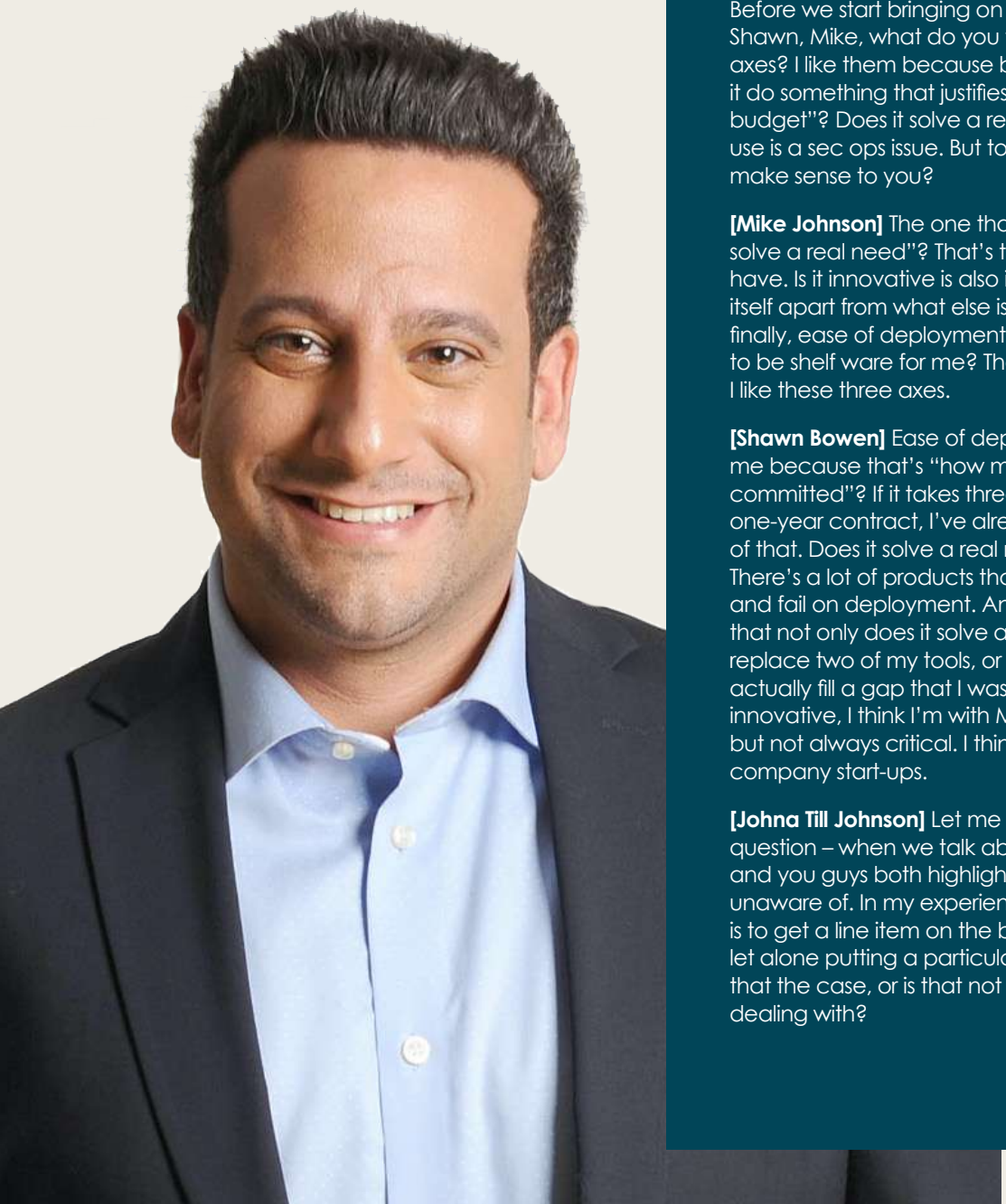
CAPTURE THE CISO

FEATURING VOTIRO CTO, AVIV GRAFI

In a recent pilot for the new podcast, Capture the CISO, representatives from Conveyor, Pantera and Votiro went head-to-head to attempt to capture the attention of guest CISOs. What follows is an extract from that podcast, featuring the presentation content from Votiro founder and CTO, Aviv Grafi.



[Johna Till Johnson] Welcome to Capture the CISO. I'm your host, Johna Till Johnson. We have three companies competing today – Conveyor, Pentera, and Votiro. All are vying for a CISO's interest.

These companies aren't direct competitors, but they are being assessed along three axes – is their solution innovative, is it solving a real need, and how easy is it to deploy? I'd also like to introduce this episode's CISO judges. We have Shawn Bowen, who is the CISO at World Fuel Services, and Mike Johnson, the CISO of Fastly. Our judges have already watched demos of each company's product, so they know what the products do, and they've come armed with questions.

Before we start bringing on the contestants CISOs, Shawn, Mike, what do you think about these three axes? I like them because basically innovation is "does it do something that justifies my putting a line item in my budget"? Does it solve a real need? Ditto. And easy to use is a sec ops issue. But to you guys, do these metrics make sense to you?

[Mike Johnson] The one that I like the most is "does it solve a real need"? That's the first question that I always have. Is it innovative is also interesting. How does it set itself apart from what else is in the industry? And then finally, ease of deployment – is it something that's going to be shelf ware for me? Then I don't want to buy it. So, I like these three axes.

[Shawn Bowen] Ease of deployment is a big one for me because that's "how much am I going to be committed"? If it takes three months to install it on a one-year contract, I've already wasted a quarter of that. Does it solve a real need, I'm with you, Mike. There's a lot of products that are PowerPoint deep and fail on deployment. And so it's one of those things that not only does it solve a real need but is it going to replace two of my tools, or three of my tools, or does it actually fill a gap that I was unaware of? And similarly innovative, I think I'm with Mike on it. It's interesting but not always critical. I think that's more important to company start-ups.

[Johna Till Johnson] Let me ask you just a wild card question – when we talk about "does it fill a need", and you guys both highlighted the gap that I'm unaware of. In my experience, one of my hardest things is to get a line item on the budget for filling that need, let alone putting a particular product in that line item. Is that the case, or is that not a problem that you guys are dealing with?

[Shawn Bowen] For me, I think that's about prepping the battlefield. You start with one quarter. You kind of start to hint that there's a gap. And the problem when you deal with salespeople is they want to sell it the same day that they demoed it for you. The reality is it's going to take you probably a couple quarters to get through the right approval processes.

[Johna Till Johnson] I love that phrase – prepping the battlefield. Mike?

[Mike Johnson] I totally agree with Shawn that you can have a demo or have an evaluation maybe even a year before you do a purchase. So that when you are coming back, you're like, "Oh, I saw this thing in the past. This is a gap that I've identified. I will put this as a line item in my budget." But the other thing that I would say is we're constantly reprioritizing. There might be something that we thought we needed at the beginning of the year, and it was the right thing at that time. But later in the year, it's not as important to us. And something else has come along that, "Oh, this is a gap. This is something that's really significant for me. I'll shuffle budget around so that this now becomes a line item in my budget."

[Johna Till Johnson] Before we kick off the segment, I just want to stress again how brave these companies are for joining us because they're also sponsors. So, a huge thank you to our contestants for supporting our brand-new show.

[Aviv Grafi] I came up with the idea of Votiro when I was at Pinterest, and I found that the easiest way to hack into an organisation was still sending a malicious document. And I thought "what would be the best way to solve that problem"?

[Johna Till Johnson] That was Aviv Grafi, founder and CTO of Votiro. Thanks for joining us.

[Aviv Grafi] Thank you for having me here.

[Johna Till Johnson] Aviv, go ahead and give us a quick 30-second summary of what Votiro does.

[Aviv Grafi] Votiro's API proactively disarms content of known and unknown threats at scale that other security solutions miss without adding any friction, without blocking files, and without interrupting the users.

Votiro reduced the work for IT and security teams, reducing the risk while enabling seamless and instant flow of safe content and data into the organisation. We do that by applying content disarm and reconstruction technology, which actually turned the problem on its head. And instead of looking for bad stuff, we always deliver good, known content.

[Johna Till Johnson] So, is it fair to say that you're constantly filtering content to look for stuff which is not good because you're using the good stuff as the whitelist, and if you discover something that needs to be addressed, you're seamlessly behind the scenes addressing and remediating it?

[Aviv Grafi] So, actually we know what the good parts of the documents are, let's say the content, the text paragraph, and things that really matter for productivity. And by delivering only the good content we're just keeping behind all the unknown maybe malicious, maybe not. So, we're not in the game of trying to guess whether this is bad or not. We're just allowing the good content. And in that way, we're just enabling the business productivity where the users just don't care whether this file is malicious or not because they can just open it and work with it.

[Johna Till Johnson] But the key thing here is continuous content filtering.

[Aviv Grafi] Yeah, so we continue to filter the good parts and delivering that, correct.

[Mike Johnson] I really liked the approach. The whole idea of, "Oh, we're not going to try and find badness because that's an always changing environment." So, I like the idea of "We know what's good." A few things I'm curious about. One is… So, I'm a Gmail shop. We use Gmail. I'm trying to understand how this is better than like the built-in preview of Gmail. If I just have an attachment come in via Gmail, I click on it. I get a preview. Nothing is downloaded locally. So, how do you compare against that?

[Aviv Grafi] Yeah, so the preview is just to get a dumb version of the documents. So, usually if you're talking about Word documents, if you're a legal firm, you need to see the changes that are tracked. You need to see the features that's actually in those very sophisticated file formats. So, the preview, maybe that's nice. But if you really want to be productive and need to do your job, you need to see the entire file on your desktop.

[Mike Johnson] So, again, getting the fat document. How are you dealing with Excel documents that actually have important macros? Usually these products just discard all macros, but I've now received a spreadsheet that's utterly useless because the macros are gone. How do you handle macros in this world?

[Aviv Grafi] Yeah, so you're correct, some of the solutions are dropping the macros all together. But we understood that for productivity a lot of financial organisations…not just financial…they need to work with macro enabled documents. So, we enabled a CDR approach that used machine learning in order to understand that this is a benign macro – this is a legitimate macro. So, we know how to profile those good macros. And in that way, we know that this is good, and we're allowing the macro to go in as opposed to some suspicious macro that we may want to drop or may want to quarantine. Yeah.

[**Mike Johnson]** I'm Mac shop as well. How does your product help me as a Mac shop versus, again, the traditional Windows world that everyone has all sorts of file-based viruses to worry about? So, for those in the Mac world, how does your product help?

[Aviv Grafi] Votiro's technology is an operating system and end point agnostic because we do that on the gateway level, and we focus on the file format. We focus on the specification of the documents and the content, and this has nothing to do with the end point, nor the application that actually opened that file. It can be a mobile device. It can be a Mac. It can be a Linux operations system. It doesn't really matter. We focus on the file itself, on the content itself. And that's why we are agnostic to any endpoint feature.

[Shawn Bowen] We all love security. You're talking to security people. I want this applied to everything. But how absolutely annoyed are the users with this process? Because I understand a financial company or a defence company or someone that's used to the security life of having to badge in 35 times just to get to the bathroom, etc., and passwords everywhere. But for most companies, this seems like we're going to tick off a lot of users. So, how are we kind of balancing that, or what's the feedback from users living through this?

[Aviv Grafi] Votiro solution is actually seamless and transparent to users because we're delivering the exact same file format, exact same features, exact same user experience. In fact, the user doesn't really know that Votiro were there, and we processed those documents. The way that we're doing that is that we're the file format experts. We know how to replicate those documents in the way that we preserve all features. So, from the end user point of view, it's actually way better than the other traditional solutions that might block or might quarantine their documents or emails that they now need to call the help desk. We're always delivering the version that they can work with, and they can be productive. So, from their point of view, they actually don't know that Votiro is there.

[Shawn Bowen] Mike kind of touched on one of the questions about how you're not destroying the documents, but what about the history or the metadata that's following those files that sometimes is important. If you're recreating the document, how are we translating that over to the document to keep the history and some of the underlying content that may be important for tracking purposes?

[Aviv Grafi] We're not flattening the document. We're allowing all the history to be kept, to be moved to the delivered content, delivered piece of file. And actually we're moving all the metadata like the author's name, the properties of the document. Anything that really the users might look for including the history. The history, that's the structured data that we know how to process and how to recreate. So, the user actually can work with tracked changes, all those features that you actually mentioned.

[Shawn Bowen] Is that not corrupting the integrity from a forensics standpoint? If you're able to recreate a file with essentially a fake history. I guess I have a lot of hmm about that. Just kind of thinking through that. Like if you're recreating a file, but you're traveling all that over, how does that stand up?

[Aviv Grafi] So, the way that we're doing that, we keep for a retention period the original document. So that if you need the original for any reason, we keep that for weeks, or months, or years – depends on your configuration. So, we can always access the original if you need it for any purpose, including legal purposes.

[Johna Till Johnson] Are you able to run this on backups? So, if I have for example backed up all of my content, but I have a sneaking suspicion that I may have backed up some ransomware, is that a potential use case, or no?

[Aviv Grafi] Yes. We see more and more organisations where they're moving their backup or actually their old file service to the Cloud, and they now want to retain everything on S3 buckets. So, we have our product connected to their AWS S3 buckets. So, anything that now moves to the Cloud either from the historical backup or new from any client facing application goes through Votiro, and we're doing the same process for terabytes of data that move to the Cloud or goes through that application.

[Johna Till Johnson] That's actually a very, very interesting use case I want to highlight because most people don't think about the need for constantly filtering content that is backed up because ransomware attackers have now learned to implant ransomware in backed up content.

[Shawn Bowen] In your demo, you walk through obviously a simulation. But if a file that is like business correct – it's got good necessary data – but has some malicious content in it, are we still able to maintain some of that integrity and help kind of do forensic analysis to look at where that may have happened in the process? I'm thinking a valid file being sent between a couple of employees, and somewhere along the line it gets some sort of malware ingested into it through whatever method. But are we able to kind of start to use this as an incident response capability, or is this just purely end user protection?

[Aviv Grafi] Actually Votiro solution can integrate with the threat intelligence solutions that you might have already in your organisation. So, we can either share the data on the original structure of the documents, so to get some hints and deliver those hints to threat intelligence. This is one. And on top of that, we have a process that we call retrospective scanning. We send those files a week after they've been received to a traditional detection solution that maybe they can find something in it. So, after the fact, you go, "Look, a week ago a malicious file…someone tried to hack me. Don't worry. We're safe, but you should now know that this is the artifact that was malicious and infected."

[Johna Till Johnson] What do our CISOs think? Mike, Shawn, we've come to the point of the show where it's time to hear your final thoughts before you give us the scores. The contestants have all dropped off, so we can be honest here. As a reminder, these companies are being judged on innovation, ease of deployment, and solving a real need.

[Mike Johnson] I like the way that Votiro is going about solving the problem. I asked about macros because I'm so used to these kinds of solutions just removing macros and saying, "Hey, we've solved your problem." And it doesn't. It renders the files useless in most cases. I like the approach of "we know what's good", and we're going to only copy that over.

One of the things we didn't talk about in the interview, but they mentioned in their video is they handle password protected files. The workflow there is actually reasonable. I thought they solved that. Traditional file scrubbers just completely delete the file, "This is encrypted. We can't do anything with it, so therefore you can't have it," but they recognise there's a problem and approach that. So, I think this is one, there's still the question of how many companies really run this much on attachments that it's that important to them. But it's solving an old problem in a new way, which I give them a lot of credit for.

[Shawn Bowen] Votiro, I think is, again as Mike articulated… this has been around for a while. We have host-based protection that will catch this file when you open it up. We even have defenders and other products that are embedded into a file when you open the file. Sometimes they'll say, "Hold on. It's read only while we're scanning." And there is some existing technology around this space in defending us. I am concerned… I know that the answer was "it's relatively real time", but I could see… In their demo it appeared you had to open up a PDF, and then it translated back to a Word document. It just seemed… I could see some users being highly annoyed. And depending on the industry you're in, you may or may not have users that are comfortable with that level of security. And so I think it's a solid product for those sectors that security is on the forefront.

Final Scores

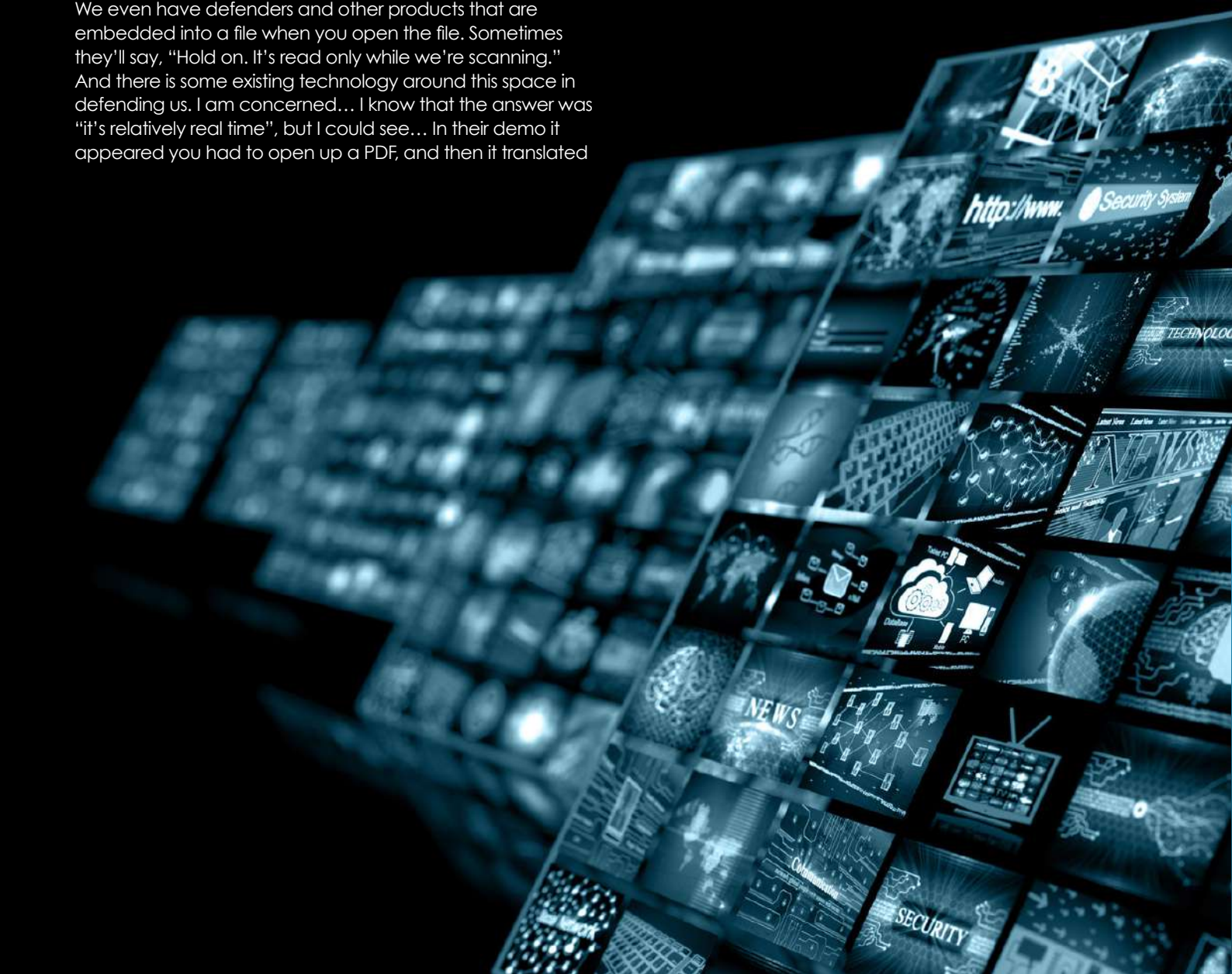
[Johna Till Johnson] Both of you made some excellent points. And with that, now is the time for us to give us your scores. Mike, can you give us your total scores for each of the companies?

[Mike Johnson] For Conveyor, 21 points. For Pentera, 17 points. For Votiro, 20 points.

[Johna Till Johnson] Okay, great. Shawn, can you give us your scores for each of these companies?

[Shawn Bowen] Conveyor, 15 points. Pentera, 18 points. Votiro, also 18 points.

[Johna Till Johnson] What that gives us is a total score for Conveyor of 36, for Pentera 35, 38 for Votiro, which makes Votiro our winner. But wow, these are really, really close scores. Votiro will be joining us for our live finale on June 17th to compete against the other first round winners.



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