Forcepoint

Gateway eXtension

Protects web users from known, zero-day, and unknown content threats, guaranteed.

Existing perimeter web defenses (web gateways and firewalls) are failing to cope with the onslaught of known, unknown, and zero-day threats concealed in business documents and images. Extend the capability of your perimeter web defense using the Forcepoint Gateway eXtension (GX) to completely remove these threats, guaranteed.

Key Benefits

- On-Prem Appliance
- Simple Setup
- Malware Removal
- Stegware Removal
- Bi-Directional Protection
- Off-Box Logging
- Real time protection against Zero Days and advanced attacks
- Integrates with most web gateway products over ICAP
- Prevention against all file based attacks
- Steganography prevention outbound (DLP) but also inbound (code smuggling)

No more zero day content threats – guaranteed

The Forcepoint Gateway eXtension uses Zero Trust Content Disarm and Reconstruction (CDR) to always deliver safe, threat-free content without the need to detect the threat or isolate users from the business content they need. Stop ransomware, defeat zero-day threats, and destroy steganography exploits without inspecting or relying on signatures. Even the most sophisticated, targeted attack or stealthy data loss tactics will fail. By using the Forcepoint Gateway eXtension, you are completely protected from the threat of a zero-day exploit concealed in business content.

Seamless integration with existing defenses

The Forcepoint GX integrates seamlessly with existing perimeter web defenses, secure web gateways, next-generation firewalls, and web application firewalls using the industry standard ICAP protocol. Deployed as part of the Forcepoint Zero Trust CDR for web solution, the Gateway eXtension receives business documents from your existing perimeter defense over ICAP, transforms them to remove any concealed threat, and passes them back, offering a low risk, low cost route to total protection from content borne threats crossing the web boundary.

Zero Trust CDR – digitally pure

Forcepoint's unique content transformation technology assumes every business document or image could contain a threat. It intercepts the content at the boundary and then re-creates it from scratch, clean and safe on the other side. This destroys the threat. Nothing travels end-to-end but safe content. The user's browsing experience is safe and the integrity of the documents and images they download and upload over the web is assured. The organization enjoys the reputational benefit that comes with the knowledge that business information crossing the web boundary is always digitally pure and threat free.

Destroy stegware

Steganography is the covert hiding of data within seemingly innocuous files. It's a way of encoding a secret message inside another message, called the carrier, with only the desired recipient able to read it. Steganography has long been used to communicate without the authorities finding out, but now stegware, the weaponization of steganography by cyber attackers, is on the rise. This is bad news for IT professionals using tools that identify unsafe data, since steganography is impossible to detect. With the Forcepoint Gateway eXtension, your perimeter web defense destroys stegware concealed in images and stops it being used to infiltrate malware, exfiltrate high value data, or operate Command and Control (CnC) channels.

Forensic analysis

The Gateway eXtension can be configured to provide in-depth data analytics. A graphical dashboard provides real-time views of the business documents and images it is rendering threat-free while a dedicated steganography section provides indicators of the probable presence of stegware in images. A drill-down capability makes it easy to observe browsing behavior while a "before and after" view enables members of the SOC team to perform forensic investigation on documents and hold users to account. Auditing and logging information can be routed off-box into the organization's data lake and used to inform a SIEM system.

Key benefits

- → **Simple setup.** Intuitive GUI and (optional) pre-built ICAP integration with leading web gateways and firewalls.
- → **Malware removal.** Threats concealed in Office documents and PDFs are removed during transformation.
- → **Stegware removal.** Threats concealed in web images and social media feeds using steganography (stegware) are removed during transformation.
- → **Bi-directional protection.** Stops malware being infiltrated, prevents covert outbound data loss, and smashes CnC channels.
- → **Auditing and off.** Box logging for offline forensic examination.

Platforms

- → **Physical.** Forcepoint HRB Appliance.
- → **Virtual.** Minimum specification: Memory: 64GB, Cores: 16, Disk: 80GB+.

Operating system

- → Secure Proprietary Operating System
- → Browser
- → Any HTML5 compliant browser

Supported file types

- → Microsoft Word
- → Microsoft Excel
- → Microsoft PowerPoint
- → Adobe PDF
- → GIF image format
- → PNG image format
- → JPG image format
- → BMP image format
- → TIFF image format
- → JSON
- → XML
- → CSV
- → ZIP
- → TXT
- → Extended support with optional sidecar facility

Steganography stealth techniques & algorithm

- → Undetectable Steganography
- → Least Significant Bit Replacement
- → Least Significant Bit Matching
- → Redundant Data Stuffing
- → Palette Ordering
- → F5 DCT Coefficient Ordering

Data lake

- → Ability to send original documents to the customers data lake for forensic analysis if required.
- → Supported Gateway/Firewall Integration
- → GX can be deployed with any ICAP capable web gateway, next-generation firewall or web application firewall.
- → ICAP integration between the GX and the McAfee web Gateway Version 7.6.2 and above has been approved as McAfee Compatible.

Throughput

- → A single physical instance supports up to 5,000 users (typical web browsing usage).

For more information, visit www.forcepoint.com

Forcepoint

[FP-Datasheet-Gateway eXtension-US-EN] 12Jan2022