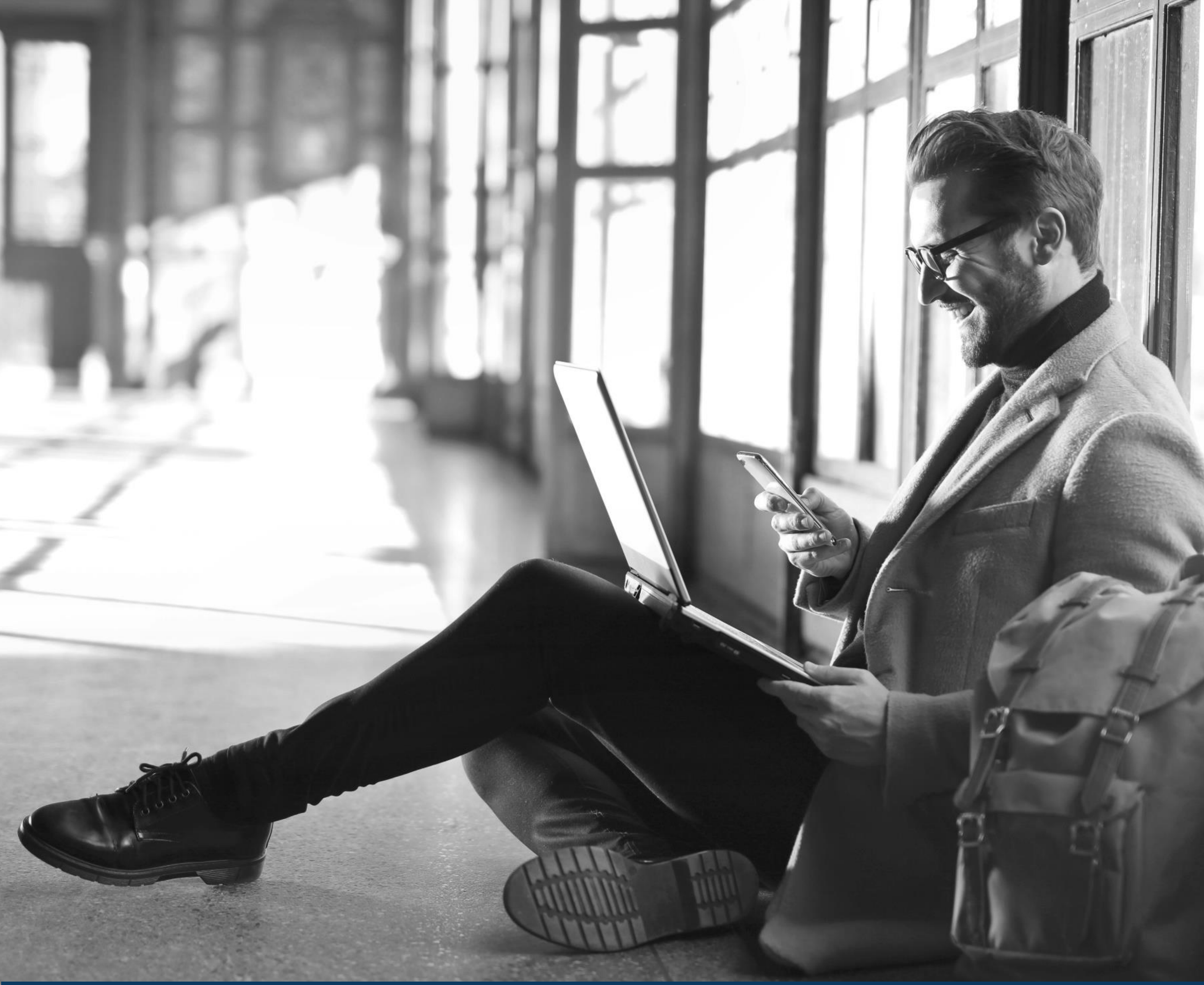


30 Million Viruses? No Problem.

With Content Threat Removal

DEEP SECURE

Introducing Content Threat Removal

The everyday business requirement of accessing files and documents from the Internet, exposes the user to significant risk from attackers, intent on stealing their credentials and/or compromising the endpoint device to gain access to the corporate network.

The attackers conceal malware in files and documents so that it will bypass gateway, anti-virus, firewall and sandbox defences.

Deep Secure Content Threat Removal is a unique technology that enables everyone in the organisation to open files from the Internet with confidence that they will be completely safe.

It works by transforming the original content into 100% safe new data which is editable and in the same file format – while ensuring that none of the original content ever reaches the endpoint.

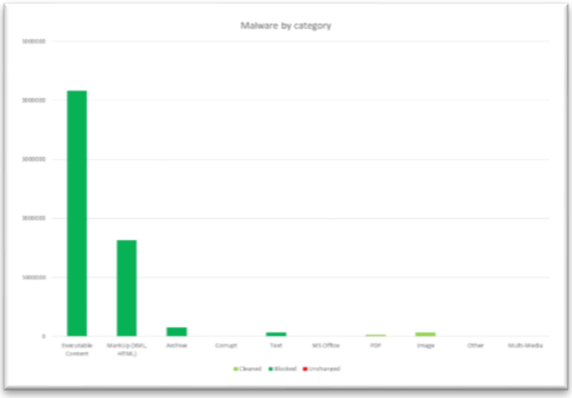
The result? Deep Secure provides true protection against all known - and unknown – viruses and malware.

Tried and Tested

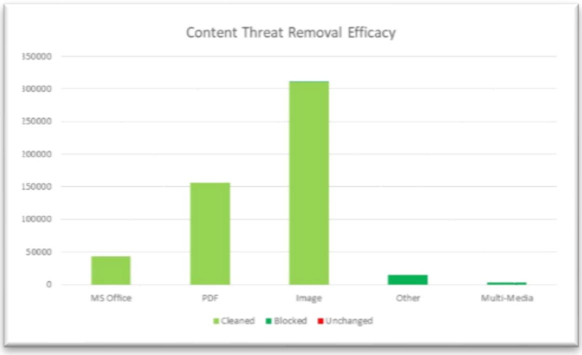
Content Threat Removal is proven against over 30 million samples of known malware

In 2019, Content Threat Removal (CTR) was put to the test with over 30 million examples of known malware.

The most common type of sample malware in the test was executable files and these were blocked by Content Threat Removal because they could not be safely transformed.



The remaining files, shown in light green, were transformed into safe versions. These included Microsoft Office, PDF and image files that contained known malware.



Nothing got through the Content Threat Removal defence. Every file was either transformed (Light Green) into a safe, clean, equivalent file, or blocked (Dark Green) because it was an executable or so corrupt that no useful information could be extracted from it..

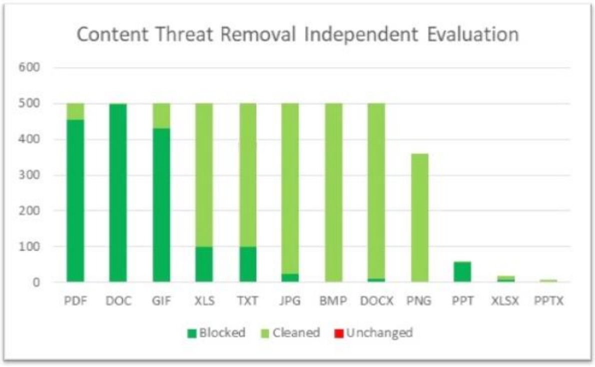
Previously Unseen Malware

100% effective against previously unseen malware

Following this test, a national government agency contracted its engineering arm to perform an independent test.

This time, the testing was not using publicly available viruses, but malware created specifically to test the effectiveness of content security solutions and unseen by Deep Secure.

The malware was specially crafted and concealed in a range of common file format types, including Microsoft Office Word, Excel, PowerPoint, Adobe Portable Document Format (PDF) and a selection of image file formats including GIF, JPG, BMP and JPG.



Nothing got through the Content Threat Removal defence. Every file was either transformed (Light Green) into a safe, clean, equivalent file or blocked (Green) because it was an executable or so corrupt that no useful information could be extracted from it.

Results

No malicious content gets through the transformation process

Comprehensive in-house and independent testing conclusively shows that Deep Secure Content Threat Removal is 100% effective against known and previously unseen malware. No malicious content gets past the defence.

Content Threat Removal is a "zero trust" technology that transforms every file, irrespective of whether it contains a threat. There is no change to user experience, no endpoint software installation, it operates at enterprise scale, and eliminates the cost of multiple security alerts and false positives.

With Content Threat Removal you can open any file with confidence, knowing it will be threat-free.

For more in-depth information on the tests, download the Testing the Efficacy of Content Threat Removal technical paper from our website.

"Office documents, PDFs and images allowed in over the Web are processed by Content Threat Removal for Web Gateways, to ensure they are completely threat-free."

Major UK Financial Institution