KuppingerCole Report

EXECUTIVE VIEW

by Martin Kuppinger | July 2018

Deep Secure Content Threat Removal Platform

The Content Threat Removal Platform by Deep Secure operates at the network boundary, intercepts and analyzes incoming data, extracts only the useful business information while eliminating malicious content and then creates new, clean data for onward delivery. In this way, it defeats zero-day attacks and prevents covert data loss, all transparent to end users.

by **Martin Kuppinger**
mk@kuppingercole.com
July 2018

Content

Related Research

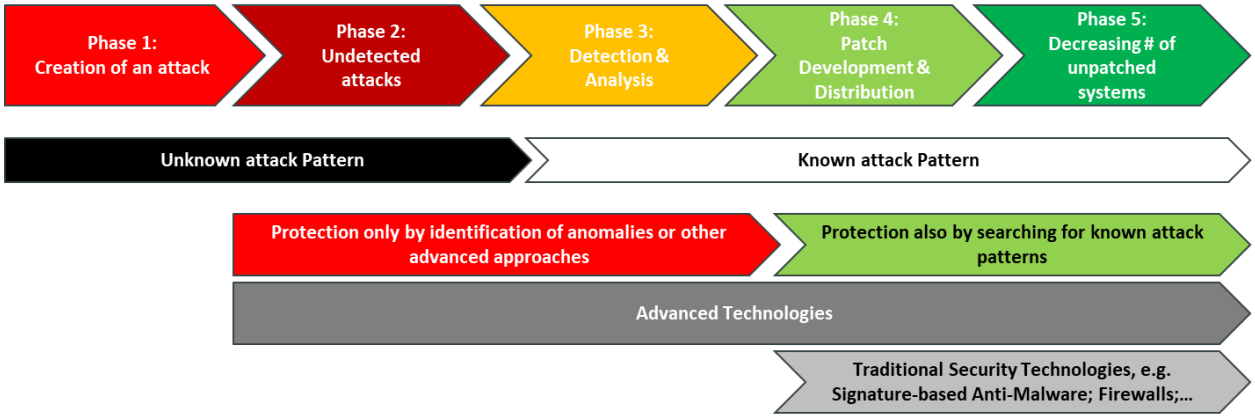
Advisory Note: Firewalls Are Dead - How to Build a Resilient, Defendable Network – 72163

Leadership Brief: How to close the skill gap in your Cyber Defense Center - 72800

Leadership Brief: Defending against ransomware - 70336

1 Introduction

Over the course of the past few years, the threat of cyberattacks has been on a constant rise. There are no signs that this will change in the foreseeable future. Organizations must defend themselves against such attacks, which is a challenge for several reasons. Among these reasons are a dynamic, ever-increasing attack surface, but also the fact that attacks remain unknown for a certain period, until someone detects them. On the other hand, the need for exchanging information constantly increases in the hyperconnected business world we face in the age of Digital Transformation. New and better solutions for cyber-defense are a must nowadays.



Phases of an attack – moving from the unknown to the known.

When we look at the phases of attacks, there is a period where these attacks are unknown, and it takes additional time to protect against attacks once they are identified. The most critical phase is what is indicated as phase 2 in figure 1, the time where attacks are run but haven't been identified. This period can be very short, e.g. in the case of many ransomware attacks that become immediately visible, but also can run for years. But even in phase 3, after identification, it takes from a couple of hours to days or even longer until effective protection by traditional approaches is available, during which time other less skilled attackers can create new attacks exploiting the same vulnerabilities.

In other words: Traditional security technologies such as signature-based Anti-Malware that protect against the "known" can only be one element in a protection strategy, as they are not sufficient anymore. The need is for additional security technologies that go beyond detection and protect against so called "zero-day attacks", which are attacks using a yet not known attack pattern.

The second reason why organizations must act is the ever-growing attack surface. This dynamic attack surface is due to the rise of the IoT, the increase in communication, the distributed and hybrid IT infrastructures using cloud services, and so on.

Factually, exchanging information with business partners, customers, and consumers is at the core of the Digital Transformation. Organizations must be able to share information and receive information, without being constantly exposed to threats. Establishing a track record for guaranteeing its customers, business partners, and users access to clean, secure business content is essential in the age of ever-increasing cyber-attacks. Providing secure data is about removing barriers for successful collaboration.

When we look at approaches for protecting against the unknown, we observe several ways to support organizations. There is the emerging field of "Cognitive Security", where AI (Artificial Intelligence) and other advanced technologies are applied to, e.g., identify anomalies. On the other hand, we observe a growing number of approaches for isolation, which provide a separate environment for dangerous activities such as web browsing. Other technologies – marketed as Content Disarm and Reconstruct – try to analyze content and strip everything that could be part of an attack vector. These approaches are not contradictory but compatible elements of an IT security infrastructure that is better suited to protect against the unknown. Organizations need to look at these new techniques and enhance their traditional IT infrastructure for mitigating the risk imposed by cyber-attackers.

Content Threat Removal as a rather new approach goes one step further. It focuses on analyzing content to find the useful business content, discarding everything else, and then building new data to carry the information safely to its destination. By doing this, everything that could be malicious is simply left behind.

Securing content by transformation is not a simple challenge, given that attacks can be woven deep into content, such as macros that are required to work with office documents. However, we see vendors appearing on the market that deliver on that promise. Even while there remains some trade-off, the potential increase in security makes it worth evaluating such tools and adding them to the IT security infrastructure.

Deep Secure is a UK-based cybersecurity software provider, delivering its products to a variety of sectors including leading defense and intelligence agencies. The company was founded back in 2009 and currently employs over 50 staff. Since its establishment in 2009, Deep Secure started catering to customers in UK. Over the past years, Deep Secure has started international expansion, now also serving customers in Europe, the US, Middle East, and the APAC region. Deep Secure provides a sophisticated solution for Content Threat Removal, which protects a variety of content such as PDF files, image formats, and others.

2 Product description

Deep Secure has long standing products that provide Deep Content Inspection, which they call "guards". The company offers Mail, Web, XML, and File guards to protect information on multiple levels. For instance, security labelling is one such level whereby a module will compare a document's security label against policy to determine if the data in question can be passed to the requestor. User authentication relies on the client's identity and access management environment and typically uses digital signatures to secure information.

The modules used for integrating with the various supported environments have extensive file format knowledge to protect data leakage from, as well as malware insertion into, protected networks. They utilize a common policy manager. Deep Secure content inspection provides deep content inspection for email, messaging systems, web browsing, web services, file transfer and directory replication. These modules also can be used to identify and block/remove active content and to compare security labels, clear email addresses, remove attachments, validate digital signatures and decrypt messages.

Deep Secure's new offering is the Content Threat Removal Platform, which works by transforming all data rather than using Deep Inspection. This is built around three components, which can be deployed on physical hardware, virtualized, or in the cloud. One component extracts the information content from data, one verifies the content, one builds new data to carry the content.

The Content Threat Removal Platform is the solution that Deep Secure offers for combating unknown content threats. It works by extracting the useful business information, i.e. the real content, from the data and constructing new, clean data to carry the information to its destination. Deep Secure calls this an information extraction approach to content transformation. Content Threat Removal removes the threat immediately, rather than just detecting or isolating it without delivery to the recipient. The goal is delivering secured content immediately, instead of blocking information flow.

Therefore, malicious content hiding inside the meta data is discarded and the business information is passed from one network to the other independently using new connections. In addition, the Content Threat Removal platform controls all the information that passes across a network boundary, whereby only clean business information can pass, preventing a sophisticated breach and stopping hidden data from leaking outbound.

Content Threat Removal platform uses a multi-layer inspection to extract useful information from deep down inside data structures where malicious behavior and zero-day threats could be hiding. Another highlight of this product is that it prevents covert data loss, as the multi-layered inspection leaves no hidden or unused data that can act as data leakage pathways to ensure that no sensitive data escapes.

Furthermore, the Content Threat Removal platform is equipped with next-generation technology which removes the human element from the network security and enables the devices to automatically respond and prevent threats. In addition, the platform has a self-defending architecture, so the system's attack surface is not simply moved to the security device – it is actually eliminated.

The platform offers application level proxies for Mail, File Transfer, and Web, as well as sidecar services (ICAP) for existing web gateways, to protect information at multiple levels. The Mail solution effectively defends against advanced attacks by focusing on the content. With this solution, the business content in messages and attachments is re-created without any of the meta-data or constructs that might contain an exploit or threat.

For File Transfers, the platform supports a simple protocol for moving files between servers and provides utilities that make use of this. The utilities interface to the file systems and applications, delivering support for moving files between stores and mirroring stores. This is particularly useful for passing software updates into a sensitive system.

The Web proxy is designed for business-to-business traffic and back end services accessed through web services protocols. This solution blocks the spread of malware and leaks of sensitive information by transforming the structured data content, in formats such as XML and JSON, while checking that the data matches the application's data schemas. Lastly, it ensures that messages are authentic and preserves the secrecy of messages.

As mentioned above, the technology can also be deployed as a "sidecar" to Web Gateways or Firewalls using the ICAP protocol, so that it integrates with existing perimeter web defenses. The gateway or

firewall passes Office documents and images to the Content Threat Removal "sidecar", which transforms the data to remove any concealed threat and passes them back.

A crucial part of the Content Threat Removal platform is the ability to combat threats concealed in images using steganography or "stegware". That component works by intercepting content like images and again builds a clean new content, thus eliminating potentially malicious content such as inbound malware, outbound data loss, and covert command and control channels. It also typically is deployed as a sidecar to an existing web gateway.

3 Strengths and Challenges

The Deep Secure Content Threat Removal Platform, with its various application layer proxies for common protocols and data handlers for common types of content, delivers an interesting approach for protecting against unknown attacks, by transforming specific types of content. Deep Secure works based on a well-thought-out and sophisticated architecture with well-isolated components and a modular approach. The latter allows for adding additional types of content translation and transformation.

Deep Secure already delivers support for a variety of document formats including emails, PDF files, the common image formats found on the Internet, Office documents and structured data in JSON and XML format. Support for more specialist and proprietary formats – which are complex to handle and test – is provided by an optional add-on "sidecar" capability, which is developed on a per-customer basis.

As with every approach that deconstructs, extracts and builds new content, there is a potential risk of some loss in performance. However, aside from access to web sites, which can be secured by taking an isolation approach, the focus is on non-real-time delivery channels such as file transfer and email exchange, where the potential slow-down is less relevant. Furthermore, the appliance-based approach of Deep Secure not only increases security but also delivers good performance. Beyond that, when comparing with detection-based approaches, there is no measurable negative performance effect, according to the claims of Deep Secure. By relying on the "sidecar" approach with standard integration to network security components and due to the specific use cases, we don't expect a negative impact on performance from the user perspective.

Overall, Deep Secure delivers an interesting offering that helps organizations set up secure interactions with customers and citizens across all important communication channels. From our perspective, Deep Secure Content Threat Removal Platform should be evaluated as one of the components to leverage existing IT infrastructures to a level which also can deal successfully with unknown attacks.

Strengths	Challenges
• Content transformation technology ensures real-time transparent protection from unknown threats • Multiple communications channel support including web, email, file transfer and chat protocols • Well-thought-out architecture with a choice of physical hardware, virtualized, and cloud-based deployment models • Support for broad range of document formats including PDF, OfficeX and image formats – additional specialist and proprietary formats can be added on a per-customer basis • Protects web services by analyzing JSON & XML formats • Strong focus on highly regulated industries	• Still limited but growing market presence outside of UK • Small technology ecosystem, but standards-based integration with other security solutions • Small company with limited capabilities for providing local and localized technical support

4 Copyright

The Future of Information Security – Today

KuppingerCole supports IT professionals with outstanding expertise in defining IT strategies and in relevant decision-making processes. As a leading analyst company, KuppingerCole provides first-hand vendor-neutral information. Our services allow you to feel comfortable and secure in taking decisions essential to your business.

KuppingerCole, founded in 2004, is a global Analyst Company headquartered in Europe focusing on Information Security and Identity and Access Management (IAM). KuppingerCole stands for expertise, thought leadership, outstanding practical relevance, and a vendor-neutral view on the information security market segments, covering all relevant aspects like: Identity and Access Management (IAM), Governance & Auditing Tools, Cloud and Virtualization Security, Information Protection, Mobile as well as Software Security, System and Network Security, Security Monitoring, Analytics & Reporting, Governance, and Organization & Policies.

For further information, please contact **clients@kuppingercole.com**

Kuppinger Cole Ltd.
Wilhelmstraße 20-22
65185 Wiesbaden | Germany

Phone +49 (211) 23 70 77 – 0
Fax +49 (211) 23 70 77 – 11
www.kuppingercole.com