CITRIX

Customer Case Study / Glasswall FileTrust™ ATP for Email

GLASSWALL

CITRIX'S CHALLENGE

Citrix provides industry-leading technology to a global, growing customer base, but this success creates a rich target for hackers. Like many global enterprises, the organization faces the challenge of preventing malware sent in malicious email attachments. To combat these threats, Citrix deploys best-of-breed security technologies and services, conducts continuous user training, and enforces robust policies in tune with the risk appetite of the business.

Citrix's security operations are led by Stan Black, 2018 Cyber Security Professional of the Year. Black found that while his current security stack immediately filtered off approximately 85% all emails, of those that were permitted to pass, malicious files were still evading even the most robust detection-based products. His goal was to reduce his vulnerability to file-based threats to zero without any disruption to user's work flow.

Black recognized that dealing with evasive malware at the desktop would not be optimal for Citrix resources or workforce productivity, so another layer of defense was sought at the gateway, one that would bring the fight back to the perimeter where it's more efficient to manage.

In considering Glasswall FileTrust™ ATP for Email, a number of key objectives were set:

- Provide demonstrable and significant additional protection over existing technologies
- Have no impact on the user experience and operational workflows
- Show significant ROI based on threats avoided and business costs saved

> **"The entire security industry is used to buying products that find problems, not products that solve problems. It's almost non-existent, to find a technology like Glasswall that actually eliminates a threat vector. It is absolutely critical in mitigating my corporate risk."**
>
> ***- Stan Black, CSO Citrix***

THE GLASSWALL METHODOLOGY

Glasswall FileTrust™ ATP for Email works with the existing secure email gateway suite as a last line of defense, disarming advanced and unknown malware threats in less than a second at the gateway. It does this using its patent-protected d-FIRST™ methodology, a three-part process applying **d**eep-**F**ile **I**nspection, **R**emediation and **S**anitization **T**echnology.

- **deep-File Inspection:** Incoming files are compared to published manufacturer standards and inspected for any deviations. 80% of document-based threats are hidden deep in the file structure, and these are flagged as deviations from the standard during inspection.
- **Remediation:** Once inspected, the file is fully rebuilt by Glasswall's core engine, remediating all deviations, bringing the file structure into line with the published specification with any hidden threats removed during this process.
- **Sanitization:** Distinct from structural threats, approximately 20% of malware can be triggered by document features and functions, such as Macros. Glasswall sanitizes these risks by policy, reflecting the operational needs and risk appetite of an organization.

These processes combine to create a clean, safe version of the original file in its original format, fully aligned to corporate policy, and presented to the user in real time as a perfect and useable document.

For more information, contact sales@glasswallsolutions.com

CITRIX

Customer Case Study / Glasswall FileTrust™ ATP for Email

GLASSWALL

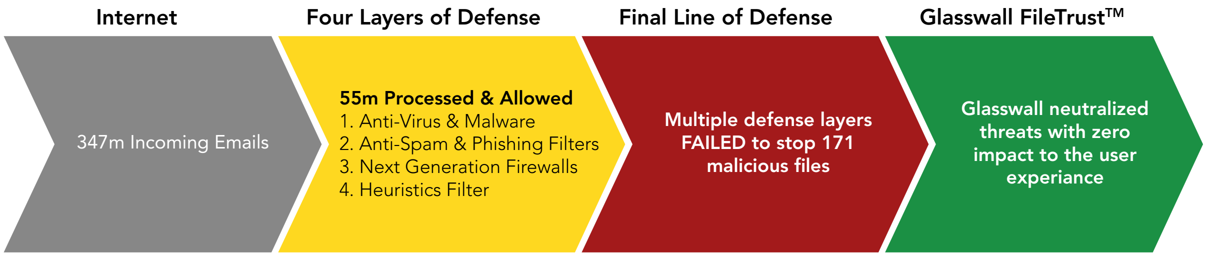
UNPARALLELED RESULTS

Since the product went live in 2016, Citrix has experienced zero malware by email while the company's employees don't even know it's there. On average, Glasswall's Filetrust™ ATP for Email prevents at least one malicious file per day from entering the organization, each with the potential to impact thousands of users and which could lead to significant financial, operational and reputational damage to the business.

Key product advantages for Citrix:

/ Zero malware via email for over two years
/ Zero visibility, distraction or disruption to users
/ Detailed Threat Intelligence on neutralized threats
/ $1.4M average monthly saving from avoiding file-based malware

By the numbers: How Glasswall FileTrust™ ATP for Email protects Citrix


Internet
Four Layers of Defense
Final Line of Defense
Glasswall FileTrust™
347m Incoming Emails
55m Processed & Allowed
1. Anti-Virus & Malware
2. Anti-Spam & Phishing Filters
3. Next Generation Firewalls
4. Heuristics Filter
Multiple defense layers FAILED to stop 171 malicious files
Glasswall neutralized threats with zero impact to the user experiance

Threats from unstructured productivity files including MS Office, pdf, graphics, etc. constantly evolve.

The Body of email still requires filtering.

Security technology is unable to protect against past and present threats

Approximately one file per day eludes traditional security technology.

"My security team are both experienced and skeptical, and carefully review the merits of emerging technologies. I asked them to trust me and we've had no malware by email since deploying Glasswall"

"Email attachments that would take days for other security vendors to identify as malicious were disarmed in real time with the workforce blissfully unaware we had even deployed the technology"

"Glasswall's weekly reports are a vital part of my data feed, they tell me that my company has been protected, and that the product is delivering continuous value"

THE ADDED VALUE OF GLASSWALL FILETRUST™ THREAT INTELLIGENCE

Glasswall's Threat Intelligence Service delivers proof of value on a weekly basis to Citrix by providing reports on malware neutralized by Glasswall, with comparative timelines for how long it took for anti-virus products to develop signatures for those threats. Detailed information about each file can be leveraged to shape policy, further enhancing the security posture of the business, while maintaining optimal business operations.

Their reports show that in many cases, Glasswall neutralizes threats aimed at Citrix over seven days before detection-based products have signatures for the malware. In some cases, the delay in detection is well over 30 days.

For more information, contact sales@glasswallsolutions.com