Better IT Security Comes with Ease in Overhead for Rural Virginia County

Transcript of a discussion on how a small team of IT administrators at a rural Virginia county government has built a technically advanced security posture that blends the right amounts of automation with flexible administration.

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.

Managing IT for a rural Virginia county government means doing more with less, even as the types and sophistication of cybersecurity threats grow. For County of Caroline, a small team of IT administrators has built a technically advanced security posture that blends the right amounts of automation with flexible administration.

Farmer

Here to share their story on improving security in a public sector organization are Bryan Farmer, System Technician at County of Caroline in Bowling Green, Virginia. Welcome, Bryan.

Bryan Farmer: Thanks for having me.

Gardner: We are also here with David Sadler, Director of Information Technology for County of Caroline. Welcome, Dave.

David Sadler: Thanks. It's great to be here.

Gardner: Dave, tell us about County of Caroline and your security requirements. What makes security particularly challenging for a public sector organization like yours?

Sadler: As everyone knows, small governments in the State of Virginia -- and all across the United States and around the world -- are being targeted by a lot of bad guys. For that reason, we have the responsibility to safeguard the data of the citizens of this county -- and also of the customers and other people that we interact with on a daily basis. It's a paramount concern for us to maintain the security and integrity of that data so that we have the trust of the people we work with.

Gardner: Do you find that you are under attack more often than you used to be?

Sadler

Sadler: The headlines of nearly any major newspaper you see, or news broadcasts that you watch, show what happens when the bad guys win and the local governments lose. Ransomware, for example, happens every day. We have seen a major increase in these attacks, or attempted attacks, over the past few years.

Gardner: Bryan, tell us a bit about your IT organization. How many do you have on the frontlines to help combat this increase in threats?

Farmer: You have the pleasure today of speaking with the entire IT staff in our little neck of the woods. It's just the two of us. For the last several years it was a one-man operation, and they brought me on board a little over a year-and-a-half ago to lend a hand. As the county grew, and as the number of users and data grew, it just became too much for one person to handle.

Gardner: You are supporting how many people and devices with your organization?

Small-town support, high-tech security

Farmer: We are mainly a Microsoft Windows environment. We have somewhere in the neighborhood of 250 to 300 users. If you wrap up all of the devices, Internet of Things (IoT) stuff, printers, and things of that nature, it's 3,000 to 4,000 devices in total.

Sadler: But the number of devices that actually touch our private network is in the neighborhood of around 750.

Farmer: We are a rural area so we don't have the luxury of having fiber in between all of our locations and sites. So we have to resort to virtual private networks (VPNs) to get traffic back and forth. There are airFiber connections, and we are doing some stuff over the air. We are a mixed batch. There is a little bit of everything here.

Gardner: Just as any business, you have to put your best face forward to your citizens, voters, and taxpayers. They are coming for public services, going online for important information. How large is your county and what sort of applications and services you are providing to your citizens?

Farmer: Our population is 30,000?

Sadler: Probably 28,000 to 30,000 people, yes.

Farmer: A large portion of our county is covered by a U.S. Army training base, it's a lot of nonliving area, so to speak. The population is condensed into a couple of small areas.

We host a web site and forum. It's not as robust as what you would find in a big city or a major metropolitan area, but people can look up their taxes, permit prices, things of that nature; basic information that the average citizen will need such as utility information.

Gardner: With a potential of 30,000 end users -- and just two folks to help protect all of the infrastructure, applications, and data -- automation and easy-to-use management must be super important. Tell us where you were in your security posture before and how you have recently improved on that.

Finding a detection solution

Sadler: Initially when I started here, and I came over from the private sector, we were running one of the big companies that had a huge name but was basically not showing us the right amount of good protection, you could say.

So we switched to a second company, Kaspersky, and immediately we started finding detections of existing malware and different anomalies in the network that had existed for years without protection from Symantec. So we settled on Kaspersky. And anytime you go to an enterprise-level antivirus (AV) endpoint solution, the setup, adjustment, and on-boarding process takes longer than what a lot of people would lead you to believe.

It took us about six months with Kaspersky. I was by myself, so it took me about six months to get everything set up and running like it should, and it performed extremely well. I had a lot of granularity as far as control of firewalls and that type of product.

The granularity is what we like because we have users that have a broad range of needs. We have to be able to address all of those broad ranges under one umbrella.

Unfortunately, when the US Department of Homeland Security decided to at first recommend that you not use [Kaspersky] and then later banned that product from use, we were forced to look for a replacement solution, and we evaluated multiple different products.

We were looking for granularity because we wanted to be able to address the needs of everyone under the umbrella with one particular product.

Again, what we were looking for was granularity because we wanted to be able to address the needs of everyone under the umbrella with one particular product. Many of the different AV endpoint solutions we evaluated lacked that granularity. It was, more or less, another version of the software that we started with. They didn't give a real high level of protection or did not allow for adjustment.

When we started evaluating a replacement, we were finding things that we could not do with a particular product. We spent probably about six months evaluating different products -- and then we landed on Bitdefender.

Now, coming from the private sector and dealing with a lot of home users, my feelings for Bitdefender were based on the reputation of their consumer-grade product. They had an extremely good reputation in the consumer market. Right off the bat, they had a higher score when we started evaluating. It doesn't matter how easy a product is to use or adjust if their basic detection level is low, then everything else is a waste of time.

Bitdefender right off the bat has had a reputation for having a high level of detection and protection as well as a low impact on the systems. Being a small, rural county government, we use machines that are unfortunately a little bit older than what would be recommended, five to six years old. We are using some older machines that have lower processing power, so we could not take a product that would kill the performance of the machine and make it unusable.

During our evaluations we found that Bitdefender performed well. It did not have a lot of system overhead and it gave us a high level of protection. What's really encouraging is when you switch to a different product and you start scaling your network and find threats that had been existing there for years undetected. Now you know at least you are getting something for your money, and that's what we found with Bitdefender.

Gardner: I have heard that many times. It has to, at the core, be really good at detecting. All the other bells and whistles don't count if that's not the case. Once you have established that you are detecting what's been there, and what's coming down the wire every day, the administration does become important.

Bryan, what is the administration like? How have you improved in terms of operations? Tell us about the ongoing day-to-day life using Bitdefender.

Managing mission-critical tech

Farmer: We are Bitdefender GravityZone users. We host everything in the cloud. We don't have any on-premises Bitdefender machines, servers, or anything like that, and it's nice. Like Dave said, we have a wide range of users and those users have a wide range of needs, especially with regards to Internet access, web page access, stuff like that.

We are Bitdefender GravityZone users. We host everything in the cloud … and it's nice.

For example, a police officer or an investigator needs to be able to access web sites that a clerk in the treasurer's office just doesn't need to be able to access. To be able to sit at my desk or take my laptop out anywhere that I have an Internet connection and make an adjustment if someone cannot get to somewhere that they need is invaluable. It saves so much time.

We don't have to travel to different sites. We don't have to log-in to a server. I can make adjustments from my phone. It's wonderful to be able to set up these different profiles and to have granular control over what a group of people can do.

We can adjust which programs they can run. We can remove printing from a network. There are so many different ways that we can do it, from anywhere as long as we have a computer and Internet access. Being able to do that is wonderful.

Gardner: Dave, there is nothing more mission-critical than a public safety officer and their technology. And that technology is so important to everybody today, including a police officer, a firefighter, and an emergency medical technician (EMT). Any feedback when it comes to the protection and the performance, particularly in those mission-critical use cases?

Sadler: Bitdefender has allowed us the granularity to be able to adjust so that we don't interfere with those mission-critical activities that the police officer or the firefighter are trying to perform.

So initially there was an adjustment period. Thank goodness everybody was patient during that process and I think now we are finally -- about a year into the process, a little over a year -- and we have gotten stuff set pretty good. The adjustments that we are having to make now are minor. Like Bryan said, we don't have an on-premises security server here. Our service is hosted in the cloud, and we have found that that is an actual benefit. Before, with having a security server and the software hosted on-premises, there were machines that didn't touch the network. We are looking at probably 40 to 50 percent of our machines that we would have had to manage and protect [manually] because they never touch our network.

The Bitdefender GravityZone cloud-based security product offers us the capability to be able to monitor for detections, as well as adjust firewalls, etc., on machines that we never touch or never see on our network. It's been a really nice product for us and we are extremely happy with its performance.

Bitdefender GravityZone offers us the capability to be able to monitor for detections, as well as adjust firewalls, etc., on machines that we never touch or never see on our network.

Gardner: Any other metrics of success for a public sector organization like yours with a small support organization? In a public sector environment you have to justify your budget. When you tell the people overseeing your budget why this is a good investment, what do you usually tell them?

Sadler: The benefit we have here is that our bosses are aware of the need to secure the network. We have cooperation from them. Because we are diligent in our evaluation of different products, they pretty much trust our decisions.

Justifying or proving the need for a security product has not been a problem. And again, the day-to-day announcements that you see in the newspaper and on web sites about data breaches or malware infections -- all that makes justifying such a product easier.

Gardner: Any examples come to mind that have demonstrated the way that you like to use these products and these services? Anything come to mind that illustrates why this works well, particularly for your organization?

Stop, evaluate, and reverse infections

Farmer: Going back to the cloud hosting, all a machine has to do is touch the Internet. We have a machine in our office here right now that one of our safety officials had and we received an email notification that something was going on. That machine needed to be disinfected, we needed to take a look at this machine.

The end-user didn't have to notice it. We didn't have to wait until it was a huge problem or a ransomware thing or whatever the case may be. We were notified automatically in advance. We were able to contact the user and get to the machine. Thankfully, we don't think it was anything super-critical, but it could have been.

The end-user didn't have to notice it. We were notified automatically in advance. We were able to contact the user and get to the machine.

That automation was fantastic, and not having to react so aggressively, so to speak. So the proactivity that a solution like Bitdefender offers is outstanding.

Gardner: Dave, anything come to mind that illustrates some of the features or functions or qualitative measurements that you like?

Sadler: Yes, with Bitdefender GravityZone, it will sandbox a suspicious activity and watch its actions and then roll back if something bad is going on.

We actually had a situation where a vendor that we use on a regular basis from a large company, well-respected, called in to support a machine that they had in one of our offices. We were immediately notified via email that a ransomware attack was being attempted.

So this vendor was using a remote desktop application. Somehow the end-user got directed to a bad site, and when it failed the first time on their end, all they could tell was, "Hey, my remote desktop software is not working." They stopped and tried it again.

We were notified on our end that a ransomware attack had been stopped, evaluated, and reversed by Bitdefender. Not once, but twice in a row. So we were immediately able to contact that office and say, "Hey, stop what you are doing."

Then we followed up by disconnecting that computer from the network and evaluating them for infection, to make sure that everything had been reversed. Thank goodness, Bitdefender was able to stop that ransomware attack and actually reverse the activity. We were able to get a clean scan and return that computer back to service fairly quickly.

Gardner: How about looking to the future? What would you like to see next? How would you improve your situation, and how could a vendor help you do that?

Meeting future government requirements

Sadler: The State of Virginia just passed a huge bill dealing with election security and everybody knows that that's a huge, hot topic when it comes to security right now. And because most of the localities in Virginia are independent localities, the state passed a bill that allows state Department of Elections and the US Homeland Security Department to step in a little bit more to the local governments and monitor or control the security of the local governments, which in the end is going to be a good thing.

But a lot of the products or solutions that we are now being required to be able to answer about are already answered by the Bitdefender product. For example, automated patch management notification of security issues.

So, Bitdefender right now is already answering a lot of the new requirements. The one thing that I would like to see … from what I understand the cloud-based version of Bitdefender does not allow you to do mobile device management. And that's going to be required by some of these regulations that are coming down. So it would be really nice if we could have one product that would do the mobile device management as well as the cloud-based security protection for a network.

It would be really nice if we could have one product that would do the mobile device management as well as the cloud-based security protection for a network.

Gardner: I imagine they hear you loud and clear on that. When it comes to compliance like you are describing from a state down to a county, for example, many times there are reports and audits that are required. Is that something that you feel is supported well? Are you able to rise to that occasion already with what you have installed?

Farmer: Yes, Bitdefender is a big part of us being able to remain compliant. The Criminal Justice Information Services (CJIS) audit is one we have to go through on a regular basis. Bitdefender helps us address a lot of the requirements of those audits as well as some of the upcoming audits that we haven't seen yet that are going to be required by this new regulation that was just passed this past year in the Commonwealth of Virginia.

But from the previews that we are getting on the requirements of those newly passed regulations, it does appear that Bitdefender is going to be able to help us address some of those needs, which is good. By far, it's the capability to be able to answer some of

those needs with Bitdefender that is superior to the products that we have been using in the past.

Gardner: Given that many other localities, cities, towns, municipalities, counties are going to be facing similar requirements, particularly around election security, for example, what advice would you give them, now that you have been through this process? What have you learned that you would share with them so that they can perhaps have an easier go at it?

Research reaps benefits in time, costs

Farmer: I have seen in the past a lot of places that look at the first line item, so to speak, and then make a decision on that. Then when they get down the page a little bit and see some of the other requirements, they end up in situations where they have two, three, or four pieces of software, and a couple of different pieces of hardware, working together to accomplish one goal. Certainly, in our situation, Bitdefender checks a lot of different boxes for us. If we had not taken the time to research everything properly and get into the full breadth of what's capable, we could have spent a lot more money and created a lot more work and headaches for ourselves.

A lot of people in IT will already know this, but you have to do your homework. You have to see exactly what you need and get a wide-angle view of it and try to choose something that helps do all of those things. Then automate off-site and automate as much as you can to try to use your time wisely and efficiently.

You have to do your homework. You have to see exactly what you need and get a wide-angle view of it and try to choose something that helps do all of those things.

Gardner: Dave, any advice for those listening? What have you learned that you would share with them to help them out?

Sadler: The breadth of the protection that we are getting from Bitdefender has been a major plus. So again, like Bryan said, find the product that you can put together under one big umbrella -- so that you have one point of adjustment. For example, we are able to adjust firewalls, virus protection, and off-site USB protection -- all this from one single control panel instead of having to manage four or five different control panels for different products.

It's been a positive move for us, and we look forward to continuing to work with that product and we are watching the new product still under development. We see new features coming out constantly. So if anyone from Bitdefender is listening, keep up the good work. We will hang in there with you and keep working.

But the main thing for IT operators is to evaluate your possibilities, evaluate whatever possible changes you are going to make before you do it. It can be an investment of money and time that goes wasted if you are not sure of the direction you are going in.

Use a product that has a good reputation and one that checks off all the boxes like Bitdefender.

Farmer: In a lot of these situations, when you are working with a county government or a school you are not buying something for 30, 60, or 90 days – instead you are buying a year at a time. If you make an uninformed decision, you could be putting yourself in a jam time- and labor-wise for the next year. That stuff has lasting effects. In most counties, we get our budgets and that's what we have. There are no do-overs on stuff like this. So, it speaks back to making a well-informed decision the first time.

In most counties, we get our budgets and that's what we have. There are no do-overs … So, it speaks back to making a well-informed decision the first time.

Gardner: Yes, it's always important to think strategically whenever you can. I'm afraid we'll have to leave it there. You have been listening to a sponsored BriefingsDirect discussion on how a rural county in Virginia improved its security posture and ability to operate and manage a vast number of operational endpoints with a very small crew.

Please join me in thanking our guests, Bryan Farmer, System Technician at County of Caroline in Bowling Green, Virginia. Thank you so much, Bryan.

Farmer: Thank you, I appreciate the opportunity.

Gardner: And we have also been here with Dave Sadler, Director of Information Technology at the County of Caroline. Thank you so much, Dave.

Sadler: Thank you, sir. We appreciate your time.

Gardner: I'm Dana Gardner, Principal Analyst at Interarbor Solutions, your host and moderator for this ongoing series of BriefingsDirect use case discussions. A big thank you 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.

You may also be interested in:

- SambaSafety's mission to reduce risk begins in its own datacenter security partnerships

- How MSP StoredTech brings comprehensive security services to diverse clients using Bitdefender
- For a UK borough, solving security issues leads to operational improvements and cost-savings across its IT infrastructure
- How an Architectural Firm Retains Long-Term Security Confidence Across a Fully Virtualized and Distributed Desktop Environment
- 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 a Florida school district tames the Wild West of education security at scale and on budget