Deep Secure

BUSINESS USE CASES

1 An Introduction to Deep Secure

The essential everyday business requirement of downloading documents and images - or receiving uploaded content - from the internet opens the user to significant risk from attackers, intent on stealing the user's credentials and/or compromising the endpoint device to gain access to the corporate network.

Deep Secure Content Threat Removal (CTR) eliminates all file-based malware attacks by eliminating the risks associated with downloading – and uploading - web documents and images. Our unique, military-grade technology transforms digital content – documents and images - in real-time and guarantees the only thing sent to the user is 100% safe data. Deep Secure provides a seamless user experience and supports the all common business document and image file formats.

Deep Secure is designed around a military-grade **True Zero Trust Security Model** where all downloaded content is assumed to be potentially malicious. Our unique technology ensures none of the original content from web document downloads - and uploads - can ever reach the endpoint.

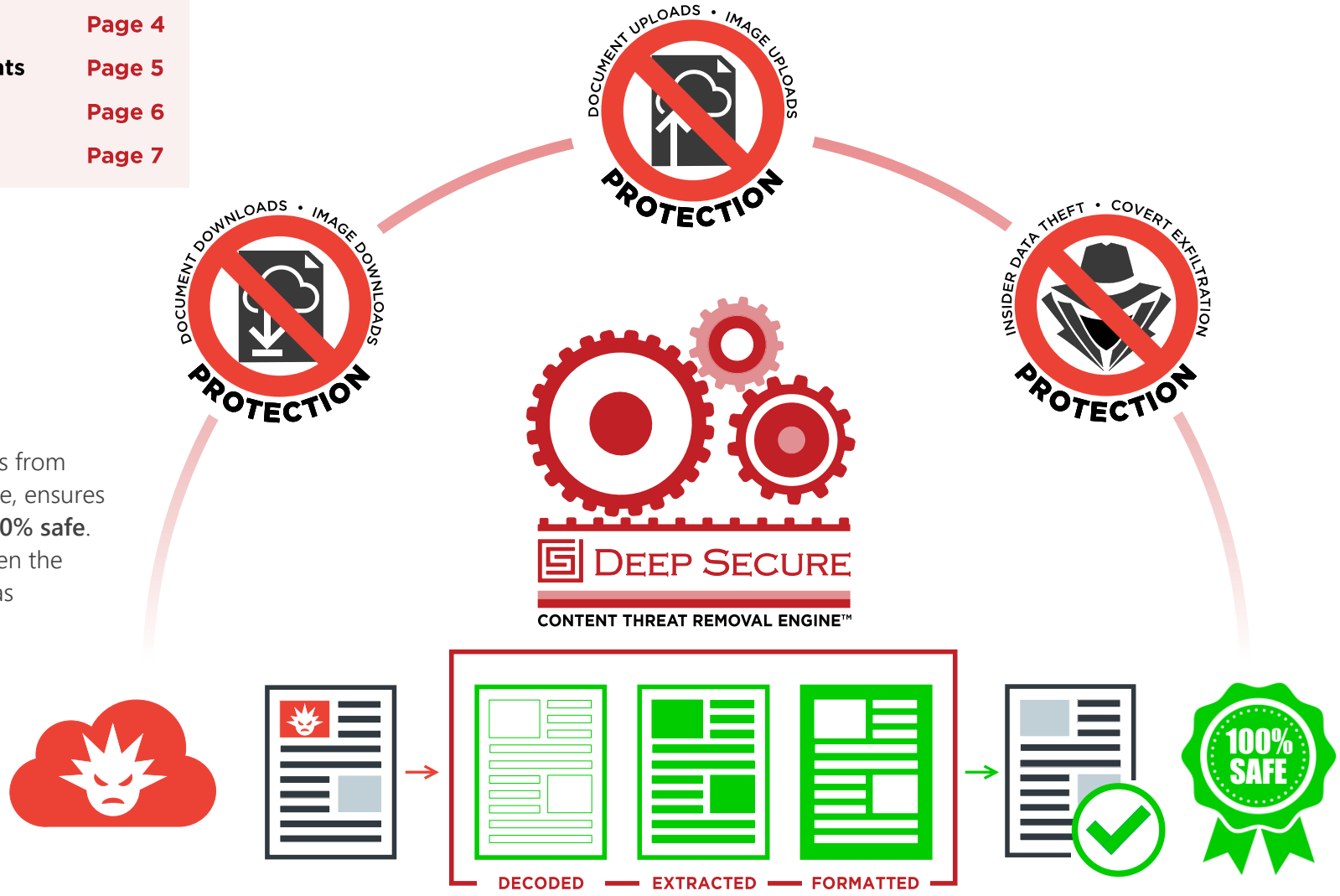
Deep Secure operates at scale, delivers **100% safe documents and images**, requires no endpoint agent software, and does not impact the user experience. We are trusted by many of the world's most targeted military, government and commercial organisations to provide protection against even the most advanced document and image-based cyber threats.

2 Deep Secure Business Use Cases

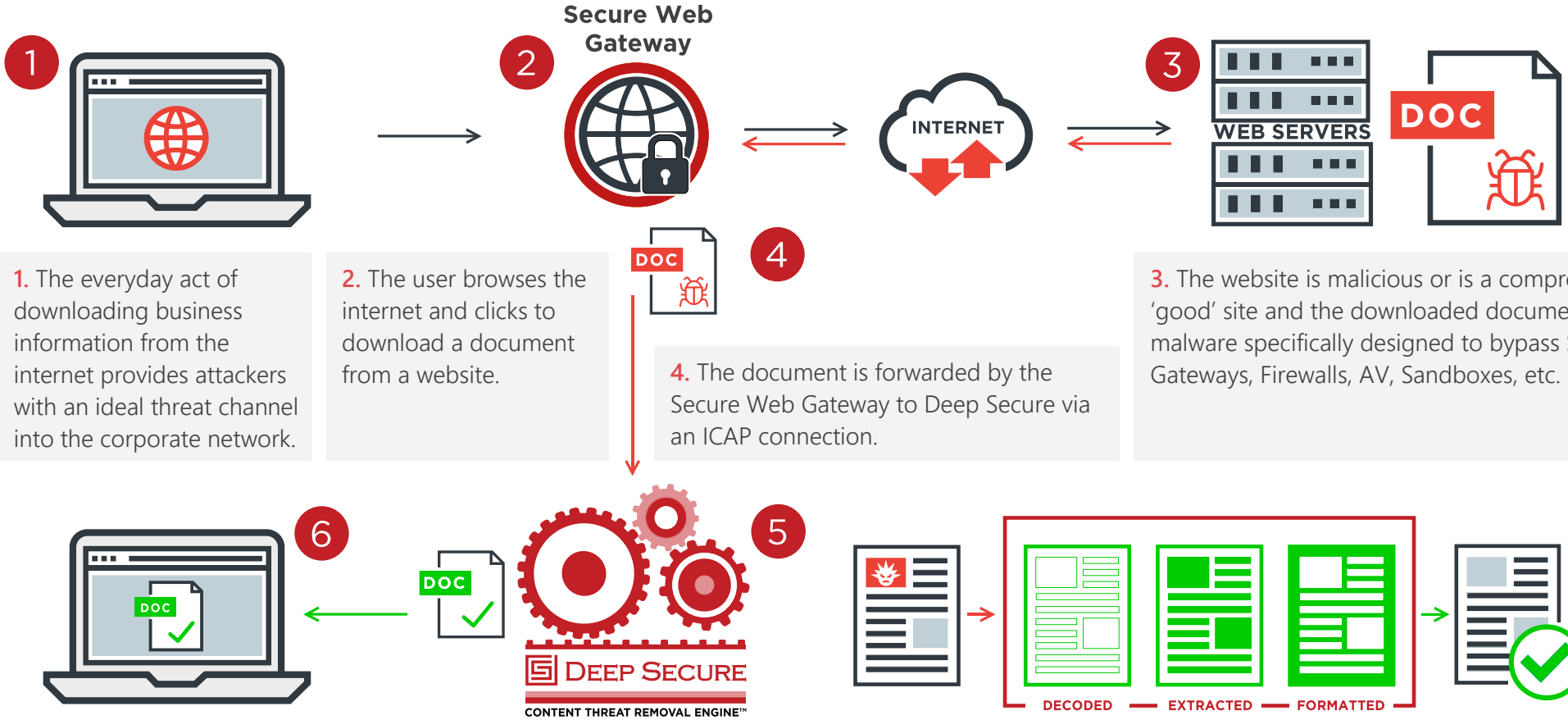
The following sections of this document outline a number of key business use cases for the Deep Secure Content Threat Removal technology.

Key Business Use Cases include:

By transforming documents and images from untrusted external sources, Deep Secure, ensures all downloaded/uploaded content is **100% safe**. Our unique CTR technology defeats even the most advanced malware attacks, such as polymorphic, zero day, stegware, etc.



3 Business Use Case: File Download



1. The everyday act of downloading business information from the internet provides attackers with an ideal threat channel into the corporate network.

2. The user browses the internet and clicks to download a document from a website.

3. The website is malicious or is a compromised 'good' site and the downloaded document contains malware specifically designed to bypass Secure Web Gateways, Firewalls, AV, Sandboxes, etc.

4. The document is forwarded by the Secure Web Gateway to Deep Secure via an ICAP connection.

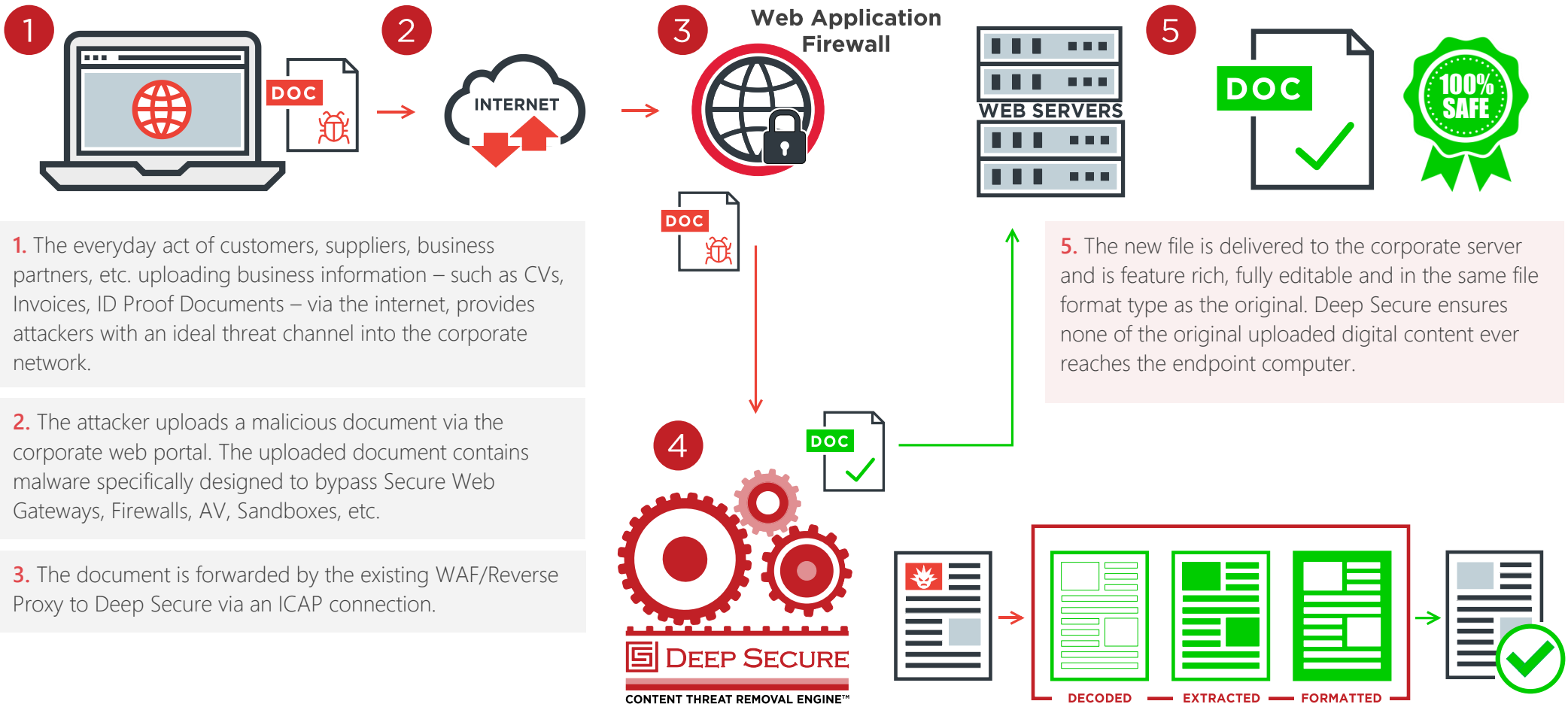
6. The file is delivered to the user and is feature-rich, fully editable, and the same file type as the original. Deep Secure ensures none of the original digital download ever reaches the endpoint computer.

5. Deep Secure Content Threat Removal receives the downloaded document. 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, unnecessary metadata, active code or malware: alternatively, the original download can be securely stored for forensic analysis. A wholly new file is created using the extracted business information and is then formatted to match the original.

Symantec. TIPP TECHNOLOGY INTEGRATION PARTNER PROGRAM

McAfee COMPATIBLE

4 Business Use Case: File Upload



1. The everyday act of customers, suppliers, business partners, etc. uploading business information – such as CVs, Invoices, ID Proof Documents – via the internet, provides attackers with an ideal threat channel into the corporate network.

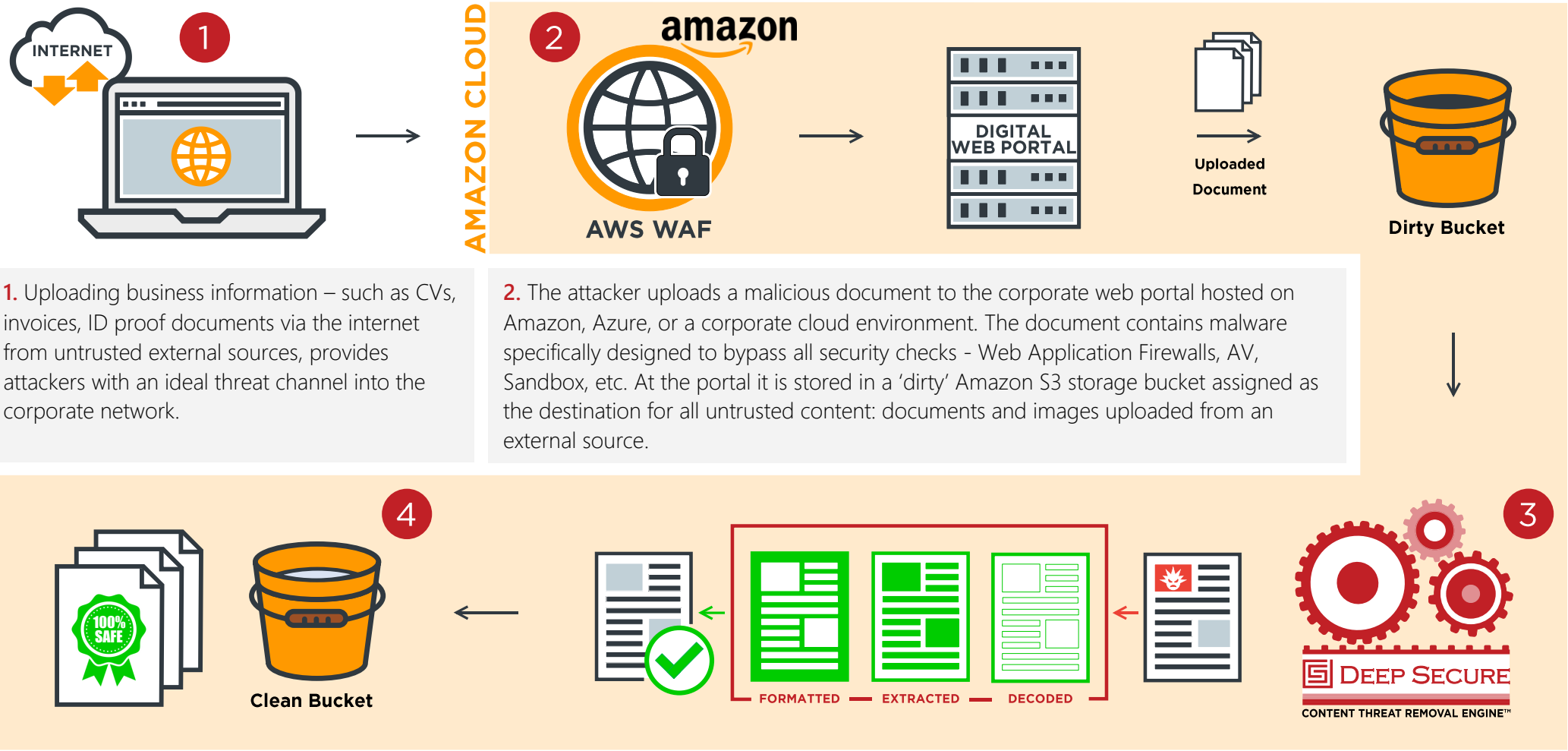
2. The attacker uploads a malicious document via the corporate web portal. The uploaded document contains malware specifically designed to bypass Secure Web Gateways, Firewalls, AV, Sandboxes, etc.

3. The document is forwarded by the existing WAF/Reverse Proxy to Deep Secure via an ICAP connection.

5. The new file is delivered to the corporate server and is feature rich, fully editable and in the same file format type as the original. Deep Secure ensures none of the original uploaded digital content ever reaches the endpoint computer.

4. Deep Secure Content Threat Removal receives the downloaded document. 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, unnecessary metadata, active code or malware. Alternatively, the original download can be securely stored for forensic analysis. The extracted business information is then formatted to match the original. A wholly new file is created, populated with the valid business information.

5 Business Use Case: File Upload for Cloud Environments



1. Uploading business information – such as CVs, invoices, ID proof documents via the internet from untrusted external sources, provides attackers with an ideal threat channel into the corporate network.

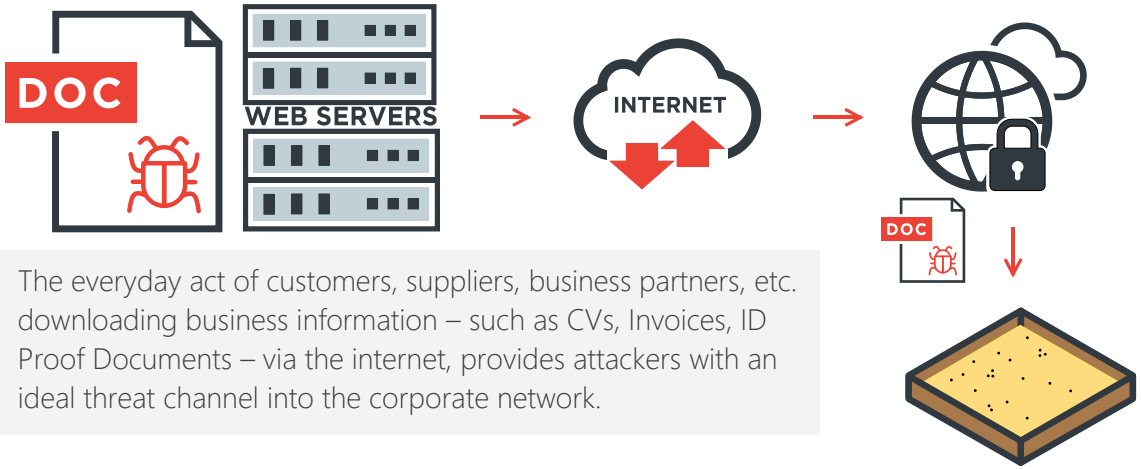
2. The attacker uploads a malicious document to the corporate web portal hosted on Amazon, Azure, or a corporate cloud environment. The document contains malware specifically designed to bypass all security checks - Web Application Firewalls, AV, Sandbox, etc. At the portal it is stored in a 'dirty' Amazon S3 storage bucket assigned as the destination for all untrusted content: documents and images uploaded from an external source.

4. The transformed file can be accessed from the 'clean' S3 storage bucket. The document is **100% safe**, feature-rich, fully editable and in the same file format type as the original.

3. Deep Secure Content Threat Removal receives the uploaded document. The content is decoded and just the valid business information is extracted from it. The extracted business information is then formatted to match the original. A wholly new file is created, populated with the valid business information, and forwarded to a 'clean' Amazon S3 storage bucket.

6 Business Use Case: Sandbox Replacement

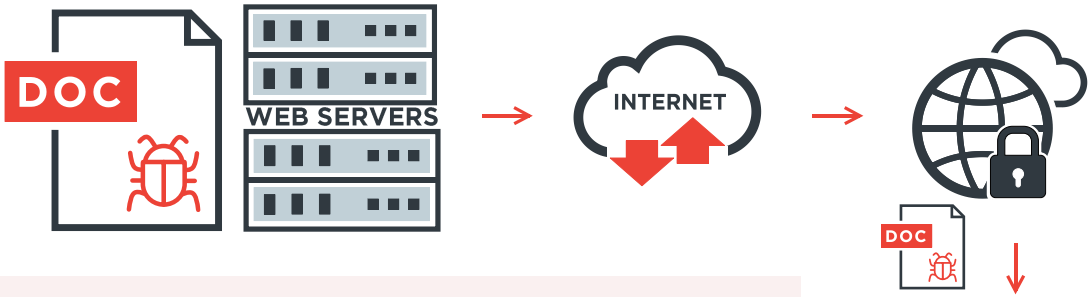
File Download Protection with Sandbox Technologies:



The everyday act of customers, suppliers, business partners, etc. downloading business information – such as CVs, Invoices, ID Proof Documents – via the internet, provides attackers with an ideal threat channel into the corporate network.

Sandbox technologies quarantine downloaded content for security analysis to determine if malware is present. However, users can experience considerable delays whilst the document goes through the sandbox process. Also, malware is often designed to evade sandboxes - making them obsolete.

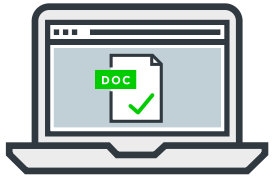
File Download Protection with Deep Secure:

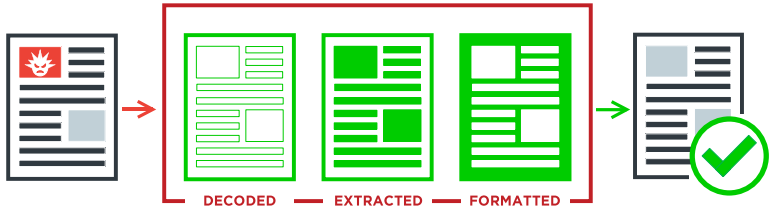


Deep Secure Content Threat Removal receives the downloaded document from the web gateway. This content is decoded and just the valid business information is extracted from it. The original file is then discarded, along with any encoding context, unnecessary metadata, active code or malware. The extracted business information is then formatted to match the original. A wholly new file is created, populated with only valid business information.

The new file is delivered to the user and is feature rich, fully editable and is the same file type as the original.

Deep Secure ensures none of the original uploaded digital content ever reaches the endpoint computer.





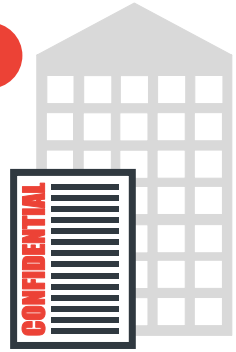
7 Business Use Case: Insider Data Theft

Insider Data Theft + Covert Exfiltration without Deep Secure protection:

1

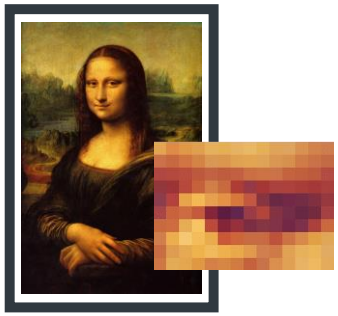
1. There are several reasons why an employee can opt to become involved with malicious insider activity, such as **financial gain** and **espionage**.

2



STOLEN CORPORATE DATA

3



STOLEN DATA ENCRYPTED IN IMAGE

4

IMAGE WITH THE DATA HIDDEN

2. The main problem for the malicious insider is how to exfiltrate the stolen data without being detected.
3. Using freely available steganography tools the stolen data is secretly encoded into another file such as an image.
4. The image containing the hidden data looks identical to the original version.

5

6

Today's most damaging security threats are originating from trusted insiders

90% of organisations feel vulnerable to Insider Attacks

CA Technologies

62% of business users have access to company data they shouldn't see

Ponemon Institute

60% of Cyber Attacks are an inside job

IBM

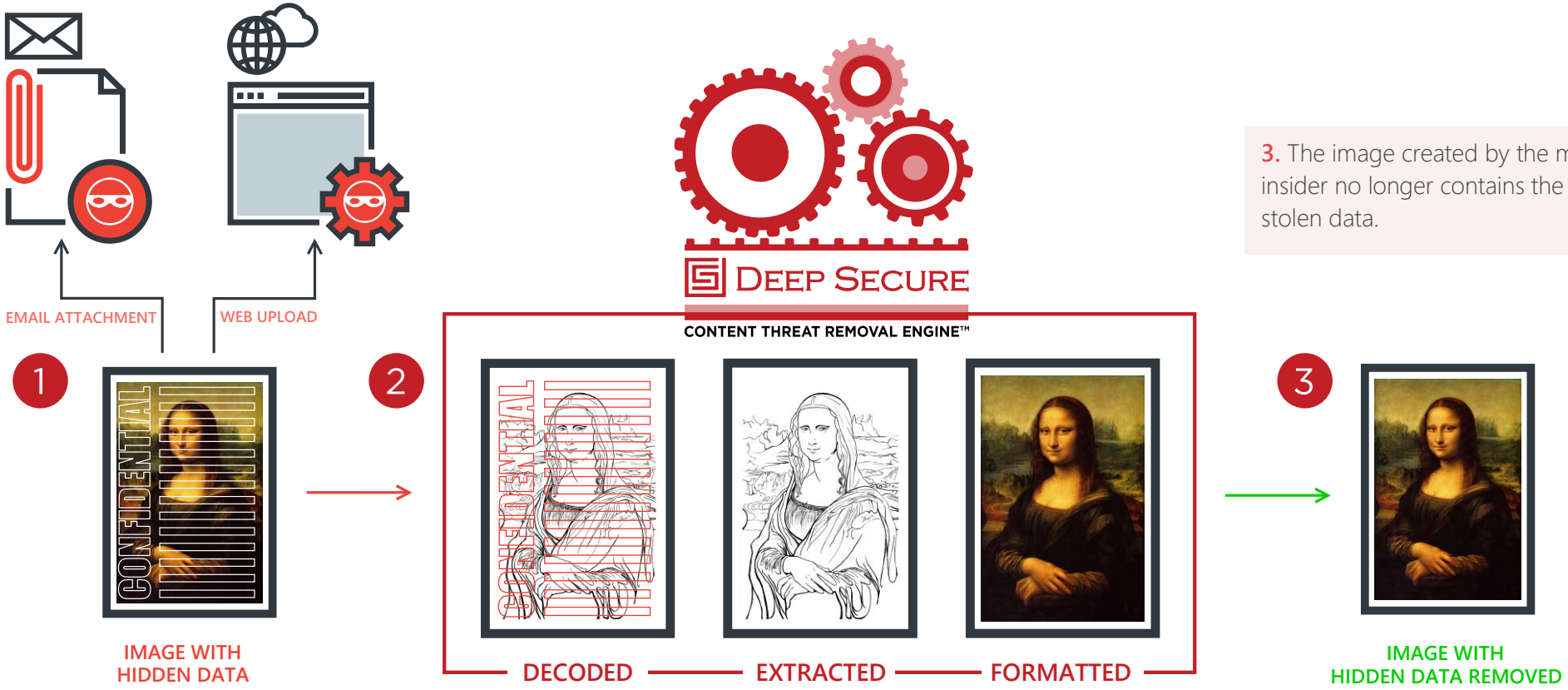
6. The email is received, and the image is downloaded. The image file is then decoded to reveal the hidden data.

The target data has been successfully stolen and covertly exfiltrated by the malicious insider.

5. The image containing the hidden data is attached to an email or uploaded on the web and sent out of the company. The stolen data hidden in the image evades all corporate security and Data Loss Prevention controls.

Business Use Case: Insider Data Theft

Insider Data Theft + Covert Exfiltration with Deep Secure protection:



3. The image created by the malicious insider no longer contains the encoded stolen data.

1. Deep Secure provides 100% effective protection against the covert exfiltration of stolen corporate data by eliminating the ability of the malicious insider to obfuscate the data by using steganography.

2. Working with the existing web gateway, **Deep Secure Content Threat Removal** receives the uploaded digital content such as documents and images. This content is decoded and any encoding context, unnecessary metadata, etc. are removed – this includes any data hidden by steganography techniques. Only the business information is retained, and this is formatted into a new document or image.

4

4. PROTECTED!
The stolen data has not been exfiltrated.

8 Contact Us

Please contact us for further information about Deep Secure:

Marc Ewin
Tel: +44 7973 883623
E-mail: marc.ewin@deep-secure.com

Visit us at: www.deep-secure.com