

**SOLUTION BRIEF**

# Carbon Black Enterprise Protection for Fortinet FortiSandbox

**Together, Fortinet and Carbon Black Provide Customers With Highly Effective, Automated Protection Against Advanced Threats and Previously Unknown Malware**

## Accelerate Incident Response

The integration of the Cb Enterprise Protection within Fortinet Advanced Threat Protection increases efficiency and response time to previously unknown threats—reducing the risk of lost data and business continuity—by prioritizing high risk alerts while filtering out non-actionable events. Specifically, when Fortinet FortiSandbox detects previously unknown malware on the network (in sniffer, on-demand, or integrated mode together with FortiGate, FortiMail, FortiWeb, or FortiClient), Cb Enterprise Protection automatically confirms the location, scope, and severity of the threat on endpoints and servers. It can also be configured to take immediate automated or operator-assisted response actions.

## Verify All Files Entering the Environment

At the same time, as new files arrive on endpoints and servers, Cb Enterprise Protection can automatically submit these files to Fortinet FortiSandbox to determine their risk. Based on the granular FortiSandbox ratings (malicious, high/medium/low risk, or clean), Cb Enterprise Protection can automatically take action to allow, monitor, or stop the file from running, and prevent it from spreading to additional endpoints and servers as necessary. Integrating Cb Enterprise Protection with Fortinet Advanced Threat Protection helps organizations close security gaps inherent within multivendor security infrastructures, reduce the operational effort of such heterogeneous infrastructures, reduce incident response time and effort, and improve their overall security postures.

## Joint Solution Components

- Fortinet FortiSandbox, Advanced Threat Protection (ATP), FortiGate, FortiMail, FortiWeb, FortiClient
- Carbon Black Enterprise Edition

**Integrating Carbon Black Enterprise Protection with Fortinet FortiSandbox delivers a certified and independently top-rated advanced threat protection solution from the network edge through endpoints and servers.**

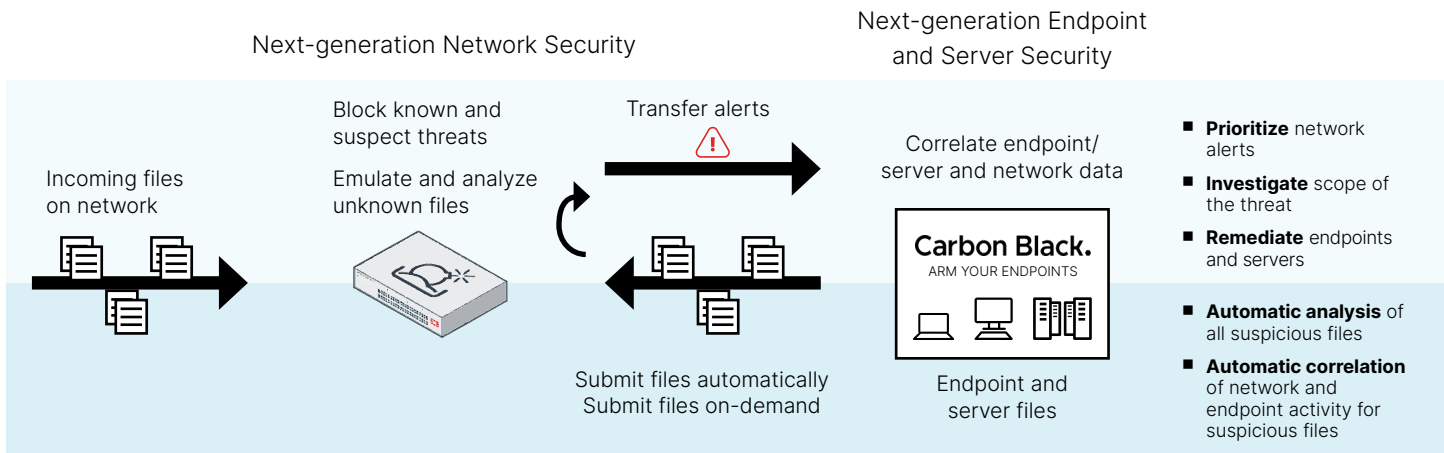


Figure 1: Carbon Black CB Enterprise Protection process diagram.

## Carbon Black Enterprise Edition

The Cb Enterprise Protection continuously monitors and records all activity on servers and endpoints to detect and stop cyber threats that evade traditional security defenses. It can identify new, apparently benign, files for additional inspection by Fortinet FortiSandbox in order to uncover the most sophisticated attacks.

### CB Enterprise Protection

- The industry’s **only real-time endpoint sensor and recorder** provides real-time and historical data for every server and endpoint. Organizations get a central repository of real-time data readily available without any scanning or polling.
- **Policy-driven trust-based security** allows organizations to define trusted software and deny everything else by default.
- A complete **inventory of files** that exist in an organization’s environment for instant file retrieval from any endpoint or server for submission to Fortinet FortiSandbox. Or the files can be removed based on FortiSandbox intelligence.

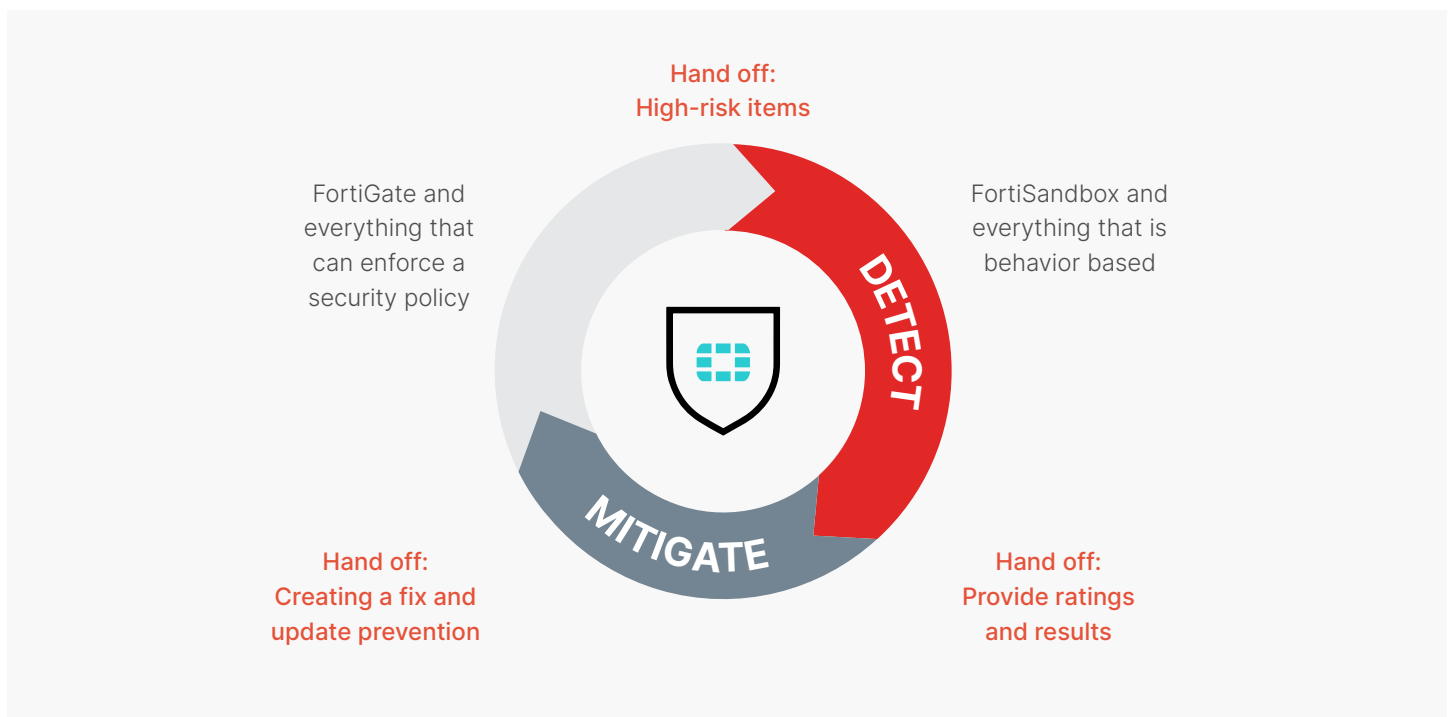


Figure 2: FortiGuard teams, Fortinet partners, and automation.

## Fortinet Advanced Threat Protection

Fortinet Advanced Threat Protection (ATP) delivers integrated and automated threat prevention, detection, and mitigation throughout the entire organization and across the full attack life cycle.

Comprised of independently top-rated components for network, email, web application, and endpoint security as well as sandboxing, Fortinet Advanced Threat Protection covers all attack vectors and seamlessly shares information for an efficient as well as effective defense against advanced threats. Together with Carbon Black, it also hardens endpoint devices/servers while offering richer forensics and faster remediation.

## **This Powerful Combination of Endpoint/Server and Network Security Solves Four Key Security Challenges**

### **Analyze**

Automatic Analysis: **When files arrive on my endpoints and servers, how do I know which ones are malicious and need to be stopped?**

Use Cb Enterprise Protection to automatically submit all new files arriving on your endpoints and servers to Fortinet's dual-level sandbox to quickly determine the risk of each file and whether it needs to be stopped. Use criteria-driven rules to determine which files to submit.

### **Prioritize**

**I am receiving alerts. How do I prioritize them?**

Cb Enterprise Protection automatically correlates granular risk-based alerts from Fortinet FortiSandbox with Carbon Black's real-time endpoint sensor and recorder data to determine which are most actionable and prioritize them based on the number of systems infected. Quickly decide if an alert requires escalation.

### **Investigate**

**Is there a real threat and what is the scope?**

Locate every instance of a suspicious file across your endpoints and servers to accelerate incident response. Find out where a file landed, if it executed, how many machines it is affecting, and if you need to take further action.

### **Remediate**

**How do I stop the attack and prevent it from happening again?**

Automatically enforce endpoint and server security policies based on intelligence. Immediately stop malicious software from spreading throughout your enterprise and prevent it from affecting your machines again.



[www.fortinet.com](http://www.fortinet.com)

Copyright © 2021 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.