

ELEVENPATHS METASHIELD FOR ICAP & FORTINET SECURITY SOLUTION

Comprehensive Protection of Information and Assets

Background

Increased storage, connectivity options and networking bandwidth enable organizations to provision web resources and deliver information content closer to the user. However, to achieve this goal, organizations are forced to expose more and more content on the Internet, causing a higher level of sensitive and confidential information leaks, which can lead to serious economic impacts and loss of trust.

Most common information leaks occur through unseen channels such as metadata and unseen document information. As described by the Reconnaissance phase of the Cyber Attack Kill Chain, this metadata information could be used by the attackers to learn more about their targets, and to carry out cyber-compromising activities, such as a social engineering attack (e.g. ransomware or spear-phishing), because metadata could provide useful information about the employees and the company's IT infrastructure.

Moreover, businesses and organizations are subject to compliance with regulations regarding the security and protection of personal information, such as the upcoming new General Data Protection Regulation (GDPR). Even metadata with no obvious identifier is considered under the GDPR's definition of personal data, and therefore they will need to prevent data breaches and leaks of sensitive information resulting from metadata.

Solution Description

The solution features ElevenPaths' Metashield for ICAP integrated with Fortinet's FortiGate enterprise firewall, and ensures that web files are properly processed, free of sensitive or confidential information that may pose a risk of leaks due to their metadata and hidden information.

Metashield for ICAP provides the constant and real-time protection needed to protect the integrity of confidential information contained as metadata in all documents and multimedia files provided under web requests, while maintaining the integrity of the internal files. Metashield is a flexible product with great operational capacity, perfect for its implementation in your organization's preventive structure integrated with your FortiGate enterprise firewall solution through the ICAP protocol, and prevents the disclosure of sensitive or confidential information.

Fortinet's award-winning FortiGate enterprise firewall platform delivers the highest levels of network security protection with unparalleled performance. FortiGate mitigates exposure to network threats while using the Fortinet security processing architecture to enable heavy content-processing features, such as SSL inspection without compromising network or application performance. The Fortinet Security Fabric uses a collaborative approach based on interoperability and is achieved by adopting industry standards such as RFC 3507. The Fortinet Security Fabric's integrated, collaborative and adaptive architecture delivers broad, powerful and automated security without compromise to address security needs.

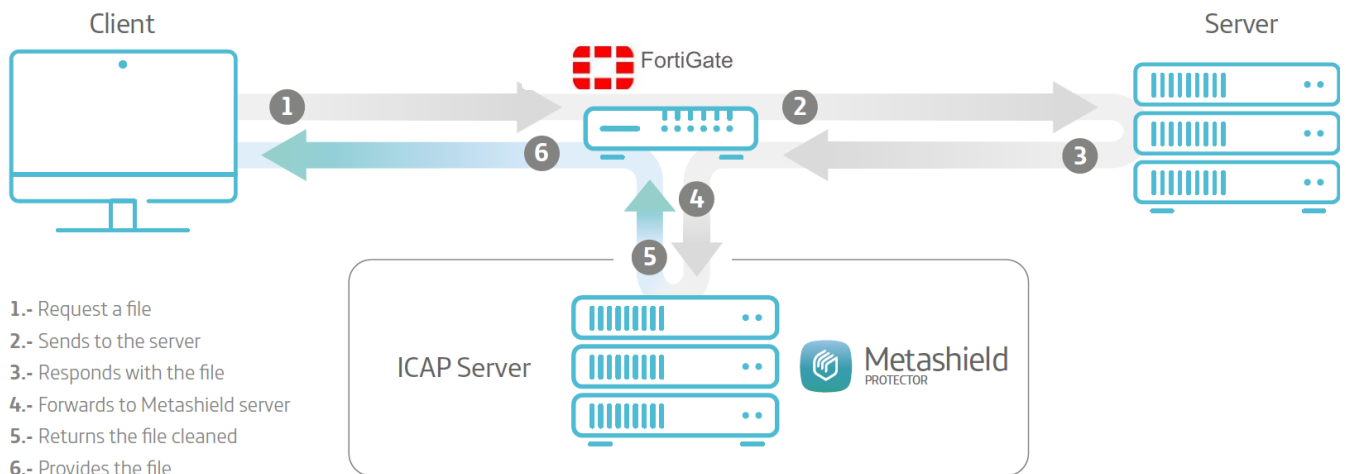
Solution Benefits

- Prevention and detection of leaks of sensitive information hidden in documents or digital files.
- Implementation of homogeneous corporate policies to prevent leaks of sensitive information data.
- Management of all hidden information associated with documents allowing control over the processing profiles and implementation on the desired extensions.
- Reduction of the economic and reputational impact resulting from the malicious use of metadata.
- Facilitation of compliance with regulations regarding the security and protection of personal information, including General Data Protection Regulation (GDPR), ENS (Spanish National Security Framework), PCI DSS, HIPAA, GLBA, SOX.

Removing metadata with Metashield for ICAP and Fortinet

By integrating ElevenPaths' Metashield for ICAP with Fortinet's FortiGate enterprise firewall, customers can easily implement homogeneous corporate policies to prevent and detect leaks of sensitive information, and reduce the economic and reputational impact resulting from the malicious use of exposed metadata.

The combined solution involving Metashield for ICAP and FortiGate is realized through the Respmod mode of the ICAP protocol, and creates the perfect secure environment for the web service, and is completely transparent to users. The functioning of the joint solution is summarized in the illustration below.



Metashield for ICAP operates on a Windows Server environment, receiving all files from the ICAP Client (FortiGate) that must be served, processing them, and then returning them to FortiGate for final delivery to the requesting user.

This innovative joint solution involving Telefónica and Fortinet products working in synergy provides differentiated value, actively works with your organization's security preventive systems and provides safer and reliable environments.

Want to find out more? Contact us: partners@elevenpaths.com | More info: partners.elevenpaths.com

About ElevenPaths

At [ElevenPaths](#), Telefónica Cyber Security Unit, we believe in the idea of challenging the current state of security, an attribute that must always be present in technology. We're always redefining the relationship between security and people, with the aim of creating innovative security products which can transform the concept of security, thus keeping us one step ahead of attackers, who are increasingly present in our digital life.

About Fortinet

At [Fortinet](#) we provide top-rated network and content security, as well as secure access products that share intelligence and work together to form a cooperative fabric. Our unique security fabric combines Security Processors, an intuitive operating system, and applied threat intelligence to give you proven security, exceptional performance, and better visibility and control--while providing easier administration.

2017 © Telefónica Digital España, S.L.U. All rights reserved.

The information disclosed in this document is the property of Telefónica Digital España, S.L.U. ("TDE") and/or any other entity within Telefónica Group and/or its licensors. TDE and/or any Telefonica Group entity or TDE'S licensors reserve all patent, copyright and other proprietary rights to this document, including all design, manufacturing, reproduction, use and sales rights thereto, except to the extent said rights are expressly granted to others. The information in this document is subject to change at any time, without notice.

Neither the whole nor any part of the information contained herein may be copied, distributed, adapted or reproduced in any material form except with the prior written consent of TDE.

This document is intended only to assist the reader in the use of the product or service described in the document. In consideration of receipt of this document, the recipient agrees to use such information for its own use and not for other use.

TDE shall not be liable for any loss or damage arising out from the use of the any information in this document or any error or omission in such information or any incorrect use of the product or service. The use of the product or service described in this document are regulated in accordance with the terms and conditions accepted by the reader.

TDE and its trademarks (or any other trademarks owned by Telefonica Group) are registered service marks.
