Architectural Firm Retains Long-Term Security Confidence Across Fully Virtualized and Distributed Desktops Environment

Transcript of a discussion on how BLDD Architects gains better overall security, management, and data center consolidation from being nearly 100 percent virtualized while preserving the highest workspace performance, even across multiple distributed offices.

Listen to the **podcast**. Find it on **iTunes**. **Download** the transcript. Sponsor: **Bitdefender**.

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

Better security over data and applications remains a foremost reason IT organizations embrace and extend the use of client virtualization. Yet performance requirements for graphics-intense applications and large files remain one of the top reasons the use of thin clients and virtualized desktops trails the deployment of full PC clients.

For a large architectural firm in Illinois, gaining better overall security, management, and data center consolidation had to go hand in hand with preserving the highest workspace performance -- even across multiple distributed offices.

The next BriefingsDirect security innovations discussion examines how BLDD Architects, Inc. developed a protection solution that fully supports all of its servers and mix of clients in a way that's invisible to its end users.

Here to share the story of how to gain the best cloud workload security, regardless of the apps and the data, is Dan Reynolds, Director of IT at BLDD Architects in Decatur, Illinois. Welcome to BriefingsDirect, Dan.

Reynolds: Thank you, Dana.

Gardner: Dan, tell us about BLDD Architects. How old is the firm? Where you are located? And what do you have running in your now-centralized data center?

Reynolds: We are actually 90 years old this year, founded in 1929. It has obviously changed names over

Reynolds

the years, but the same core group of individuals have been involved the entire time. We used to have five offices: three in central Illinois, one in Chicago, and one in Davenport,

Iowa. Two years ago, we consolidated all of the Central Illinois offices into just the Decatur office.

When we did that, part of the initiative was to allow people to work from home. Because we are virtualized, that was quite easy. Their location doesn't matter. The desktops are still here, in the central office, but the users can be wherever they need to be.

On the back-end, we are a 100 percent Microsoft shop, except for VMware, of course. I run the desktops from a three-node Hewlett Packard Enterprise (HPE) DL380 cluster. I am using a Storage Area Network (SAN) product called the StarWind Virtual SAN, which has worked out very well. We are all VMware for the server and client virtualization, so VMware ESXi 6.5 and VMware Horizon 7.

Gardner: Please describe the breadth of architectural, design, and planning work you do and the types of clients your organization supports.

Architect the future, securely

Reynolds: We are wholly commercial. We don't do any residential designs, or only very, very rarely. Our biggest customers are K-12 educational facilities. We also design buildings for religious institutions, colleges, and some healthcare clinics.

Recently we have begun designing senior living facilities. That's an area of growth that we have pursued. Our reason for opening the office in Davenport was to begin working with more school districts in that state.

A long time ago, I worked as a computer-aided design (CAD) draftsman. The way the architecture industry has changed since then has been amazing. They now work with clients from cradle to grave. With school

> *The way the architecture industry has changed has been amazing. They now work with clients from cradle to grave.*

districts, for example, they need help at the early funding level. We go in and help them with campaigns, to put projects on the ballot, and figure out ways to help them – from gaining money all the way to long-term planning. There are several school districts where we are their architect-of-record. We help them plan for the future. It's amazing. It really surprises me.

Gardner: Now that we know what you do and your data center platforms, let's learn more about your overall security posture. How do you approach security knowing that it's not from one vendor, it's not one product? You don't just get security out of a box. You have to architect it. What's your philosophy, and what do you have in place as a result?

Reynolds: I like to have a multilayered approach. I think you have to. It can't just be antivirus, and it can't just be firewall. You have to allow the users freedom to do what

they need to do, but you also have to figure out where they are going to screw up -- and try to catch that.

And it's always a moving target. I don't pretend to know this perfectly at all. I use OpenDNS as a content filter. Since it's at the DNS level, and OpenDNS is so good at whitelisting, we pick up on some of the content choices and that keeps our people from accidentally making mistakes.

In addition, last year I moved us to Cisco Meraki Security Appliances, and their network-based malware protection. I have a site-to-site virtual private network (VPN) for our Davenport office. All of our connections are Fiber Ethernet. In Illinois, it's all Comcast Metro E. I have another broadband provider for the Davenport office.

And then, on top of all of that, I have Bitdefender GravityZone Enterprise Security for the endpoints that are not thin clients. And then, of course, for the VMware environment I also use GravityZone; that works perfectly with VMWare NSX virtual networking on the back-end and the scanning engine that comes with that.

Gardner: Just to be clear Dan, you have a mix of clients; you have got some zero clients, fat clients, both Mac and Windows, is that right?

Diversity protects mixed clients

Reynolds: That's correct. For some of the really high-end rendering, you need the video hardware. You just can't do everything with virtualization, but you can knock out probably 90 to 95 percent of all that we do with it.

And, of course, on those traditional PC machines I have to have conventional protection, and we also have laptops and Microsoft Surfaces. The marketing department has Mac OSX machines. There are just times you can't completely do everything with a virtual machine.

Gardner: Given such a diverse and distributed environment to protect, is it fair to say that being "paranoid about security" has paid off?

Reynolds: I am confident, but I am not cocky. The minute you get cocky, you are setting yourself up. But I am definitely confident because I have multi-layers of protection. I build my confidence by making sure these layers overlap. It gives me a little bit of cushion so I am not constantly afraid.

> *I am definitely confident because I have multi-layers of protection.*

And, of course, another factor many of us in the IT security world are embracing is around better educating the end users. We try to make them as aware to help share your paranoia with them to help them understand. That is really important.

On the flip side, I also use a product called StorageCraft and I encrypt all my backups. Like I said, I am not cocky. I am not going to put a target on my back and say, "Hit me."

Gardner: Designers, like architects, are often perfectionists. It's essential for them to get apps, renderings, and larger 3D files the way they want them. They don't want to compromise.

As an IT director, you need to make sure they have 100 percent availability -- but you also have to make sure everything is secure. How have you been able to attain the combined requirements of performance and security? How did you manage to tackle both of them at the same time?

Reynolds: It was an evolving process. In my past life I had experience with VMware and I knew of virtual desktops, but I wasn't really aware of how they would work under [performance] pressure. We did some preliminary testing using VMware ESXi on high-end workstations. At that point we weren't even using VMware View. We were just using remote desktops. And it was amazing. It worked, and that pushed me to then look into VMware View.

Of course, when you embrace virtualization, you can't go without security. You have to have antivirus (AV); you just have to. The way the world is now, you can't live without protecting your users -- and you can't depend on them to protect themselves because they won't do it.

> *The way the world is now, you can't live without protecting your users – and you can't depend on them to protect themselves because they won't do it.*

The way that VMware had approached antivirus solutions -- knowing that native agents and the old-fashioned types of antivirus solutions would impact performance -- was they built it into the network. It completely insulated the user from any interaction with the antivirus software. I didn't want anything running on the virtual desktop. It was completely invisible to them, and it worked.

Gardner: When you go to fully virtualized clients, you solve a lot of problems. You can centralize to better control your data and apps. That in itself is a big security benefit. Tell me your philosophy about security and why going virtualized was the right way to go.

Centralization controls chaos, corruption

Reynolds: Well, you hit the nail on the head. By centralizing, I can have one image or only a few images. I know how the machines are built. I don't have desktops out there that users customize and add all of their crap to. I can control the image. I can lock the image down. I can protect it with Bitdefender. If the image gets bad, it's just an image. I throw it away and I replace it.

I tend to use full clones and non-persistent desktops simply for that reason. It's so easy. If somebody begins having a problem with their machine or their [Revit](#) software gets corrupted or something else happens, I just throw away the old virtual machine (VM) and roll a new one in. It's easy-peasy. It's just done.

Gardner: And, of course, you have gained centralized data. You don't have to worry about different versions out there. And if corruption happens, you don't lose that latest version. So there's a data persistence benefit as well.

Reynolds: Yes, very much so. That was the problem when I first arrived here. They had five different silos [one for each branch office location]. There were even different versions of the same project in different places. They were never able to bring all of the data into one place.

I saw that as the biggest challenge, and that drove me to virtualization in the first place. We were finally able to put all the data in one place and back it up in one place.

Gardner: How long have you been using Bitdefender GravityZone Enterprise Security, and why do you keep renewing?

Reynolds: It's been about nine years. I keep renewing because it works, and I like their support. Whenever I have a problem, or whenever I need to move -- like from different versions of VMware or going to NSX and I change the actual VMware parts -- the Bitdefender technology is just there, and the instructions are there, too.

> *Whenever I have a problem, or whenever I need to move, … the Bitdefender technology is just there, and the instructions are there, too.*

It's all about relationships with me. I stick with people because of relationships -- well, the performance as well, but that's part of the relationship. I mean, if your friend kept letting you down, they wouldn't be your friend anymore.

Gardner: Let's talk about that performance. You have some really large 2-D and 3-D graphics files at work constantly. You're using Autodesk Revit, as you mentioned, [Bluebeam Revu](#), [Microsoft Office](#), [Adobe](#), so quite a large portfolio.

These are some heavy-lifting apps. How does their performance hold up? How do you keep the virtualized delivery invisible across your physical and virtualized workstations?

High performance keeps users happy

Reynolds: Number one, I must keep the users happy. If the users aren't happy and if they don't think the performance is there, then you are not going to last long.

I have a good example, Dana. I told you I have Macs in the marketing department, and the reason they kept Macs is because they want their performance with the Adobe apps. Now, they use the Macs as thin clients and connect to a virtual desktop to do their work. It's only when they are doing big video editing that they resume using their Macs natively. Most of the time, they are just using them as a thin client. For me, that's a real vote of confidence that this environment works.

Gardner: Do you have a virtualization density target? How are you able to make this as efficient as possible, to get full centralized data center efficiency benefits?

Reynolds: I have some guidelines that I've come up with over the years. I try to limit my hosts to about 30 active VMs at a time. We are actually now at the point where I am going to have to add another node to the cluster. It's going to be compute only, it won't be involved in the storage part. I want to keep the ratio of CPUs and RAM about the same. But generally speaking, we have about 30 active virtual desktops per host.

Gardner: How does Bitdefender's approach factor into that virtualization density?

Reynolds: The way that Bitdefender does it -- and I really like this -- is they license by the socket. So whether I have 10 or 100 on there, it's always by the socket. And these are HPE DL380s, so they are two sockets, even though I have 40 cores.

I like the way they license their coverage. It gives me a lot of flexibility, and it helps me plan out my environment. Now, I'm looking at adding another host, so I will have to add a couple of more cores. But that still gives me a lot of growth room because I could have 120 active desktops running and I'm not paying by the core, and I'm not paying by the individual virtual desktop. I am paying for Bitdefender by the socket, and I really like it that way.

> *[Bitdefender] gives me a lot of flexibility, and it helps me plan out my environment.*

Gardner: You don't have to be factoring the VMs along the way as they spin up and spin down. It can be a nightmare trying to keep track of them all.

Reynolds: Yes, I am glad I don't have to do that. As long as I have the VMware agent installed and NSX on the VMware side, then it just shows up in GravityZone, and it's protected.

Prevent, rather than react, to problems

Gardner: Dan, we have been focusing on performance from the end-user perspective. But let's talk about how this impacts your administration, your team, and your IT organization.

How has your security posture, centralization, and reliance on virtualization allowed your team to be the most productive?

Reynolds: I use GravityZone's reporting features. I have it tell me weekly the posture of my physical machines and my virtual machines. I use the GravityZone interface. I look at it quite regularly, maybe two or three times a week. I just get in and look around and see what's going on.

I like that it keeps itself up to date or lets me know it needs to be updated. I like the way that the virus definitions get updated automatically and pushed out automatically, and that's across all environments. I really like that. That helps me, because it's something that I don't have to constantly do.

> *I like that [GravityZone] keeps itself up to date or lets me know it needs to be updated.*

I would rather watch than do. I would rather have it tell me or e-mail me than I find out from my users that their machines aren't working properly. I like everything about it. I like the way it works. It works with me.

Gardner: It sounds like Bitdefender had people like you, a jack of all trades, in mind when it was architected, and that wasn't always the case with security. Usually before the security would play catch-up to the threats, rather than anticipating the needs of those in the trenches fighting the security battle.

Reynolds: Yes, very much so. At other places I have worked and with other products, that was an absolute true statement, yes.

Gardner: Let's look at some of the metrics of success. Tell us how you measure that. I know security is measured best when there are no problems.

But in terms of people, process, and technology, how do we evaluate in terms of costs, man hours, of being proactive? How do we measure success when it comes to a good security posture for an organization like yours?

Security supports steady growth

Reynolds: I will be the first to admit I am a little weak in describing that. But I do have some metrics that work. For example, we didn't need to replace our desktops often. We had been using our desktops for eight years, which is horrible in one sense, but in another sense, it says we didn't have to. And then when those desktops were about as dead as dead could be, we replaced them with less expensive thin clients, which are almost disposable devices.

I envision a day when we're using Raspberry Pi as our thin clients and we don't spend any big money. That's the way to sum it up. All my money is spent on maintenance for applications and platform software, and you are not going to get rid of that.

Another big payoff is around employee happiness. A little over two years ago, when we had to collapse the offices, more people could work from home. It kept a lot of people that probably would have walked out. That happened because of the groundwork and foundation I had put in. From that time, we have had two of the best years the company has ever had, even after that consolidation.

And so, for me, personally, that was kind of like I had something to do with that, and I can take some pride in that.

Gardner: Dan, when I hear your story, the metrics of success that I think about are that you're able to accommodate growth, you can scale up, and if you had to – heaven forbid -- you could scale down. You're also in a future-proofing position because you've gone software-defined, you have centralized and consolidated, you've gone highly virtualized across-the-board, and you can accommodate at-home users and bring your own devices (BYOD).

Perhaps you have a merger and acquisition in the works, who knows? But you can accommodate that and that means business agility. These are some of the top business outcome metrics of success that I know companies large and small look for. So hats off to you on that.

Reynolds: Thank you very much. I hate to use the word "pride" but I'm proud of what I've been able to accomplish the last few years. All the work I have done in the prior years is paying off.

Gardner: One of my favorite sayings is, "Architecture is destiny." If you do the blocking and tackling, and you think strategically -- even while you are acting tactically -- it will pay off in spades later.

Okay, let's look to the future before we end. There are always new things coming out for modernizing data centers. On the hardware side, we're hearing about hyper-converged infrastructure (HCI), for example. We're also seeing use of automated IT ops and using artificial intelligence (AI) and machine learning (ML) to help optimize systems.

Where does your future direction lead, and how does your recent software and security posture work enable you to modernize when you want?

Future solutions, scaled to succeed

Reynolds: Obviously, hyper-converged infrastructure is upon us and many have embraced it. I think the small- to medium-sized business (SMB) has been a little reluctant because the cost is very high for an SMB.

I think that cost of entry is going to come down. I think we are going to have a solution that offers all the benefits but is scaled down for a smaller firm. When that happens, everything I have done is going to transfer right over.

I have software-based storage. I have some software-based networking, but I would love to embrace that even more. That would be the icing on the cake and take some of the physical load off of me. The work that I have to do with switches and cabling and network adapters -- if I could move that into the hyper-converged arena, I would love that.

> *The work that I have to do with switches and cabling and network adapters – if I could move that into the hyper-converged arena, I would love that.*

Gardner: Also, more companies are looking to use cloud, multi-cloud, and hybrid cloud. Because you're already highly virtualized, because your security is optimized for that, whatever choices your company wants to take with vis-à-vis cloud and Software-as-a-Service (SaaS) you're able to support that.

Reynolds: Yes, we have a business application that manages our projects, does our time keeping, and all the accounting. It is a SaaS app. And, gosh, I was glad when it went SaaS. That was just one thing that I could get off of my plate -- and I don't mean that in a bad way. I wanted it to be handled even better by moving to SaaS where you get economy of scale that you can't provide as an IT individual.

Gardner: Any last words of advice for organizations -- particularly those wanting to recognize all the architectural and economic benefits, but might be concerned about security and performance?

Research renders rewards

Reynolds: Research, research, research -- and then more research. When I started, everybody said there's no way we could virtualize Revit and Autodesk. Of course, we did and it worked fine. I ignored them, and you have to be willing to experiment and take some chances sometimes. But by researching, testing, and moving forward gently, it's a long road, but it's worth it. It will pay off.

Gardner: I'm afraid we'll have to leave it there. You've been listening to a sponsored BriefingsDirect discussion on how a large architectural firm gains better overall security, management, and data center consolidation while preserving the highest workspace performance.

We learned how Bitdefender GravityZone Enterprise Security is meeting the challenges related to a top performer with nearly 100 percent virtualized clients across a distributed, multi-office environment.

So please join me in thanking our guest, Dan Reynolds, Director of IT at BLDD Architects in Decatur, Illinois. Thanks so much, Dan.

Reynolds: Thank you, Dana.

Gardner: I am Dana Gardner, Principal Analyst at Interarbor Solutions, your host and moderator for this ongoing series of BriefingsDirect use case discussions. A big thank you also to our sponsor, Bitdefender, for supporting these presentations.

Lastly, thanks to our audience for joining. Please pass this along to your IT community and do come back next time.

Listen to the **podcast**. **Find it on iTunes**. **Download** the transcript. **Sponsor: Bitdefender.**

Transcript of a discussion on how BLDD Architects gains better overall security, management, and data center consolidation from being nearly 100 percent virtualized while preserving the highest workspace performance, even across multiple distributed offices. Copyright Interarbor Solutions, LLC, 2005-2019. All rights reserved.

You may also be interested in:

- Regional dental firm Great Expressions protects distributed data with lower complexity thanks to amalgam of Nutanix HCI and Bitdefender security
- How MSPs Leverage Bitdefender's Layered Approach to Security for Comprehensive Client Protection
- How a large Missouri medical center developed an agile healthcare infrastructure security strategy
- Kansas Development Finance Authority gains peace of mind, end-points virtual shield using Hypervisor-level security
- How IT innovators turn digital disruption into a business productivity force multiplier
- How a Florida school district tames the Wild West of education security at scale and on budget
- The next line of defense—How new security leverages virtualization to counter sophisticated threats
- Cybersecurity standards: The Open Group explores security and safer supply chains