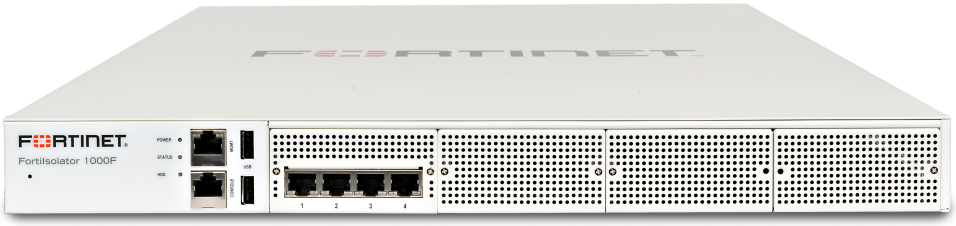
DATA SHEET

FortiIsolator™

Available in:

Appliance Virtual Machine

Advanced Threat Protection



Fortinet's Browser Isolation platform, FortiIsolator, 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, FortiIsolator 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.

Provide broad coverage of the attack surface with Security Fabric

Integrated with FortiGate, FortiProxy, 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 FortiIsolator, 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 enhancing productivity

FEATURE HIGHLIGHTS

Product Summary

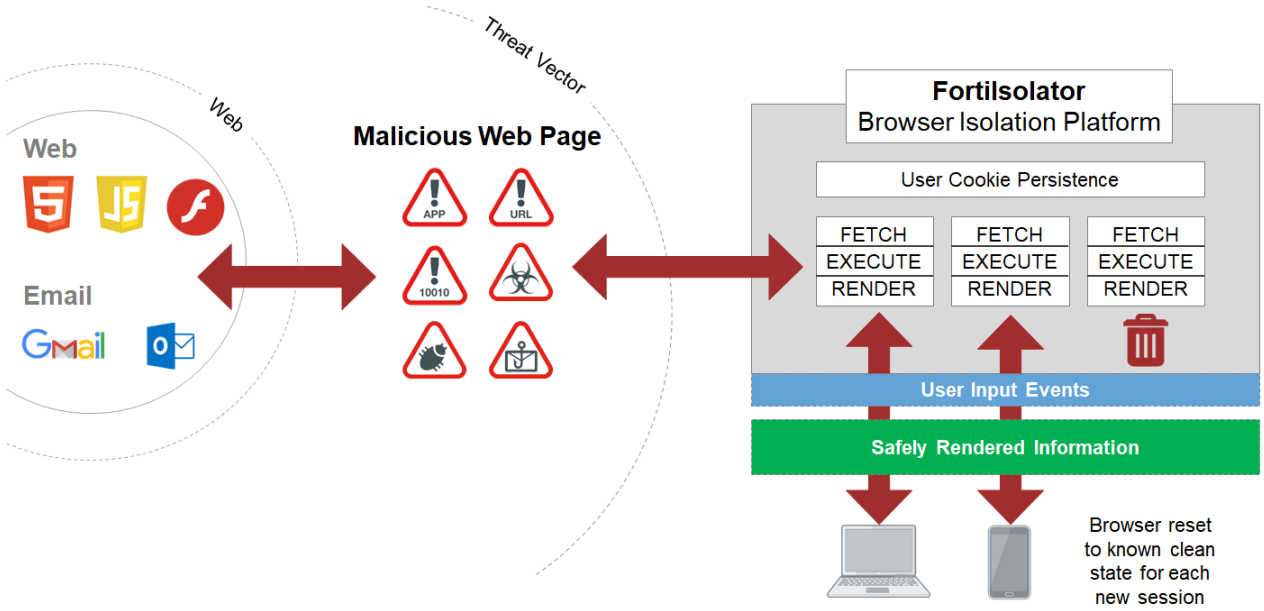
FortiIsolator is a clientless browser isolation solution that allows the user to access potentially malicious content using their regular browser without the risk of compromising their browser, desktop or mobile device. FortiIsolator is designed to work as unobtrusively as possible, interoperating with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

FortiIsolator prevents drive-by and watering hole attacks by accessing the potentially malicious content in a trusted execution container that 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%) and the majority of which is delivered via web links. Steps can be taken to filter known malicious and unrated links, however, the latter may impact productivity. By combining FortiIsolator 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	1× 1 TB
Form Factor	1RU
Power Supply	Single (Dual Optional)
System Specifications	
Concurrent Browser Sessions	250*
Supported Browsers	Chrome, Firefox, Microsoft Edge, Safari, Opera
Integration Methods	Proxy, IP forwarding, URL rewrite
Performance (Messages/Hour) [Without queuing based on 100 KB message size]	
Concurrent browser sessions	250
Dimensions	
Height x Width x Length (inches)	1.73 × 17.24 × 22.83
Height x Width x Length (mm)	44 × 438 × 580
Weight	22 lbs (9.98 kg)
Environment	
Power Source	100–240V AC, 50–60 Hz
Maximum Current	100V/5.0A, 240V/3.0A
Maximum Power Required	117 W
Power Consumption (Average)	67 W
Heat Dissipation	423.77 BTU/h
Humidity	5%–90% non-condensing
Operating Temperature	32°–104°F (0°–40°C)
Storage Temperature	-4°–158°F (-20°–70°C)
Compliance	
	FCC Part 15 Class A, RCM, VCCI, CE, UL/cUL, CB, BSMI, RoHS

* 20% of the sessions are video sessions

	FORTIISOLATOR-VM
Technical Specifications	
Hypervisors Supported	VMware vSphere Hypervisor ESX/ESXi versions 6.0 and 6.5 KVM QEMU version 0.12.1 and higher Hyper-V Manager version 10.0.18362.1 and higher
Minimum / Maximum Virtual CPUs Supported	8 / Unlimited
Virtual NICs Required (Minimum / Maximum)	4 / 4
Virtual Machine Storage Required (Minimum /Maximum)	20 GB / Unlimited
Virtual Machine Memory Required (Minimum /Maximum)	24 GB / Unlimited
System Specifications	
Concurrent Browser Sessions	Base VM license includes five concurrent sessions for testing. FortiIsolator Security Protection Concurrent session licenses can be purchased on annual subscription basis in blocks of 50 sessions.
Supported Browsers	Chrome, Firefox, Microsoft Edge, Safari, Opera
Integration Methods	Proxy, IP forwarding, URL rewrite

ORDER INFORMATION

Product	SKU	Description
FortiIsolator 1000F	FIS-1000F	Browser Isolation appliance — 4x GE RJ45 ports, 1 TB storage.
FortiIsolator-VM	LIC-FIS-VM	FortiIsolator-VM Software virtual appliance designed for VMWare ESXi platforms.
FortiIsolator Security Protection — 50 Concurrent Session License	FC-10-FISVM-624-02-DD	FortiIsolator Security Protection — Includes Web Isolation, Web Filtering, AV with 24×7 support. 50 concurrent session license (minimum order 1 and up to 20 per virtual appliance).
Accessories		
Power Supply for FIS-1000F	SP-FSA1000F-PS	Additional AC power supply for FIS-1000F.

FORTINET

www.fortinet.com