DEEP SECURE

Next Generation Threat Removal is Here

Summer 2020

Threat Removal 2.0 is the next generation cybersecurity defence, designed around a zero trust approach to exchanging information and engineered for the hyper connected digital age.

Complete Immunity from Malware

Threat Removal 2.0 doesn’t need to detect the presence of threats to defeat them. Instead, it implements a zero trust data approach to the UK’s National Cyber Security Centre (NCSC) data import and export patterns.

Threat Removal 2.0 delivers malware-free data and prevents covert exfiltration, using a unique process of transformation that extracts just the business information from incoming data, verifies it is safe and then builds new data to carry the information onwards.

This unique process ensures complete immunity from the malware threat. It is future proof and evasion proof. It defeats threats that aren’t even known about yet, and there is no way that an attacker can invent a way to evade the defence because there’s no attempt to detect them. You’re immune. Now and forever.

Pixel Perfect Data Every Time

With completely re-engineered support for Microsoft Office files, Threat Removal 2.0 delivers pixel perfect transformations to satisfy even the most demanding power user, including improved support for embedded links to videos, charts, text boxes and graphics within Office files.

Reduced Operational Costs and Increased Productivity

Threat Removal 2.0 reduces IT operational costs by eliminating false positives that would otherwise need managing and removing detection-based technologies that need constant monitoring and continual updates. Team productivity increases as less time and resource is spent on remediation. With Threat Removal 2.0 the defence is future proofed, so vulnerabilities can be patched and legacy applications replaced in a considered fashion, rather than in a dangerous rush.

Increased File Format Support

Threat Removal transforms over 50 different file formats including Microsoft and Open Office, PDF and image files as well as structured data formats such as XML, JSON and CSV. Office documents containing macros can be blocked or transformed with the macros redacted or preserved on a per filetype or per user basis while legacy Office file formats are “uplifted” to the latest supported equivalents. Now, with Threat Removal 2.0, Office files generated by Mac applications, Google Docs and Office Online can all be transformed and rendered 100% malware-free.

Enhanced Reliability and Performance

Threat Removal 2.0 includes a host of new features designed to enhance reliability, including controls to manage machine resource/memory usage and secure administrative access. New performance enhancements including stateless processing, line speed verification and non-stop scalable operation ensure users always get instant access to the threat-free information they need.

Simplified Administration

Threat Removal 2.0 includes enhanced logging to enable faster forensic analysis, while a remote system update feature simplifies administration.

How it Works

Everyone needs to share information. But to receive information you must accept data and data can carry malware. So, if data is the infection path for malware, why not simply stop it coming in? It’s not as crazy as it sounds, because it’s not the data you’re after – it’s only the information it’s carrying. That’s how Threat Removal works.

Rather than checking the data for malware, Threat Removal extracts the information and discards or stores the original. It then verifies that the information is safe and well structured, before building new data to carry the information to its destination. The new data is known to be safe and the attacker can’t evade the defence.

Threat Removal can be delivered through the cloud, hybrid, as on-premise appliances or with the extra assurance of a hardware logic verifier for cross-domain applications.

NEW FEATURES AT-A-GLANCE

Core Threat Removal engine enhancements:

Improved Office Transformations

- Enhanced user experience and support for a wider set of Office applications

Enhanced ZIP Handling

- Support for ZIP64 format and control over limits on decompressed ZIP files

Improved reliability and throughput

- Memory and time limits during processing to ensure more efficient use of the machine resources

Enhancements to information eXchange (iX) VERSION 2.0:

Improved Operations

- The profile and type mapping used in a transaction is reported in the logs for improved diagnosis
- Logging filenames in the sidecar supports improved tracking
- Ability to download a portion of the diagnostic log rather than the whole file
- Manual update of the logfile when in Don’t Update mode
- Ability to upgrade the iX software automatically via the management API

Customisation

- Redacted text and filename configurable in multiple languages

Migration / Bulk File Transfer using File Transfer Utilities

- File ownership maintained when files are transferred
- Feedback can be provided to users when files fail to transfer
- Support for DHCP in the File Mover clients
- Support for multiple iX Appliances using the File Mover Dropper

Enhancements to Gateway eXtension (GX) VERSION 2.0:

Improved Operations

- Maintenance mode allows upgrade of GX in service
- Diagnostic logging of filenames in the sidecar supports improved tracking
- Ability to upgrade the GX software automatically via the management API
- Ability to download a portion of the diagnostic log rather than the whole file
- Manual update of the logfile when in Don't Update mode

Enhancements to Application eXchange (AX) VERSION 2.0:

Availability on AWS Market Place

- Allowing quick and easy access to the APIs

Migration / Bulk Loading of file stores

- Support for pre-translation of file formats will allow file stores with legacy Office documents to be passed to the service for transformation
- Support for ZIP files in the service will provide greater flexibility in uploading new or existing documents to the service
- Support for EML, WMF and EMF file formats

Integration with cloud applications using public APIs

- Support for structured data formats (XML / JSON / CSV)

Availability

Threat Removal 2.0 is available in cloud or on-premise, ensuring web browsing, portal/file uploads, mail, web services, file transfers and cross domain applications are all immune from the malware threat.

Threat Removal 2.0 is automatically available to existing supported customers of Deep Secure Threat Removal 1.x.