EVERFOX

DATASHEET

Information eXchange (iX)

Complete malware protection for email, file transfers, web application services and beyond.

Benefits

- Two one-way direction flows: protection for both the in bound and outbound.
- Steganography prevention outbound and inbound (code smuggling).
- Multiple cross boundary applications can share one iX.
- Bi-directional protection that stops malware being infiltrated, prevents covert outbound data loss and smashes CnC channels.
- Auditing and off-box logging for offline forensic examination.

Stop Advanced & Zero Day Threats

Everfox iX Appliance is an advanced boundary protection appliance, defeating Zero Day Attacks and data leaks rather than detecting them when it is too late.

Everfox does this by implementing Content Disarm and Reconstruction (CDR) in a unique way. The Everfox CDR process can be split into 2 stages enabling its use at the boundary of a network to provide protocol and data breaks. For ultimate assurance, the iX Appliance can be split across a hardware verification device (Everfox High Speed Verifier) providing a protocol and content break for bi-directional traffic with full hardware logic verification of the protocol and the content.

Stopping ransomware attacks, defeating zero-days and destroying steganography exploits without relying on signatures. Even the most sophisticated, targeted attack or stealthy data loss tactics will fail.

Using the Everfox iX Appliance , you are protected from the threats concealed in everyday business content.

Complete Threat Protection

Everfox iX Appliance can handle a wide range of protocols and associated data formats, supporting email, file transfer and web applications and streamed UDP and TCP data such as syslog.

Located at the network perimeter, iX operates inline to remove threats from business content and in the case of web applications to help ensure application traffic is constrained to match pre-defined schemas.

Hardware Logic Verification

For systems that face the most sophisticated attacks and require a minimal attack surface, a pair of iX units can be deployed connected via Everfox High Speed Verifier (HSV).

The HSV provides independent verification implemented in hardware logic and as such, uses none of the software and networking components that might house a backdoor exploit or make it vulnerable to attack.

Everfox iX Appliance is available as a physical or virtual appliance built on a hardened, cut down Linux kernel. It can be deployed as a single machine or in a split configuration either side of an Everfox High Speed Verifier for connections to high threat networks

Digitally Pure Data

Everfox iX Appliance extracts useful business information from data, leaving behind any hidden malware or sensitive information that might be hiding, and builds a new clean data structure to carry the information to its destination. The iX Appliance provides real protection against advanced cyber attacks and damaging leaks.

Forensic Analysis

Auditing and logging information can be routed off-box into the organization's data lake and used to inform a SIEM system.

Nothing Travels End-to-End But Safe Content

The user's experience is safeguarded. The integrity of the business content in email, file transfers and web applications are assured. The organization enjoys the reputational benefit that comes with the knowledge that business information is safe and digitally pure.

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 most forms of steganography are almost impossible to detect. People have managed to do it but success rates for detection are less than 20%.

The Everfox iX Appliance destroys stegware concealed in images carried over email, embedded in Web services applications or brought in as files, ensuring these vectors cannot be used to infiltrate malware, exfiltrate high value data or operate Command and Control channels.

Figure 1.0

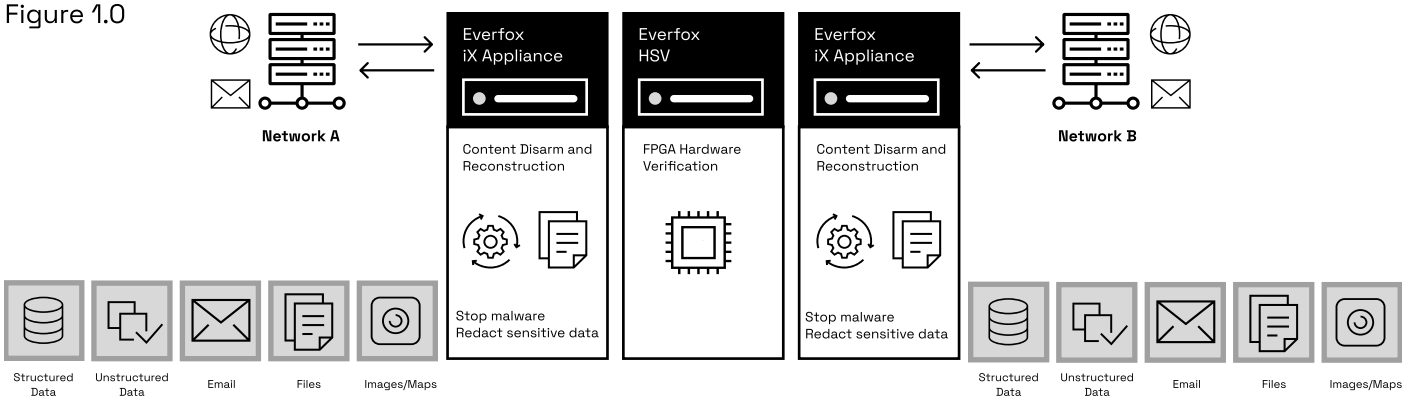


Figure 1.0

Our in-line iX appliance (for Email, Web Services and File Transfers) we can make the verification process non bypassable by putting it on our FPGA based hardware.

Specifications

Platforms	
Physical	Everfox HRB Appliance
Virtual	Min specification - 1 processor core, 4GB Memory, 50GB Hard disk, 2 network interfaces
Cloud	Available as AWS EC2 instances or docker container for all major cloud platforms

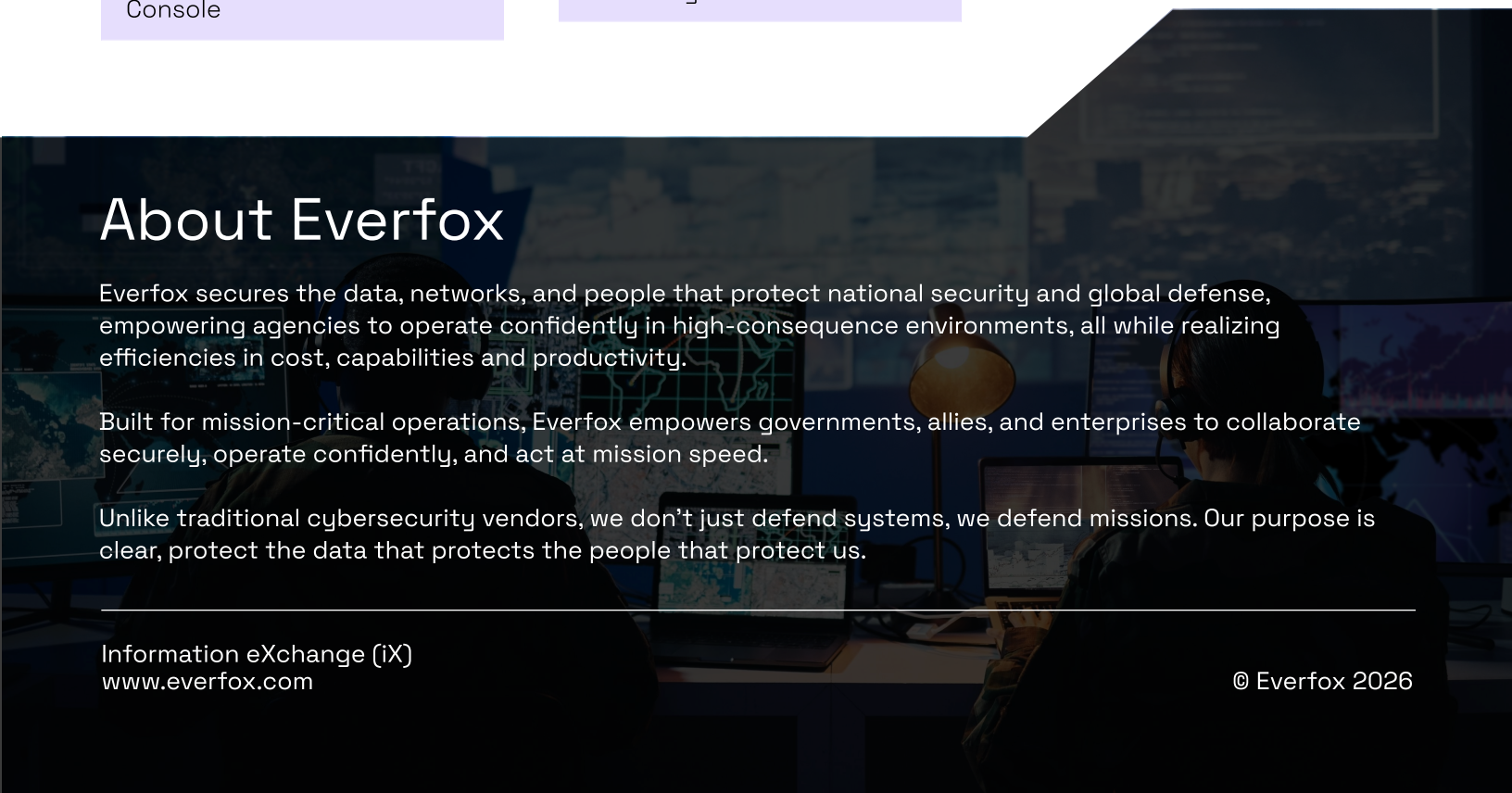
Deployments	
Uno	A single unit
Paired	Two units, one connected to the low network, one connected to the high network
High Assurance	As paired but interconnected via High Speed Verifier (HSV) for a minimal attack surface

Supported Protocols
HTTP/HTTP(S)
SMTP
DSFSP (File Transfer)
Framed TCP, UDP

Remote Management
Any HTML5 Compliant Browser
SSH
Console

Supported File Examples
Microsoft Word
Microsoft Excel
Microsoft PowerPoint
Adobe PDF
GIF Image Format
PNG Image Format
JPG Image Format
BMP Image Format

Cont.
TIFF Image Format
JSON
XML
CSV
ZIP
TXT



About Everfox

Everfox secures the data, networks, and people that protect national security and global defense, empowering agencies to operate confidently in high-consequence environments, all while realizing efficiencies in cost, capabilities and productivity.

Built for mission-critical operations, Everfox empowers governments, allies, and enterprises to collaborate securely, operate confidently, and act at mission speed.

Unlike traditional cybersecurity vendors, we don't just defend systems, we defend missions. Our purpose is clear, protect the data that protects the people that protect us.

Information eXchange (iX)
www.everfox.com