AN INTERVIEW WITH JULIAN FAY,

SENETAS CTO

Hello and welcome to this EM 360 podcast. My name is Doctor Eric Cole, your host for today's podcast. I am the founder and CEO of Secure Anchor Consulting, a company that is focused on building out effective security road maps that actually work to protect the organisation.

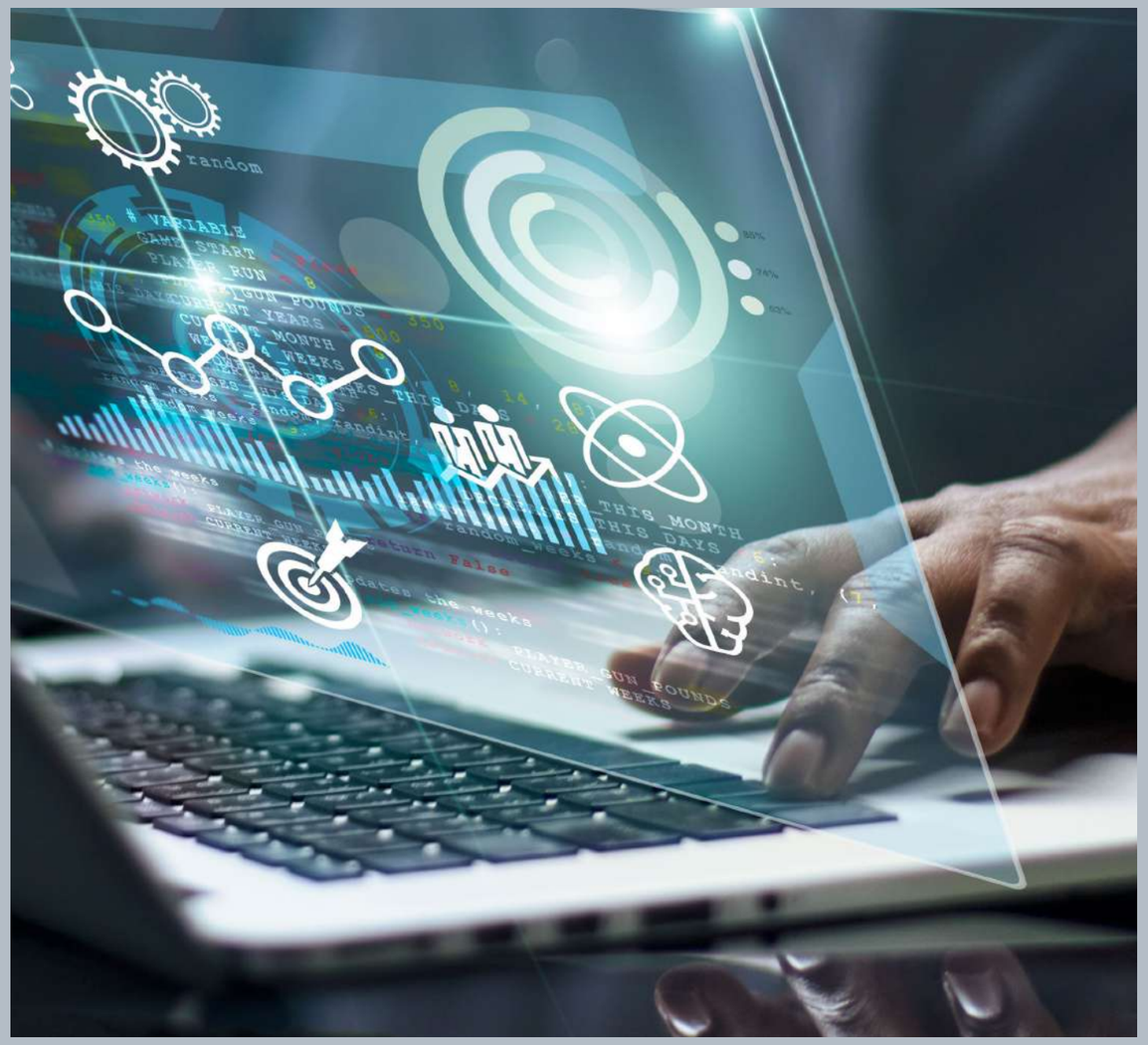
In today's podcast I'll be speaking with Julian Fay, CTO at Senetas, a global partner of Thales. We're going to be looking at data in motion and futureproofing from a quantum perspective.

Thank you for joining me today, Julian. If we could kick things off by you letting us know a little bit about yourself and how you got started in cybersecurity?

"It's good to be with you today. My background is I grew up in England and I studied electronic engineering. The first few years of my career I was working and developing various hardware and software solutions and then, just over 20 years ago I moved over to Australia, which was an exciting opportunity for me. My first role there was working on network security for some very old network protocols that some of your audience may remember, called X25. This was an early packet-switched network and frame relay, which got me really interested in communications and how we build network infrastructure.

"That was a period when we were really just starting to evolve our high-speed communication backbones from copper to high-speed fibre optics and it kind of begged the question how are we actually going to secure this new high-speed infrastructure. I was lucky enough to be partnered with a couple of colleagues and we started a small business to build an encryption solution to secure some of these early high-speed networks. We took years to develop the first technical solution, but I guess we were pretty naïve when it came to the commercial side of things. We quite literally started emailing around anyone who we thought might have an interest in this product. To our great delight, we actually got a response from Thales over in the US and they said you better come over here because we've got a customer who needs some high-speed optical encryption.

"To cut a long story short, that was the start of many conversations and many trips from Melbourne Australia to the US. We were lucky enough to basically win the contract to secure a US Department of Defence high-speed fibre optic backbone in the Asia Pacific region, in partnership with Thales, so that was great for a small company. What we've really done over the last few years is built on that heritage to work very hard to design network encryption solutions as networks have continued to evolve and get faster."



That was great. Let's go ahead and jump right into it. So, when we talk about data in motion, what are the primary concerns with network security in this arena?

"From my perspective, network security has two fundamental roles. It has a protection role and a prevention role. On the protection side, it's all about keeping the information that is sent across the network secure and protected. When we think about the best way to do that, we normally think about the CIA triad – the standard cybersecurity models for data protection. That's confidentiality to protect information from unauthorised access across the network. It's integrity to protect data from modification and availability to ensure that the network and information remains accessible to authorised users at all times.

"Then there's the prevention side of it, which is really about stopping the network itself being weaponized and becoming an attack vector for entry into the organisation. The network is often the attack surface, whereby malware or ransomware can get into organisation. Denial of service is also another example. So, those two are the fundamental roles and I guess we have a number of tools that we use to help us with that prevention and protection role.

"They include the obvious ones like firewalls, access control, intrusion detection intrusion prevention, network monitoring etc, but I think that the bedrock of network security is encryption. I like to think of it as a kind of digital cement, because I think it provides the foundation upon which all of our other cybersecurity goodness is built. I guess the particular challenge when it comes to network security is building security that is good enough to keep the information protected, but also allow the network to do its sole job; which is to get information from point A to point B. Often security can become a real bottleneck and have a real impact on user experience, so the particular challenge with network security is keeping the network up and running and performing well."

I love that, that encryption is the cement that holds it all together. Because you're spot on. If that information isn't protected and secured, were not going to be able to have proper network security in place.

So, it's my understanding that Thales recently published a survey. Can you just share a summary for the audience of the key findings from that survey?

"This was a global survey that Thales and TechTarget recently conducted. It was sent to more than 500 IT and cybersecurity decision makers in global organisations, and it asked questions about their current use of network security, and encryption in particular, and what they saw as some of the future challenges that were coming up in this rapidly changing world. We got the results recently and we published a white paper on it, and I guess they were a little surprising, to the extent that they have highlighted some concerns about how organisations think about and implement network security solutions.

"I'll just talk about two or three of those findings. The first one was the nearly half the respondents, about 42%, stated that they either don't encrypt their network traffic, or they don't actually know if they do, which I personally found very surprising. That indicates a kind of a lethargy and a lack of strategic focus on the network encryption side of their cyber defences. You can imagine asking a CISO or CIO, do you guys have a firewall, or do you use AV tools in your business, and they'd look at you like you clearly don't know what you're doing. It's clear that every organisation has those, so it was really surprising to hear that nearly 50% either don't know or are definitely not using encryption across their network.

"So, I would say that actually reveals a bit of a misunderstanding about the security of both private and public networks because, simply put, no networks are inherently secure. It doesn't matter whether it's a carrier provided private network or the public Internet, these networks do not come with built in security. It's really up to us as organisations to make sure that we put adequate protection in environments to keep us safe.

"A second finding that is complementary to that was that, even amongst those who are encrypting, they're not actually thinking about the tools that they use to encrypt. They're not thinking about how to optimise their use of encryption from a security or performance direction, and they tend to just turn on whatever encryption tool is available in the other equipment that they already have running. So, many respondents indicated they just turn on encryption in the firewall, or in the router or the switch.

Of course today, encryption is pervasive. You can turn on IPsec or MACsec in any router, or switch, or firewall that you get. And that may well be fine for many customers, but the truth is that not all encryption solutions are the same.

They vary significantly in terms of security, especially in terms of impact on the network performance, and have different hidden operational costs. I think like all tools, all IT infrastructure, encryption should actually be a proactive choice. Customers should actually understand the different approaches that are available on the market and how to optimise them for their business from a performance and security aspect. That's going to include things as simple as key size and key management - how often is an encryption key rotated? How often is it changed? Are you using a simple pre-shared key that may be used for 20 years and nobody actually thinks about changing? What is the performance impact on the network?

"All security imposes some sort of overhead and network encryption can, if not implemented properly, have a devastating impact on network performance. But it doesn't have to be that way. With modern approaches and modern tools, today you can build solutions that effectively let networks run as well with encryption as they can do without. Then I guess the final part of that was regulatory compliance. A lot of customers are running in industries where you do need to meet compliance with regulatory bodies, so making sure that you actually understand that the solutions you're using do meet those requirements.

"On the positive side, another finding from the survey, when we asked about what challenges you see in the future and how are you going to keep your environments future-proof, nearly three quarters of the respondents recognised that we're living in a rapidly evolving and changing world and that both networks themselves and the threat landscape are really changing. In particular, there was a recognition of the threat posed by quantum computing to certain types of cryptography, so it's good to see that's on the radar. I think that's really important, that we start having more of the conversation about what's going to become an upcoming cryptographic transition for all of us, and that needs to get on the list register in my opinion of all organisations, both large and small."

Now, you mentioned quantum computing there, so let's drill down. That's an area to me where a lot of people have heard the term, but they don't necessarily know what that means. Can you tell us, what is quantum computing and what are quantum resistant network encryption solutions?

"Absolutely. It's an area I'm personally very interested and following very actively, because it's going to have a very large impact for all of us as we're all users of cryptography. I'll just sort of try to summarise it in a simple way. I should say I'm not a quantum physicist, so apologies to any listeners who understand this far better than I do. There is obviously a lot of work, a lot of money, going into the development of a new type of computing model, which we call quantum computing. This is a fundamentally different approach to computing architectures, based on the strange properties of quantum mechanics, which physicists started understanding about 100 years ago.

"Some very clever people realised that we could exploit the properties of quantum mechanics to build a computing system that would allow us to drastically accelerate certain types of computation that were simply not possible on a classical computer. Without going into the physics of it, that's because of the very strange properties of quantum mechanics like superposition and entanglement. There is a lot of money going into trying to develop a useful quantum computer, but we don't have any such one today. We have very small-scale quantum computers.

"Many of your audience probably would have heard about Google building a quantum computer called Sycamore. Now, it had 53 qubits. (A qubit is the quantum equivalent of a digital bit). 53 doesn't sound like very much, and it isn't very much, but it did allow Google to prove something called quantum supremacy, which was a demonstration of the solving of a particular chosen algorithm on a small quantum computer that is not achievable on a classical computer. It sounds kind of scary when you put it like that, you kind of go wow, is this our Terminator moment? Are the quantum computers taking over? Actually no. It was just a deliberately chosen, kind of useless problem, but it did demonstrate that even at small scale quantum computers can do certain optimization very efficiently.

"The problem when it comes to cryptography is that should we be able to build a large-scale quantum computer - and we don't know for sure if we can do that. Many people think we can do it in the next five years; some people think we can do it in the next 10 years. I'd say the working consensus at the moment is that it's going to take 15 to 20 years to build a large-scale quantum computer. If and when we can do that, the challenge is that we know that one of the optimizations such a quantum computer would be able to do is to break the mathematical assumptions of security that about half of our current encryption technologies use. That's what's called public key cryptography, also known as asymmetric cryptography, using algorithms you'll be familiar with - such as RSA or elliptic curve. It's based on mathematical hardness and the assumption the mathematical challenge is so difficult we can't actually solve it in any useful time using today's tools and technologies.

"But a quantum computer would completely change that if it was big enough, and essentially would break public key cryptography in a very short time frame. Now that's very scary, because PKI or public key infrastructure is the bedrock of our Internet security and digital economy, so we have to take this extremely seriously. Industry and the NIST agency in the US (the National Institute of standards and technology) have been working hard for five years to prepare us for this. They've been working on a new class of public key algorithms that are called quantum resistant cryptography. They're sometimes called post quantum cryptography as well, though I find that term a little bit confusing, but essentially, they are the replacement for today's RSA and elliptic curve that we believe will be safe against a large-scale quantum computer.

"So those standards have been worked on for the last five years and we're being told that the draught standards for those algorithms might be released as soon as next year (2022) in draught form. That process has worked through a kind of competition, and they basically went out to the best cryptographers in the industry and asked for lots of algorithms. They started with about 76 I think, and they've now whittled that list down to 7 finalists. Of course, we'd like more than one algorithm to keep us secure. So, to cut to the chase, over the next few years we're going to see an inevitable transition in our public key cryptography. This will happen independently of progress in quantum computing because these will become new standards for national security and enterprise, and all of us will follow these standards over the next five or ten years.

"In a practical sense, that means we face a massive upgrade of all the computing devices we use today that use any type of public key cryptography. So, at Thales, we've been working very hard to prepare our customers for this transition and our objective is to provide a stepping-stone to move from today's world to the future world by using what's called hybrid encryption. This is a way of combining today's trusted security with tomorrow's emerging and future security. If you put those two together then you can actually have a very secure solution, which is still safe as we know and trust it today but gives us protection in the future. I kind of think of it like a COVID vaccine, you know. There's been lots of vaccines out there on the market that have different strengths and trade-offs etc, and it's good that there's lots of them. In the same way, we have lots of quantum safe encryption algorithms that we'll start to hear a lot more about in the next two or three years."

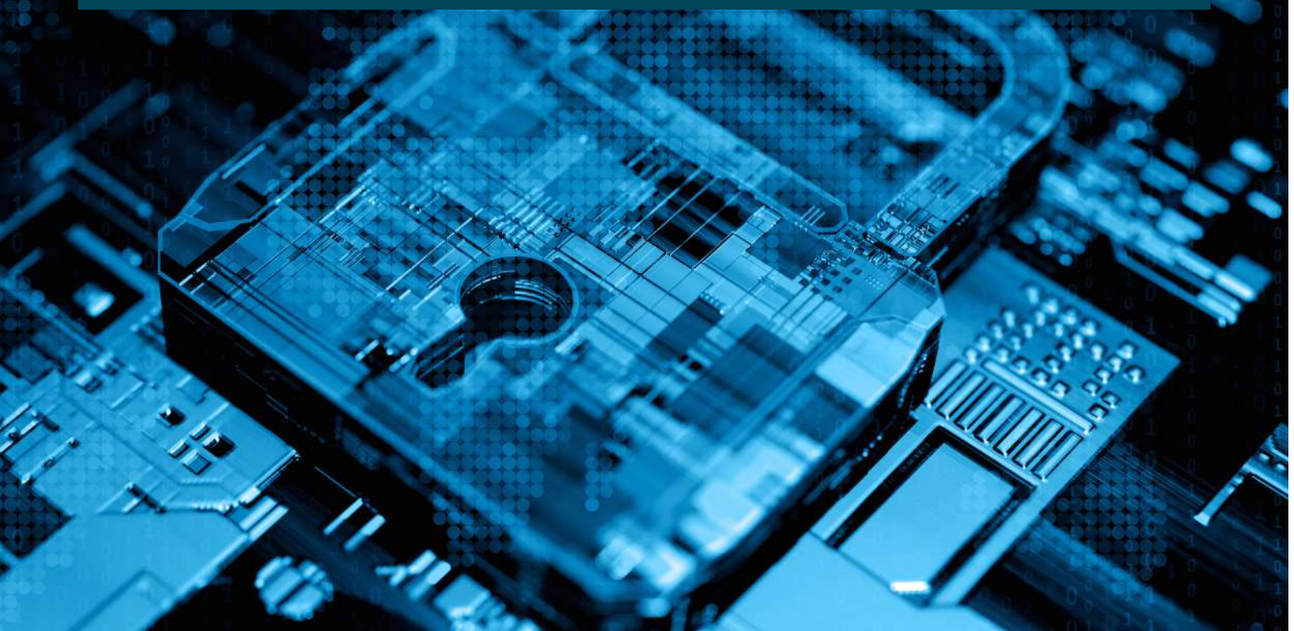
Thank you for that great explanation. It sounds like it's not just as simple as implementing encryption, there's a lot of things that organisations have to think about. So, in terms of recommending a solution today, what are some key areas that you recommend that organisations need to focus on?

"That's a great question. I think, particularly on the encryption side, as our survey indicated they really do need to take a more strategic approach to the use of encryption. Let's be honest, encryption isn't the most exciting technology. Nobody gets out of bed in the morning and gets excited about their encryption; it's all about cloud and AI and sort of sexy technologies. I think encryption, as I said, I believe it is the bedrock of our cyber security, so organisations do need to start taking a more strategic approach to it. Certainly they need to put in place that basic cyber hygiene mechanism, that CIA triad, and of course they really need solutions that are going to provide them with long term protection without compromising their network and application performance.

"I can tell you from some hard-won experience that usability always overrides security, so if you turn on an encryption solution in your environment that reduces your effective throughput by say 30 to 50%, then in reality you're probably going to turn that encryption off. I've seen many instances over the last few years where encryption was actually being physically disabled and turned off because it had a significant performance impact on the network. But it really doesn't have to be that way. I mean, we've worked very hard for 20 years to build efficient, optimised encryption engines that effectively should allow networks to run as well with encryption turned on as they do with it off. So, I really would encourage organisations to think about the approaches and the technologies that they're using in their environments and then, of course, back to the quantum threat, they do really need to have an eye to the future.

"Networks are evolving very quickly. We've seen a massive amount of innovation with the way that networks have been built and delivered. Most organisations are moving to cloud-centric environments, but the cloud is network-centric by design, and I always think of the network as the on ramp into the cloud infrastructure. So even if you sort of think, all of my assets and all of my infrastructure is increasingly in the cloud, the network is what takes you there. So, you actually need to think about how you're going to get there in what in reality is going to be a whole range of different complex network topologies. You know, most organisations have got data cantres that they need to protect traffic between. They've still got traditional carrier MPLS backbones, they're using SD WAN type environments to get into cloud access, so they really need to start thinking about that.

"In particular, when it comes to the quantum transition, I would encourage all CISOs to get this on the risk register of an organisation and to start actually understanding within your environment, what is your use of public key cryptography, therefore what is your exposure. You know it's not out of the question that somebody will make a massive breakthrough in quantum computing that will really shorten the timeline and, of course, all encrypted information has a digital shelf life. If you're protecting information today that you have to keep secret for the next 5-10 years then that information, even in its current encrypted form, is already at risk. Because if we build a quantum computer in a shorter time frame than the lifetime of that data, somebody can decrypt it in the future. I'm hearing from intelligence agencies about the harvest and decrypt threat, in which bad actors are actually storing encrypted data today with the hope that they will be able to decrypt it at some point in the future."



You're talking about the future and quantum computing and what organisations need to think about, but what are some things they can do today to prepare for the future? So they're sort of ready for this and not caught off guard?

Yeah, that's a great question. We've been thinking hard about this question, and I think we've seen a lot of investment, like I said, in the way that networks themselves have evolved, but not a lot in terms of network security, network encryption protocols in particular. Most enterprise network encryption today is using protocols and algorithms that are more than 20 years old, like IPsec or MAC sec for example. And they're fine for many use cases but they weren't built for today's modern environments. What we're seeing is that the days of the traditional wide area network, the WAN, the kind where you just basically connect all your branch offices over a carrier MPLS network back to a data centre, they're going. They're rapidly changing. Those services will still remain but they're being complemented more and more by cloud connectivity and your high-speed Internet, SD Wan type deployment.

"The truth is that most enterprises have a mix of network connectivity that they need to protect, that encompasses high speed fibre, cloud access plus the traditional WAN. So, when we think about how organisations can best protect themselves, we've been really trying to think about what should network security look like in this modern and rapidly evolving world. You know, one of the key components there is performance, as I said, which can actually be a real impediment to security. So, I think organisations need to actually go and have a serious look at the performance and latency requirements that they have for different traffic types running across that mixed environment.

"What we've been focusing on is basically trying to make network security much more commensurate with the way that we approach modern networks. So, in an SD-WAN type environment for example, you might be sending traffic over multiple different core networks. You might be sending some traffic over a private MPLS layer two circuit, you might be sending other data over the public Internet, some might be going over a satellite or a cellular network, and you basically use SD WAN to steer data over the network that best meets its security and performance needs. There's no one size fits all anymore and we think that encryption should be the same way. We don't need to encrypt everything using exactly the same approach by wrapping it inside an IPsec tunnel with header after header that drastically increases the size of the data and significantly reduces throughput.

"We've been focusing on building what we call network independent encryption, which we think is a more modern approach to securing modern network environments and allows you to basically simultaneously encrypt different traffic flows at the most efficient layer, to meet the security and performance needs of the data. For example, you might send some data over a high-speed layer two circuit because you're still using a carrier to get back to the corporate data centre. Other data might be going over the public Internet, so you might need to encrypt that at layer 3 in the IP layer, or you might be running a service that's got traffic flow steering or some policy-based routing in the middle of the network, where you need to expose the TCP and the UDP headers.

There's no one size fits all for these different requirements, so the idea with these more modern approaches is that you can do this in a very efficient, tunnel-free way. Keep the network highly secure. Provide confidentiality and integrity protection but allow the encryption and the network to run at a very high-performance level. So, I think organisations need to actually do some work and understand what's available on the market and how these technologies are rapidly evolving in line with the innovations that we're seeing in network security as well.

As we start to wrap up with our final question, can you give us a case study that ties together everything we've discussed today?

"Sure. There's lots of use cases I could talk about. Just to give you a quick snapshot of a few perhaps if that's alright. We're securing a lot of core cloud backbone infrastructure for some of the largest cloud providers in the US and internationally. There, the use case is to provide very high-speed fibre optic connectivity. Today it's 100 gigabits per second for many of those large cloud providers. Soon it will be 400 gigabits per second and those organisations are really concerned about extremely high-speed throughput. You can imagine, if you're a large cloud provider, the amount of volume of traffic you've got across your backbone. But also in that case they have to meet very strict government regulatory requirements, so in our products we've got them certified to FIPS 140, Common Criteria and various defence certifications around the world, including NATO. For organisations who are trying to attract federal government customers and defence organisations onto their infrastructure that's when you need to use that kind of solution.

"At the other end of the scale, we're doing a lot of work in critical national infrastructure, that's with utility providers in the power space. We recently did a project in the UK for a power company where we were securing some of their infrastructure, and that's very interesting because obviously industrial control systems are critical infrastructure and very vulnerable to cyberattacks. We recently worked with a customer who had a gas pipeline running through central Europe and there they weren't so concerned about confidentiality of data; it was more about the prevention aspect of weaponizing the network. They were running a range of IoT type sensors and devices, SCADA protocols etc, and their concerned about somebody actually accessing the network, opening a valve letting gas escape where it shouldn't escape, re-routing information or turning on power it shouldn't be turned on. So, the security that was required in that environment was as much about integrity and ensuring that everything that is sent is really authenticated, has not been modified maliciously, as it was about keeping data confidential - which is how we often think about encryption.

"Finally, we recently got called in to protect a national airport network where they were running a bunch of high-definition CCTV cameras around the network infrastructure. This was in the arrival's hall as well as all the warehouses and the security parts of the airport. This was being monitored 24/7 and they were very concerned about the security of that data, that video traffic. So they decided to encrypt it and they put on encryption in a little firewall from a well-known provider. It's a great little product but what they found was, as soon as they turned on the encryption, that the overhead that was introduced meant that basically they couldn't monitor the video feeds in real time. They couldn't pan and tilt and zoom into the cameras that they wanted to because the performance overhead was so high that it basically slowed the network to a crawl. So we were able to in there and we put in some high-speed hardware devices that use FPGA technology to encrypt data basically a full line speed with extremely low latency and we were able to demonstrate that they could run that network with encryption to meet their security needs but still have full utility of the information and get all the video access that they wanted to. So a few different examples there of where customers have taken different approaches to meet different requirements.

Thanks, Julian, for your great insight on today's topic, and thank you to everyone who listened to our conversation. If you would like more information on what we've discussed today make sure you head over to senetas.com

ABOUT SENETAS

Senetas, is an Australian public company (ASX:SEN) specialising in cybersecurity. Senetas solutions have been trusted to protect much of the world's most sensitive information for more than 20 years.

A global leader in the protection of data transported across high-speed networks, Senetas provides network independent encryption hardware and virtualised solutions. These share a crypto-agile and quantum resistant cybersecurity platform.

Senetas content security solutions include the most secure file-sharing and collaboration application with 100% data sovereignty control, and proactive anti-malware solutions providing enterprise-wide file security.

Senetas solutions are distributed and supported internationally by Thales, the world's largest security company.

ENCRYPTION SOLUTIONS

Certified by leading independent authorities (Common Criteria, FIPS and NATO), Senetas hardware and virtualised encryption solutions leverage end-to-end encryption and state-of-the-art key management to provide long-term data protection without compromising network performance or user experience.

ANTI-MALWARE SOLUTIONS

Votiro Secure File Gateway leverages patented content disarm and reconstruction (CDR) technology to provide proactive protection against the most persistent cyberattacks, including unknown or zero-day exploits. Votiro is a subsidiary of Senetas and prevents malicious content and malware attacks via email, web and other high-risk file gateways.

COLLABORATION SOLUTIONS

SureDrop is the secure file-sharing and collaboration application with 100% data sovereignty control. It provides the information security and data sovereignty control essential in a world dominated by remote working. SureDrop has the usability of box-type file-sharing and collaboration tools, but with the added benefits of best-in-class encryption security and Microsoft 365, Outlook and Azure integration.

Contact Senetas

Senetas Global
312 Kings Way, South Melbourne, VIC 3205 Australia

T: +61 (0)3 9868 4555 **E:** info@senetas.com

Regional Contacts:

Asia Pacific	**T:** +65 8307 3540	**E:** infoasia@senetas.com
Australia & New Zealand	**T:** +61(03) 9868 4555	**E:** info@senetas.com
Europe, Middle East & Africa	**T:** +44 (0)1256 345 599	**E:** infoemea@senetas.com
The Americas	**T:** +1 949 436 0509	**E:** infousa@senetas.com

SENETAS