VOTIRO CLOUD

BEST IN CLASS PROTECTION AGAINST RANSOMWARE, MALWARE AND UNDISCLOSED ATTACKS FOR THE ENERGY SECTOR

VOTIRO

“We needed a robust solution that was effective against all types of malware, without impacting on systems performance or user experience.”

400+ customers worldwide

SONY SAMSUNG Fuji Electric MOTOROLA SIEMENS NEC NTT DATA TOKYO STOCK EXCHANGE GROUP

MITIGATING THE THREATS OF MALICIOUS CONTENT

CYBERSECURITY LANDSCAPE

As critical infrastructure and utilities companies (such as energy generation and distribution) embrace digital transformation, they come under increased threat of cyber-attack. The most damaging attacks are those that target critical assets and control systems.

Catastrophic ransomware and other malware attacks may be launched by sophisticated cyber-gangs, rogue states or organised crime syndicates, all of whom seek to infiltrate the energy sectors' IT systems through malicious code embedded in files used in daily business activities.

CUSTOMER PROFILE

Our client is a globally recognised provider of products and services to the energy generation and distribution market. With over 400,000 product lines, it plays an essential role in the world's critical national energy infrastructure.

- **20,000+** employees
- **400,000+** products
- Offices in over **100** countries
- Annual revenues over **$8 billion**

DATA SECURITY CHALLENGE

In an organisation of this size, tens of thousands of emails, attachments and files are sent or shared every day.

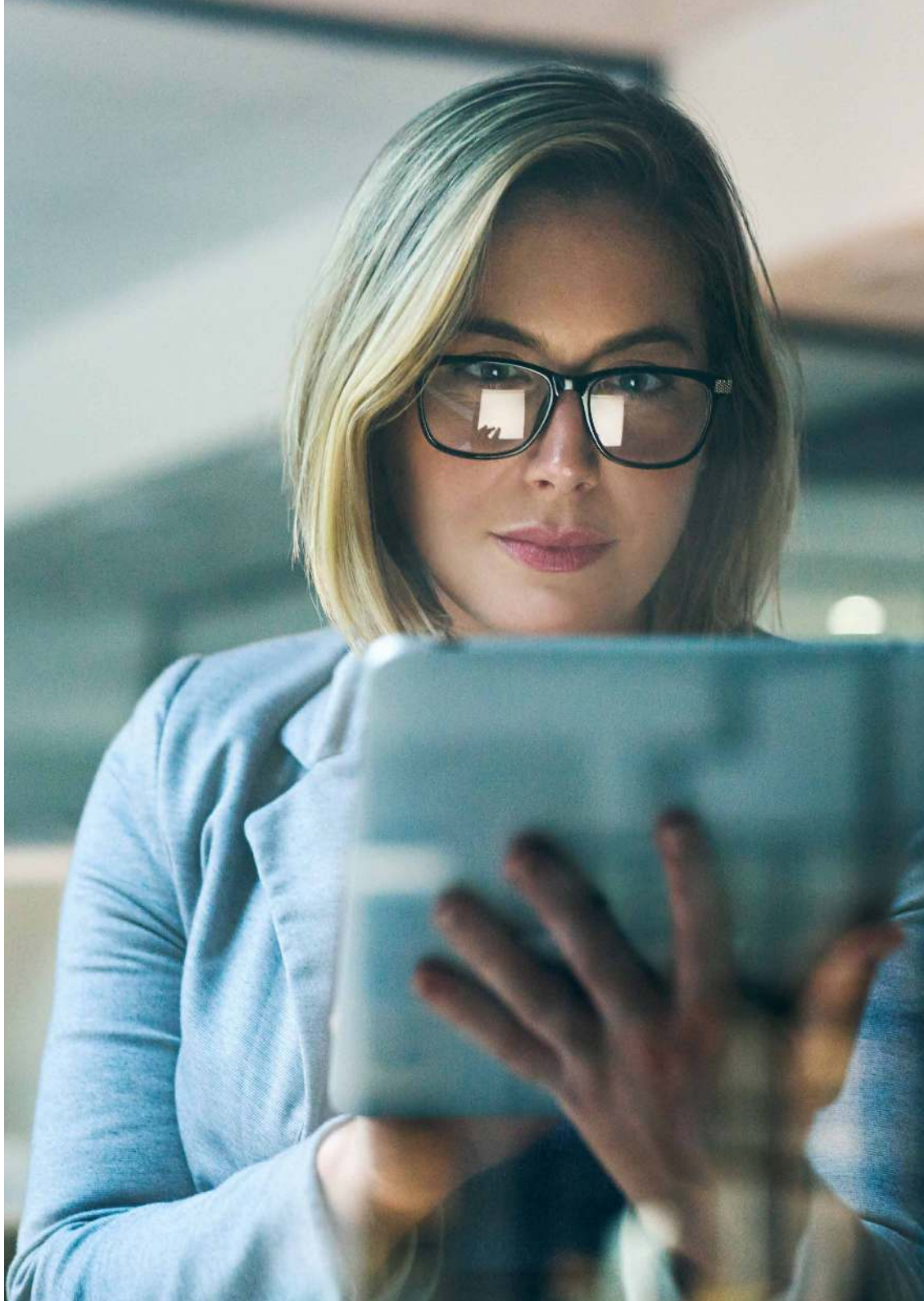
The scale of this exchange is magnified when you consider the size and complexity of the supply chain required to support a multinational organisation, and the diverse nature of its customer base.

MS Office files, video clips, PDFs, rich-text documents, images and other file types represent a potential threat to the organisation's internal systems' integrity.

These files are ideal vehicles in which to conceal malicious code, including malware, ransomware, adware and spyware.

In 2020, the average cost of a data breach in the energy sector rose to $6.39million. The impact of the Colonial Pipeline attack in December 2020 serves as a reminder of what happens when cybersecurity is not up to the challenge.

File-sharing is an essential part of business as usual for our client. With documents exchanged via email, flash drives, FTP and cloud-based collaboration platforms, the company was also seeking to exert a degree of control over user behaviour and minimise the risk of "infection".



EVALUATING THE ALTERNATIVES

Effective prevention against malicious embedded code requires more than conventional file sanitisation.

An evaluation of cybersecurity products highlighted the need for effective security against unknown, or zero-day attacks, as well as previously disclosed threats.

Our client also required a solution that could manage a high volume of files per day, without disrupting systems performance and users' work.

Sandboxing, anti-virus and other legacy prevention technologies were not fit for purpose. Reliant as they are on threats being previously known, they do not provide protection against signature-less, zero-day or undisclosed attacks.

That's why it decided to deploy Votiro Cloud.

POSITIVE SELECTION TECHNOLOGY

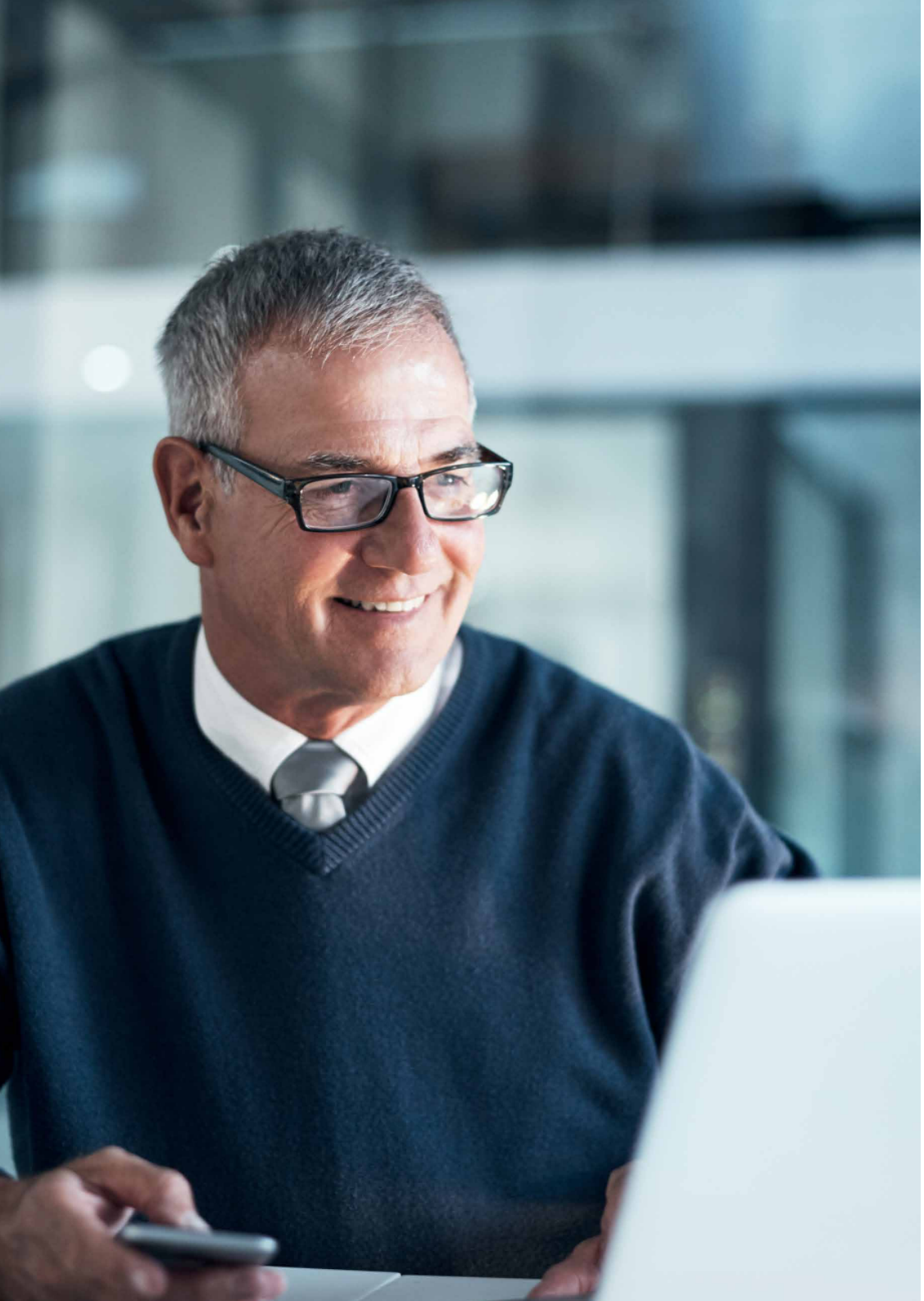
For decades, we've relied on predictive analytics to detect and block malicious files. But predicting threats based on historical data is by definition imperfect. Even 99% accuracy guarantees 100% chance of attack.

To be fully protected we can't just improve our predictions or threat detection. We need an entirely new approach.

Positive Selection

Keeping only what belongs instead of searching for what doesn't.

Unlike detection-based file security solutions that scan for suspicious elements and block some malicious files, Positive Selection singles out only the safe elements of each file, ensuring every file that enters your organisation is 100% safe.



VOTIRO SECURE FILE GATEWAY

Votiro Cloud is an award-winning cybersecurity solution that is used to secure all channels of incoming and intra-organisation data. It can be deployed across email, web, file-sharing, FTP and portable device infrastructure, and across applications using the Votiro API.

Votiro Cloud leverages patented technology to deconstruct, analyse, disarm and reconstruct files. A proactive, signature-less technology, Votiro provides protection against the most advanced and persistent forms of cyber-attack.

Unlike traditional antivirus and sandbox tools, Votiro is equally effective against undisclosed and zero-day attacks as it is against known threats.

Whilst security was a primary concern, it was important that the solution did not have an adverse impact on user experience and systems' performance.

Votiro delivers high-speed, low-latency content security. It is designed to provide frictionless security for large volumes of content moving into and within large organisations.

"We needed a robust solution that was effective against all types of malware, without impacting on systems performance or user experience."

VOTIRO

ABOUT VOTIRO

Established in 2010 by a team of senior cybersecurity experts, Votiro develops and licenses Votiro Cloud, a security solution based on award-winning, patented technology. With the aim of securing organisations throughout their digital transformation, Votiro is committed to allowing the safe and free use of data, with full protection against unknown threats.

Votiro CyberSec is a subsidiary of Senetas Corporation Limited (ASX:SEN)

T: +61 (0)3 9868 4555
E: infoanz@senetas.com
W: www.senetas.com