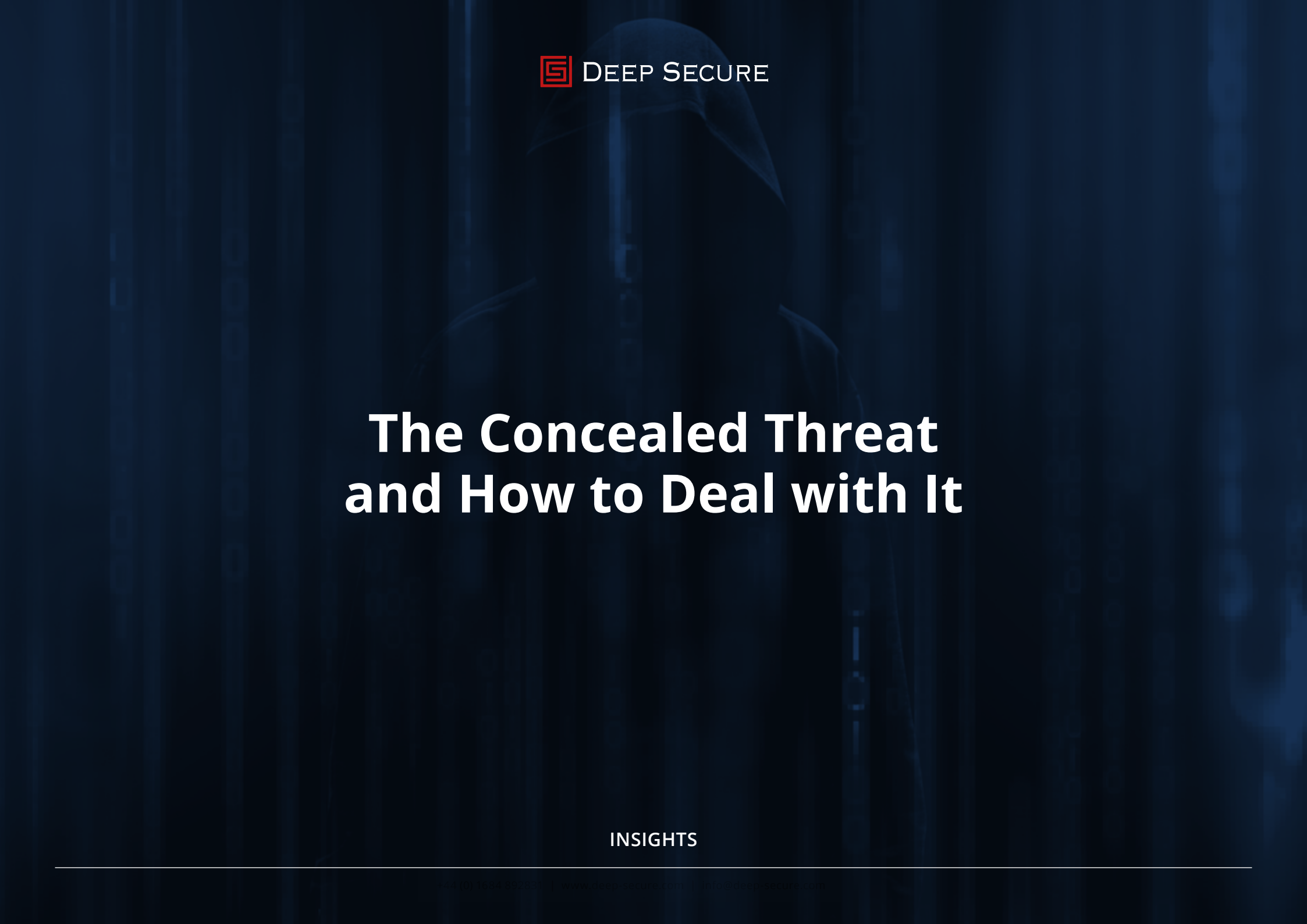


DEEP SECURE

The Concealed Threat and How to Deal with It

INSIGHTS

+44 (0) 1684 89 3831 | www.deep-secure.com | info@deep-secure.com

From ransomware in documents to banking trojans in spreadsheets, seemingly innocuous business data is the carrier of choice for the attacks used by today's cybercriminals. And yet this business data is the lifeblood of any enterprise. We can't live without it, and yet we might regret handling it. So how do we deal with the concealed threat and leverage the value of 100% pure and safe data?

A Game of Cat and Mouse

Cybersecurity has long concerned itself with the problem of the threat concealed in data – the documents and images we handle as part of our daily lives. History tells the story of an "arms race" where the attacker has continually had the upper hand. Anti-virus came first, and polymorphic viruses were developed to defeat it. Sandboxed detonation arrived and was heralded as the saviour, promising the ultimate defence against advanced persistent threats. But the attackers just got on with developing evasion techniques and rendered it obsolete almost immediately.

Meanwhile, highly sensitive government systems were employing Deep Content Inspection (DCI) to block anything that was merely capable of carrying an attack, but even here the increasing sophistication of attacks made it impossible for the defenders to stay ahead.

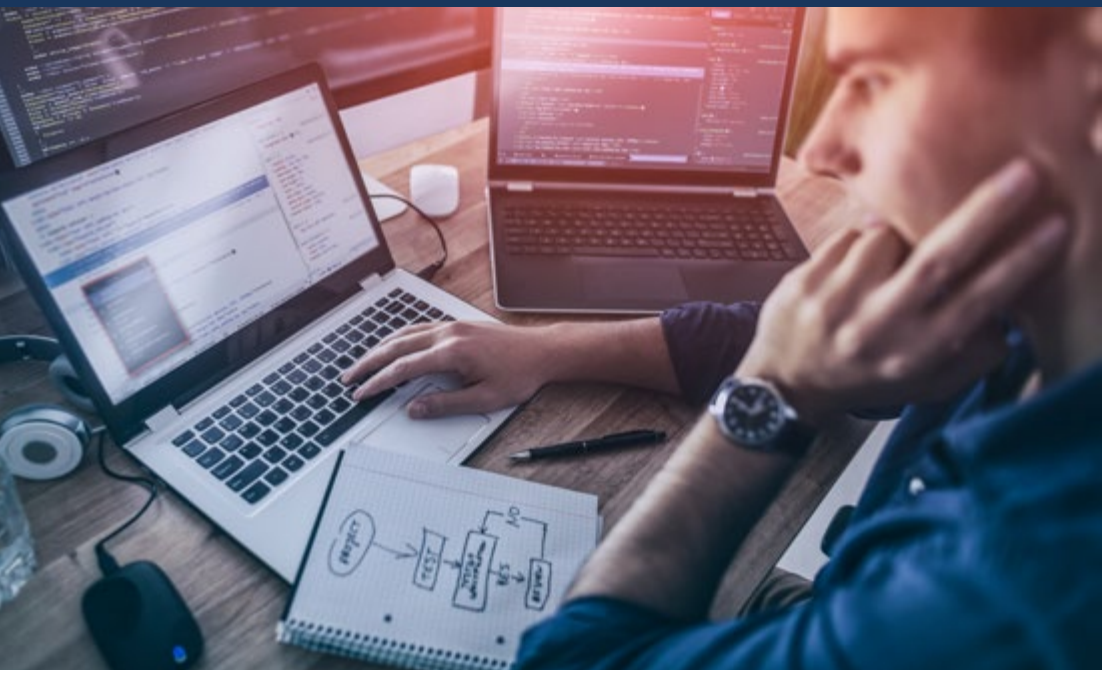
In the commercial world, a new line of defence - Content Disarm and Reconstruction (CDR) - offered the promise of being able to block anything capable of carrying an attack. The trouble was that CDR is the same technology as DCI so suffers from the same problem – the defence is only as good as the defenders' skill in predicting what attackers will do next, and the attackers always have the upper hand in such a race.

Ultimately, CDR/DCI does not remove the threat to business, it just removes those threat vectors that are understood by the defenders. The threat is reduced, but what's left is a threat that is not understood.

Facing the Unknown

If a defence removes all the threat that is known and understood, what remains is an unquantifiable risk. You have no idea if an attacker can still just walk into your system by exploiting a flaw you had not thought of.

The board members who are authorising the big spend on cyber defences used to ask "how many attacks were stopped?", on the assumption that stopping lots of attacks meant there can't be many left to worry about. But from Sony to Travelex, the fallacy of this is now being realised. Now it's a question of "what attacks does this let through" and neither Anti-Virus, Sandboxed Detonation nor CDR/DCI can answer that question – leaving an unquantifiable risk.



A Radical Transformation

As governments found attackers catching up with both DCI and CDR, they started looking for a radical alternative.

A technique that didn't depend on detection to stop the threat. The answer turned out to be a concept called "transformation". Developed behind the closed doors of the defence and intelligence community, the first visible clue of this work came in 2004 in a patent filed by the QinetiQ team working on the UK MoD's cyber security research programme.

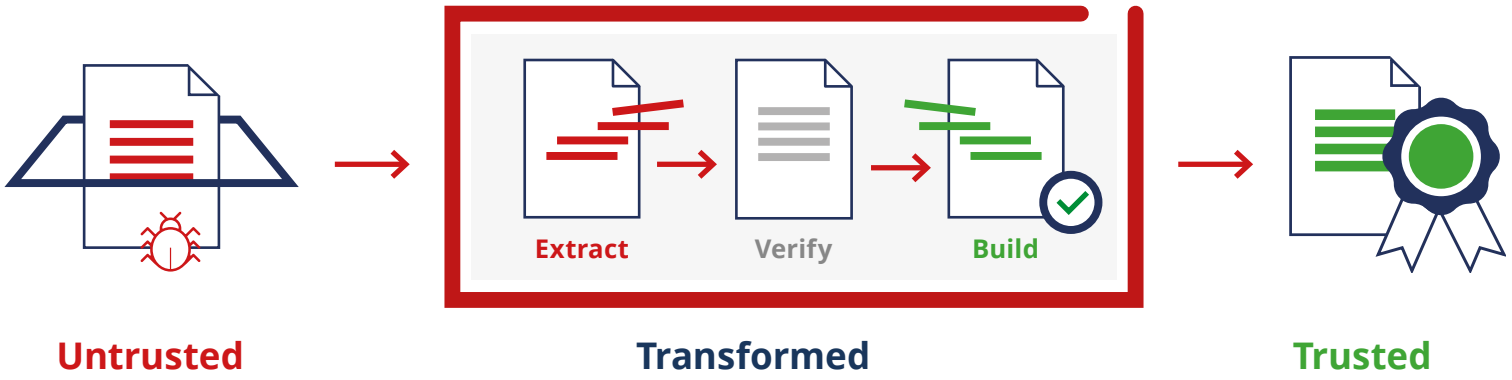
A transformation-based approach doesn't rely on detecting unsafe data or behaviour. Instead it transforms the data into something that is simple and obviously safe, so any concealed threat that was present is removed. This is a
"zero-trust" approach meaning the transformation happens even if there's no threat – the data is transformed anyway, and the recipient just gets what they need.

Unfortunately, in its initial incarnation, transformation wasn't a generally applicable technology and was restricted to very expensive, bespoke solutions.
Applying zero-trust transformation to products and services that could be easily deployed and were scalable and resilient for the mass market, seemed impossible. Until now.

Dealing with the Concealed Threat

Deep Secure developed the ***Deep Secure Threat Removal platform*** to make a zero-trust transformation-based cyber defence available to every enterprise and deal with the concealed threat once and for all.

Threat Removal works by assuming that all data is unsafe. It doesn't try to distinguish good from bad. This goes far beyond alternatives that only block data deemed to be unsafe. So how does it work?



Threat Removal extracts the business information as it arrives and discards the source data, including any hidden threats. Completely new data is then built to carry the information to its destination. The new data is digitally pure and independent of the source data, ensuring 100% protection (inbound and outbound). Deep Secure's approach to the problem of the threat concealed in data follows the recommendations laid down in the UK Government's National Cyber Security Centre (NCSC) "Pattern: For Safely Importing Data", a document that sets out best practice guidelines for accepting documents and images from untrusted sources.

Note that zero-trust transformation will eradicate a threat concealed in outbound data – say a trade secret hidden in a seemingly innocent image, just as certainly as it will remove a piece of ransomware concealed in an incoming Office document.

Note also that in environments requiring the very highest levels of assurance such as cross-domain and cloud interconnections, Step 3 – Data Verification – can be implemented in hardware using Field Programmable Gate Arrays (FPGAs) to protect the verification process and present a minimal attack surface to the cybercriminal.

Risk-free Data Exchange

The Deep Secure Threat Removal platform transforms data to prevent any possibility of malware transmission. It protects portals, web browsing, mail and web services, enabling organisations to reduce their organisational risks and leverage their data safely and with confidence.

It protects public cloud deployments, private clouds and high assurance situations, covering user-to-user, user-to-machine and machine-to-machine scenarios and giving customers an unprecedented level of choice. The same technology can be deployed in different parts of the business to achieve different effects, avoiding costly over-engineering while bringing cost savings through commonality.

Of course, the Deep Secure Threat Removal platform doesn't obviate the need for other security measures. End point security is still needed as there are other ways into a system that the platform does not control and the system boundary still needs to be maintained. Internal monitoring and data leakage protection controls will still be essential because insiders will continue to pose a threat. But with threat removal in place, a lot of the "noise" that makes these other mechanisms hard to manage fades away.

Threat Removal cannot be beaten. As a zero-trust transformation-based defence it delivers real-time, risk-free data exchange. The security team is satisfied because the threat is removed. The business team is satisfied, because they get the information they need.