GLASSWALL

NAIS
Native American Industrial Solutions LLC

GSA IT Schedule 70
Contract 47QTCA19D004X

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 AV, Sandboxes and Firewalls, Glasswall still finds:

- One in 6000 files are still malicious despite being filtered through several layers of security
- 84% of malware has no AV signature available, protection lag from other vendors can take days or weeks
- Over 90% of malicious Office documents contain a Macro, with DDE appearing in 20% of Excel files

Advanced Protection

In less than a second, Glasswall's unique technology disarms any file-based threat, enabling the workforce 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 known and unknown malware before it enters the organisation, delivering only 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 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
- Glasswall FileTrust™ Threat Intelligence proves product value and powers continuous, tangible ROI
- 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

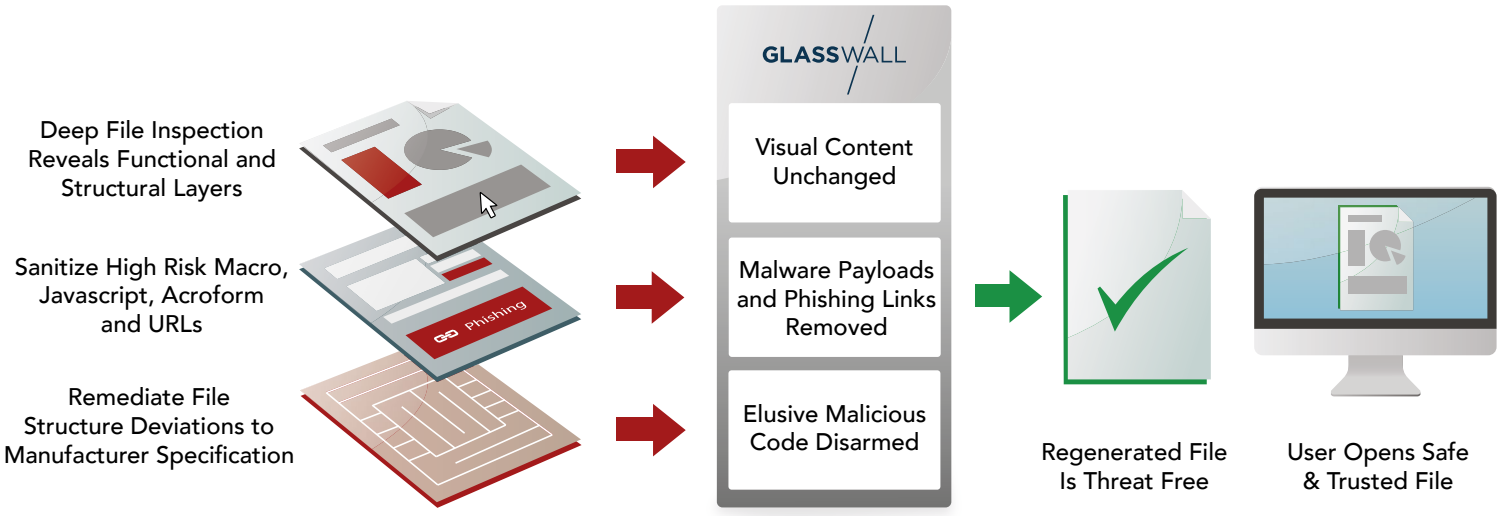
Our experienced team of engineers will guide you through an end-to-end process to assist with business justification.

- Complimentary 30-day Risk Assessment
- 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 insight 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

Cloud Hosted Service

- Resilient and scalable protection
- Secure Administration Portal
- Integrated Threat Intelligence Dashboards

Software Solutions

- Supports on premise physical/virtual platforms
- Option to self-hosted on Azure/AWS
- Seamlessly deploys within Microsoft environments

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

NAIS
NATIVE AMERICAN INDUSTRIAL SOLUTIONS LLC

QUESTIONS? CONTACT US

USA: +1 (512) 653-1744

admin@nais-llc.com

GSA IT Schedule 70
Contract 47QTCA19D004X