

BIDX1 Case Study

Background

LoughTec, one of Ireland's and the UK's leading IT infrastructure specialists, was selected by BidX1 to deliver its secure file upload solution across the company's network. This is used to ensure all sensitive files uploaded are free from malicious malware. This stops any opportunities for malware, zero-day attacks or sensitive data leakage.

BidX1 is Europe's leading digital property investment platform – a platform that connects users across the globe with real estate opportunities in multiple markets and enables them to complete the entire transaction online, using technology developed in Dublin.

Their mission is to combine property expertise with technology to provide unparalleled levels of transparency, analytics and global reach.

Headquartered in Dublin, where their model was first developed, BidX1 currently operates in the UK, Ireland, South Africa, Spain and Cyprus. The Company has sold over 10,000 properties to date, more than €2.5bn-worth of real estate.



The challenge

Cyber security threats continue to increase across the globe, with the risk to financial institutions being particularly prominent. For any business, attacks from malware can have catastrophic consequences, with the threat level only increasing year on year.

Ebenezer Akintunde, Software Delivery Manager at BidX1 managed the process of finding a suitable solution. Here he explains the company's requirements:

"As a rapidly growing business whose expertise is in high-value online transactions, cyber security is always top of mind for us. It is our responsibility to ensure sensitive documents uploaded onto our platform by our customers are stored securely and that these documents are free from malicious software and viruses that could harm our business."

"LoughTec is one of the leading Cyber Security systems providers worldwide and our research highlighted that they provide one of the most advanced file upload malware protection and detection solutions."

BidX1 faced the following challenges and risks around file uploads:

- Web applications account for 43% of security breaches. Users no longer need to install a rogue application to get infected. Even opening what appears to be an invoice, a courier receipt, a mortgage application, or any other productivity file can successfully deliver a malware payload that enables cybercriminals to take over the entire network.
- BidX1 wanted to ensure that all types of files uploaded into their network by customers or employees, including Word, Excel and PDF files, were free from malicious malware.
- In addition to being secure, any solution also needed to be quick to deploy and have a clear user interface.

The LoughTec approach

LoughTec worked in conjunction with their US and EMEA partners OPSWAT to implement BidX1's new file scanning solution, MetaDefender Cloud.

The solution scans all files that are uploaded into critical networks, such as Cloud storage like AWS, Box and Azure. This ensures BidX1 are protected from file borne malware threats that may lie within files, even if they appear innocent.

Ebenezer Akintunde continued, *"At various stages of our business process, we require different documents from external vendors as well as our property buyers and sellers. To ensure these files were malware-free, we were able to implement a malware scanning service built on top of LoughTec's malware detection platform."*

LoughTec's file scanning solution provided to BidX1 uses technologies such as:



Multi-scanning - advanced threat detection and prevention technology that increases detection rates, decreases outbreak detection times and provides resiliency to anti-malware vendor issues. Multi-scanning files with over 35 anti-malware engines helps to deliver enhanced protection from a variety of cyber threats.



Data sanitisation (Content disarm and reconstruction) - an advanced threat prevention technology that does not rely on detection. This assumes all files are malicious and sanitises and rebuilds each file, ensuring full usability with safe content for the user. This technology is highly effective for preventing known and unknown threats, including zero-day targeted attacks and threats that are already equipped with malware evasion technology.



REST API, to ensure a true plug-and-play deployment, takes the burden of managing software infrastructure away from organisations.



Built-in privacy, through private scanning, allows users to submit files to be analysed by OPSWAT, without sharing the file content. After the analysis is completed, files are deleted from OPSWAT servers.

"The partnership and service development process has been extremely smooth due to the brilliant collaboration by the LoughTec team, especially Jonathan Adams who was very informative in explaining and guiding us through the implementation and setup process."

Benefits to BidX1 include:

- The ability to scan over 100 different file types, such as Word, Excel, PowerPoint and PDF.
- Ensures that all files entering their network are free from malicious malware.
- Ease of use, with the ability to scan hundreds of files per minute.
- Fulfils regulatory requirements, such as GDPR and PII.

"This partnership with LoughTec gives us the confidence and assurance that every file system uploaded through our platform is malware and virus free, allowing us to focus on our core business of selling property."