EVERFOX

DATASHEET

Gateway eXtension (GX)

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 Everfox Gateway eXtension (GX) to remove these threats.

Remove zero-day content threats

Remove zero-day content threats with the GX, utilizing Zero Trust Content Disarm and Reconstruction (CDR) to consistently deliver secure content, with threats removed. This approach ensures safety without the need to detect or isolate users from essential business content, thwarting ransomware, defeating zero-day threats, and neutralizing steganography exploits, all without relying on signatures.

Seamless integration with existing defenses

As part of Everfox CDR solutions for web,the GX collaborates with your current perimeter defense, transforming business documents to eliminate concealed threats and providing a cost-effective pathway to comprehensive protection against content-borne threats.

Simple integration with your existing perimeter web defenses, secure we gateways, next-generation firewalls, and web application firewalls using the ICAP protocol.

Content Disarm & Reconstruction (CDR) - digitally pure content

Experience digitally pure content with Everfox's unique content transformation technology. Intercepting content at the boundary, it recreates content from scratch, ensuring cleanliness and safety when delivered, destroying potential threats.

This provides a safe browsing experience for users and ensures the integrity of documents and images exchanged over the web, solidifying the

Challenge

Existing perimeter web defenses (web gateways & firewalls) are failing to cope with the increasing onslaught of known, unknown, and zero-day threats concealed in business documents and images..

Solution

A security solution meticulously crafted to fortify organizations against the today's landscape of cyber threats.

Everfox's GX ensures that files entering a system from untrusted locations are delivered via CDR technology, to consistently deliver secure, threat-reduced content.

Empowering organizations to stay ahead in the ever-evolving landscape of cybersecurity challenges.

Benefits

- HardSec, on-premises appliance
- Simple setup
- Stegware removal
- Bi-directional protection
- Off-box logging
- Real time protection against zero-day and advanced threats
- Integrates with most web gateway products over ICAP
- File based malware prevention

organization's reputation for digitally pure business information crossing the web boundary.

Destroy stegware threats

Steganography conceals data within seemingly innocent files, allowing secret messages to be encoded in carriers with only the intended recipient able to read them. The rising threat of stegware, the weaponization of steganography by cyber attackers, poses a challenge for IT professionals as traditional tools struggle to detect this covert technique.

The GX acts as a solution, destroying stegware hidden in images and preventing its use in infiltrating malware, exfiltrating valuable data, or establishing command and control channels.

Enhanced forensic analysis

Configure the Gateway eXtension to offer comprehensive data analytics. A graphical dashboard provides real-time insights into business documents and images to remove threats. A dedicated steganography section highlights potential indicators of stegware in images. With drill-down capabilities, observing browsing behavior becomes seamless, while a "before and after" view enables SOC team members to conduct forensic investigations on documents and hold users accountable.

Audit and log information can be seamlessly directed off-box into the organization's data lake, informing SIEM systems effectively.

Platforms

Physical

- Everfox HRB Appliance

Virtual

- Minimum specification - 1 processor core, 4GB memory, 50GB hard disk, 2 network interfaces

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

Steg stealth tech & algorithm

- Least Significant Bit Replacement
- Least Significant Bit Matching
- Redundant Data Stuffing
- Palette Ordering
- F5 DCT Coefficient Ordering Steganography stealth techniques & algorithm

Data lake

- Ability to send original documents to the customer's 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)

Learn More: www.everfox.com