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

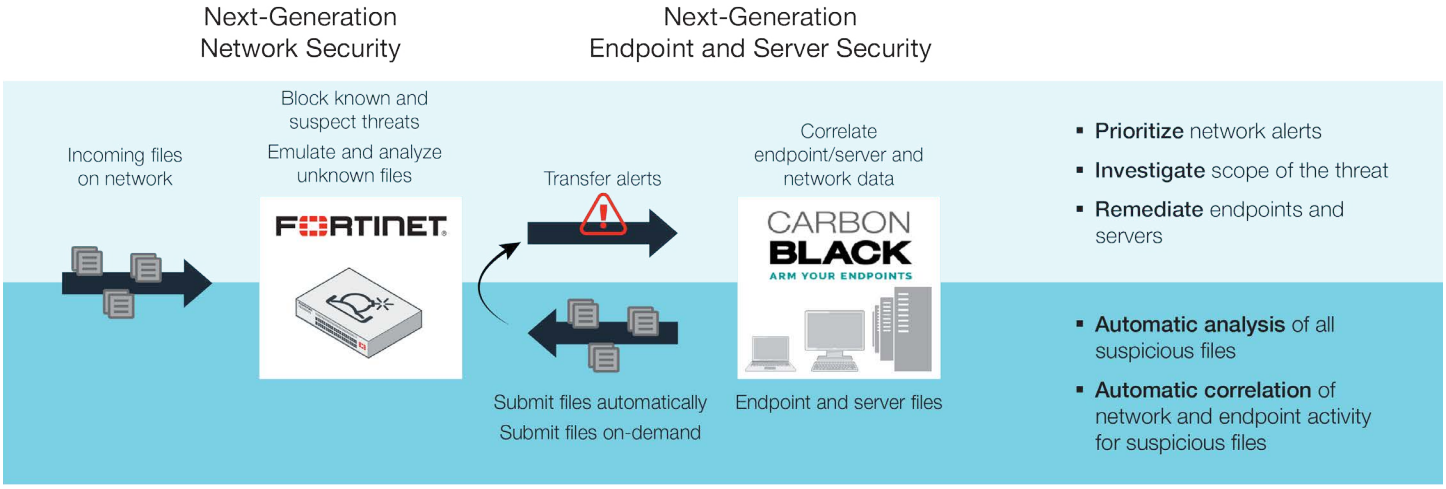
The integration of the Cb Enterprise Protection within Fortinet Advanced Threat Protection increases efficiency and response time to previously unknown threats – reducing the risk of lost data and business continuity – by prioritizing high risk alerts while filtering out non-actionable events. Specifically, 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 your endpoints and servers. It can also be configured to take immediate automated or operator-assisted response actions.

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.

FORTINET Fabric-Ready

Verify All Files Entering Your 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 multi-vendor security infrastructures, reduce the operational effort of such heterogeneous infrastructures, reduce incident response time and effort, and improve their overall security postures.



Carbon Black Enterprise Edition

The Cb Enterprise Protection continuously monitors and records all activity on servers and endpoints to detect and stop cyberthreats 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** that provides real-time and historical data for every server and endpoint. You'll have a central repository of real-time data available at your fingertips without any scanning or polling.
- **Policy-driven trust-based security** allows you to define the software you trust in your environment and deny everything else by default.
- A complete **inventory of files** that exist in your environment so you can instantly retrieve files from any endpoint or server- to submit to Fortinet FortiSandbox or remove based on FortiSandbox intelligence.

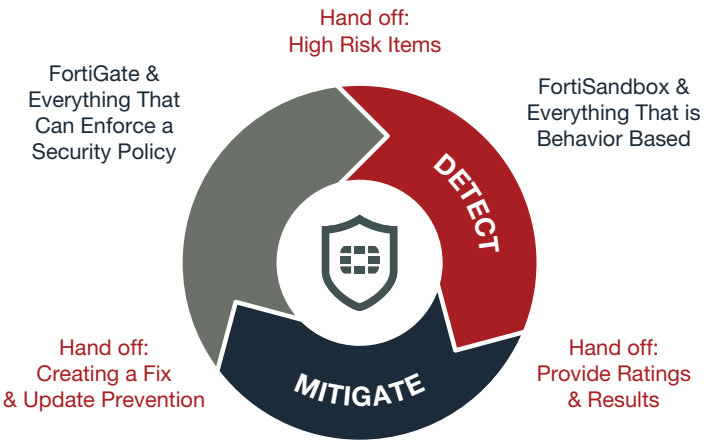


Figure 2: FortiGuard teams, Fortinet partners and automation.

Fortinet Advanced Threat Protection

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

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 riskbased 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 yourendpoints 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.

FORTINET

www.fortinet.com

June 8, 2019 4:53 AM

D:\Fortinet\Solution Brief\TEAL SB\Fortinet CB Enterprise\FA - SB - CB Enterprise Protection

429119-A-0-EN