OPSWAT.

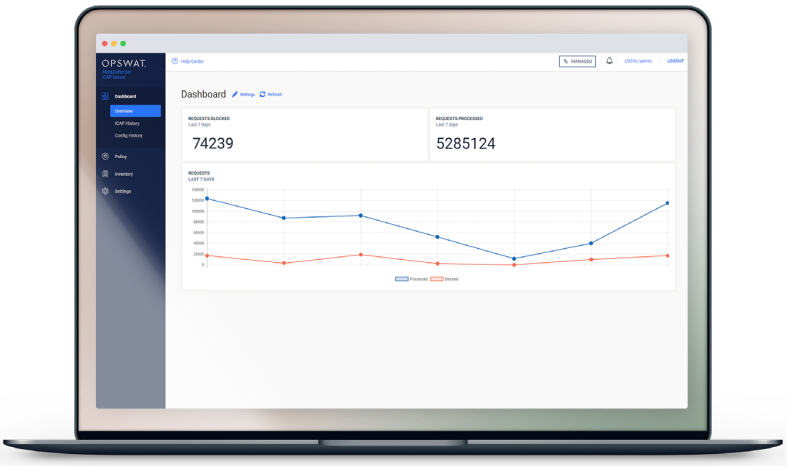
DATASHEET

MetaDefender® ICAP Server

提供網路流量所需的安全性

駭客將惡意軟體上傳到您的系統、員工不小心存取惡意網站、外部用戶傳送了含有機敏資訊的檔案。

MetaDefender ICAP Server 能強化您的網絡流量安全，同時維持既有生產力。



配置．分析．滿足需求

當客戶將文件上傳到您的網站時，會被防毒軟體掃描，但若當中夾帶未被檢測到的威脅時，該怎麼辦？如果包含非預期的機敏資訊，如身分證號碼，又該怎麼辦呢？

MetaDefender ICAP Server 可檢查每個在企業網路傳輸的檔案，以保護企業系統。每個檔案都會被掃描是否具有惡意軟體或漏洞，一旦發現可疑檔案就會加以阻擋或清洗；機敏的檔案內容則會進行遮蔽或刪除。所有檔案在被終端用戶存取前都會被校正。

MetaDefender ICAP Server 能保護您的用戶免於惡意網路內容的危害。

效益

領先業界的多防毒引擎(Multiscanning)
整合30種以上的防毒引擎

可疑檔案清洗
移除未知內容，輸出乾淨、可用的檔案

檔案為主的漏洞偵測
在漏洞攻擊進入內部環境前就先發現

避免機敏資料外洩
檢測、遮蔽或阻擋機敏資料

客製化政策和使用者權限
依據檔案來源進行工作流程和分析規則配置

OPSWAT.

MetaDefender ICAP Server

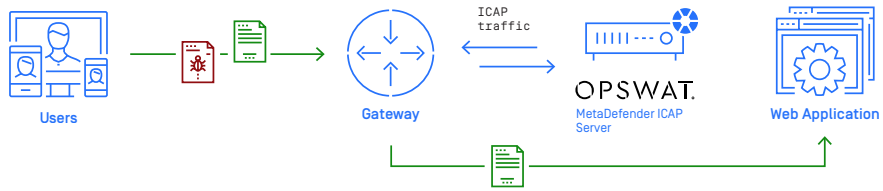
架構配置

MetaDefender ICAP Server 可與任何支援 ICAP 協定的產品整合，並能安裝在不同的網路節點以保護檔案傳輸。 例如：

反向代理/ 網路應用程式防火牆/負載平衡

保護應用程式網路伺服器免於惡意檔案上傳的危害。

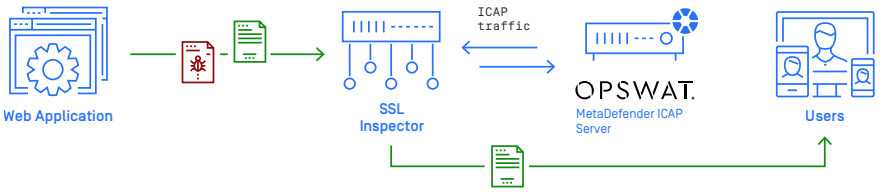
支援：*F5 Advanced WAF™, F5 Big-IP® ASM™, F5 Big-IP LTM™, Symantec BlueCoat ProxyAG™*



SSL Inspection

在解密時整合各種MetaDefender功能，以使流程更簡化便捷。

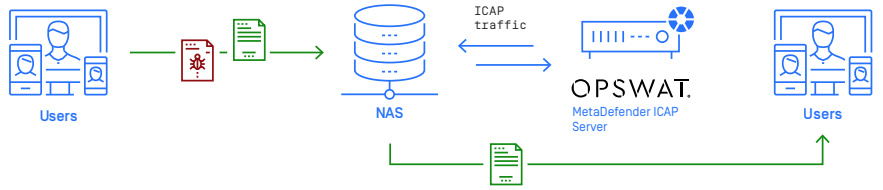
支援：*F5 SSL Orchestrator™, A10 Networks Thunder® SSLi®*



NAS網路硬碟

從NAS掃描檢索到的檔案，以避免機敏資訊或惡意軟體散佈。

支援：*Dell EMC® Isilon*



轉發代理(Forward Proxy)/網路閘道(Web Gateway)/防火牆

在網路流量傳送到安全網路前加以防護。

支援：*Squid, ARA Networks JAGUAR5000, McAfee Web Gateway™, Fortinet FortiGate®*

技術規格

支援作業系統

- **Windows**
  Windows 7, 10, Server 2012, Server 2016, Server 2019
- **Linux**
  Red Hat (6.6+, 7.0+), Ubuntu (16.04, 18.04), CentOS (6.6+, 7.0+), Debian (8.0+, 9.0+)

硬體需求

最小RAM: 2GB,
最小HDD 空間: 20GB

支援瀏覽器

Chrome, Firefox, Safari,
Microsoft Edge, Internet Explorer 11

Ports

Inbound (1344, 8048),
Outbound (8008)

支援檔案系統

NTFS, FAT32, AFS, Linux EXT2, 3 & 4

部屬方式

Online/Offline、實體/虛擬

OPSWAT.
Trust no file. Trust no device.