

Fortisolator™

Fortisolator 1000F and VM



Fortinet's Browser Isolation platform, Fortisolator, provides a next level of Advanced Threat Protection (ATP) that integrates with Fortinet's Security Fabric. It addresses the need to access shared links and web content for business purposes while maintaining the most robust internet hygiene. Specifically, Fortisolator allows web content to be accessed without the risk of user compromise by maintaining an "air-gap" between the user's browser and the web content.



Allow user access to potentially malicious content while maintaining strict security

Native integration methods allow the use of standard browsers to access potentially malicious web content without the risk of compromising the user's desktop – preventing zero-day infections.



Broad Coverage of the Attack Surface with Security Fabric

Integrated with FortiGate and FortiMail for defense against advanced targeted attacks across network, application layers and endpoint devices.

Highlights

Problem

- Zero-day malware and phishing threats delivered over the web, in email and in downloaded PDF files may result in data loss, compromise or ransomware.

Solution

- With Fortisolator, web content is executed in a remote disposable container and displayed to the user, isolating any threat.

Benefits

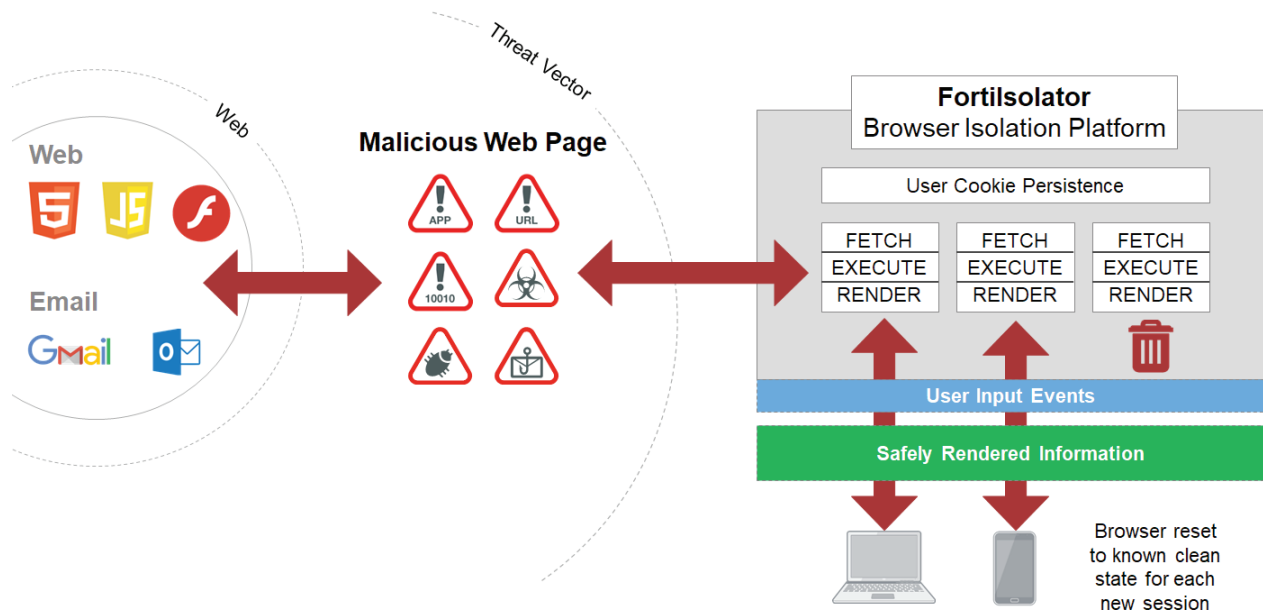
- Protects against known and unknown malware, ransomware and other zero-day threats.
- Allows users to access URLs while maintaining security and enhances productivity.

Highlights

Product Summary

Fortisolator is a clientless browser isolation solution which allows the user to access potentially malicious content using their regular browser without the risk of compromising their browser, desktop or mobile device. Fortisolator is designed to work as unobtrusively as possible, interoperating with any modern HTML5 capable browser (ie: Edge, Chrome, Safari, Firefox), meaning no requirement for any client or plugin software on the end user device.

Fortisolator prevents drive-by and watering hole attacks by accessing the potentially malicious content in a trusted execution container which is disposed of at the end of the browser session and presenting the user with a visual rendering of the web page. This rendered version of the web page can still be interacted with e.g. videos viewed, links clicked, and PDF files opened. However, the rendering process prevents any content from being able to cross over to the user's system.



Critical threat vectors

Email is the most common attack vector for malware (92.4%) and social attacks such as phishing (96%)¹ and the majority of that is delivered via web links. Steps can be taken to filter known malicious and unrated links, however, the latter may impact productivity. By combining Fortisolator with your Secure Mail

Gateway, Firewall, Secure Web Gateway or Desktop Client, you are able to allow users to access URLs while maintaining security — increasing productivity.

¹ Verizon Databreach Report 2018
https://www.verizonenterprise.com/resources/reports/rp_DBIR_2018_Report_en_xg.pdf

Specifications

FORTIISOLATOR 1000F	
Hardware Specifications	
10/100/1000 Interfaces (Copper, RJ45)	4
Storage	1x 1 TB
Form Factor	1RU
Power Supply	Single (Dual Optional)
System Specifications	
Concurrent Browser Sessions	250*
Supported Browsers	Chrome, Firefox, Microsoft Edge, Microsoft Internet Explorer, Safari, Opera
Integration Methods	Proxy, URL Rewrite, Transparent Inline
Performance (Messages/Hour) [Without queuing based on 100 KB message size]	
Concurrent browser sessions	250
Dimensions	
Height x Width x Length (inches)	1.73 x 17.24 x 22.83
Height x Width x Length (mm)	44 x 438 x 580
Weight	25 lbs (11.4 kg)
Environment	
Power Source	100–240V AC, 50–60 Hz
Maximum Current	110V/5.0A, 220V/3.0A
Maximum Power Required	117 W
Power Consumption (Average)	67 W
Heat Dissipation	398 BTU/h
Humidity	5–90% non-condensing
Operating Temperature	32–104°F (0–40°C)
Storage Temperature	-40–158°F (-40–70°C)
Compliance	
	FCC Part 15 Class A, C-Tick, VCCI, CE, UL/cUL, CB, BSMI, RoHS

* 20% of the sessions are video sessions

FORTIISOLATOR-VM	
Technical Specifications	
Hypervisors Supported	VMWare 6.0/6.5 KVM QEMU version 0.12.1 and higher
Maximum Virtual CPUs Supported	Unlimited
Virtual NICs Required (Minimum / Maximum)	3 / 3
Virtual Machine Storage Required (Minimum / Maximum)	500 MB / 4 TB
Virtual Machine Memory Required (Minimum / Maximum)	8 GB / 128 GB
System Specifications	
Concurrent Browser Sessions	Base VM license includes 2 concurrent sessions for testing. Fortisolator Security Protection Concurrent session licenses can be purchased on annual subscription basis in blocks of 50 sessions.
Supported Browsers	Chrome, Firefox, Microsoft Edge, Microsoft Internet Explorer, Safari, Opera
Integration Methods	Proxy, URL Rewrite, Transparent Inline

Order Information

Product	SKU	Description
Fortisolator 1000F	FIS-1000F	Browser Isolation appliance — 4x GE RJ45 ports, 1 TB storage.
Fortisolator-VM	LIC-FIS-VM	Fortisolator-VM Software virtual appliance designed for VMWare ESXi platforms.
Fortisolator Security Protection — 50 Concurrent Session License	FC-10-FISVM-624-02-DD	Fortisolator Security Protection — Includes Web Isolation, Web Filtering, AV with 24x7 support. 50 concurrent session license (minimum order 1 and up to 1,000).
Accessories		
Power Supply for FIS-1000F	SP-FSA1000F-PS	Additional AC power supply for FIS-1000F.



www.fortinet.com

Copyright © 2019 Fortinet, Inc. All rights reserved. Fortinet®, FortiGate®, FortiCare® and FortiGuard®, and certain other marks are registered trademarks of Fortinet, Inc., and other Fortinet names herein may also be registered and/or common law trademarks of Fortinet. All other product or company names may be trademarks of their respective owners. Performance and other metrics contained herein were attained in internal lab tests under ideal conditions, and actual performance and other results may vary. Network variables, different network environments and other conditions may affect performance results. Nothing herein represents any binding commitment by Fortinet, and Fortinet disclaims all warranties, whether express or implied, except to the extent Fortinet enters a binding written contract, signed by Fortinet's General Counsel, with a purchaser that expressly warrants that the identified product will perform according to certain expressly-identified performance metrics and, in such event, only the specific performance metrics expressly identified in such binding written contract shall be binding on Fortinet. For absolute clarity, any such warranty will be limited to performance in the same ideal conditions as in Fortinet's internal lab tests. Fortinet disclaims in full any covenants, representations, and guarantees pursuant hereto, whether express or implied. Fortinet reserves the right to change, modify, transfer, or otherwise revise this publication without notice, and the most current version of the publication shall be applicable. Fortinet disclaims in full any covenants, representations, and guarantees pursuant hereto, whether express or implied. Fortinet reserves the right to change, modify, transfer, or otherwise revise this publication without notice, and the most current version of the publication shall be applicable.