VOTIRO DISARMER

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

VOTIRO
SECURED

“It’s the only solution we could trust with certainty. Votiro Disarmer was the only solution that met all our needs.”

400+ customers worldwide

ELIMINATING MALWARE FROM COMMON FILE TYPES

CYBERSECURITY LANDSCAPE

Financial services organisations are consistently in the top three industries targeted by cyber-criminals. Unknowingly, consumers are the most common source of malware, with Microsoft Office files having the highest risk of embedded malicious code.

With the number of malware variants rising every year, all it takes is one successful attack to bring down an entire platform and ruin a reputation.

CUSTOMER PROFILE

Our client is a US-based consumer lending organisation, offering a range of personal loans, car financing and credit card services.

- Over **1 million** borrowers
- **80,000** loans processed annually
- Over **$6 billion** loaned
- **3,000** documents shared daily

DATA SECURITY CHALLENGE

With more than 300 loan applications processed every day, the sheer volume of documents being sent, received and circulated represents a security risk.

Whilst MS Office documents are common, prospective customers also send PDF and image files to support their applications.

The impact of a single successful cyber-attack could be catastrophic.

Microsoft Office files (Word, PowerPoint and Excel) constitute the most prevalent group of file extensions; accounting for 38% of infected files.

Our client was looking for a robust solution that addressed the traditional weaknesses of anti-virus, sandbox and file sanitisation alternatives.

With a dynamic and evolving threat landscape, it was essential that the chosen technology could provide protection against unknown and zero-day attacks.

EVALUATING THE ALTERNATIVES

With such a diverse group of contributors, the chosen solution would need to offer the broadest range of file security; capable of disarming and reconstructing more than simple word documents or PDF files.

Importantly, files would need to be sanitised as they arrived from a variety of channels - via the web, as email attachments and even on physical USB devices.

“A high success rate for disarming and reconstruction was essential, but it was also important to retain all the original functionality of the files. We didn’t want to just end up with a flattened version of the original.”

With more than 3,000 documents being processed daily, it was also important that security didn’t come at the cost of efficiency. Our client was seeking a low-latency solution that would not disrupt day-to-day work flows.

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.

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: info@senetas.com
W: www.senetas.com