GLASSWALL

FileTrust™ ATP for Email

Next generation Advanced Threat Protection.
Sub-second elimination of cyber attacks from malicious files and documents with no disruption to users.

Your Biggest Threat

With over 66% of attacks launched by attachments in email, one of the biggest security challenges today is that current technologies often miss sophisticated or unknown malware delivered to organizations through malicious files. Despite best protection efforts by enterprises using traditional technologies like anti-malware and anti-spam, Glasswall still finds:

- One in 5,000 emails contains malware
- One in 15,000 attachments are malware
- 65% of the malware that Glasswall identifies and removes is unknown to all the major AV vendors
- The remaining 35% is generally known to the AV vendors but is still evading their traditional pattern based and sandboxing protection

Advanced Protection

In less than a second, Glasswall's unique technology disarms any file-based threat, allowing users to operate without disruption and senior management to avoid headline-grabbing PR disasters and regulatory fines.

How It Works

Traditional security technologies are failing because they attempt to identify 'known bad' malware through signatures and pattern detection. Glasswall remediates file structure and sanitizes risky objects such as Macros and JavaScript, regenerating a file that conforms to a standard of 'known good'. Secure and trusted files reach users every time.

Understand Risks & Value

Gain insight into the threats unique to your organization

- Understand product value through intuitive reports
- Monitor threats specifically aimed at your users or business groups
- Tangible ROI to deliver the value message to senior management
- Cloud-based service minimizes costs with immediate results
- Scheduled reporting provides continued insight and visibility

Product Features

- Disarms all known or unknown malware from entering the organization while allowing in clean and safe files
- Granular policy controls to sanitize known file based risks such as malicious URLs, Macro, JavaScript and encrypted embedded payloads
- Simple Administrator UI allows configuration of robust policy uniquely tailored to the organization's risk appetite
- Requires no updates or signatures to achieve complete protection
- File Preview feature keeps severely malformed files at a distance, while providing users real-time access to document content
- Transparent user experience enhances business continuity
- Granular reporting provides at-a-glance insight to deep forensics
- Tangible ROI continually proves product value powered by Threat Intelligence
- Supports all major file types such as .pdf, Microsoft Office files and images

//

"By bringing files into a standard of 'known good', Glasswall completely eliminates the risk of file-based malware and that is critical in helping me mitigate my corporate risk. Since I installed the product over two years ago, I have had zero malware by email and my users don't even know it's there."

Stan Black, CSO, Citrix

Simple to Evaluate and Deploy

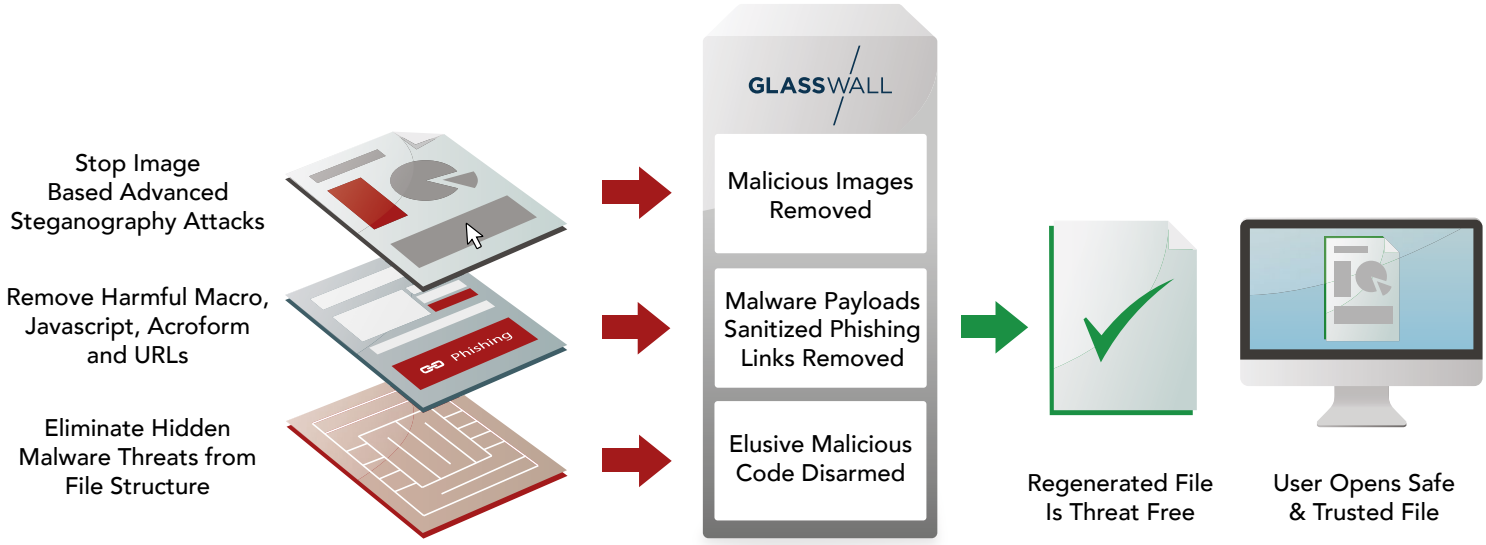
Our experienced team of engineers will guide you through an end-to-end process to assist with business justification.

- Tangible metrics in clear and concise reports
- Daily and weekly digests
- Full evaluation summary

Flexible evaluation options adapt to any infrastructure and range from zero touch to inline performance testing, providing full insights into product value.

Ease of Ownership

- Reduce risk of business disruption through email attachment cyber attacks
- Reduce drain on resources through minimal product configuration and helpdesk impact
- Leverage existing physical servers, virtualized infrastructure or deploy within Private Cloud
- Manageable and predictable costs with flexible user-based subscription
- Dashboard for Administrators allows easy management of policy, user workflows and operational monitoring



Deployment Options

PRIVATE CLOUD

- Integration with O365
- Leverage Azure or AWS platforms
- Scalable and flexible

ON PREMISES

- Seamlessly integrates into Microsoft environments
- Resource efficient reduces operating costs
- Secure administration via Web based console

Deployment Requirements

GATEWAY SERVER
Minimum of 2 Core Microsoft 2012 R2 Server, with IIS 8 enabled, with 2GB RAM

MANAGEMENT SERVER
Minimum of 2 Core Microsoft 2012 R2 Server, with IIS 8 enabled, with 2GB RAM

DATABASE
Minimum of 2 Core Microsoft 2012 R2 Server, with 3.5GB RAM, and SQL Servers

QUESTIONS? CONTACT US

UK: +44 (0) 203 814 3900
USA: +1 (866) 823 6652

info@glasswallsolutions.com
glasswallsolutions.com