RT: Can you talk a bit about Webroot's growth?

AN: Yes. Webroot's really grown over the last five to 10 years to become a cloud-first security provider. First and foremost, we're a threat intelligence provider, and some of that finds its way into the hardware of a few of the bigger names in the IT industry.

We also use this intelligence for our own platform and to back up our business-led solutions. Our strategic focus is MSPs (managed service providers) and delivering security services to them has helped us in the last three or four years. We want to make life easier for them, to reduce administration, optimise their customers' IT environment and improve efficacy.

RT: I know Webroot have a customer-facing division as well, where you protect users' PCs, Macs and networks. I'd like to focus on the business side of your offering, particularly the managed service provider programme.

In a nutshell, tell us how you help MSPs to keep their clients safe in what is an increasingly unsafe cyber world?

AN: Our platform provides three solutions which are integrated into one, and the idea behind that is to secure the end point - the server and the network (with DNS web filtering) – and also the human, which is the riskiest element. This refers the user who can click on a web link or visit a site they shouldn't be.

Our three solutions are antivirus, managed straight from the cloud using just cloud intelligence to make detections and DNS (Domain Name Server) web filtering which does this based on categories and allows you to stop users wasting time and visiting inappropriate sites.

The security awareness training we offer is primarily phishing simulation and keeping users from making a false move and clicking a link that they shouldn't. We deliver training in a targeted way to those users who've accidentally fallen foul of a phishing campaign.

Increasingly, malware is becoming more advanced and able to evade detection so it can find its way into the network through a variety of different means. The MSP needs to help their users spot something that may not be suspicious to raise awareness levels. With the GDPR (General Data Protection Regulation) legislation on the horizon, making sure that your users are trained is almost becoming a legal requirement.

RT: You've touched on two areas that I want to dig deep into – the technology and the human element. The target of this blog and podcast is MSPs, and I know if they could just get rid of clients and employees their businesses would run absolutely fine!

Before we get going with that, I'd like to talk about something else. In a short time, the name Webroot has become synonymous with managed service providers and security, and most of the progressive MSPs are using the platform.

When these companies became aware of Webroot, they were blown away by the innovative nature of the platform. Why would you say it's become the top choice for the world's top MSPs?

AN: Antivirus (AV) is boring! Let's face it – who wants to spend hours managing it, making sure it's up to date? The reason that MSPs have chosen us is because our solution is really easy to implement. Inherently, people don't choose an AV solution which isn't effective, and our efficacy rates are really strong.

Most of our customers tell us that when they move to Webroot they see a drastic reduction in the number of viruses they deal with. MSPs want to spend less time managing things they think should be automated, and we do a good job of detecting, protecting and remediating without a great deal of intervention from them.

Reducing the total cost of ownership is something that a lot of business owners mention when they're talking about their IT solutions, but we believe that the stats speak for themselves – most of our customers tell us that they spend 70-80% less time managing AV once they've moved to Webroot.

I think efficacy should be expected as a given, because you don't choose a solution that doesn't work, and it's something that's strong for us. The product is light and fast, and that's an added benefit, because an MSP's customers tend to be happier that Webroot helps their computers run faster.

In the 21st century, most computers are fast and responsive, but even in today's enhance IT environment, Webroot can still improve the performance of your endpoints. Happier customers and happier support teams, along with better efficiencies are the reasons why MSPs choose us.

RT: One of the things that jumps out about Webroot in the world of modern MSPs is that integration is key, and this is something it does well. Many MSPs build stacks of solutions that they offer, and of course they all need to talk to one another. Tell me more about Webroot's approach to integration, specifically 'The Unity API' (application programming interface), which helps MSPs go deep.

AN: We've recognised that we're an add on, a solution. We're not what the MSP uses to manage their business, because that'll be an RMM (remote monitoring and management) and a PSA (professional services automation), so our integrations with those tools is key to our success. We work with the big players in the industry – AutoTask, ConnectWise, Kaseya, Continuum, Ninja, Atera – so we're integrated with most of the RMMs out there.

This makes it easier for the MSPs to manage everything from one pane of glass, and the Unity API itself gives some flexibility outside of an RMM if the MSP has technical staff who can code. It allows them to deploy, configure, report and manage, so anything you can do in Webroot can also be done through the API.
You can take data from the portal and create your own dashboard of what's happening within the Webroot world in your organisation. It can also do things such as policies and deploy clients.

It's gives flexibility to MSPs who aren't using an RMM, who want some bespoke integration work into their ticketing system or other areas of the business, as the Unity API helps them to achieve that.

RT: I'd like to touch on something you mentioned before, which was around total cost of ownership. All these tools that we talk about cost MSPs money, and one of the arguments that I hear from MSPs when they speak to their clients is that they either can't or won't pay for any more cyber security. How do you coach MSPs on how to educate their clients on why solutions like Webroot are essential?

AN: That's an important point, and I'm glad you touched on it. It's a software solutions provider's job to arm an MSP with positioning arguments for their customers, because at the end of the day we should know how to position our solutions to different types of customers, be they MSP or end user.

An MSP strongly aligns themselves with the idea of ‘improved security and reduced infections’ that all of our solutions lend themselves well to, but how that MSP then takes that message and communicates it to its customers is really important.

With DNS-based filtering, we can tell an MSP that they’ll drastically reduce the number of threats that make it onto your network in the first place, but the customer doesn’t care about that. We need to arm the MSP with positioning arguments around productivity improvement, because a business owner understands why getting an extra 15% of working time out of their staff will impact their bottom line.

How we position the MSPs to allow them to showcase the strengths of the solution to their customer is key. Things like security awareness training is important for the MSP to understand why an end user would need to be trained around security and to talk about downtime with their customers.

Positioning security awareness to a company so they understand that if a team member clicks on a URL that launched a virus that can’t be stopped by your antivirus, or did something unusual and opened a back door for someone to get onto your network, that there’s a cost to the business when it goes offline, can make a difference.

Giving MSPs positioning arguments to talk to their customers about the solutions that you’re selling is really important, because otherwise they’re not going to spend the time working out how to do that themselves.

RT: I’d like to dig a bit deeper into one of your previous roles at Webroot. You used to look after the partners as a channel manager. What makes a good partner for Webroot, do you think?
AN: It’s probably the same as in any industry. A partnership is about two people working towards a common goal, so someone that’s properly engaged, wants to take your messaging out to your customer, wants to interact with you and the sales, marketing and support teams is great.

It’s not a partnership if you’re not working towards a common goal. I hope we give a responsive, commercial, marketing support experience to our customers. We won SE Magazine’s ‘Best Support’ for the second year in a row, and I think that’s because we try to take a more engaged approach with our customers.

I always ask people to let me know if they have a problem so I can try to fix it, because you need to provide a little more than your competition provides, and that more personal touch is what an MSP’s looking for as well.

RT: Webroot talks about cloud-based security. In practical terms, how does that differ from the traditional, agency-based antivirus solutions that many people are familiar with? What does it look like and how is it different?

AN: It's a rapidly changing threat landscape, and being able to store all of the intel about new threats as they happen, in one central source to draw upon, for all of your customers, has to be a better approach.

The quantity of new pieces of malware we see just in a Windows environment is around 200 million a year or more. Creating definitions and rule sets to detect those is not going to be the most effective way of protecting your customers. I think a central repository constantly fed by agents around the world (i.e. – everyone who uses Webroot reinforces it) is a common-sense approach.

There are other AV providers that offer some of same components as us, but our approach is around preventing any type of malware virus worm from running on your machine and affecting the way that the machine operates.

We're not so bothered about detecting something for detection's sake unless it's going to impact the operating system negatively. We don't scan every folder on the computer, but we look at specific folders where there could be an email loaded into memory, and we scan anything loaded from scripts and websites. We also scan when things are recorded to disc, because that's the point where something could happen.

Our approach is slightly different as we're not scanning the whole hard disc to find something suspicious, we're looking for what could affect you as the user or the operating system. It has to be cloud-based, because that's the only way to keep up to speed with the growing cyber-criminal industry.

More money is made from cyber crime than from traditional methods of fraud and extortion, so inevitably cyber criminals are becoming more innovative, because the rewards are bigger year on year – more than $5m was generated using ransomware in 2017, and potentially that could double.

RT: I want to pick up on something you've mentioned a couple of times – DNS protection. It's a service I see the more progressive MSPs offer, and it seems to have evolved from an antivirus agent installed on a computer to a multi-tiered, multi-faceted approach. Where does DNS protection come in and how does it all fit together?

AN: We've always advocated a multi-layered approach to securing your endpoints, because viruses find their way into networks from so many different locations and vectors. If you haven't patched your operating system with the latest updates, even if you've got the world's best antivirus it might be unable to stop it being leveraged within an environment.

There are a few things we talk about around having a layered approach to security – making sure you've got good endpoint technology is important, as is backing up your data, so that if the worst comes to the worst you've always got a backup.

User education, such as making sure they're aware of what threats are out there and what could go wrong with clicking links or opening emails or attachments, is also important.

Disabling the execution of script files on the network is a great way to stop random scripts running and loading malware.

It sounds old-fashioned, but updating software and patching is still as relevant now as it was 20 years ago. WannaCry (a cyber-attack in 2017) was such a big deal because people hadn't done their patching three months after the patch was released.

This is not just for Windows, but for other third-party applications such as Java, so patch straight away, because they will inevitably have things which can be leveraged.

Other things include making sure that passwords are strong, ensuring that RDP (Remote Desktop Protocol) is locked down, because we see lots of breaches from where people have used public-facing IP addresses for RDP machines and using weak passwords. Once an RDP server has been compromised you've got the main access and credentials.

There are few different ways to protect your network. Filtering traffic at the network level is also key, because if you can stop all devices that are communicating out into the world, not just Windows machines, from communicating with malicious IPs or URLs that will make your environment more secure. Putting some kind of network filtering in place is going to reduce risk.

RT: Back in 2010, Webroot acquired BrightCloud, web reputation and content classification technology. It seems to be a huge part of Webroot's cloud-first approach, so what is BrightCloud and how do things like network anomaly detection work?

AN: BrightCloud is the cloud intel we use for our business solutions – AV, security manager training and DNS filtering – but also it's the technology we white label into other vendors' solutions, such as for Cisco, Palo Alto and F5. They use some of that URL and content classification to allow them to route traffic safely.

Inevitably, as a cloud-based company, that's our most valuable and prized asset. The reason that some of these bigger technology players choose to work with Webroot is because we've got a broad customer base, and they see who else we work with in the industry.

It's definitely an important part of the portfolio, which we make available to partners who want to take that data and use our threat intelligence to correlate against alerts that they see. We integrate with software such as LogRhythm to give you detections around the things that you see in alerts.

As that threat landscape evolves ever further and it becomes increasingly challenging to stop attacks as they come in from a myriad of different vectors, being able to understand what anomalous behaviour looks like is really important for the IoT (Internet of Things) space.

You're no longer looking at an operating system to see if something malicious is running, you're looking to see if a callout from a specific machine at a specific time of day to a certain location could be deemed to be unusual. If so, how do you then put in place something to block that traffic or start to investigate that traffic?

That's why we acquired Cyber Flow in 2016, because that gave us the anomaly detection capability that we could then plug into our threat detection intelligence and link the two together and provide a more robust solution for MSPs. We're working on integrating that into the portfolio.

RT: I want to return to tech in a bit, but I'm conscious that one of the massive vectors for cyber security and hackers to get in is humans, and it's fair to say that they're the weakest link in any cyber defence policy.

How can MSPs help their clients become more aware of cyber security? Is it fair to say that even with the best tools in the world, if someone clicks on a link they're uneducated about, there's only so much an MSP can do to protect their clients?

AN: I think it's more about improving the vigilance of the staff. Increasingly these days phishing attacks are so good that I've been fooled, as have techy guys in our business, by things that look like a totally legitimate email.

One of my colleagues talks about buying a file online from someone and then he received a bill from the same website with a PDF attached. As he was expecting it, he clicked on the link and was asked for his Gmail credentials. This was not unusual, but he realised that the domain was being spoofed and was leading him down the garden path.

It's quite easy to make a phishing website look legitimate, and there are far fewer typos in the emails than we used to see, or African princes looking for funds! It's more professionally done and more targeted. The African prince scam is looking for someone gullible to respond to the email, but someone computer literate will be fooled by something else.

Social engineering is something we're seeing a lot more of, and it's very difficult to train against it. If someone calls up and says they're ringing on behalf of your MP and you need to pay a bill, or you get an email asking you to change the bank account registered on file from a legitimate email address, it seems convincing. Making people more cautious before they do anything that's unusual or non-standard is important, and security awareness training can hopefully help with that.

RT: In practical terms, how would you recommend that Webroot partners and MSPs in general get started with that security awareness training for their customers?

AN: GDPR is a good talking point to start off with. Legally, businesses are expected to understand the regulation and train their staff on what it means for the business. Using a security awareness training programme allows you to help them understand it, and it's good if you need a justification.

I think having a play with it to see what it looks like, testing it out on a customer is something that can be done free of charge, and nine times out of 10 the customer will say, ‘that was good, and I can see why this will be valuable for my business.’

Most of the time, you’ll see that 30-40% of users will click on a phishing link on the first email you send, and I think that’s quite enlightening for a business, because they realise the risk their staff are taking at that point.

RT: A lot of MSPs I talk to are getting inbound enquiries from small businesses about GDPR, because it’s raising the bar a bit.

Let’s go a bit deeper with the tech talk – earlier this year there was a lot of panic around the Spectre (security) vulnerability. For the uninitiated, what would you say is the difference between a vulnerability, an exploit (such as malware) and a virus? Can you run us through the basic technology phrases?

AN: A vulnerability into computer security is a weakness that can be exploited by someone to do something within your environment. It could be an unpatched server that allows someone to use an exploit to get into your network, such as a piece of code that allows them to overpower the operating system.

If it hasn’t been patched and there’s a bug in the system, that’s a vulnerability because otherwise an exploit can be leveraged to get into the network. Exploits are code or mechanisms by which you can take advantage of vulnerabilities in software, so they’re quite closely linked.

In the industry, we tend to talk about malware, which is anything bad, usually a virus of some description or an application which has malicious intent at heart. A virus, in theory, is something that is self-replicating and can move across the network.

What we’re seeing now is a move back to employing worm-like capabilities in viruses. Worms were designed to move across the network without any assistance, and as we saw with things like WannaCry, that had a worm element that allowed it to continue infecting systems.

For some reason, worms became old hat for a while, but now they’re back with a vengeance and allow viruses to have their impact. They search through the network looking for other devices which have the vulnerability, move across to them and infect further with the virus.

RT: And that’s why intelligence is so important for you? These things are changing so quickly, so unlike the old days you can’t just have a template or a file agent that shows what a virus looks like and how to detect and protect against it. Nowadays, they’re morphing all the time.

AN: Absolutely. Polymorphism is the norm, which means that a virus can change and have different attributes dependent upon which operating system it's on, the time of day, the other applications installed, the language used. Polymorphism means that the virus changes every time it's run, depending on the environment it's in.

That makes it hard to track and stop, because it might do something different on a Spanish operating system compared to an English one, for example. Viruses are designed to evade capture, and that's the only reason they work in the wild, because they need to exist and work somewhere.

Cyber criminals are increasingly using new techniques to beat detection, for example antivirus process hollowing, where the virus takes advantage of a good process to do things within the operating system. Fileless malware involves not using portable executables, which is how we usually see viruses being executed in an environment – instead it's stored in a registry key and loaded into the memory.

There are various things you can do to lock down your environment, and if you can put in place things to stop the scripts from running, making sure you've got a good antivirus web filtering solution and you've backed up your data, even if a new technique is used in theory it won't be able to harm your machines.

RT: So on one hand we hear a lot about the Dark Web and script keys, but it's actually really easy for someone without technical knowledge to buy tools and information to make cyber-attacks. On the flip side, what's the most bizarre intrusion you've come across, or one that you've even had grudging admiration for because it was innovative?

AN: I always find it quite crazy how easy it is to perform social engineering to extort money out of businesses, and that's not particularly innovative. We hear it all the time from our MSPs – 'someone called up and said they needed us to pay a bill, so we paid it.'
We ask them where their checks and balances were for a new supplier calling up and saying they needed to be paid? They need to find the order that was made, a delivery note and so on. We rely so much on computers that we get duped by something that's not related to them but is social engineering.

If someone asks us to pay money we do it, because we think that's what we should do, and that surprises me quite a lot. The world is increasingly online, and I find denial-of-service attacks to be the most worrying, because you see some of the biggest websites of the world being taken down by them.

Most of the time they're using computers that have been hijacked and are part of a bot net to send data through to a specific website or online service, but they're also increasingly using IT devices, and one of the biggest outages caused by a DDos (distributed denial-of-service) attack recently was where remote cameras being used were compromised due to a security weakness.

There are some good DDos mitigation services out there which will take the traffic and redirect it somewhere else, but I find that an interesting new way of extorting in the online age.

RT: We've talked about the Internet of Things (IoT) and we're increasingly hearing more about IP connected devices – home automation and so on. What are the dangers this new, IP-enabled world presents to MSPs? How can they help their clients stay safe?

AN: I think understanding what their customer has within their environment and a proper inventory of what internet-enabled devices exist too is key in order to understand what their risk profile looks like.

I think good password best practises for IoT devices is the place to start. When I first started in IT, Oracle came provided with the user name and password set as 'system' and 'manager', and the amount of people who didn't change either of these was crazy – the government, police, help services would leave databases with all of their information available.

An MSP could definitely help their clients by running an audit of the IoT or internet enabled devices across a customer's network and making sure that their username and password isn't set to default - that they've got a comprehensive password set – and increase the security on those devices where possible.

They may also change the ports that the devices are accessed from, so that a script key or someone with limited information but who knows that devices of a certain type communicate on a specific IP with a certain port and user name and password, won't be able to compromise those devices.

RT: There are a couple of other technologies that I've recently picked up on via the Webroot blog (which I recommend it to anyone interested in cyber security), so could we discuss them? The first was the IP Reputation service, and the second is the Streaming Malware Detection. Could you explain both of those?

AN: The real-time anti-phishing uses a lot of data points and correlates information from our database to allow us to make decisions about new websites as they appear, and already having quite a big database of cloud data and scanning the IP addresses several times a day allows us to see what's new. We've also got a history of whether or not a website has ever been malicious or linked to anything else malicious.

We use a technology called Maximum Entropy Discrimination. It tries to identify whether a specific URL is a phishing site when it's accessed and differentiate between specific site features and behaviours to determine whether or not there is a phishing risk on the site. It's known to be more effective than other mechanisms we've used in the past.

It uses information from the website in real time to make a decision about whether or not what something is trying to do is malicious or not. It's machine learning technology, in the

same way that all the other security providers and IT companies are trying to leverage AI (artificial intelligence).

It's not possible to have a team of researchers big enough to make determinations about threats, because of the vast quantities of threats we see on a daily basis, so using some form of machine learning is the only way to deal with the volumes.

Streaming Malware Detection is a service that allows us to identify and stop malicious files using our Bright Cloud Reputation Service. Our partners send us files, we make determinations about them and send that back to the customer.

It allows you to block known threats, whitelist good files and allows us to research the unknowns that are coming. It's designed to be a service that's consumed by other technology companies or larger organisations that want to analyse the data they're seeing and getting an opinion on if it's malicious.

RT: These are some of the innovations we're seeing that are making Webroot the market leader, and while MSPs don't need to know what's going on in the background, they want the confidence that you're doing the work to respond to all the changes in the threat landscape.

AN: The ethos behind our platforms is that they're easy to manage, and they want to take the heavy lifting out of providing security to managed customers, which I think we've done with all our platforms.

Things should be quick to set up, and the ongoing maintenance and management should be really minimal. Efficacy is the benchmark that everyone uses to make a decision about buying a solution, and I think ours is robust.

RT: Let's talk about one more area of tech that everyone's familiar with – mobile. How important is mobile security, and what are Webroot doing to help with that in the wider security debate?

AN: We've got a mobile option that third party technology providers leverage in order to get reputation analysis on new apps, and we've got a mobile security product that's designed to run on Android and iOS (for Apple mobiles).

I personally thought that BYOD (bring your own device) was going to be huge and the next big growth area for the tech industry, but it doesn't feel like it has been. I think that's down to the fact that the mobile technology providers, Google and Apple have done a good job of their securing their operating systems, while Android is less secure.

Our solutions for the Apple devices is a light MDM (mobile device management), so it gives you the option to remote lock or wipe your devices and secures the types of communication you can use, but it's not really an antivirus solution, because we don't tend to see viruses in the Apple space. The Mac OS also has far fewer viruses than a Windows device.

For the Android, it's definitely weaker in terms of security aspects, but again we have a malware scanner and MDM light options in the same way, so if your device gets lost you can delete sensitive data.

There is also a malware scanner on the mobile version of Webroot if needed, although it's not that popular in our customer base. That might be because it's harder to manage if you're not a full MDM, but it's an area of growth for us.

RT: What is the one action you'd like MSPs to take as a result of listening to this interview?

AN: I'd love a dialogue, because we like talking to MSPs and hearing about the trends they see, their successes and pain points so we can learn from the community. I'd love to think that if you're not using Webroot you might give it a try – it's so easy to set up that I think proof of concept takes less than five minutes.

If you're already using Webroot, take a look at our new solutions, such as the DNS awareness and the security awareness training solutions. These can add new streams of revenue to an MSPs portfolio, and I think with the right positioning you could definitely get customers to buy into these technologies.