

Deep Secure information eXchange (iX)

Inline content threat removal 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, Deep Secure's iX acts as an application layer firewall removing threats from business content carried in email, Web applications and network/logging traffic.

No More Zero Day Content Threats – Guaranteed

The Deep Secure information eXchange (iX) uses Content Threat Removal 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 Deep Secure iX, you are completely protected from the threat of a zero-day exploit concealed in business content.

Inline Threat Removal

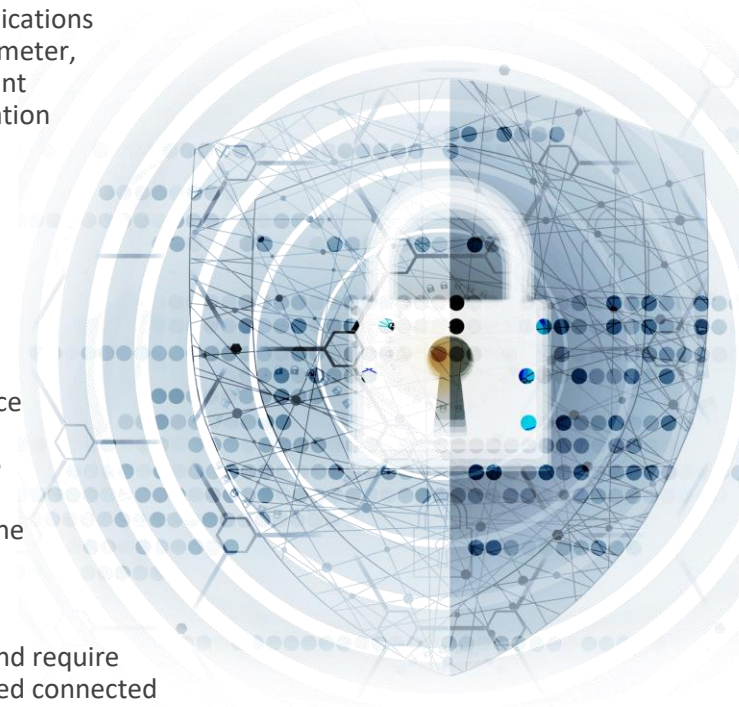
iX handles a wide range of protocols and associated data formats enabling threat removal for email, file transfer, web applications and network/logging traffic. Located at the network perimeter, iX operates inline to remove threats from business content and – in the case of Web applications – to ensure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

Content Threat Removal – Digitally Pure

Deep Secure'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 experience is 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 crossing the boundary is always digitally pure and threat free.

Minimal Attack Surface

For systems that face the most sophisticated attackers and require a minimal attack surface, a pair of iX units can be deployed connected via Deep Secure'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 impossible to detect. The Deep Secure 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 organisation'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-channelled – 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: Deep Secure HRB Appliance
- Virtual: Minimum specification - 1 processor core, 4GB Memory, 50GB Hard disk, 2 network interfaces
- In AWS

Operating System

- Deep Secure Operating System (DSOS)

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

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

Supported Protocols

- HTTP/HTTPS
- 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
- Paired – as above but interconnected via Deep Secure High Speed Verifier (HSV) for a minimal attack surface

Learn More

For more information on how the iX is deployed in the Content Threat Removal for Mail, Content Threat Removal for File Transfer and Content Threat Removal for Web Services solutions, visit www.deep-secure.com/solutions.