VOTIRO DISARMER

SAFE AND SECURE: BEST PRACTICE FILE-SHARING FOR THE ENERGY SECTOR

VOTiRO
SECURED

“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 FILE 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.

Bad actors can include cyber-terrorists, rogue states and 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.

According to Accenture (2019) the average cost of a cyber-attack has risen to $2.4million. Most of this impact (54%) is felt in terms of lost productivity, with negative user experience representing the bulk of what remains (43%).

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.

Sandbox, antivirus and other prevention technologies were found to not provide enough assurance against emerging threats; nor could they meet our client's file volume and real-time performance needs.

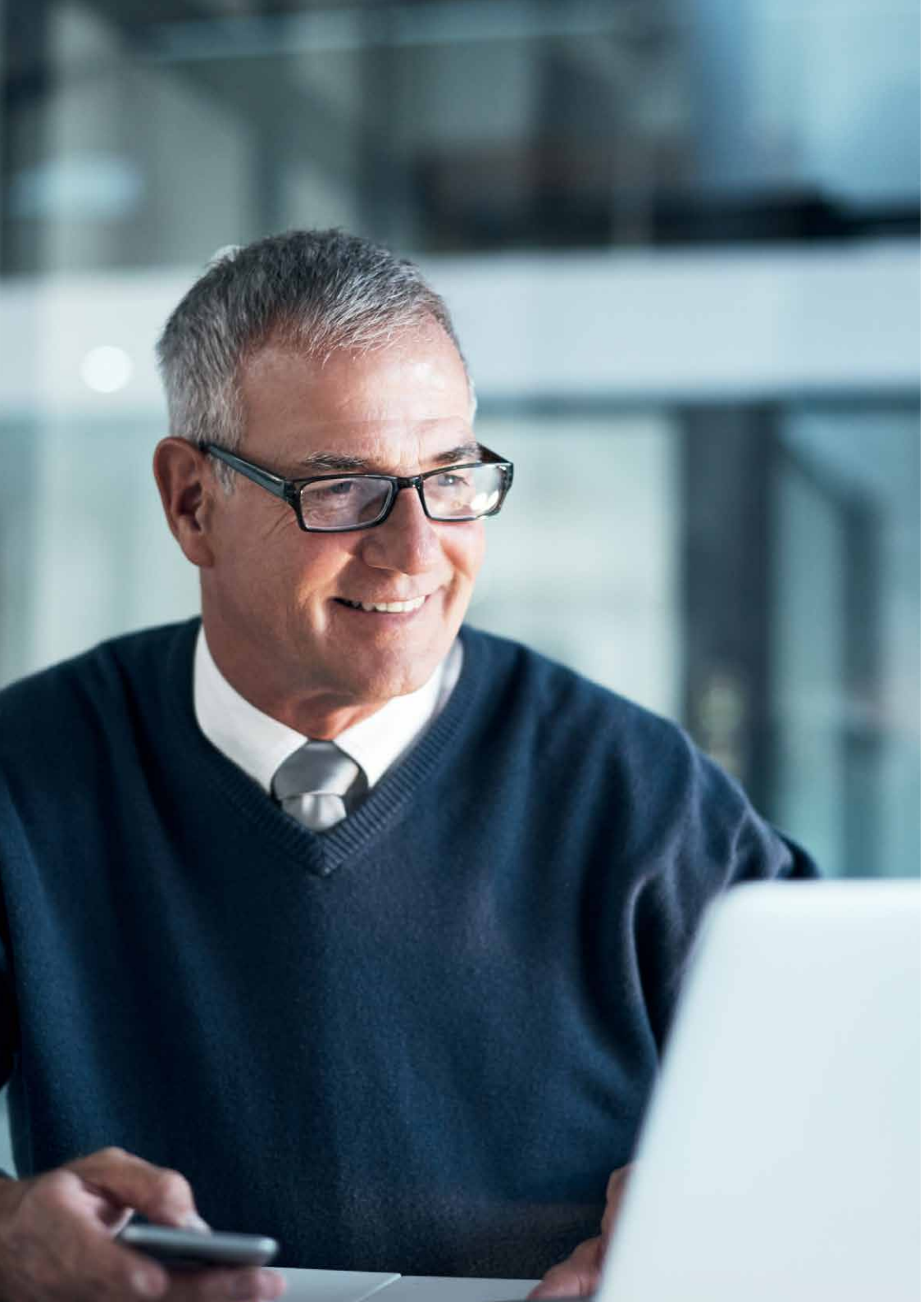
That's why it decided to deploy Votiro Disarmer.

CONTENT DISARM AND RECONSTRUCTION (CDR)

CDR is an advanced cyber-threat prevention technology that is not dependent upon successful detection of malicious code (malware).

CDR assumes every file is malicious. It deconstructs all content before analysing and removing any suspicious code or known threats. Once disinfected, the file is reconstructed, ensuring 100% usability is retained.

CDR technology is highly effective against both known and unknown threats; including zero-day targeted attacks, undetectable malware and obfuscation attacks.



VOTIRO FILE DISARMER

Votiro Disarmer 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 Disarmer API.

Votiro Disarmer leverages patented CDR technology to deconstruct, analyse, disarm and reconstruct files. A proactive, signature-less technology, Votiro Disarmer 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 Disarmer delivers high-speed, low-latency content disarm and reconstruction. 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
SECURED

ABOUT VOTIRO

Established in 2010 by a team of senior cybersecurity experts, Votiro develops and licenses File Disarmer, a security solution based on award-winning, patented Content Disarm & Reconstruction (CDR) 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.

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