


Move Beyond Detection

Eliminate the Zero Day Threat in Digital Content

“Detect and Protect” has Failed



Digital content is the vector of choice for cyber criminals to use for malware, attacks and exploits. From Web browsing and email, to portal uploads and social media, digital content is routinely embedded with known, zero day and even totally undetectable threats concealed in the documents and images we use every hour of the working day. For over 25 years, we’ve tried to combat these threats using “detect and protect” cyber defences operating on the basis of: “I think this is bad because I’ve seen it before and it was bad then”. It’s an approach typified by anti-virus or anti-malware products and it is trivially easy to evade – just change the signature of the exploit and the malware-laced document or image crosses the security boundary unimpeded.

This approach may be fine for “run of the mill” protection but it’s not good enough to close the zero-day window and it’s no match for threats concealed in content that you don’t even know about, for highly evasive exploits that use steganography, polymorphic and polyformatted files.

Eliminate the Zero Day Threat

Now there’s a way to eliminate the zero-day threat, forever. Deep Secure’s Content Threat Removal technology doesn’t use detection to determine if something contains a threat. It doesn’t try to make educated guesses as to whether some particular piece of content is intrinsically good or bad. Instead, it trusts nothing and renders everything safe, using a process called content transformation to defeat attacks embedded in content – even zero-day exploits.

Whatever the exploit and whatever the motive, Content Threat Removal ensures digital content is 100% threat-free.

100%
Threat free
Digital
Content

**For mail, web,
file, portal,
social and
much more!**

Digitally Pure Content

Deep Secure Content Threat Removal can be deployed alongside your existing Web gateway, or as part of an email security solution. It can be used to protect Internet-facing portals, file transfers and pretty well any scenario that involves accepting digital content from an untrusted source.

Whatever the security boundary, Content Threat Removal means your organisation – your staff, customers and supply chain partners - can be confident that the business content they handle is 100% digitally pure and guaranteed threat free.

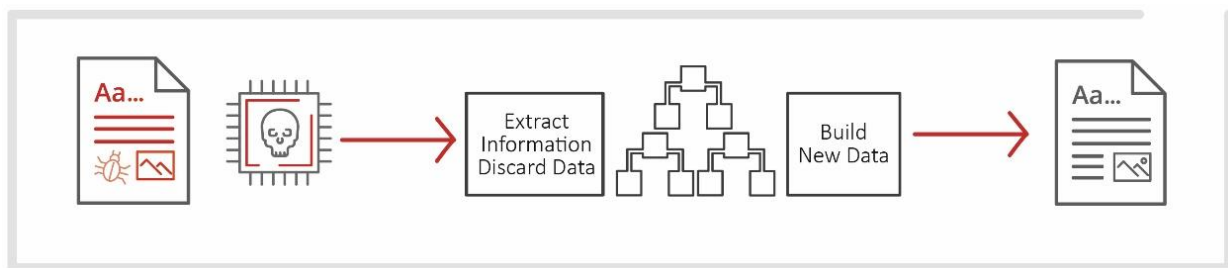
Destroy Threats Concealed in Images using Steganography

Cybercriminals are now using steganography to conceal exploits inside images, creating completely undetectable threats, encoded into the image pixels, the colour and transparency values. These images appear perfectly normal. The presence of the threat simply cannot be detected. Only the individual that encoded the exploit knows it is there and can decode it.

Deep Secure Content Threat Removal is the only solution to the problem of threats concealed in images using steganography (stegware). The content transformation process destroys anything concealed in the image, guaranteeing it is free from highly evasive exploits such as the outbound theft of IP concealed in images using steganography and the inbound risk of malware infiltration concealed in images using steganography.

How Does Content Transformation Work?

At the boundary, Deep Secure Content Threat Removal intercepts digital content such as documents and images. This content is decoded and just the valid business information is extracted from it. The original file is then discarded, along with any encoding context, un-necessary metadata, active code or malware.



The extracted business information is then passed through an intermediate data format, something the attacker has no influence over. The process of transformation is then completed when a wholly new file is created, populated with only valid business information, and handed over for onward delivery.

Transform your Cyber Defence

Deep Secure Content Threat Removal has been tested and proven against over 30 million viruses, and totally eliminates even zero day and undetectable threats. Zero-day exploits concealed in everyday office documents that routinely evade detection-based defences. Fileless malware that takes advantage of applications to “live off the land”, never being written to disk and therefore never being seen by detection-based virus scanners and polymorphic malware that continuously mutates to avoid detection. If it is a threat carried in digital content, Content Threat Removal defeats it.

**Cloud
On premise
Hybrid**

No scanning, No Sandboxing, No Waiting

Content transformation doesn't use detection, so there's no waiting for the system to scan content and try to detect known threats. It doesn't use sandboxing, so there's no lengthy delays in crucial business processes while content is isolated for inspection. The content transformation process takes a fraction of a second, meeting the business need for information that is both safe and available without latency. Far from impeding the speed with which users can access the content they need, this is a solution that delivers business content quickly and without compromise.

Content Threat Removal transforms over 50 file formats including OfficeX, Adobe PDF and Image Formats, delivering digitally pure content that is guaranteed safe, pixel perfect and fully revisable.