



LANDSBANKINN

CASE STUDY



A division of **LoughTec**

4 Bankmore Business Park,
Omagh, Co. Tyrone, BT79 0BQ

T: +44 (0)28 82 25 2445
E: info@LoughTec.com
W: LoughTec.com

Background

LoughTec, one of the UK and Ireland's leading IT infrastructure specialists, was selected by Landsbankinn to deliver their cybersecurity suite across the Bank's operations. This was used to identify, detect and remediate advanced security threats from data and devices on their enterprise network.

Landsbankinn is a leading Icelandic financial institution. Headquartered in Reykjavík, the Bank offers a full range of financial services and is the market leader in the Icelandic financial service sector.

The challenge

Cyber security threats are continuing to rise, and the risk to financial institutions such as banks is particularly prominent. With this threat in mind, Landsbankinn needed to establish an advanced and robust cyber security solution, that would help form part of the Bank's layered IT security strategy. Any solution would be required to cover their full enterprise network, which covers 800 staff across their 36 branch network and 130,000+ personal and corporate customers.

The LoughTec approach

LoughTec worked in conjunction with their US and EMEA partners OPSWAT to implement the Bank's new cybersecurity suite. The suite provides cutting edge agentless cyber incident detection and response, standard compliance assurance, file integrity monitoring, endpoint vulnerability detection and remediation, asset management, shadow IT discovery and advanced business intelligence.

LoughTec's advanced cyber-security solution protects Landsbankinn from content and device-based threats:

- MetaDefender Internet Content Adaptation Protocol (ICAP) was integrated with the Bank's network appliances to protect against

advanced threats in network traffic and storage devices. Industry-leading multi-scanning, vulnerability scanning and data sanitisation (content disarm and reconstruction (CDR)), vulnerability assessment and data loss prevention (DLP) technologies were also implemented, ensuring users can respond in seconds to the next threat that affects their servers and systems.

- Data sanitisation (CDR) is an advanced threat prevention technology that does not rely on detection. LoughTec's technology 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, including fully undetectable malware (FUD), VMware detection and obfuscation.
- Multi-scanning is an advanced threat detection and prevention technology that increases detection rates, decreases outbreak detection times and provides resiliency to anti-malware vendor issues. LoughTec's US and EMEA partners OPSWAT pioneered the concept of multi-scanning files with over 30 anti-malware engines available, to deliver enhanced protection from a variety of cyber threats. Landsbankinn are now able to utilise this technology for their enterprise network.

Hakon Akerlund, IT Security Manager at Landsbankinn, said, "We at Landsbankinn look forward to working with LoughTec over the next three years. The OPSWAT technology stack has given us an additional layer to our current security and enabled us to give our customers the same experience online as they can have at a branch office. The entire OPSWAT stack was efficient to implement and integrated seamlessly with our current application programming interface (API), without any development requirements."