How a Large Missouri Medical Center Developed a Comprehensive Healthcare Infrastructure Security Strategy

Transcript of a how a large Missouri medical center developed a comprehensive healthcare infrastructure security strategy from the edge to the data center and everything in between.

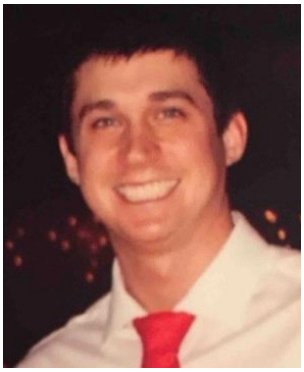
Listen to the podcast. Find it on iTunes. Get the mobile app. Download the transcript. Sponsor: Bitdefender

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

Healthcare provider organizations are among the most challenging environments to develop and implement comprehensive and agile security infrastructures. These are usually sprawling campuses with large ecosystems of practitioners, suppliers, and patient-facing facilities. They also operate under stringent compliance requirements, with data privacy as a top priority.

At the same time, large hospitals and their extended communities are seeking to become more patient outcome-focused as they deliver ease-of-use, the best applications, as well as up-to-date data analysis to their staffs and physicians.

This BriefingsDirect security insights discussion examines how a large Missouri medical center developed a comprehensive healthcare infrastructure security strategy from the edge to the data center -- and everything in between.



Yarbro

To learn how healthcare security can become more standardized and proactive with unified management and lower total costs, please join me now in welcoming Phillip Yarbro, Network and Systems Engineer at Saint Francis Healthcare System in Cape Girardeau, Missouri. Welcome, Phillip.

Phillip Yarbro: Hi, thanks for having me. It's a pleasure to be here.

Gardner: When it comes to security nowadays, Phil, there's a lot less chunking it out, of focusing on just devices or networks separately or on data centers alone. It seems that security needs to be deployed holistically -- or at least strategically – with standardized solutions, focused on across-the-board levels of coverage.

Tell us how you've been able to elevate security to that strategic level at Saint Francis Healthcare System.

Healthy digital recordkeeping

Yarbro: As a healthcare organization, we have a wide variety of systems from our electronic medical records (EMR) that we are currently using, to our 10-plus legacy EMRs, our home health system, payroll time and attendance, and -- like you said -- that's a wide variety of systems to keep up-to-date with antivirus solutions, making sure all of those are secure, especially with them being virtualized. All of those systems require a bunch of different exclusions and whatnot.

With our previous EMR, it was really hard to get those exclusions working and to minimize false positives. Over the past several years, security demands have increased. There are a lot more PCs and servers in the environment. There are a lot more threats taking place in healthcare systems, some targeting protected health information (PHI) or financial data, and we needed a solution that would protect a wide variety of endpoints; something that we could keep up-to-date extremely easily, and that would cover a wide variety of systems and devices.

Gardner: It seems like they're adding more risk to this all the time, so it's not just a matter of patching and keeping up. You need to be proactive, whenever possible.

Yarbro: Yes, being proactive is definitely key. Some of the features that we like about our latest systems are that you can control applications, and we're looking at doing that to keep our systems even more secure, rather than just focusing on real-time threats, and things like that.

Being proactive is definitely key. We like to control applications to keep our systems even more secure, rather than just focusing on real-time threats.

Gardner: Before we learn more about your security journey, tell us about Saint Francis Healthcare System, the size of organization and also the size of your IT department.

Yarbro: Saint Francis is between St. Louis and Memphis. It's the largest hospital between the two cities. It's a medium-sized hospital with 308 beds. We have a Level III neonatal intensive care unit (NICU) and a Level III trauma center. We see and treat more than 700,000 people within a five-state area.

With all of those beds, we have about 3,000 total staff, including referring physicians, contractors, and things like that. The IT helpdesk support, infrastructure team, and networking team amounts to about 30 people who support the entire infrastructure.

Gardner: Tell us about your IT infrastructure. To what degree are you using thin clients and virtual desktop infrastructure (VDI)? How many servers? Perhaps a rundown of your infrastructure in total?

Yarbro: We have about 2,500 desktops, all of which are Microsoft Windows desktops. Currently, they are all supplied by our organization, but we are looking at implementing a bring-your-own-device (BYOD) policy soon. Most of our servers are virtualized now. We do have a few physical ones left, but we have around 550 to 600 servers.

Of those servers, we support about 60 Epic servers and close to 75 Citrix servers. On the VDI side, we are using VMware Horizon View, and we are supporting about 2,100 virtual desktop sessions.

Gardner: Data center-level security is obviously very important for you. This isn't just dealing with the edge and devices.

Virtual growth

Yarbro: Correct, yes. As technology increases, we're utilizing our virtual desktops more and more. The data center virtualization security is going to be a lot more important going forward because that number is just going to keep growing.

Gardner: Let's go back to your security journey. Over the past several years, requirements have gone up, scale has gone up, complexities have gone up. What did you look for when you wanted to get more of that strategic-level security approach? Tell us about your process for picking and choosing the right solutions.

Yarbro: A couple of lessons that we learned from our previous suppliers is that when we were looking for a new security solution we wanted something that wouldn't make us experience scan storms. Our previous system didn't have the capability to spread out our virus scans, and as a result whenever the staff would come in, in the morning and evenings, users were negatively affected by latency because of the scans. Our virtual servers all scanned at the same time.

So whenever those were set to scan, our network just dragged to a halt. We were looking for a new solution that didn't have a huge impact on our virtual environment. We have a wide variety of systems and applications. Epic is our main EMR, but we also have 10 legacy EMRs, a picture archiving and communication system (PACS), rehab, home health, payroll, as well as time and attendance apps. There are a wide variety of systems that all have different exclusions and require different security processes. So we were hoping that our new solution would minimize false positives.

We have a wide variety of systems and applications. Epic is our main EMR, but we also have 10 legacy EMRs, a picture archiving and communication system (PACS), rehab, home health, payroll, as well as time and attendance apps.

Since we are healthcare organization, there is PHI and there is sensitive financial data. We needed a solution that was Health Insurance Portability and Accountability Act (HIPAA)-compliant as well as Payment Card Industry Data Security Standard (PCI DSS)-compliant. We wanted a system that made a really good complement and that made it easy to manage everything.

Our previous ones, we were using Trend Micro in conjunction with Malwarebytes, were in two consoles. A lot of the time it was hard to get the exclusions to apply down to the devices when it came time to upgrade the clients. We had to spend time upgrading clients twice. It didn't always work right. It was a very disruptive do-it-yourself operation, requiring a lot of resources on the backend. We were just looking for something that was much easier to manage.

Defend and prevent attacks

Gardner: Were any of the recent security breaches or malware infections something that tripped you up? I know that ransomware attacks have been on people's minds lately.

Yarbro: With the WannaCry and Petya attacks, we actually received a proactive e-mail from Bitdefender saying that we were protected. The most recent one, the Bad Rabbit, came in the next day and Bitdefender had already said that we were good for that one as well. It's been a

great peace-of-mind benefit for our leadership here knowing that we weren't affected, that we were already protected whenever such news made its way to them in the morning.

It's been a great peace-of-mind benefit for our leadership to hear from Bitdefender that we were already protected (from ransomware attacks).

Gardner: You mentioned Bitdefender. Tell me about how you switched, when, and what's that gotten for you at Saint Francis?

Yarbro: After we evaluated Bitdefender, we worked really closely with their architects to make sure that we followed best practices and had everything set up, because we wanted to get our current solutions out of there as fast as possible.

For a lot of our systems we have test servers for testing computers. We were able to push Bitdefender out within minutes of having the consoles set up to these devices. After we received some exclusion lists, or were able to test on those, we made sure that Bitdefender didn't catch or flag anything.

We were able to deploy Bitdefender on 2,200 PCs, all of our virtual desktops and VDI, and roughly 425 servers between May and July with minimal downtime, knowing that the downtime we had was simply to reboot the servers after we uninstalled our previous antivirus software.

We recently upgraded the remaining 150 or so servers, which we don't have test systems for. They were all of our critical servers that couldn't go down, such as our backup systems. We were able to push Bitdefender out to all of those within a week, again, without any downtime, and straight from the console.

Gardner: Tell us about that management capability. It's good to have one screen, of course, but depth and breadth are also important. Has there been any qualitative improvement, in addition to the consolidation improvement?

Yarbro: Yes. Within the Bitdefender console, with our various servers, we have different policies in place, and now we can get very granular with it. The stuff that takes up a lot of resources we have it set to scan, maybe every other day instead of every day, but you can also block off servers.

Bitdefender also has a firewall option that we are looking at implementing soon, where you can group servers together as well as open the same firewall roles, and things like that. It just helps give us great visibility into making sure our servers and data center are protected and secured.

Gardner: You mentioned that some of the ransomware attacks recently didn't cause you difficulty. Are there any other measurements that you use in order to qualify or quantify how good your security is? What did you find improved with your use of Bitdefender GravityZone?

Yarbro: It reduced our time to add new exclusions to our policies. That used to take us about 60 minutes to do because we had to login to both consoles, do it, and make sure it got pushed out. That's down to five minutes for us. So that's a huge timesaving.

It reduced our time to add new exclusions to our policies. That used to take us about 60 minutes. It's down to five minutes. That's a huge timesaving.

From the security administration side, by going into the console and making sure that everything is still reporting, that everything still looks good, making sure there haven't been any viruses on

any machines -- that process went down from 2.5 to three hours a week to less than 15 minutes.

GravityZone has a good reporting setup. I actually have a schedule set every morning to give me the malware activity and phishing activity from the day before. I don't even have to go into the console to look at all that data. I get a nice e-mail in the morning and I can just visually see what happened.

At the end of the month we also have a reports setup that tells us the 10 highest endpoints that were infected with malware, and we can be proactive and go out and either re-educate our staff if it's happening with a certain person. Not only from the security administration time has it saved us, it also helps us with security-related trouble calls. I would say that they have probably dropped at least 10 percent to 15 percent on those since we rolled out Bitdefender hospital-wide.

Gardner: Of course, you also want to make sure your end-users are seeing improvement. How about the performance degradation and false positives? Have you heard back from the field? Or maybe not, and that's the proof?

User-friendly performance

Yarbro: You said it best right there. We haven't heard anything from end-users. They don't even know it's there. With this type of roll out, no news is good news. They didn't even notice the transition except an increase in performance. But otherwise they didn't even know that anything was there, and the false positives haven't been there.

We have our exclusion policy set, and it really hasn't given us any headaches. It has helped our physicians quite a bit because they need uninterrupted access to medical information. They used to have to call whenever our endpoints lost their exclusion list and their software was getting flagged. It was very frustrating for them. They must be able to get into our EMR systems and log that information as quickly as possible. With Bitdefender, they haven't had to call IT or anything like that, and it's just helped them greatly.

Gardner: Back to our high-level discussion about going strategic with security, do you feel that using GravityZone and other Bitdefender technologies and solutions have been able to help you elevate your security to being comprehensive, deep, and something that's more holistic?

Multilayered, speedier security

Yarbro: Yes, definitely. We did not have this level of control with our old systems. First of all, we didn't have antivirus on all of our servers because it impacted them so negatively. Some of our more critical servers didn't even have protection.

Just having our entire environment at 100 percent coverage has made us a lot more secure. The extra features that Bitdefender offers -- not just the antivirus piece but also the application blocking, device control, and firewall roles control just adds another level of security that we didn't even dream about with our old solutions.

Gardner: How about the network in the data center? Is that something that you've been able to better applying policies and rules to in ways that you hadn't before?

Yarbro: Yes, now with Bitdefender there is an option to offload scanning to a security server. We decided at first not to go with that solution because when we installed Bitdefender on our VDI endpoints, we didn't see any increased CPU or memory utilization across any of our hosts, which is a complete 180-degrees from what we had before.

But for some of our other servers, servers in our DMZ, we are thinking about using the security server approach to offload all of the scanning. It will further increase performance across our virtualized server environment.

Gardner: From an economic standpoint, that also gives you more runway, so to speak, in terms of having to upgrade the hardware. You are going to get more bang for your buck in your infrastructure investments.

Yarbro: Yes, exactly. And with that servers-level security, it's beneficial to note that if there's ever an upgrade for software or patches, that once a server checks into it first, if another server checks in or another desktop checks in, it already has that exclusion. It doesn't have to send that file back or check it again -- it already knows. So it just speeds things up, almost exponentially, on those other devices.

With servers-level security, it doesn't have to send that file back or check it again -- it already knows. That just speeds things up, almost exponentially.

Gardner: Just a more intelligent way to go about it, I would think.

Yarbro: Yes.

Gardner: Have you been looking to some of the other Bitdefender technologies? Where do you go next in terms of expanding your horizon on security?

One single pane of secure glass

Yarbro: The extra Bitdefender components that we're kind of testing right now are device control and firewall, of being able to make sure that only devices that we allow can be hooked up, say via USB ports. That's critical in our environment. We don't want someone to come in here with a flash drive and install or upload a virus or anything along those lines.

The application and website blacklisting is also something that's coming in the near future. We want to make sure that no malware, if it happens, can get past. We are also looking to consolidate two more management systems into just our Bitdefender console. That would be for encryption and patch management.

Bitdefender can do encryption as well, so we can just roll our current third-party software into Bitdefender. It will give us one pane of glass to manage all of these security features. In addition to patch management, we are using two different systems; one for servers, one for Windows endpoints. If we can consolidate that all into Bitdefender, because those policies are already in there, it would just be a lot of easier to manage and make us a lot more secure.

Gardner: Anything in terms of advice for others who are transitioning off of other security solutions? What would you advise people to do as they are going about a change from one security infrastructure to another?

Slow and steady saves the servers

Yarbro: That's a good question. Make sure that you have all of your exclusion lists set properly. Bitdefender already in the console has Windows, VMware's and Citrix's best practices in their policies.

You only have to worry about your own applications, as long as you structure it properly from the beginning. Bitdefender's engineers helped us with quite a bit. Just go slow and steady. From May to July we were able to do 425 servers. We probably could have done more than that, but we didn't want to risk breaking something. Luckily, we didn't push it to those more critical servers because we did change a few of our policy settings that probably would have broken a few of those and had us down for a while if we had put it all in right away.

Gardner: I'm afraid we'll have to leave it there. You've been listening to a sponsored BriefingsDirect discussion on how a large Missouri medical center developed a comprehensive healthcare infrastructure security strategy -- from the edge to the data center, and everything in between.

And we've learned how security at this major healthcare organization has become more standardized and proactive thanks to a unified management approach. They have delivered better results to their end users. So please join me now in thanking our guest, Phillip Yarbro, Network and Systems Engineer at Saint Francis Healthcare System. Thank you, Phillip.

Yarbro: Thank you. Thanks for having me.

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

Follow me on Twitter @Dana_Gardner and find more security-focused podcasts at BriefingsDirect.com. Again, thanks to our audience for joining. Please pass this content along in your IT community, and do come back next time.

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

You may also be interested in:

- 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

- 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