Bitdefender MSP StoredTech brings comprehensive security services to diverse clients

Transcript of a discussion on how security technology can make or break a managed service provider's ability to scale and maintain top quality customer service.

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.

For managed service providers (MSPs) seeking to grow rapidly while remaining efficient, their bedrock security technology can make or break their ability to scale and maintain top quality customer service.

By simultaneously slashing security-related trouble tickets and management costs by more than 75 percent, Stored Technology Solutions, or StoredTech, grew its business *and* quality of service at the same time.

Stay with us now as we learn how StoredTech adopted Bitdefender Cloud Security for Managed Service Providers to dramatically improve the security of their end users -- and develop enhanced customer loyalty.

Here to discuss the role of the latest Bitdefender security technology and making MSPs more like *security* services providers is Mark Shaw, President of StoredTech in Raleigh, North Carolina. Welcome, Mark.

Mark Shaw: Thanks for having me.

Gardner: Mark, what trends are driving the need for MSPs like yourself to provide security that enhances the customer experience?

Shaw: A lot of things are different than they were back in the day. Attacks are very easy to implement. For a dollar, you can buy a malware kit on the dark web. Anyone with a desire to create havoc with malware, ransomware, or the like, can do it. It's no longer a technical scenario, it's simply a financial one.

At the same time, everyone is now a target. So back in the day, obviously, there were very needy targets. People would spend a lot of time, effort, and technical ability to hack large enterprises. But now, there is no business that's too small. If you have data and you don't want to lose it, you're a target. Of course, the worst part for us is that MSPs are now directly being targeted. So no matter what the size, if you are an MSP, they want access to your clients.

China has entire groups dedicated to hacking only MSPs. So the world landscape has dramatically shifted.

Gardner: And, of course, the end user doesn't know where the pain point is. They simply want all security all the time -- and they want to point the finger at you as the MSP if things aren't right.

Shaw: Oh, absolutely right; that's what we get paid to do.

Gardner: So what were your pain points? What from past security providers and vendors created the pain that made you seek a higher level of capability?

Shaw: We see a lot of pain points when it comes to too many layers. We talk about security being a layering process, which is fantastic. You want the Internet provider to be doing their part. You want the firewall to do its part.

When it comes to security, a lot of times we see way too many security applications from different vendors running on a machine. That really decimates the performance. End users don't really care; they care about security -- but they're not going to sacrifice performance.

We also see firms that spend all their time meeting all the industry and government regulations -- and they are still completely exposed. What we tell people is just because you check a box in security, doesn't mean you are in compliance. It doesn't mean you're secure.

For small business owners, we see all these pain points in how they handle their compliance and security needs. And, of course, in our world, we are seeing a lot of pain points because insurance for cyber security is becoming more prevalent and paying out

through crypto virus and ransomware attacks. That insurance is becoming more prevalent. And so we are seeing a chicken-and-egg thing, with a recent escalation in malware and ransom attacks [because of those payments].

Gardner: Tell us about StoredTech. What's your MSP about?

Shaw: We are both an MSP and a *master MSP*. We refer to it as "the one throat to choke." Our job is to provide solutions that have depth of scale. For us, it's all about being able to scale.

We provide the core managed services that most MSPs provide, but we also provide telco services, we help people select and provide Internet services, and we spend a lot of time working with cameras and access control, which require an entirely different level of security and licensing.

We refer to ourselves as the "one throat to choke." If it's technology-related, we don't want customers pointing fingers and saying, "Well, that's the telephone guys' problem," or, "That's the guy with the cameras and the access control, that's not us."

We remove all of that finger-pointing. Our job is to delight our customers by finding ways to say, "Yes," and to solve all of their technology needs.

Gardner: You have been in business for about 10 years. Do you focus on any particular verticals, size of company, or specialize?

Shaw: We really don't, unlike the trends in the industry today. We are a product of our scars. When I worked for corporate America, we didn't know we were getting laid off until we read it in the newspaper. So I don't want to have any one client. I don't want to have anybody surprising us.

We have the perfect bell-curve distribution. We have clients that are literally one guy with a PC in his basement running an accounting firm, all the way up to global clients with 30,000 end-points and employees.

We have diverse geographies as well as technical verticals among our clients -- everything from healthcare to manufacturing, retail, other technology companies; you name it. We re-sell them as well. For us, we are not siloed. We run the gamut. Everybody needs technology.

Gardner: True that. So one throat to choke is your value and you are able to extend that and scale up to 30,000 employees or scale down to a single seat. You must have been very choosy about improving your security posture. Tell us about your security journey.

Shaw: Our history goes way back. We started with the old GFI LanGuard for Macs product, which was a remote monitoring and management (RMM) that tied to VIPRE. SolarWinds acquired that product and we got our first taste of the Bitdefender engine.

We loved what Bitdefender did. When Kaseya was courting us to work with them, we told them, “Guys, we need to bring Bitdefender with us.”

At that point in time, we had no idea that Bitdefender also had an entire GravityZone platform with an MSP focus. So when we were able to get onto the Bitdefender GravityZone platform it was just amazing for us.

We actually used Bitdefender as a sales tool against other MSPs and their security platforms by saying, “Hey, listen. If we come in, we are going to put in a single agent that’s the security software, right? Your antivirus, your content filtering, your malware detection and prevention – and it’s going to be lighter and faster. We are going to speed up your computers by putting this software on.”

We went from VIPRE software to the Bitdefender engine, which really wasn’t the full Bitdefender, to then the full Bitdefender GravityZone when we finally moved with the Kaseya product. Bitdefender lit up our world. We were able to do deployments faster and quicker. We really just started to scale at that point.

Gardner: And just as you want to be one throat to choke to your customers, I am pretty sure that Bitdefender wants to be one throat to choke for you. How does Bitdefender help you protect yourselves as an MSP?

Shaw: For us, it’s really about being able to scale quickly and easily. It’s the ability to have customizable solutions whether we are deploying it on a Mac, SQL Server, or in a Microsoft Azure instance in the cloud, we need scalability. But at the same time, we need customizing ability to change and modify exactly what we want out there.

The Bitdefender platform gives us the ability to either ramp up or scale down the solution based on what applications are running and what the end user expects. It’s the best of both worlds. We have this 800-pound gorilla, one single point of security, and at the same time we can get so granular with it that we can solve almost any client’s needs without having to retool and without layering on multiple products.

In the past, we used to use other antivirus products, layered them on with the content filtering products -- we just had layer after layer after layer, which for our engineers meant if you want to see what’s wrong, you had to log into one of the four consoles. Today, it’s log-in to this one console and you can see the status of everything.

By making it simple, the old KISS method, we were able to dramatically scale and ramp up -- whether that’s 30,000 end points or one. We have a template for almost anything.

We have a great hash-tag here called *automate-or-die.* The concept is to automate so we can give every customer exactly what they need without totally having to retool the environment or add layer upon layer of products, all of which have an impact on the end user.

Gardner: You are a sophisticated enough organization that you want automation, but you also want customization. That's often a difficult balance. What is it about Bitdefender Cloud Security for MSPs that gets that balance?

Shaw: Being able to see everything in one dashboard -- to have everything laid out in front of you – and be able to apply different templates and configurations to different types of machines based on a core functionality. That allows us to provide customization without large overhead from manual configuration every single time we have to do it.

To be able to add that value -- but not add those additional man-hours -- really brings it all together. Having that single platform, which we never had before in the old days, gives us that. We can see it, deploy it, understand it, and report on it. Again, it's exactly what we would tell our customers, come to us for one throat to choke.

And we basically demanded that Bitdefender have that same throat to choke for us. We want it all easy, customizable -- we want everything. We want the Holy Grail, the golden goose -- but we don't want to put any effort into it.

Gardner: Sounds like the right mix to me. How well has Bitdefender been doing that for you? What are the results? Do you have some metrics to measure this?

Shaw: We had some metrics and you mentioned them. We understand by what we have to do, how much time we have to support, and how quickly we can implement and deploy.

We have seen malware infections reduced by about 80 percent. We took weekly trouble tickets from previous antivirus and security vendors from 50 down to about 1 a week. We slashed administration cost by about 75 percent. Customer satisfaction has never been higher.

In the old days of multiple layers of security, we got calls, "My computer is running slow." And we would find that an antivirus agent was scanning or a content filtering app was doing some sort of update.

Now we are able to say, "You know what? This is really easy." We have one Bitdefender agent to deploy. We go out there, we deploy it, and it's super-simple. We just have a much easier time now managing that entire security apparatus versus what we used to do.

Gardner: Mark, you mentioned that you support a great variety of sizes of organizations and types of vertical industries. But nowadays there's a great variety between on-premises, cloud, and a hybrid continuum. It's difficult for some vendors to support that continuum.

How has Bitdefender risen to that challenge? Are you able to support your clients whether they are on-premises, in the cloud, or both?

Shaw: If you look at the complexion of most customers nowadays that's exactly what you see. You see a bunch of people who say, "I am never, ever taking my software off-premises. It's going to stay right here. I don't trust the cloud. I am never going to use it." You have those "never" people.

You have some people who say, "I'd really love to go to the cloud 100 percent, but these four or five applications aren't supported. So I still need servers, but I'd love to move everything else to the cloud."

And then, of course, we have some clients who are literally born in the cloud: "I am starting a new company and everything is going to be cloud-enabled. If you can't put it up in the cloud, if you can't put it in Azure or something of this sort, don't even talk to us about it."

The nice part about that is, it doesn't really matter. At the end of the day, we all make jokes. The cloud is just somebody else's hardware. So, if we are responsible for either those virtual desktop infrastructure (VDI) clients, or those servers, or those physical workstations -- whatever the case may be -- it doesn't matter. If it's an Exchange Server, a SQL Server, an app server, or an Active Directory server, we have a template. We can deploy it. It's quick and painless.

Knowing that Bitdefender GravityZone is completely cloud-centric means that I don't have to worry about loading anything on-premises. I don't have to spin up a server to manage it – it just doesn't matter. At the end of the day, whatever the complexion of the customer is we can absolutely tailor to their needs with a Bitdefender product without a lot of headaches.

Gardner: We have talked about the one throat and the streamlining from a technology and a security perspective. But as a business you also want to streamline operations, billing, licensing, and make sure that people aren't being overcharged or undercharged. Is there anything about the Bitdefender approach, in the cloud, that's allowed you to have less complexity when it comes to cost management?

Shaw: The nice part about it, at least for us is, we don't put a client out there without Bitdefender. For us it's almost a one-to-one. For every RMM agent deployed, it's one Bitdefender deployed. It's clean and simple, there is no fuss. If a client is working with us, they are going to be on our solutions and our processes.

Going back to that old KISS method, we want to just keep it simple and easy. When it comes to the back-office billing, if we have an RMM agent on there, it has a Bitdefender agent. Bitdefender has a great set of APIs. Not to get super-technical, but we have a developer on staff who can mine those APIs, pull that stuff out, make sure that we're synchronized to our RMM product, and just go from there.

As long as we have a simple solution and a simple way of billing on the back-end, clients don't mind. Our accounting department really likes it because if there's an RMM agent on there, there's a Bitdefender agent, and it's as simple as that.

Gardner: Mark, what comes next? Are there other layers of security you are looking at? Maybe full-disk encryption, or looking more at virtualization benefits? How can Bitdefender better support you?

Shaw: Bitdefender's GravityZone Full Disk Encryption is fantastic; it's exactly what we need. I trust Bitdefender to have our best interests in mind. Bitdefender is a partner of ours. We really mean that, they are not a vendor.

So when they talk to us about things that they are seeing, we want to make sure that we spend a lot of time and understand that. From our standpoint, encryption, absolutely. Right now we spend a lot of time with clients who have data that is not necessarily personally identifiable information (PII), but it is data that is subject to patents, or is their secret sauce -- and it can't get out. So we use Bitdefender to do a lot of things like locking down USB drives and things like that.

I know there is a lot of talk about machine learning (ML) and artificial intelligence (AI) out there. To me they are cool buzzwords, but I don't know if they are *there* yet. If they get there, I believe and trust that Bitdefender is going to say, "We are there. We believe it's the right thing to do."

I have seen a lot of next-generation antivirus software that says, "We use only AI or we use ML only." And what I see is they miss apparent threats. They slow the machines into a crawl, and they make the end-user experience miserable.

As Bitdefender looks down these roads of ML and AI, just make sure to be cutting edge here, but don't be bleeding edge because nobody wants to hemorrhage cash, time, and everything else.

We are vested in the Bitdefender experience. The guys and girls at Bitdefender, they know what's coming. They see it all time. We are happy to play along with that. Typically by the time it hits an end user or a customer in the enterprise space, it's old hat. I think the real cutting edge, bleeding edge stuff happens well before an MSP tends to play in that space.

But there's a lot of stuff coming out, a lot of security risk, on mobile devices, the Internet of everything, and televisions. Every day now you see how those are being hacked -- whether it's a microphone, the camera, or whatever. There is a lot of opportunity and a lot of growth out there, and I am sure Bitdefender is on top of it.

Gardner: Before we close out, any advice for organizations on how to manage security better as a culture, as an ongoing never-ending journey? You mentioned that you peel back the onion, and you always hit another layer. There is something more you have to solve the next day. This is a non-stop affair.

What advice do you have for people so that they don't lose track of that?

Shaw: From an MSP's standpoint, whether you're an engineer, in sales, or an account manager -- it's about constant learning. Understand, listen to your clients. Your clients are going to tell you what they need. They are going to tell you what they are concerned about. They are going to tell you their feelings.

If you listen to your clients and you are in-tune with them, they are going to help set the direction for your company. They are going to guide you to what's most important to them, and then that should parlay into what's most important for you.

In our world, we went from just data storage and MSP services into then heading to telco and telephones, structured cabling, cameras, and access control, because our clients asked us to. They kept saying these are pain points, can you help us?

And for me that's the recipe to success. Listen to your clients, understand what they want, especially when it comes to security. We always tell everybody, eat your own dog food. If you are selling a security solution you are putting out there for your clients, make sure your employees have it on all of their machines. Make sure your employees are using it at home. Get the same experience with the customers. If you are going through cyber security training, put your staff through cyber security training, too. Everyone, from the CEO right down on to the person managing the warehouse should go through the same training.

If we put ourselves in our customers' shoes and we listen to our customers -- no matter what it is, security, phones, computers, MSP, whatever it is -- you are going to be in-tune with your customers. You're going to have success.

We just try to find a way to say, "Yes," and delight our customers. At the end of the day if you are doing that, if you are listening to their needs, that's all that matters.

Gardner: I'm afraid we'll have to leave it there. You have been listening to a sponsored BriefingsDirect discussion on how MSPs' bedrock security technology can make or break their ability to scale and maintain top-quality customer service.

And we have learned how StoredTech adopted Bitdefender Cloud Security for MSPs to dramatically improve security and develop enhanced customer loyalty. So please join me in thanking our guest, Mark Shaw, President of StoredTech in Raleigh, North Carolina. Thanks so much, Mark.

Shaw: Thank you.

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

Transcript of a discussion on how security technology can make or break a managed service provider's ability to scale and maintain top quality customer service.

You may also be interested in:

- 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
- 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