The Content Threat

And how to deal with it!

Digital content – the essential life-blood of business and commerce – is the carrier of choice for the cyber threats used by today's attackers. We can't live without it, and yet we might regret handling it.

A Game of Cat and Mouse

Cyber security has long concerned itself with the problem of digital content threat. History tells a 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.

A Radical Transformation

As governments found attackers catching up with DCI, 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 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 .

This kind of defence doesn't rely on detecting unsafe data or behaviour. Instead it transforms the data into something that is simple and obviously safe, so any threat present is removed. This transformation happens even if there's no threat – the data is transformed anyway, which doesn't matter as the recipient still gets what they need.

But this wasn't very general-purpose technology, so was far from a solution suitable for business use. It was ok for special purpose bespoke solutions costing incredible sums of money, but extending this to make products and services that are easily deployed, scalable and resilient, applicable across a wide range of applications, is a whole new undertaking. And until recently the market was not there to make this happen, so the technique lay overlooked in its obscure niche.

The New Old Way

Meanwhile, continuing failure of content defence technology based on detection, caused some to take a fresh look at the Deep Content Inspection technology that was previously the preserve of sensitive government systems. This is Content Disarm and Reconstruction (CDR) – a commercial realisation of the idea of blocking anything capable of carrying an attack.

This takes the stance that any active content is likely to be unsafe and so must be stopped. This is a draconian approach, because it blocks some content that is safe, and while it used to be only government systems that faced a threat serious enough to make this necessary, now many business systems are in the same position.

The trouble is, 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. The thing is, CDR/DCI does not remove the threat, 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, some threat remains. Even if the defence removes a considerable amount of threat, that doesn't mean the threat that remains is insignificant. 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 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 are able to answer that one.

It gets worse. Attackers no longer seem satisfied with defeating the defences we have in place now. They have taken evasion to new heights. In particular they are using steganography to hide attacks, conceal command and control channels, and to stealthily exfiltrate sensitive information. Even though they already have the upper hand, they've jumped further ahead – employing information hiding techniques that render detection completely impossible. It's not a matter of the attacker playing catch-up any longer. They are miles ahead.

The Answer to the Digital Threat

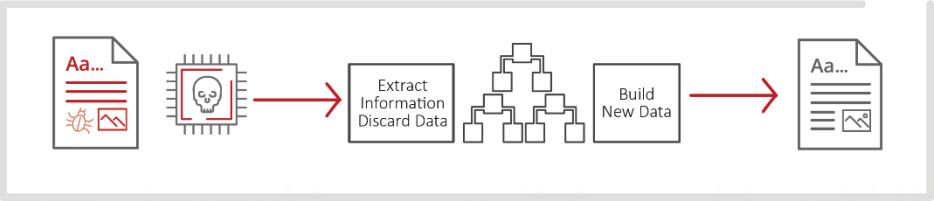
There's no way the defenders are going to catch up. At least not by playing by the rules and running faster. What's needed is something radically different that instantly leaps in from the attackers and blocks their path forever. It's time to go back to that idea of transformation and make it a commercial reality. It's time to look at what Deep Secure have been doing.

Transformation is the way to get ahead of the attackers and stay ahead, because it eliminates the threat and leaves no opportunity for evasion techniques to be developed. We call the approach Content Threat Removal (CTR), because that's what it does.

The original idea was to transform data coming from potential attackers into simple data that is obviously safe. This is good, but it is limited because it only works with data formats that are simple. That's not very general purpose so of little use in a commercial setting. The advance that Deep Secure have developed takes this to the next level – instead of transforming data, we transform the way information is represented.

CTR works by assuming that all data is unsafe. It doesn't try to distinguish good from bad. Whatever data an attacker sends in gets blocked. This goes far beyond CDR/DCI, which only blocks data that is thought to be unsafe. There's no decision to make about safe versus unsafe, so there's nothing to get wrong. But how does this work? How will the business get the information it needs?

CTR works by extracting the business information from the digital content received. The data carrying the information is then discarded and new safe data is created to carry the business information to its destination. This way the attackers cannot get in and the business gets what it needs. When it comes to the content threat, in terms of efficacy this approach cannot be beaten. The security team is satisfied because the threat is removed. The business team is satisfied, because they get the information they need.



This sounds deceptively easy, but to make it work CTR software needs a deep understanding of the way content is constructed and used. It has to know how information is represented, be able to extract it and build the new data. It has to do this without losing any business information, while at the same time denying an attacker any ability to influence how the information is delivered. Doing this for one simple format is hard, but having to repeat it for every complex format does not create a scalable, supportable solution. Solving this problem is one of the breakthroughs Deep Secure have made to bring CTR to life.

Flexibility – the Key to Success

If transformation is to escape from its obscure niche and become a success in the market, a CTR technology is needed that can be deployed in many different ways to meet different business requirements. Most businesses can rely on the isolation and separation functions built into a cloud service to keep their information away from other service users. These businesses need CTR to be deployed in a cloud friendly way. Other businesses need private clouds, and here CTR has to be part of the isolation mechanism that protects the cloud. In extreme cases, such as government defence and intelligence systems, the isolation mechanisms need to be high assurance and maintain full isolation of the business system.

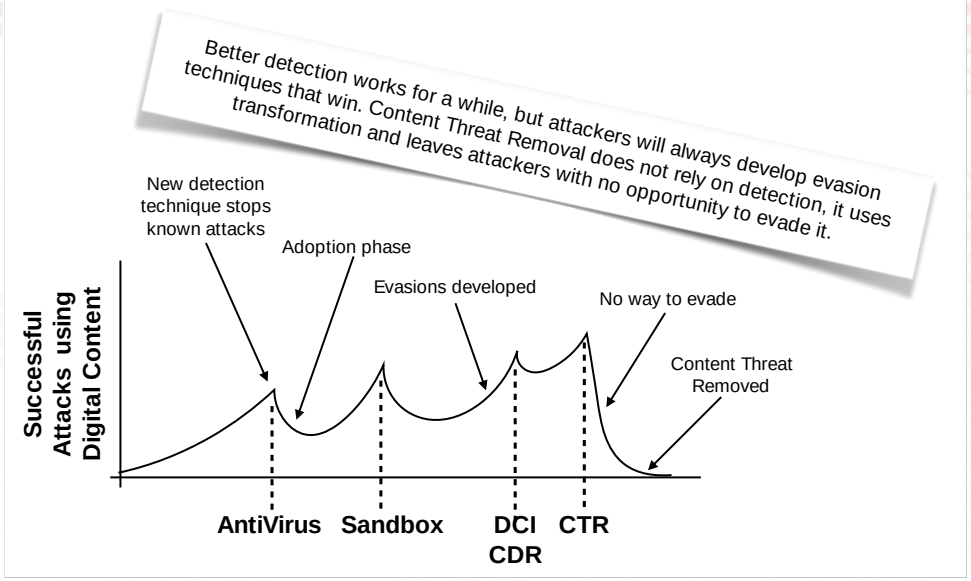
Delivering on this is Deep Secure's other breakthrough. By making the same implementation work for public cloud deployments, private clouds and high assurance situations, covering user-to-user, user-to-machine and machine-to-machine scenarios, Deep Secure have given their customers unprecedented choice. 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.

The real proof of the power of CTR is in its position regards steganography. Defences based on detection stand no chance, because it is undetectable. But CTR makes no attempt to detect the threat. Steganography works by hiding information in redundant parts of data. CTR works by extracting useful information from data, and this process naturally leaves behind any information encoded in redundant data. CTR defeats steganography by ignoring it – everything else will fail to defeat steganography because it cannot see it.

The Future

As attacks have become more sophisticated, defences that detect the attacks have improved. But each time defences advanced, the attackers developed new techniques to evade them. However, it looks like the end of the line for "the detectors", as attackers are now hiding behind steganography which is impossible to detect. The future has to be something radically different – Content Threat Removal – a defence that defeats the digital content threat posed by attackers once and for all.

CTR doesn't spell the end of other security measures. End point security is still needed as there will be other ways into a system that CTR is not controlling 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 CTR in place, a lot of the "noise" that makes these other mechanisms hard to manage fades away.



Another winner will be Business Analytics. Because CTR extracts business information from content, it is able to supply high grade information about what the business is doing. Rather than focus on network activity in an attempt to figure out what is happening in the business, future analytics capabilities can work directly with the relevant material, providing deeper insight and an enhanced capability to detect fraud.

CTR is the only way forward. And Deep Secure have it ready in its Content Threat Removal Platform.

Learn More

For more information, visit **www.deep-secure.com**.