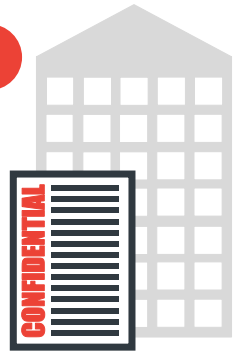
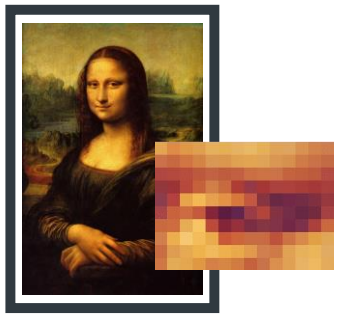
Deep Secure: Insider Data Theft Protection

Insider Data Theft + Covert Exfiltration without Deep Secure protection:

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



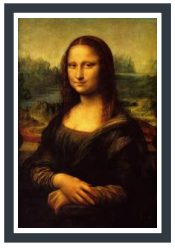
STOLEN CORPORATE DATA



STOLEN DATA ENCRYPTED IN IMAGE

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.



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.

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

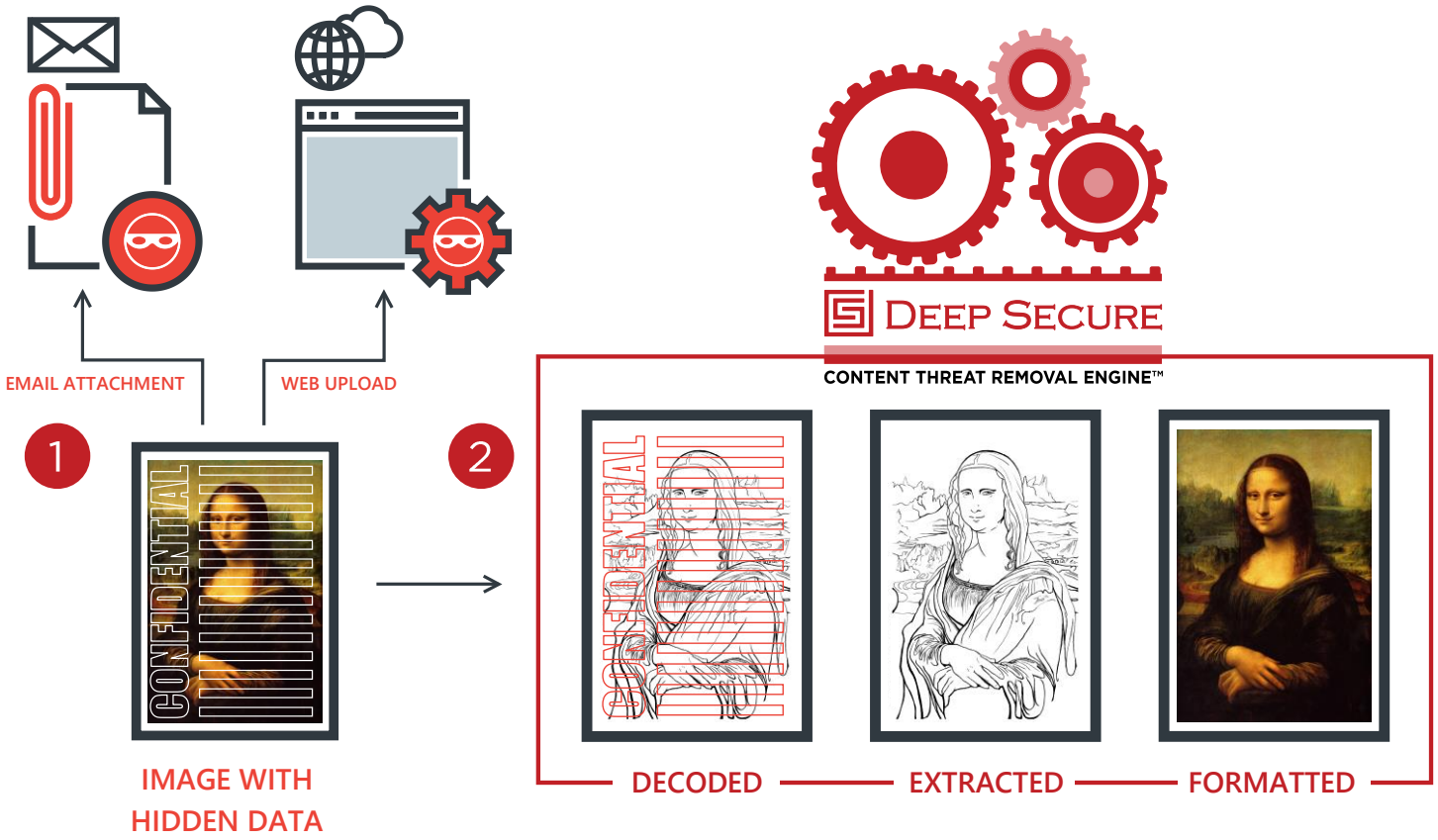
60% of Cyber Attacks are an inside job

IBM

Visit us at www.deep-secure.com or contact us e: info@deep-secure.com t: +44 (0) 203 950 5116

Deep Secure: Insider Data Theft Protection

Insider Data Theft + Covert Exfiltration with Deep Secure protection:



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 and/or email gateway, Deep Secure Content Threat Removal intercepts 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.

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

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

Visit us at www.deep-secure.com or contact us e: info@deep-secure.com t: +44 (0) 203 950 5116