For a UK Borough, Solving Security Issues Leads to Operational Improvements and Cost-Savings Across its IT Infrastructure

Transcript of a discussion on how a large metropolitan borough council in South Yorkshire, England thwarted recurring ransomware attacks but also gained a catalyst to wider infrastructure performance, cost, operations, and management benefits.

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.

Solving tactical challenges around data center security can often unlock strategic data center operations benefits. For a large metropolitan borough council in South Yorkshire, England, an initial move to thwarting recurring ransomware attacks ended up being a catalyst to wider infrastructure performance, cost, operations, and management benefits.

This next BriefingsDirect security innovations discussion examines how the Barnsley Metropolitan Borough Council Information and Communications Technology (ICT) team rapidly deployed malware protection across 3,500 physical and virtual workstations and servers.

Furniss

Here to share the story of how one change in security software led to, a year later, far higher levels of user satisfaction and a heightened appreciation for the role and impact of IT is Stephen Furniss, ICT Technical Specialist for Infrastructure at Barnsley Borough Council.

Welcome to BriefingsDirect, Stephen.

Stephen Furniss: Hi, thank you.

Gardner: Stephen, tell us about the Barnsley Metropolitan Borough. You are one of 36 metropolitan counties in England, and you have a population of about 240,000. But tell us more about what your government agencies provide to those citizens.

Simply small, but mighty

Furniss: As a Council, we provide wide-ranging services to all the citizens here, from things like refuse collection on a weekly basis; maintaining roads, potholes, all that kind of stuff, and making sure that we look after the vulnerable in society around here. There is a big raft of things that we have to deliver, and every year we are always challenged to deliver those same services, but actually with less money from central government.

So it does make our job harder, because then there is not just a squeeze across a specific department in the Council when we have these pressures, there is a squeeze across everything, including IT. And I guess one of our challenges has always been how we deliver more or the same standard of service to our end users, with less budget.

So we turn to products that provide single-pane-of-glass interfaces, to make the actual management and configuration of things a lot easier. And [we turn to] things that are more intuitive, that have automation. We try and drive, making everything that we do easier and simpler for us as an IT service.

Gardner: So that boils down to working smarter, not harder. But you need to have the right tools and technology to do that. And you have a fairly small team, 115 or so, supporting 2,800-plus users. And you have to be responsible for all aspects of ICT -- the servers, networks, storage, and, of course, security. How does being a small team impact how you approach security?

Furniss: We are even smaller than that. In IT, we have around 115 people, and that's the whole of IT. But just in our infrastructure team, we are only 13 people. And our security team is only three or four people.

It can become a hindrance when you get overwhelmed with security incidents or issues that need resolving. Yet sometimes it's great to have that small team of people. You can bond together and come up with really good solutions to resolve your issues.

Sometimes it's great to have that small team of people. You can bond together and come up with really good solutions to resolve your issues.

Gardner: Clearly with such a small group you have to be automation-minded to solve problems quickly or your end users will be awfully disappointed. Tell us about your security journey over the past year-and-a-half. What's changed?

Furniss: A year-and-a-half ago, we were stuck in a different mindset. With our existing security product, every year we went through a process of saying, "Okay, we are up for renewal. Can we get the same product for a cheaper price, or the best price?"

We didn't think about what security issues we were getting the most, or what were the new technologies coming out, or if there were any new products that mitigate all of these issues and make our jobs -- especially being a smaller team -- a lot easier.

But we had a mindset change about 18 months back. We said, "You know what? We want to make our lives easier. Let's think about what's important to us from a security product. What issues have we been having that potentially the new products that are out there can actually mitigate and make our jobs easier, especially with us being a smaller team?"

Gardner: Were reoccurring ransomware attacks the last straw that broke the camel's back?

Staying a step ahead of security breaches

Furniss: We had been suffering with ransomware attacks. Every couple of years, some user would be duped into clicking on a file, email, or something that would cause chaos and mayhem across the network, infecting file-shares, and not just that individual user's file-share, but potentially the files across 700 to 800 users all at once. Suddenly they found their files had all been encrypted.

From an IT perspective, we had to restore from the previous backups, which obviously takes time, especially when you start talking about terabytes of data.

That was certainly one of the major issues we had. And the previous security vendor would come to us and say, "All right, you have this particular version of ransomware. Here are some settings to configure and then you won't get it again." And that's great for that particular variant, but it doesn't help us when the next version or something slightly different shows up, and the security product doesn't detect it.

That's a great [solution] for that particular variant [of ransomware], but it doesn't help us when the next version or something slightly different shows up, and the security product doesn't detect it.

That was one of our real worries and pain that we suffered, that every so often we were just going to get hit with ransomware. So we had to change our mindset to want something that's actually going to be able to do things like machine learning (ML) and have ransomware protection built-in so that we are not in that position. We could actually get on with our day-to-day jobs and be more proactive – rather than being reactive -- in the environment. That's was a big thing for us.

Also, we need to have a lot of certifications and accreditations, being a government authority, in order to connect back to the central government of the UK for such things as pensions. So there were a lot of security things that would get picked up. The testers

would do a penetration test on our network and tell us we needed to think about changing stuff.

Gardner: It sounds like you went from a tactical approach to security to more of an enterprise-wide security mindset. So let's go back to your thought process. You had recurring malware and ransomware issues, you had an audit problem, and you needed to do more with less. Tell us how you went from that point to get to a much better place.

Safe at home, and at work

Furniss: As a local authority, with any large purchase, usually over 2,500 pounds (US$3,125), we have to go through a tender process. We write in our requirements, what we want from the products, and that goes on a tender website. Companies then bid for the work.

It's a process I'm not involved in. I am purely involved in the techie side of things, the deployment, and managing and looking after the kit. That tender process is all done separately by our procurement team.

So we pushed out this tender for a new security product that we wanted, and obviously we got responses from various different companies, including Bitdefender. When we do the scoring, we work on the features and functionality required. Some 70 percent of the scoring is based on the features and functionality, with 30 percent based on the cost.

What was really interesting was that Bitdefender scored the highest on all the features and functionalities -- everything that we had put down as a must-have. And when we looked at the actual costs involved -- what they were going to charge us to procure their software and also provide us with deployment with their consultants -- it came out at half of what we were paying for our previous product.

Bitdefender scored the highest on all the features and functionalities … and it came out at half [the cost] of what we were paying for our previous product.

So you suddenly step back and you think, "I wish that we had done this a long time ago, because we could have saved money as well as gotten a better product."

Gardner: Had you been familiar with Bitdefender?

Furniss: Yes, a couple of years ago my wife had some malware on her phone, and we started to look at what we were running on our personal devices at home. And I came up with Bitdefender as one of the best products after I had a really good look around at different options.

I went and bought a family pack, so effectively I deployed Bitdefender at home on my own personal mobile, my wife's, my kids', on the tablets, on the computers in the house,

and what they used for doing schoolwork. And it's been great at protecting us from anything. We have never had any issues with an infection or malware or anything like that at home.

It was quite interesting to find out, once we went through the tender process, that it was Bitdefender. I didn't even know at that stage who was in the running. When the guys told me we are going to be deploying Bitdefender, I was thinking, "Oh, yeah, I use that at home and they are really good."

Monday, Monday, IT's here to stay

Gardner: Stephen, what was the attitude of your end users around their experiences with their workstations, with performance, at that time?

Furniss: We had had big problems with end users' service desk calls to us. Our previous security product required a weekly scan that would run on the devices. We would scan their entire hard drives every Friday around lunchtime.

You try to identify when the quiet periods are, when you can run an end-user scan on their machine, and we had come up with Friday's lunchtime. In the Council we can take our lunch between noon and 2 p.m., so we would kick it off at 12 and hope it would finish in time for when users came back and did some work on the devices.

And with the previous product -- no matter what we did, trying to change dates, trying to change times -- we couldn't get anything that would work in a quick enough time frame and complete the scans rapidly. It could be running for two to three hours, taking high resources on their devices. A lot of that was down to the spec of the end-user devices not being very good. But, again, when you are constrained with budgets, you can only put so many resources into buying kit for your users.

So, we would end up with service desk calls, with people complaining, saying, "Is there any chance you can change the date and time of the scan? My device is running slow. Can I have a new device?" And so, we received a lot of complaints.

And we also noticed, usually Monday mornings, that we would also have issues. The weekend was when we did our server scans and our full backup. So we would have the two things clashing, causing issues. Monday morning, we would come in expecting those backups to have completed, but because it was trying to fight with the scanning, neither was fully completed. We worried if we were going to be able to recover back to the previous week.

Monday morning, we would come in expecting those backups to have completed, but because it was trying to fight with the scanning, neither was fully completed.

Our backups ended up running longer and longer as the scans took longer. So, yes, it was a bit painful for us in the past.

Gardner: What happened next?

Smooth deployer

Furniss: Deployment was a really, really good experience. In the past, we have had suppliers come along and provide us a deployment document, some description, and it would be their standard document, there was nothing customized. They wouldn't speak with us to find out what's actually deployed and how their product fit in. It was just, "We are going to deploy it like this." And we would then have issues trying to get things working properly, and we'd have to go backward and forward with a third party to get things resolved.

In this instance, we had Bitdefender's consultants. They came on-site to see us, and we had a really good meeting. They were asking us questions: "Can you tell us about your environment? Where are your DMZs? What applications have you got deployed? What systems are you using? What hypervisor platforms have you got?" And all of that information was taken into account in the design document that they customized completely to best fit their best practices and what we had in place.

We ended up with something we could deploy ourselves, if we wanted to. We didn't do that. We took their consultancy as a part of the deployment process. We had the Bitdefender guys on-site for a couple of days working with us to build the proper infrastructure services to run GravityZone.

And it went really well. Nothing was missed from the design. They gave us all the ports and firewall rules needed, and it went really, really smoothly.

We initially thought we were going to have a problem with deploying out to the clients, but we worked with the consultants to come up with a way around impacting our end-users during the deployment.

We worked with the [Bitdefender] consultants to come up with a way around impacting our end users during the deployment.

One of our big worries was that when you deploy Bitdefender, the first thing it does is see if there is a competitive vendor's product on the machine. If it finds that, it will remove it, and then restart the user's device to continue the installation. Now, that was going to be a concern to us.

So we came up with a scripted solution that we pushed out through Microsoft System Center Configuration Manager. We were able to run the uninstall command for the third-party product, and then Bitdefender triggered for the install straightaway. The devices didn't need rebooting, and it didn't impact any of our end users at all. They didn't even

know there was anything happening. The only thing that would see is the little icon in the taskbar changing from the previous vendor's icon to Bitdefender.

It was really smooth. We got the automation to run and push out the client to our end users, and they just didn't know about it.

Gardner: What was the impact on the servers?

Environmental change for the better

Furniss: Our server impact has completely changed. The full scanning that Bitdefender does, which might take 15 minutes, is far less time than the two to three hours before on some of the bigger file servers.

And then once it's done with that full scan, we have it set up to do more frequent quick scans that take about three minutes. The resource utilization of this new scan set up has just totally changed the environment.

Because we use virtualization predominantly across our server infrastructure, we have even deployed the Bitdefender scan servers, which allow us to do separate scans on each of our virtualized server hosts. It does all of the offloading of the scanning of files and malware and that kind of stuff.

It's a lightweight agent, it takes less memory, less footprint, and less resources. And the scan is offloaded to the scan server that we run.

The impact from a server perspective is that you no longer see spikes in CPU or memory utilization with backups. We don't have any issues with that kind of thing anymore. It's really great to see a vendor come up with a solution to issues that people seem to have across the board.

It's really great to see a vendor come up with a solution to issues that people seem to have across the board.

Gardner: Has that impacted your utilization and ability to get the most virtual machines (VMs) per CPU? How has your total costs equation been impacted?

Furniss: The fact that we are not getting all these spikes across the virtualization platform means we can squeeze in more VMs per host without an issue. It means we can get more bank for buck, if you like.

Gardner: When you have a mixed environment -- and I understand you have Nutanix hyperconverged (HCI), Hyper-V and vSphere VMs, some Citrix XenServer, and a mix of desktops -- how does managing such heterogeneity with a common security approach work? It sounds like that could be kind of a mess.

Furniss: You would think it would be a mess. But from my perspective, Bitdefender GravityZone is really good because I have this all on a single pane of glass. It hooks into Microsoft ActiveDirectory, so it pulls back everything in there. I can see all the devices at once. It hooks into our Nutanix HCI environment. I can deploy small scan servers into the environment directly from GravityZone.

If I decide on an additional scan server, it automatically builds that scan server in the virtual environment for me, and it's another box that we've got for scanning everything on the virtual service.

It's nice that it hooks into all these various things. We currently have some legacy VMware. Bitdefender lets me see what's in that environment. We don't use the VMware NSX platform, but it gives me visibility across an older platform even as I'm moving to get everything to the Nutanix HCI.

So it makes our jobs easier. The additional patch management module that we have in there, it's one of the big things for us.

For example, we have always been really good at keeping our Windows updates on devices and servers up to the latest level. But we tended to have problems keeping updates ongoing for all of our third-party apps, such as Adobe Reader, Flash, and Java across all of the devices.

You can get lost as to what is out there unless you do some kind of active scanning across your entire infrastructure, and the Bitdefender patch management allows us to see where we have different versions of apps and updates on client devices. It allows us to patch them up to the latest level and install the latest versions.

The Bitdefender patch management allows us to see where we have different versions of apps and updates on client devices.

From that perspective, I am again using just one pane of glass, but I am getting so much benefit and extra features and functionality than I did previously in the many other products that we use.

Gardner: Stephen, you mentioned a total cost of ownership (TCO) benefit when it comes to server utilization and the increased VMs. Is there another economic metric when it comes to administration? You have a small number of people. Do you see a payback in terms of this administration and integration value?

Furniss: I do. We only have 13 people on the infrastructure team, but only two or three of us actively go into the Bitdefender GravityZone platform. And on a day-to-day basis, we don't have to do that much. If we deploy a new system, we might have to monitor and see if there is anything that's needed as an exception if it's some funky application.

But once our applications are deployed and our servers are up and running, we don't have to make any real changes. We only have to look at patch levels with third-parties, or to see if there are any issues on our end points and needs our attention.

The actual amount of time we need to be in the Bitdefender console is quite reduced so it's really useful to us.

Gardner: What's been the result this last year that you have had Bitdefender running in terms of the main goal -- which is to be free of security concerns?

Proactive infection protection

Furniss: That's just been the crux of it. We haven't had any malware any ransomware attacks on our network. We have not had to spend days, weeks, or hours restoring files back or anything like that -- or rebuilding hundreds of machines because they have something on them. So that's been a good thing.

Another interesting thing for us, we began looking at the Bitdefender reports from day one. And it had actually found, going back 5, 6, or 7 years, that there was malware or some sort of viruses still out there in our systems.

And the weird thing is, our previous security product had never even seen this stuff. It had obviously let it through to start with. It got through all our filtering and everything, and it was sitting in somebody's mailbox ready -- if they clicked on it – to launch and infect the entire network.

Straightaway from day one, we were detecting stuff that sat for years in people's mailboxes. We just didn't even know about it.

So, from that perspective, it's been fantastic. We've not had any security outbreaks that we had to deal with, or anything like that.

It's been fantastic. We've not had any security outbreaks that we had to deal with, or anything like that.

And just recently, we had our security audit from our penetration testers. One of the things they try to do is actually put some malware on to a test device. They came back and said they had not been able to do that. They have been unable to infect any of our devices. So that's been a really, really good thing from our perspective.

Gardner: How is that translated into the perception from your end users and your overseers, those people managing your budgets? Has there been a sense of getting more value? What's the satisfaction quotient, if you will, from your end users?

Furniss: A really good, positive thing has been that they have not come back and said that there's anything that we've lost. There are no complaints about machines being slow.

We even had one of our applications guys say that their machine was running faster than it normally does on Fridays. When we explained that we had swapped out the old version of the security product for Bitdefender, it was like, “Oh, that’s great, keep it up.”

For the people higher up, at the minute, I don’t think they appreciate what we’ve done. That will come in the next month as we start presenting to them our security reports and the reports from the audit about how they were unable to infect an end-user device.

From our side, from IT, we are really, really pleased with it. We understand what it does and how much it’s saving us from the pains of having to restore files. We are not being seen as one of these councils or entities that’s suddenly plastered across the newspaper and had its reputation tarnished because anyone has suddenly lost all their systems or been infected or whatever.

Gardner: Having a smoothly running organization is the payoff.

Before we close out, what about the future? Where would you like to see your security products go in terms of more intelligence, using data, and getting more of a proactive benefit?

Cloud on the horizon

Furniss: We are doing a lot more now with virtualization. We have only about 50 physical servers left. We are also thinking about the cloud journey. So we want the security products working with all of that stuff up in the cloud. It’s going to be the next big thing for us. We want to secure that area of our environment if we start moving infrastructure servers up there.

We are thinking about the cloud journey. We want the security products working with all of that stuff up in the cloud. It’s going to be the next big thing for us.

Can we protect stuff up in the cloud as well as what we have here?

Gardner: Yeah, and you mentioned, Stephen, at home that you are using Bitdefender down into your mobile devices, is that also the case with your users in the council, in the governance there or is there a bring your own device benefit or some way that you are looking to allow people to use more of their own devices in context of work? How does that mobile edge work in the future?

Furniss: Well, I don’t know. I think a mobile device is quite costly for councils to actually deploy, but we have taken the approach of -- if you need it for work, then you get one. We currently have got a project to look at deploying the mobile version of Bitdefender to our actual existing Android users.

Gardner: Now that you have 20/20 hindsight with using this type of security environment over the course of a year, any advice for folks in a similar situation?

Furniss: Don't be scared of change. I think one of the things that always used to worry me was that we knew what we were doing with a particular vendor. We knew what our difficulties were. Are we going to be able to remove it from all the devices?

Don't worry about that. If you are getting the right product, it's going to take care of lot of the issues that you currently have. We found that deploying the new product was relatively easy and didn't cause any pain to our end-users. It was seamless. They didn't even know we had done it.

Don't be afraid of change and moving into something new. Get the best use of the new products that are out there.

Some people might be thinking that they have a massive estate and it's going to be a real headache. But with automation and a bit of thinking about how and what are you going to do, it's fairly straightforward to deploy a new antivirus product to your end users. Don't be afraid of change and moving into something new. Get the best use of the new products that there are out there.

Gardner: I'm afraid we will have to leave it there. You have been listening to a sponsored BriefingsDirect discussion on how a large metropolitan borough in South Yorkshire, England solved a recurring ransomware attack problem -- but along the way gained wider infrastructure performance, cost benefits, operational benefits, and a happier overall organization.

Please join me in thanking our guest, Stephen Furniss, ICT Technical Specialist for Infrastructure at Barnsley Metropolitan Borough Council. Thank you so much, Stephen.

Furniss: Thanks for having me.

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 also 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 a large metropolitan borough council in South Yorkshire, England thwarted recurring ransomware attacks but also provided a catalyst to wider infrastructure performance, cost, operations, and management benefits.

You may also be interested in:

- 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 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