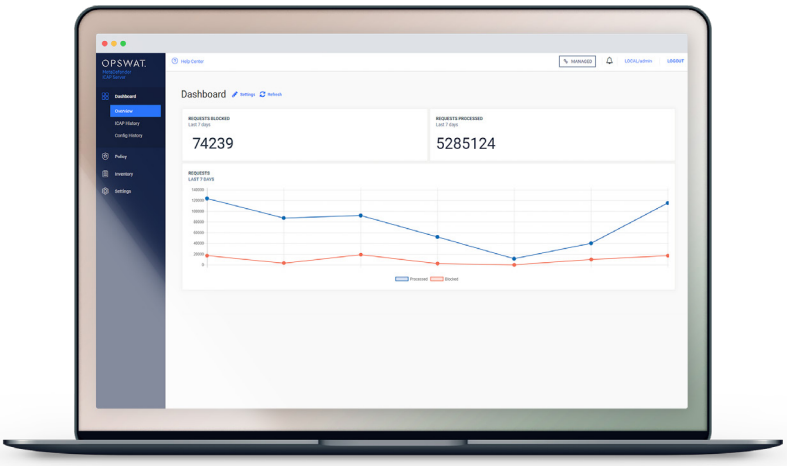
OPSWAT.

DATASHEET

MetaDefender® ICAP Server

Vertrauen Sie Ihrem Netzwerk-Traffic



Hacker versuchen ohne jegliche Rücksicht, Malware in Ihre Systeme einzuschleusen. Mitarbeiter besuchen versehentlich bösartige Websites. Externe Benutzer übermitteln Dateien mit vertraulichen Informationen.

MetaDefender ICAP Server erhöht die Sicherheit Ihres Netzwerkverkehrs und sorgt gleichzeitig dafür, dass die Produktivität erhalten bleibt.

Konfigurieren. Analysieren. Schützen.

Wenn ein Kunde eine Datei auf Ihre Website hochlädt, wird sie von einer Anti-Virus-Software gescannt. Was aber passiert, wenn die Datei eine unentdeckte Bedrohung enthält? Was, wenn sie unerwartet sensible Informationen enthält – beispielsweise eine Sozialversicherungsnummer oder andere personenbezogene Daten?

MetaDefender ICAP Server schützt Ihre Systeme, indem jede Datei, die sich in Ihrem Netzwerk bewegt, genau untersucht wird. Jede Datei wird dabei auf Malware und mögliche Schwachstellen gescannt. Verdächtige Dateien können blockiert oder gesäubert werden. Sensible Dateien können zensiert werden. Dateien werden korrigiert, bevor Anwender darauf zugreifen können.

MetaDefender ICAP Server schützt Ihre Anwender vor gefährlichen Inhalten aus dem Internet.

Vorteile

Branchenführende Multiscanning-Lösung
Integrierter Multiscanner mit über 30 Scan-Engines

Verdächtige Dateien säubern
Unbekannte Inhalte werden deaktiviert und saubere, sicher nutzbare Dateien ausgegeben

Datei-basierte Schwachstellenbewertung
Findet Exploits, bevor diese Ihre Umgebung erreichen

Verhindern Sie den Verlust sensibler Daten
Erkennen, entfernen oder blockieren von sensiblen Daten

Individuell anpassbare Richtlinien und Rollen
Konfigurieren von Workflow- und Analyseregeln, basierend auf der Dateiquelle

OPSWAT.

MetaDefender ICAP Server

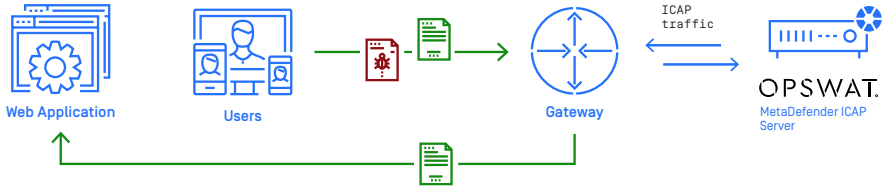
Konfigurationen

MetaDefender ICAP Server lässt sich in jedes Produkt integrieren, das das Internet Content Adaptation Protocol (ICAP) unterstützt. Die Lösung kann an verschiedenen Schnittstellen installiert werden, um die Dateiübertragung abzusichern. Zum Beispiel:

Reverse Proxy / Web Application Firewall / Load Balancer

Schützen Sie Anwendungs-Webserver vor böswilligen Datei-Uploads.

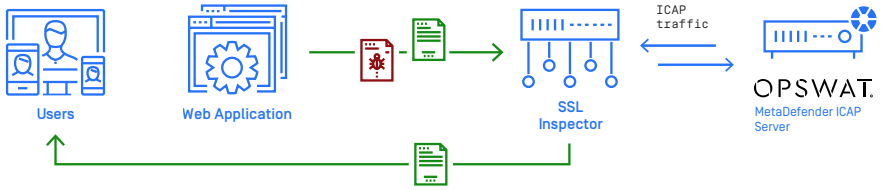
Unterstützt: *F5 Advanced WAF™, F5 Big-IP® ASM™, F5 Big-IP LTM™, Symantec BlueCoat ProxyAG™*



SSL-Prüfung

Integrieren Sie mehrere MetaDefender-Features auf Entschlüsselungs-Ebene und sorgen Sie so für einfache, agile Prozesse.

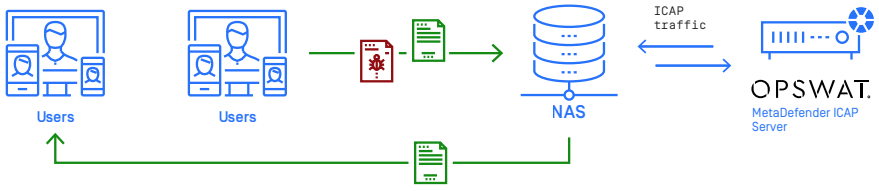
Unterstützt: *F5 SSL Orchestrator™, A10 Networks Thunder® SSLi®.*



Network Attached Storage (NAS)

Scannen Sie aus dem NAS abgerufene Dateien, um die Verbreitung von sensiblen Informationen oder Malware zu verhindern.

Unterstützt: *Dell EMC® Isilon.*



Forward Proxy / Web Gateway / Firewall

Durchleuchten Sie den Datenverkehr aus dem Web, bevor er ein abgesichertes Netzwerk erreicht.

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

Spezifikationen

Unterstützte Betriebssysteme

- **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+)

Hardware-Anforderungen

RAM (min.): 2 GB

Festplattenspeicher (min.): 20 GB

Unterstützte Browser

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

Ports

Eingehend (1344, 8048),
Ausgehend (8008)

Unterstützte Dateisysteme

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

Bereitstellungsmodell

Online/Offline, Physical/Virtual

OPSWAT.

Trust no file. Trust no device.