

Fortinet and Glasswall Solutions

Comprehensive, Integrated, and Automated Solution for Protection Against Known and Unknown Content in Common Business Documents, All at the Speed of the Internet

Executive Summary

Fortinet and Glasswall Solutions have partnered to deliver an industry-leading security solution to provide real-time malicious document threat protection, together with unparalleled network security protection provided by the FortiGate next-generation enterprise firewall and the Fortinet Security Fabric.

Customer Challenges

Business processes increasingly involve file-sharing platforms and are allowing underprotected third parties to upload files to websites and public cloud storage services. Historically, legacy antivirus protection is limited by signature updates (at best one step behind) and sandboxing technologies that are often limited by the time to process files (taking several minutes) in a “real-time” user-driven process. Both approaches are often not optimal, due to the following reasons:

- Antivirus protection is limited by reaction-based signature updates, which is ineffective in unknown malware scenarios.
- Traditional sandboxing technologies could potentially be hindered by file processing delays.

Joint Solution

Fortinet and Glasswall Solutions have partnered to deliver an industry-leading security solution to address these challenges. The integration of the Glasswall Rebuild and the FortiGate next-generation enterprise firewall platform, enabled through the Fabric-Ready Program in the Fortinet Open Fabric Ecosystem, delivers real-time leading malicious document threat protection.

Joint Solution Components

The Glasswall Rebuild ICAP server safely and quickly rebuilds commonly exploited business files (Office, PDF, Images). Leveraging the Glasswall patented, battle-hardened Content Disarm and Reconstruction (CDR) technology, the solution can validate/fix file binary structures and sanitize/remove active content to protect against known and unknown (no signature available) malicious files. Rather than trying to detect dangerous content, Glasswall regenerates all files to a safe standard of “known good,” enforcing the format’s structural specification and eradicating high-risk active content. Glasswall is a proactive solution. At no point is a signature (which is basically an understanding of bad behavior or threat) needed.

Fortinet FortiGate next-generation firewalls (NGFWs) enable security-driven networking and consolidate industry-leading security capabilities such as intrusion prevention system (IPS), web filtering, secure sockets layer (SSL) inspection, and automated threat protection. FortiGate firewalls scan and filter network traffic to protect an organization from external threats. The inspections occur at an unparalleled speed, scale, and performance without degrading user experience or creating costly downtime.

Joint Solution Components

- Fortinet FortiGate Next-Generation Firewall
- Glasswall Rebuild ICAP

Joint Solution Benefits

- Fast, robust protection against malicious document threats, including against unknown malware
- Protect previously missed malicious business document entry points involving public cloud storage services
- Use the Glasswall Rebuild ICAP server as a filter for your DMZ web/file upload servers
- Leverage the award-winning FortiGate enterprise firewall and the Fortinet Security Fabric for unparalleled network security protection

FORTINET.

Fabric-Ready

Joint Solution Integrations

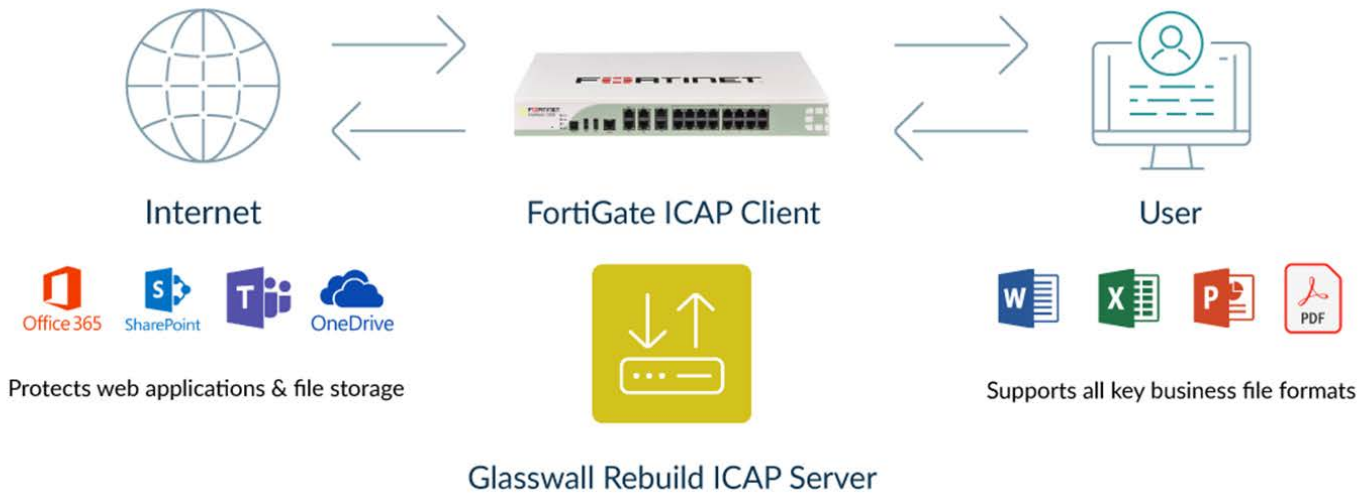


Figure 1: Enable the FortiGate ICAP client and direct traffic to the Glasswall Rebuild ICAP server platform.

Joint Use Case

FortiGate integration with the Glasswall Rebuild ICAP server offers a reliable solution that ensures files imported into your organization are regenerated to a clean, safe standard of “known good.” Leveraging this partnership provides a rapid pathway to clean files with little overhead, allowing you to focus on building business processes free from risk.

About Glasswall Solutions

Glasswall Solutions is a UK-based file-regeneration and analytics company and a leader in the field of Content Disarm and Reconstruction (CDR). Glasswall has clients across business, government, defense and the “Five Eyes” intelligence agencies. They rely on us to remove the risk of sharing files and documents. With our patented methodology we create safe, clean, and visually identical files to mitigate the risk posed by malicious documents. Rather than trying to detect dangerous content, Glasswall regenerates all files to a safe standard of “known good,” enforcing the format’s structural specification and eradicating high-risk active content. Glasswall is a proactive solution. Learn more at <https://glasswallsolutions.com>.