ACDS
ADVANCED CYBER DEFENCE SYSTEMS

File Guard

Trust no-one. Protect from known and unknown zero-day threats in common business documents.

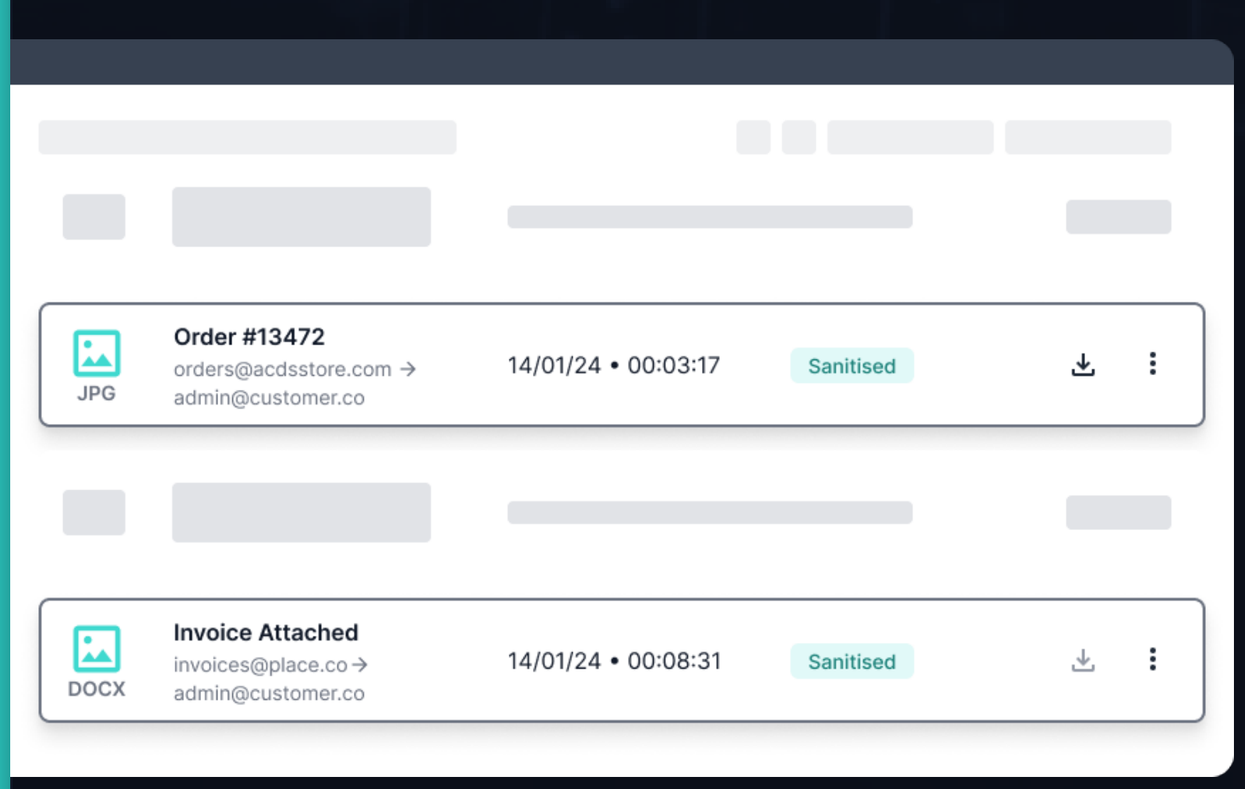
Every day, organisations of all sizes are becoming more in tune with the realisation that malware causes significant losses. Malware comes in many forms and can be continuously altered by cybercriminals to trick traditional security defences. Social engineering techniques, such as phishing and the deployment of ransomware, can damage your brand's image and result in data and financial loss.

These threats are on the rise, and as email is the top attack vector used by cybercriminals, organisations need to prioritise their email security. No matter how files are delivered, we need to approach security differently to manage the risks inherent in files.

Businesses have been approaching security wrong.

Anti-virus scanners are a good first layer of protection; however, they rely on detecting known threats. Therefore, when cybercriminals use new, never-seen-before malware, the anti-virus scanner would regard this as safe, and this leaves your organisation open to attack. ACDS' File Guard is an additional layer that can be added to combat malware sent via email attachments that have not yet been seen, even the most advanced zero-day attacks and exploits.

File Guard assumes all email attachments (PNG, GIF, JPEG, PDF and docx) are a potential threat to the user. Therefore, all active content is removed, and the file is reconstructed into its original file format before it reaches the end-user's inbox.



Receive safe emails in real time.

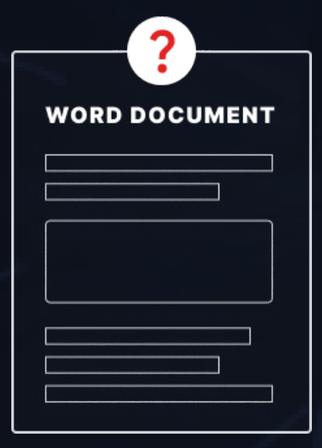
Anti-virus scanners are a good first layer of protection; however, they rely on detecting known threats. Therefore, when cybercriminals use new, never-seen-before malware, the anti-virus scanner would regard this as safe, and this leaves your organisation open to attack. ACDS' File Guard is an additional layer that can be added to combat malware sent via email attachments that have not yet been seen, even the most advanced zero-day attacks and exploits.

File Guard assumes all email attachments (PNG, GIF, JPEG, PDF and docx) are a potential threat to the user. Therefore, all active content is removed, and the file is reconstructed into its original file format before it reaches the end-user's inbox.

Who would use File Guard?

All industries and organisations, big and small, are at risk of becoming victims of an email-attachment-based phishing attack. If your organisation receives email attachments, internally or externally, there is a risk of malware being hidden in the seemingly benign files. File Guard can be deployed across specific user groups, such as the claims department, which receive a large volume of email attachments, or across the whole organisation.

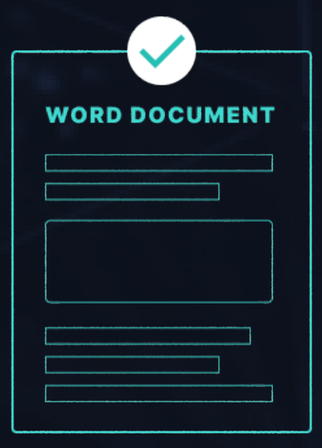
File Guard removes malware from documents before they arrive, providing end-users with the confidence to open and click on attachments. Crucially, it frees up the IT and security teams from the day-to-day chores of handling quarantined files and false positives.



A file arrives.

Text and objects are stripped out & scanned.

Active content is stripped out and converted, removing any malicious code.



The clean file is reconstructed.

Key Features:

- File Guard intercepts email attachments (PNG, GIF, JPEG, PDF and DOCX) by flattening the file, stripping out the active content, including any malicious code and reconstructing it into its original format in real-time.
- A control panel that allows the admin to download original file if required (at own risk).
- Security check any document manually via the control panel, regardless of its delivery method.

Benefits:

- Can be used in conjunction with virus scanners to help mitigate the threat of malware.
- The zero trust approach to email attachments provides a higher degree of trust to customers and suppliers.
- Visual parity for the user between the new and original file.
- Works with MS Office 365 & Google Workspace for easy implementation with your company email servers.
- Frees up the IT and security team from day-to-day chores of handling quarantined files or potential breach alerts.

ACDS
ADVANCED CYBER DEFENCE SYSTEMS