since the partnership between GravityZone and HVI is so easy to deploy, so easy to manage, it really allows our systems to grow and scale when the need is there. And we just know that with those systems in place, when I populate my network with new VMs, they are automatically protected via the policies from HVI.

Given that the security has to be protected from the ground all the way up, we rest assured that the security moves with the workload. As the workload moves across my network, it’s spawned off and onto new VMs. The same set of security policies follows the workloads. It really takes out any human missteps, if you will, along the process because it’s all automated and it all works hand-in-hand together.

Behind the screens

Gardner: It sounds like you have gained increased peace of mind. That’s always a good thing in IT; certainly a good thing for security-oriented IT folks. What about your end-users? Has the ability to have these defenses in place allowed you to give people a bit more latitude with what they can do? Is there a productivity, end-user or user experience benefit to this?

Kater: When it comes to security agents and endpoint security as a whole, I think a lot of people would agree with me that the biggest drawback when implementing those into your work environment is loss of productivity. It's really not the end-user's fault. It's not a limitation of what they can and can't do, but it's what happens when security puts an extra load on your CPU, it puts extra load on your RAM; therefore, it bogs down your systems. Your systems don't operate as efficiently or effectively and that decreases your productivity.

With Bitdefender, and the approaches that we adopted, we have seen very, very limited, almost uncomputable limitations as far as impacts on our network, impacts on our endpoints. So user adoption has been greater than it ever has, as far as a security solution.

I'm also able to manipulate our policies within that Central Command Center or Central Command Console within Bitdefender GravityZone to allow my users, at will, if they would like, to see what they are being blocked against, and which websites they are trying to run in the background. I am able to pass that through to the endpoint for them to see firsthand. That has been a really eye-opening experience.

We used to compute daily, thinking we were protected, and that nothing was running in the background. We were visiting the pages, and those pages were acting as though we thought that they should. What we have quickly found out is that any given page can launch several hundred, if not thousands, of links in the background, which can then become an exploit mechanism, if not properly secured.

Gardner: I would like to address some of the qualitative metrics of success when you have experienced the transition to more automated security. Let's begin with your time. You said you went from five or 10 percent of time spent on security to 50 or 60 percent. Have you been able to ratchet that back? What would you estimate is the amount of time you spend on security issues now, given that you are one and a half years in?

Kater: Dating back 5 to 10 years ago with the inception of VDI, my security footprint as far as my daily workload was probably around that 10 percent. And then, with the growing threats in the last two to three years, that ratcheted it up to about 50 percent, at minimum, maybe even 60 percent. By adopting GravityZone and HVI, I have been able to pull that back down to only consume about 10 percent of my workload, as most of it is automated for me behind the scenes.

Gardner: How about ransomware infections? Have you had any of those? Or lost documents, any other sort of qualitative metrics of how to measure efficiency and efficacy here?

Kater: I am happy to report that since the adoption of GravityZone, and now with HVI as an extra security layer on top of Bitdefender GravityZone, that we have had zero ransomware infections in more than a year now. We have had zero exploits, and we have had zero network impact.

We have had zero ransomware infections in more than a year now. We have had zero exploits, and we have had zero network impact.

Gardner: Well, that speaks for itself. Let's look to the future, now that you have obtained this. You mentioned earlier your interest in AI, machine learning, automating, of being proactive. Tell us about what you expect to do in the future in terms of an even better security posture.

Safety layers everywhere, all the time

Kater: In my opinion, again, security layers are vital. They are key to any successful deployment, whether you are large or small. It’s important to have all of your traditional security hardware and software in place working alongside this new interwoven fabric, if you will, of software -- and now at the hypervisor level. This is a new threshold. This is a new undiscovered territory that we are moving into with virtual technologies.

As that technology advances, and more complex deployments are made, it’s important to protect that computing ability every step of the way; again, from that base and core, all the way into the future.

More and more of my users are computing remotely, and they need to have the same security measures in place for all of their computing sessions. What HVI has been able to do for me here in the current time, and in moving to the future, is I am now able to provide secure working environments anywhere -- whether that’s their desktop, whether that’s their secure browser. I am able to leverage that HVI technology once they are logged into our network to make their computing from remote areas safe and effective.

Gardner: For those listening who may not have yet moved toward a hypervisor-level security – or who have maybe even just more recently become involved with pervasive virtualization and VDI -- what advice could you give them, Jeff, on how to get started? What would you suggest others do that would even improve on the way you have done it? And, of course, you have had some pretty good results.

Kater: It’s important to understand that everybody’s situation is very different, so identifying the best solutions for everybody is very much on an individual corporation basis. Each company has its own requirements, its own compliance to follow, of course.

The best advice that I can give is pick two or three vendors, at the least, and run very stringent POCs; no matter what they may be, make sure that they are able to identify your security restraints, try to break them, run them through the phases, see how they affect your network. Then, when you have two or three that come out of that and that you feel strongly about, continue to break them down.

> *Pick two or three vendors and run very stringent POCs; make sure that they are able to identify your security restraints, try to break them, run them through the phases, see how they affect your network.*

I cannot stress the importance of POCs enough. It’s very important to identify that one or two that you really feel strongly about. Once you identify those, then talk to the industry experts that support those technologies, talk to the engineers, really get the insight from the inside out on how they are innovating and what their plan is for the future of their products to make sure that you are on a solid footprint.

Most success stories involve a leap of faith. With machine learning and AI, we are now taking a leap that is backed by factual knowledge and analyzing techniques to stay ahead of threats. No longer are we relying on those virus definitions and those virus updates that can be lagging sometimes.

Gardner: Before we sign off, where do you go to get your information? Where would you recommend other people go to find out more?

Kater: Honestly, I was very fortunate that HVI at its inception fell into my lap. When I was looking around at different products, we just hit the market at the right time. But to be honest with you, I cannot stress enough, again, run those POCs.

If you are interested in finding out more about Bitdefender and its product line up, Bitdefender has an excellent set of engineers on staff; they are very knowledgeable, they are very well-rounded in all of their individual disciplines. The Bitdefender website is very comprehensive. It contains many outside resources, along with inside labs reporting, showcasing just what their capabilities are, with a lot of unbiased opinions.

They have several video demos and technical white papers listed out there, you can find them all across the web and you can request the full product demo when you are ready for it and run that POC of Bitdefender products in-house with your network. Also, they have presales support that will help you all along the way.

Bitdefender HVI will revolutionize your data center security capacity.

Gardner: That's a really good point that you need to do it yourself, because each site is different, and each organization is different. You really don't know until you put it into its paces what your particular results and security requirements are going to be, and how they come together. So I really appreciate your insights.

We have been listening to a sponsored BriefingsDirect discussion on how small to medium-sized businesses and government agencies are implementing and managing IT security better by relying on increased automation and intelligence.

And we have heard how Kansas Development Finance Authority in Topeka has benefited from a comprehensive and hypervisor-driven approach that cuts the time to produce better security and gain peace of mind.

So please join me in thanking our guest, Jeff Kater, Director of Information Technology and Systems Architect there at KDFA. Thank you so much, Jeff.

Kater: Thanks Dana!

Gardner: I'm Dana Gardner, Principal Analyst at Interarbor Solutions, your host and moderator for this ongoing series of BriefingsDirect security improvements discussions.

And a big thank you to our sponsor, Bitdefender, for supporting these use-case studies.

Lastly, a big thank you to our audience. Please pass along this information if you found it useful, and do come back next time.

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

Transcript of a discussion on how a Kansas economic development organization gains peace of mind by relying on increased automation and intelligence in how it secures its systems, data, and people.

You may also be interested in:

- As enterprises face mounting hybrid IT complexity, new management solutions beckon
- How mounting complexity, multi-cloud sprawl, and need for maturity hinder hybrid IT's ability to grow and thrive
- Get ready for the Post-Cloud World
- Inside story on HPC's AI role in Bridges 'strategic reasoning' research at CMU
- Philips teams with HPE on ecosystem approach to improve healthcare informatics-driven outcome
- Inside story: How Ormuco abstracts the concepts of private and public cloud across the globe
- How Nokia refactors the video delivery business with new time-managed IT financing models
- IoT capabilities open new doors for Miami telecoms platform provider Identidad IoT
- Inside story on developing the ultimate SDN-enabled hybrid cloud object storage environment
- How IoT and OT collaborate to usher in the data-driven factory of the future
- DreamWorks Animation crafts its next era of dynamic IT infrastructure