How MSPs Leverage Bitdefender's Layered Approach to Security For Comprehensive Client Protection

Transcript of a discussion on how managed service providers are building better security postures to help small- to medium-sized businesses and enterprises best manage and protect their customers' end devices and workspaces.

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 the BriefingsDirect podcast series, now in its 13th year. I'm Dana Gardner, Principal Analyst at Interarbor Solutions, your host and moderator.

As solving security concerns has risen to the top of the requirements list for just about everyone, service providers in particular have had to step up their game. Because just as cloud models and outsourcing of more data center functions have become more popular, the security needs have grown even more fast-paced and pressing.

As small- to medium-sized businesses (SMBs) have turned to managed service providers (MSPs) to be in effect their IT departments, they are also seeking MSPs to serve as their best defenses against the latest security risks.

Luckey

Today's BriefingsDirect security insights discussion examines how MSPs are building better security postures from their networks and data centers. Here to discuss the role of the latest security technology in making MSPs more like *security services providers* (SSPs) is Brian Luckey, Director of Managed Services at All Covered, IT Services from Konica Minolta, in Ramsey, New Jersey. Welcome, Brian.

Brian Luckey: Thank you for having me.

Gardner: We are also joined by Jeremy Wiginton, Applications Administrator, also at All Covered, IT Services from Konica Minolta. Welcome, Jeremy!

Jeremy Wiginton: Thank you.

Gardner: What are some of the trends that have been driving the need for MSPs like yourselves to provide even more and better security solutions?

Managing security expectations

Luckey: As MSPs, we are expected, especially for SMBs, to cover the entire gamut when it comes to managing or overseeing an organization's IT function. And with IT functions come those security services.

It's just an expectation at this point when you are managing the IT services for our clients. They are also expecting that we are overseeing the security part of that function as well.

Gardner: How has this changed from three to five years ago? What has changed that makes you more of an SSP?

Luckey: A major driver has been the awareness of needing heightened security. So all of the news, the different security breach events -- especially over the last 12 months, let alone the last couple of years -- with WannaCry and Petya.

Now, not only companies but the owners and executives are more in tune with the risks. This has sparked more interest in making sure that they are protected and feel like they are protected. This has all definitely increased the need for MPSs to provide these IT services.

Not only companies, but the owners and executives are more in tune with the risks.

Gardner: As we have had more awareness, more concerns, and more publicity, then the expectations are higher.

Jeremy, what are some of the technical advances that you feel are most responsible for allowing you as an MSP to react better to these risks?

Wiginton: The capability for the fast analytics, the fast reporting, and the fast responses that we can get out of the products and solutions that we use helps tremendously in making sure that our clients are well-protected and that security -- any security issues that might pop up -- are mitigated very, very quickly.

Gardner: The role of compliance requirements has also risen. Are your clients also seeking more security and privacy control around such things as the Health Insurance Portability and Accountability Act (HIPAA) or Payment Card Industry Data Security Standard (PCI DSS) and nowadays the General Data Protection Regulation (GDPR)?

Tools and regulations

Luckey: Oh, absolutely. We provide IT services to a variety of different industries like the financial industry, insurance, and health care. In those industries, they have high regulations and compliance needs, which are growing more and more. But there are also companies that might not fall into those typical industries yet have compliance needs, too -- like PCI and GDPR, as you mentioned.

Gardner: As Jeremy mentioned, speed is critical here. What's been a challenge for organizations like yours to react to some of these issues -- be it security or compliance?

Luckey: That's a great question. There are a couple of things. One is technology; having the right technology that fits not only our business needs, but also our clients' needs. That's a huge impact for us -- being able to provide the right service and the right fit.

But also integration points are important. Disparate systems that don't integrate well or work well together can be a difficulty for us to service our clients inappropriately. If we have internal chaos, how can we provide a great service to our clients?

The proper progression and adoption of services and solutions is also key. We are in a technological world, for sure, and as technology progresses it only gets better, faster, cheaper, and smarter. We need to be able to use those solutions and then pass along the benefits to our clients.

As technology progresses, it only gets better, faster, cheaper, and smarter. We need to be able to use those solutions and then pass along the benefits to our clients.

Gardner: Jeremy, we have been speaking generally about data center services, IT services, but what about the applications themselves? Is there something specific to applications hosting that helps you react more quickly when it comes to security?

Quick reactions

Wiginton: Most assuredly. A lot of things have been getting bloated. And when things get bloated, they get slowed down, and clients don't want them on their machines -- regardless of how it impacts their security.

So being able to deliver a modern security product that is lightweight, and so fast that the clients don't even notice it is essential. These solutions have come a long way compared to when you were constantly doing multiple things just to keep the client happy and having to compromise things that you may not have wanted to compromise.

Gardner: It wasn't that long ago that we had to make some tough tradeoffs between getting security, but without degrading the performance. How far do you think we have come on that? Is that something that's essentially solved nowadays?

Wiginton: For the most part, yes. We have a comprehensive solution, where one product is doing the job of many, and the clients still don't notice.

Gardner: Tell us more, Brian, about All Covered. You have 1,200 employees and have been doing this since 1997. What makes you differentiated in the MSP market?

Longevity makes a difference

Luckey: We have been around a long time. I think our partnership and acquisition by Konica Minolta many years ago has definitely been a huge differentiator for us. Being focused on the office workplace of the future and being able to have multiple different technologies that serve an organization's needs is definitely critical for us and the differentiating factor.

Being focused on the office workspace of the future and being able to have multiple different technologies that serve an organization's needs is definitely critical for us and the differentiating factor.

We have been providing computing and networking services, and fulfilling different application needs across multiple vertical industries for a long time, so it makes us one of the major MSP and IT players.

Gardner: But, of course Konica Minolta is a global company. So you have sister properties, if you will, around the globe?

Luckey: That is correct, yes.

Gardner: Let's find out what you did to solve your security and performance issues and take advantage of the latest technology.

Luckey: We set out to find a new endpoint security vendor that would meet the high demands of not only our clients, but also our internal needs as well to service those clients appropriately.

We looked at more than a dozen different solutions covering the endpoint security marketplace. Over about six months we narrowed it down to the final three and began initial testing and discussions around what these three endpoint security vendors would do for us and what the success factors would look like as we tested them.

We eventually choose Bitdefender Cloud Security for MSPs.

Gardner: As an MSP, you are concerned not only with passing along great security services, but you have to operate on a margin basis, and take into consideration how to cut your total cost over time. Was there anything about the Bitdefender approach that's allowed you to reduce man hours or incidents? What has been impactful from an economic standpoint, not just a security posture standpoint?

A streamlined security solution

Luckey: Bitdefender definitely helped us with that. Our original endpoint security solution involved three different solutions, including an anti-malware solution. And so just being able to condense those into one -- but still providing the best protection that we could find -- was important to us. That's what we found with Bitdefender. That definitely saved us some costs from the reduction of overall number of solutions.

But we did recognize other things in choosing Bitdefender, like the reduction of incidents; I think we reduced them by about 70 percent. That translated into a reduction of people and manpower needed to address issues. That, too, was a big win for us. And having such a wide diversity of clients -- and also a large endpoint base -- those were big wins for us when it came down to choosing Bitdefender.

Gardner: Jeremy, we're talking about endpoint security, and so that means the movement of software. It means delivery of patches and updates. It means management of those processes. What was it about Bitdefender along the logistical elements of getting and keeping the security in place?

Wiginton: Having everything managed, a single pane of glass interface for the endpoint security side, that has saved a ton of time. We are not having to go look in three different places. We are not having to deal with some of our automated things that are going on. We are not having to deal with two or three different APIs to try and get the same information or to try and populate the same information.

We have one consistent product to work with, a product that, as Brian said, has cut down on the number of things that come across our desks by at least 70 percent. The incidents still occur, but they are getting resolved faster and on a more automated basis with Bitdefender than they were in the past with our other products.

We have one consistent product to work with … that has cut down on the number of things that come across our desk by 70 percent. The incidents still occur, but they are getting resolved faster and on a more automated basis.

Gardner: Brian, where you are in your journey of this adoption? Are you well into production?

Luckey: We are well into the journey. We chose Bitdefender in mid-2016, and we were deployed in January 2017. It's been about a year-and-a-half now, and still growing.

We have grown our endpoints by about 30 percent from the time that we originally went live. Our business is growing, and Bitdefender is growing with us. We have continued to have success and we feel like we have very good protection for our clients when it comes to endpoint security.

Gardner: And now that you have had that opportunity to really evaluate and measure this in business terms, what about things like help desk, remote patch management, reporting? Are these things that have changed your culture and your business around security?

Reporting reaps rewards

Luckey: Yes, absolutely. We have been able to reduce our incidents, and that's obviously been a positive reflection on the service desk and help desk on taking calls and those type of issues.

For patching, we have a low patch remediation rate, which is great. I'm sure that Bitdefender has been a strong reflection on that.

And for reporting, it's big for us. Not only do we have more in-depth and detailed reporting for our clients, but we also have the capability to give access to our clients to manage their own endpoints, as well as to gain reports on their own endpoints.

Gardner: You're able to provide a hybrid approach, let them customize -- slice and dice it the way they want for those larger enterprise clients. Tell us how Bitdefender has helped you to be a total solution provider to your SMB clients?

Luckey: Endpoint security has become a commodity business. It's one of those things you just have to do. It's like a standard requirement. And not having to worry about our standard offerings, like endpoint security -- we just know it works, we know how it works, we are very comfortable on how it works, and we know it inside and out. All of that makes life easier for us to focus on the other things, such as the non-commodity businesses or the more advanced items like security information management (SIM) and manage unified threat management (UTM).

Not having to worry about our standard offerings, like endpoint security – we just know it works, we know how it works, we are very comfortable on how it works, and we know it inside and out. All of that makes life easier for us to focus on the other things.

Gardner: What now can you do now with such value-added services that you could not do before?

Luckey: We can focus more on providing the advanced types of services. For example, we recently acquired a [managed security services and compliance consulting] company, VioPoint, that focuses solely on security offerings. Being able to focus on those is definitely key for us.

Gardner: Jeremy, looking at this through the applications lens again, what do you see as the new level of value-added services that you can provide?

Fewer fires to extinguish

Wiginton: We are bringing in and evaluating Bitdefender technologies such as Full Disk Encryption. It has been a nice little product. I have done some testing with it, they let me in on their beta of it, which was really nice. It's really easy to use.

Also, [with Bitdefender], because there's a lot less remediation needed on security incidents, we have seen a great drop in things like ransomware. As a result, I am able to focus more on making sure that our clients are well protected and making sure that the applications are working as intended -- as opposed to having to put out a fire because the old solution let something in that it shouldn't have.

Gardner: It's been great to talk about this in the abstract, but it's very powerful too if we can get more concrete examples.

Do you have any use cases for your MSP endpoint security and management capabilities that you can point to?

Luckey: The one that comes to mind, and always sticks with me, is a legal client of ours. When we rolled out Bitdefender to replace the older security solutions they had, their business stopped. And the reason their business stopped is there was malware being detected, and we couldn't find out where it was coming from.

After additional research, we found that their main application to manage their clients and to manage billing -- basically to run their business -- the executable file that they would take and copy and actually install that application on every desktop, that had malware in it.

The previous solutions didn't catch that. Every time they were deploying this application to new users, or if they had to redeploy it, they were putting malware on every machine, every time. We weren't able to detect it until we had Bitdefender deployed. Once Bitdefender detected it, it stopped the business, which is not good. The better part was that we were able to detect the malware that was being spread across the different machines.

That's one example that I always remember because that was a big deal, obviously by stopping the business. But the most important part was that we were able to detect malware and protect that company better than they had been protected before.

The most important part was that we were able to detect malware and protect that company better than they had been protected before.

Gardner: The worst kind of problem is not knowing what you don't know.

Luckey: Exactly! Another example is a large client that has many remote offices for its dental services, all across the US. Some offices had spotty Internet access, so deploying

Bitdefender was challenging until we used Bitdefender Relay. And Relay allowed us to deploy it once to the company and then deploy most of the devices with one deployment, instead of having to deploy one agent at a time.

And so that was a big benefit that we didn't have in the past. Being able to deploy it once and then have all the other machines utilize that Relay for the deployments made it a lot easier and a lot faster due to the low bandwidth that was available in those locations.

Being able to deploy it once and then have all the other machines utilize that Relay for the deployments made it a lot easier and a lot faster.

Wiginton: We had a similar issue at a company where they would not allow their servers to have any Internet access whatsoever. We were able to set up a desktop as the Relay and get the servers connected to the Relay on the desktop to be able to make sure that their security software was up-to-date and checking in. It was still able to do what it was supposed to, as opposed to just sitting there and then alerting whenever its definitions became out of date because it didn't have Internet access.

Gardner: Let's look to the future and what comes next. We have heard a lot about encryption, as you mentioned, Jeremy. There's also a of research and development being done into things like machine learning (ML) to help reduce the time to remediation and allow the security technology to become more prescriptive, to head things off before they become a problem.

Brian, what are you looking for next when it comes to what suppliers like Bitdefender can do to help you do your job?

Future flexibility and functionality

Luckey: We have already begun testing some of the newer functionality being released to the Bitdfender MSP Cloud Security suite this month. We are looking into the advanced security and ML features, and some new functionality they are releasing. That's definitely our next approach when it comes to the next generation of the Bitdefender agent and console.

And in addition to that, outside of Bitdefender, we are also expanding the services from our new security acquisition, VioPoint, and consolidating those to provide best-in-class security offerings to our clients.

Gardner: Jeremy, what entices you about what's coming down the pike when it comes to helping to do your job better?

Wiginton: I'm really looking forward to Bitdefender's Cloud, which allows us a lot more flexibility because we are not having to allocate our own internal resources to try and do the analytics. So their Sandbox Analyzer and things that are coming soon really do

interest me a lot. I am hoping that that will further chop down the number of security incidents that come across our desk.

Gardner: What would you suggest in hindsight, now that you have made a big transition from multiple security providers to more of a consolidated comprehensive approach? What have you learned that you could share with others who are maybe not quite as far along in the journey as you?

Testing, testing

Luckey: Number one is testing. We did a pretty good job of testing. We took a three-pronged approach of internal, external, and then semi-internal, so our help desk folks. Make sure that you have a comprehensive test plan to test out how many bad guys are being protected, what kind of malware is being blocked, and the functionality. That's the big one … test, test, and test some more.

Choosing the right partner and the right vendor, if you will, is key. I believe in having partners instead of just vendors; vendors just supply products, but partners work together to be successful.

It's kind of like dating, date the right partner until you find the right one -- and Bitdefender has definitely been a great partner for us.

Otherwise, have your requirements set up for what success looks like, those are all important. But the testing -- and making sure you find the right partner – those were key for us. Once we knew what we wanted, the rest of it fell into place.

Gardner: Jeremy, from your perspective, what advice could you give others who are just starting out?

Wiginton: Make sure that you are as thorough as possible in your testing, and get it done sooner rather later. The longer you wait, the more advanced threats are going to be out there and the less likely you are going to catch them on an older solution. Do your homework and you have to be on the ball with it.

Gardner: I'm afraid we'll have to leave it there. You have been listening to a sponsored BriefingsDirect discussion on how small to medium-sized businesses have increasingly turned to managed service providers to be among their greatest defenses against the latest security risks.

And we've learned how new and increasingly intelligent security technologies from such vendors as Bitdefender are making MSPs more like SSPs for their clients.

Please join me now in thanking our guests, Brian Luckey, Director of Managed Services at All Covered in Ramsey, New Jersey. Thank you, Brian.

Luckey: Thanks for having me.

Gardner: And we have been here with Jeremy Wiginton, Applications Administrator at All Covered. Thank you so much, Jeremy.

Wiginton: Thank you, very much.

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 also to our sponsor, Bitdefender, for supporting these presentations. A big thank you as well to our audience for joining. Please pass this on to 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:

- Citrix and HPE Team to Bring Simplicity to the Hybrid Core-Cloud-Edge Architecture
- New Strategies Emerge to Stem the Costly Downside of Complex Cloud Choices
- Poor Cloud Utilization and High Complexity Demand a Better Way to Manage and Optimize Multicloud
- GDPR Forces a Rekindling of the People-Centric Approach to Marketing and Business
- Path to Modern PC Client Automation is Paved with Hyperconverged Infrastructure for New Jersey College
- How HPE and Docker Together Accelerate and Automate Hybrid Cloud Adoption
- Legacy IT evolves: How cloud choices like Microsoft Azure can conquer the VMware Tax
- How HudsonAlpha transforms hybrid cloud complexity into an IT force multiplier
- South African insurer King Price gives developers the royal treatment as HCI meets big data