How an MSP Brings Comprehensive Security Services to Diverse Clients

Transcript of a discussion on how a UK managed services provider developed the right mix of security strength and ease-of-use using Bitdefender Cloud Security for Managed Service Providers.

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.

As businesses move more of their IT services to the cloud, reducing complexity and making sure that security needs are met throughout the migration process are now top of mind.

For a UK managed services provider (MSP), finding the right mix of security strength and ease-of-use for its many types of customers became a top priority. Stay with us now as we learn how Northstar Services, Ltd. in Bristol-area England adopted Bitdefender Cloud Security for Managed Service Providers (MSPs) to both improve security for their end users and to make managing that security at scale easier than ever.

Williams

Here to discuss the role of the latest Bitdefender security technology -- and making MSPs more like security services providers -- is John Williams, Managing Director at Northstar Services, Ltd. Welcome, John.

John Williams: Hello.

Gardner: What are some of the top trends driving the need for an MSP such as Northstar to provide even better security services?

Williams: We used to get lots of questions regarding stability for computers. They would break fairly regularly and we'd have to do hardware changes. People were interested in what software we were going to load -- what the next version of this, that, and the other was -- but those discussions have changed a great deal. Now everybody is talking about security in one form or another.

Gardner: Whenever you change something -- whether it's configurations, the software, or the service provider, like a cloud -- it leaves gaps that can create security problems. How can you be doubly sure when you make changes that the security follows through?

The value of visibility, 24-7

Williams: We used to install a lot of antivirus software on centralized servers. That was very common. We would set up a big database and install security software on there, for example. And then we would deploy it to the endpoints from those servers, and it worked fairly well. Yet it was quite a lot of work to maintain it.

But now we are supporting people who are so much more mobile. Some customers are all out and about on the road. They don't go to the office. They are servicing their customers, and they have their laptop. But they want the same level of security as they would have on a big corporate network.

So we have defined the security products that give us visibility of what's happening. It means that we don't have to know that they are up to date. We have to manage those clients wherever they are on whatever device they have -- all from one place.

Gardner: Even though these customers are on the frontline, you're the one as the MSP they are going to call up when things don't go right.

Williams: Yes, absolutely. We have lots of customers who don't have on-site IT resources. They are not experts. They often have small businesses with hundreds of users. They just want to call us, find out what's going on when they see a problem on their computers, and we have got to know whether that's a security issue or an application that's broken.

But they are very concerned that we have that visibility all of the time. Our engineers need to be able to access that easily and address it as soon as a call comes in.

[Customers] are very concerned that we have that visibility all of the time. Our engineers need to be able to access that easily and address it as soon as a call comes in.

Gardner: Before we learn more about your journey to solving those issues, tell us about Northstar. How long have you been around and what's the mainstay of your business?

Williams: I have been running Northstar for more than 20 years now, since January 1999. I had been working in IT as an IT support engineer in large organizations for a few years, but I really wanted to get involved in looking after small businesses.

I like that because you get direct feedback. People appreciate it when you make an effort. They want to tell you that you did a good job, and they want to know that someone is paying attention to them.

So it was a joy to be able to get that up and going. We have a great team here now and that's what gets me out of bed in the morning -- working with our team to look after our customers.

Gardner: Smaller businesses moving to the cloud has become more the norm lately. How are your smaller organizations managing that? Sometimes with the crossover -- the hybrid period between having both on-premises devices as well as cloud services -- can be daunting. Is that something you are helping them with?

Moving to cloud step-by-step

Williams: Yes, absolutely. We often see circumstances where they want to move one set of systems to the cloud before they want to move everything to the cloud. So they generally are on a trend where they want to get rid of in-house services, especially for the smaller end of the market, for customers who are smaller. But they often have legacy systems that they can't easily port off the services from. They might have been custom written or are older versions that they can't afford to upgrade at this point. So we end up supporting partly in the cloud and partly on-premises.

And some customers, that's their strategy. They take a particular workload, a database, for example, or some graphics software that they use, that runs brilliantly on servers in their offices. But they want to outsource other applications.

So, when we look at security, we need software that's going to be able to work across those different scenarios. It can't just be one or the other. It's no good if it's just on-premises, and no good if it's just in the cloud. It has to be able to do all of that, all from one console because that's what we are supporting.

[Software] is no good if it's just on-premises, and no good if it's just in the cloud. It has to be able to do all of that, all from one console.

Gardner: John, what were your requirements when you were looking for the best security to accomplish this set of requirements? What did you look for and how did your journey end?

Williams: Well, you can talk about the things being easy to manage, things being visible and with good reporting. All those things are important, and we assessed all of those. But the bottom line is, does it pick up infections? Is it able to keep those units secure and safe? And when an infection has happened, does it clean them up or stop them in their tracks quickly?

That has to be the number one thing, because whatever other savings you might make in looking after security, the fact that something that's trying to do something bad is blocked -- that has to be number one; stopping it in its tracks and getting it off that unit as quickly as possible. The sooner it's stopped, the less damage and the less time the engineers have to spend rebuilding the units that have been killed by viruses or malware.

And we used to do quite a lot of that. With the previous antivirus security software we used, there was a constant stream of cleaning up after infections. Although it would detect and alert us, very often the damage was already done. So, we had a long period of repairing that, often rebuilding the whole operating system (OS), which is really inconvenient for customers.

And again, coming back to the small businesses, they don't have spare PCs hanging around that they can just get out of the cupboard and carry on. Very often that's the most vital kit that they own. Every moment it's out of action, that's directly affecting their bottom line. So detecting infections and stopping them in their tracks was our number-one criteria when we were looking.

Gardner: In the best of all worlds, the end user is not even aware that they were infected, not aware it was remediated, not having to go through the process of rebuilding. That's a win-win for everyone.

Automation around security is therefore top of mind these days. What you have been able to do with Bitdefender Cloud Security for MSPs that accomplishes that invisibility to the end user -- and also helps you with automation behind the scenes?

Stop malware in its tracks

Williams: Yes, the stuff was easy to deploy. But what it boils down to is that we just don't get as many issues to have to automate the resolution for. So automation is important, and the things it does are useful. But the number of issues that we have to deal with is so few now that even if we were to 100 percent automate, it wouldn't make a massive savings, because it's not interrupting us very much.

It's stopping malware in its tracks and cleaning it up. Most of the time we are seeing that it has done it, rather than us having to automate a script to do some removal or some changes or that kind of thing. It has already done it. I suppose that is automated, if you think about it, yes.

Gardner: You said it's been a dramatic difference between the past and now with the number of issues to deal with. Can you qualify that?

Williams: In the three or four years we have used Bitdefender, when we look at the number of tickets that we used to get in for antivirus problems on people's laptops and PCs, they have just dropped to such a low level now, it's a tiny proportion. I don't think it's even coming up on a graph.

In the three or four years we have used Bitdefender, when we look at the number of tickets that we used to get in for antivirus problems on people's laptops and PCs, they have just dropped to such a low level now.

You record the type of ticket that comes in, and it's a printer issue, a hardware issue. The virus removal tickets are not featuring high enough to even appear on the graph because Bitdefender is just dealing with those infections and fixing them without having to get to them and rebuild PCs.

Gardner: When you defend a PC, Mac or mobile device, that can have a degradation effect. Users will complain about slow apps, especially when the antivirus software is running. Has there been an improvement in terms of the impact of the safety net when it comes to your use of Bitdefender Cloud Security for MSPs?

Williams: Yes, it's much lighter on the OS than the previous software that we were using. We were often getting calls from customers to say that their units were running slowly because of the heavy load it was having to do in order to run the security software. That's the exact opposite of what you want. You are putting this software on there so that they get a better experience; in other words, they are not getting infected as often.

But then you're slowing down their work every day, I mean, that's not a great trade-off. Security is vital but if it has such a big impact on them that they are losing time by just having it on there -- then that's not working out very well.

Now [with Bitdefender Cloud Security for MSPs] it's light enough from the that it just isn't an issue. We don't get customers saying, "Since you put the antivirus on my laptops, it seems to be slower." In fact, it's usually the opposite.

We don't get customers saying, "Since you put the antivirus on my laptops, it seems to be slower." In fact, it's usually the opposite.

Gardner: I'd like to return to the issue of cloud migration. It such a big deal when people move across a continuum of on-premises, hybrid, and cloud – and be able to move while security is maintained. It's like changing the wings on an airplane and keeping it flying at the same time.

What is it about the way that Bitdefender has architected its solution that helps you, as a service provider, guide people through that transition but not lose a sense of security?

Don't worry, be happy

Williams: It's because we are managing all of the antivirus licenses in the cloud, whether they are on-premises, inside an office where they are using those endpoints, or whether they are out and about; whether it's a client-server running in cloud services or running on-premises, we are putting the same software on there and managing it in the same console. It means we don't worry about that security piece. We know that whatever they change to, whatever they are coming from, we can put the same software on and manage it in the same place -- and we are happy.

Gardner: As a service provider I'm sure that the amount of man hours you have to apply to different solutions directly affects your bottom line. Is there something about the administration of all of this across your many users that's been an improvement? The GravityZone Cloud Management console, for example, has that allowed you to do more with less when it comes to your internal resources?

Williams: Yes, and the way that I gauge that is the amount of time. Engineers want to do an efficient job, that's what they like, they want to get to the root of problems and fix them quickly. So any piece of software or tool that doesn't work efficiently for them, I get a long list of complaints about on a regular basis. All engineers want to fix things fast because that's what the customer wants, and they are working on their behalf.

[I am] happy because I know that [the engineers] are able to work with it, which means that they are doing the job that they want to do, which is helping our customers and keeping them happy.

Before, I would have constant complaints about how difficult it was to manage and deploy software on the units if they needed to be decommissioned. It was just troublesome. But now I don't get any complaints over it. The staff is nothing but complimentary about the software. That just makes me happy because I know that they are able to work with it, which means that they are doing the job that they want to do, which is helping our customers and keeping them happy. So yes, it's much better.

Gardner: Looking to the future, is there something that you are interested in seeing more of? Perhaps around encryption or the use of machine learning (ML) to give you more analytics as to what's going on? What would you like to see out of your security infrastructure and services from the cloud in the next couple of years?

The devil's in the data detail

Williams: One thing that customers are talking to us about quite a bit now is data security. So they are thinking more about the time when they are going to have to report the fact that they've been attacked. And no software on earth is perfect. The whole point of security is that the threat continually evolves.

At the point where you've had a breach of some kind, you want to understand what's happened. And so, having information back from the security software that helps you to understand how the breach happened -- and the extent of it -- that's becoming really important to customers. When they submit those reports, as legally they have to do, they want to have accurate information to say, "We had an infection, and that's it." If they don't know exactly what the extent of it was – or whether any data was accessed or infected or encrypted without having that detail -- that's a problem.

So the more information that we can gain from the security software about the extent, that's going to be more important going forward.

Gardner: Anything else come to mind about what you'd like to see from the technology side?

Williams: So automation is important and that artificial intelligence (AI) side of it where the software itself learns about what's happening and can give you an idea when it spots something that's out of the ordinary -- that will be more useful as time goes on.

Gardner: John, what advice do you have for other MSPs when it comes to a security, a better security posture?

Williams: Don't be afraid of defining the securing services. You have to lead that conversation, I think. That's what customers want to know. They want to know that you have thought about it, and that's at the very full front of your mind.

We go meet our customers regularly and we usually have a standard agenda that we use. The first item on the agenda is security. And that journey for each customer is different. They are starting from different places. So we like to talk about where they are, what's the next thing that they can do to make sure they are doing everything they can to protect the data they have gathered from their customers, and to look after their data about their staff, too, and to keep their services running.

We put that at the top of the agenda for every meeting. That's a great way of behaving as a service provider. But, of course, in order to do that, to deliver on that, you have to have the right tools. You have to say, "Okay, if I am going to be in that role to help people with a security, I have to have those tools in place."

If they are complicated, difficult to use, and hard to implement -- then that's going to make it horrible. But if they are simple and give you great visibility, then you are going to be able to deliver a service that customers will really want to buy.

If [your security tools] are simple and give you great visibility, then you are going to be able to deliver a service that customers will really want to buy.

Gardner: I'm afraid we'll have to leave it there. You have been listening to a sponsored BriefingsDirect discussion on how reducing complexity and making sure security needs are met throughout a process of cloud adoption is the top of mind for MSPs.

And we have learned how Northstar Services in Bristol-area England has adopted Bitdefender Cloud Security for MSPs to both improve their security for the end user and also making managing security easier than ever.

Please join me in thanking our guest, John Williams, Managing Director at Northstar Services, Ltd. Thank you so much, John.

Williams: A pleasure.

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

- Better IT security comes with ease in overhead for rural Virginia county government
- 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