Forcepoint

Information eXchange

Inline Zero Trust Content Disarm and Reconstruction (CDR) for email, file transfers, web application services and much more – removing known, zero day and unknown threats from business content.

Deployed inline on a network perimeter, Forcepoint's Information eXchange (iX) acts as an application layer firewall removing threats from business content carried in email, web applications and network/logging traffic.

Key Benefits

- 2 one-way direction flows, ensuring protection for both the inbound and outbound.
- Easily scaled
- Steganography prevention outbound (DLP) and inbound (code smuggling)
- Complete malware protection
- Simple set up
- A single iX can be used for multiple use cases through the use of channels

No more zero day content threats – guaranteed

The Forcepoint iX uses uses Zero Trust 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 and destroy steganography exploits without deep content inspection and without relying on signatures. Even the most sophisticated, targeted attack or stealthy data loss tactics will fail. Using the Forcepoint iX, you are completely protected from the threat of a zero-day exploit concealed in business content.

Inline threat removal

Forcepoint iX handles a wide range of protocols and associated data formats enabling threat removal for email, file transfer, web applications and network/logging traffic. Located at the network perimeter, iX operates inline to remove threats from business content and – in the case of web applications – to ensure application traffic is constrained to match pre-defined schemas.

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 experienceis safeguarded - the integrity of the business content in email, file transfers and web applications is assured. The organization enjoys the reputational benefit that comes with the knowledge that business information.

Hardware logic verification

For systems that face the most sophisticated attackers and require a minimal attack surface, a pair of iX units can be deployed connected via Forcepoint's 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.

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 Forcepoint iX 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 (CnC) channels.

Forensic analysis

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 configuration - up and running in under 10 minutes.
- **Multi-channeled.** Multiple cross-boundary applications can share one iX.
- **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 - 1 processor core, 4GB Memory, 50GB Hard disk, 2 network interfaces.
- **Cloud.** Description. Available as EC2 instances.

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

Supported protocols

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

Deployments

- **Uno.** A single unit
- **Paired.** Two units, one connected to the low network, one connected to the high network
- **High assurance.** As above but interconnected via Deep Secure High-Speed Verifier (HSV) for a minimal attack surface

For more information, visit www.forcepoint.com

Forcepoint

© 2022 Forcepoint. Forcepoint and the FORCEPOINT logo are trademarks of Forcepoint.
All other trademarks used in this document are the property of their respective owners.