SOLUTION BRIEF

Fortinet and Smart Hive Integrated Defense

Learn from others in less than 90 seconds. An attack on one is defense for all.

Executive Summary

Despite spending billions of dollars on cybersecurity every year, the cost of cyber breaches keeps going up. Threat actors are honing their craft at an accelerated rate, and one of the key advantages they have is the ability to collaborate and learn from each other. Vulnerabilities are bought and sold on the dark web daily. Threat actors pay premium dollar for these vulnerabilities because they know they will be able to use them against hundreds of customers, and in some cases, such as recent ransomware attacks, tens of thousands of customers. Threat actors are well aware that once organizations identify and stop an attack, they will move on to the next threat. Organizations will not stop to tell others what they did, thus giving the threat actors a massive advantage.

The Smart Hive HIVE solution enables customers to be able to, in an anonymized manner, identify an attack stopped by others, and put up defenses before the attack gets to them. This significantly narrows the window of opportunity for the threat actors and takes away their key advantage.

Joint Solution Components

- Fortinet Security Fabric with FortiGate next-generation firewall
- Smart Hive HIVE

Joint Solution Benefits

- Learn from others in real time
- Stop attacks before they show up
- Benchmark against peers
- Leverage Fortinet global threat intelligence
- Automate remediation

Joint Solution Description

The Fortinet Security Fabric has an open architecture designed to connect traditionally disparate security solutions into a unified framework, allowing them to dynamically adapt to evolving IT infrastructure in order to defend its rapidly changing attack surface. Fortinet's open approach extends the broad visibility, integrated threat detection, and automated response of its Security Fabric architecture to leading technology alliance solutions.

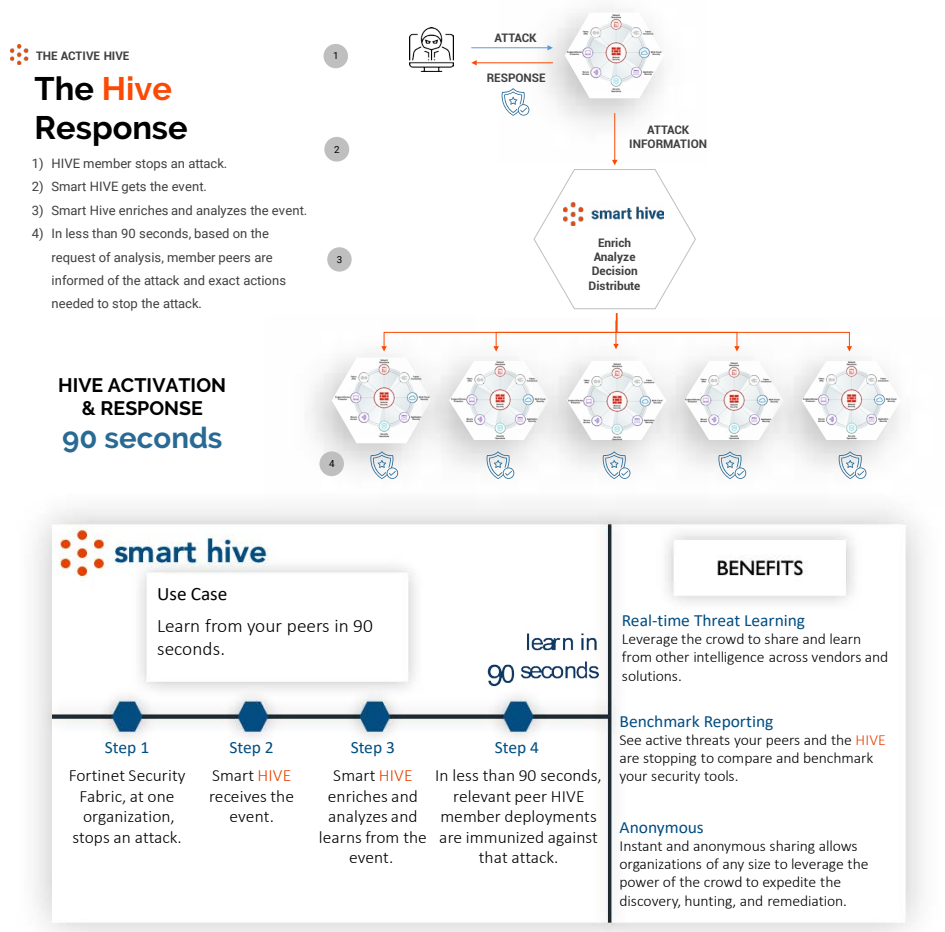
Different customers often have different security tools and vendors in their deployments. Smart Hive's HIVE platform enables organizations to anonymously learn from their peers in real time. An attack on one is defense for all; organizations no longer have to worry if they made the right technology decision or if they have overlooked the latest threat. Through Smart Hive's HIVE solution, organizations can see threats others are stopping in real time, in an anonymized manner. For example, two customers utilizing two different security tools in their respective deployments can anonymously learn from each other if they are part of the HIVE.

Onboarding to the HIVE is very simple and fast, often taking 15 minutes or less. To join the HIVE, a customer visits https://hive.smarthive.io and registers as a HIVE member. Once registered, they can configure their Fortinet solutions to forward logs to pipeline.smarthive.io. Once the data starts flowing, members of the HIVE can log in to their dashboard and see what attacks others are stopping, and what actions they need to take to stop the threats before they get to them.

Premium HIVE members will be able to download a small VM called the Echostation, which allows all logs to be forwarded locally before being sent to the HIVE. The Echostation can also automate remediation by allowing HIVE decisions to be turned into security controls and applied automatically.

As a HIVE premium option, customers could also choose to have relevant controls applied automatically. For example, a customer who may be using a third-party security tool sends their data to the HIVE, and this data will be enriched in the HIVE using Fortinet as an enrichment source. If the customer is being attacked but does not have the proper security controls in place to stop the attack, the customer can either apply the proper control or have the HIVE automate the remediation.

Smart Hive's platform is called the HIVE. The HIVE allows organizations to learn about security threats from each other in real time while remaining anonymous. Think of the HIVE as being like Waze for cybersecurity.



Every time a security tool at a customer takes an action to stop a threat, the HIVE collects that event, removes all sensitive data and anonymizes it, and does detailed analysis. In the HIVE, the data goes through machine-learning algorithms that enrich the event, and compares it to data being received in real time from other customers. Based on multiple factors such as credibility of the source, peer's type of threat, etc., the information is shared with relevant members of the HIVE. Just as Waze only tells a user about what is relevant to them at that time on their route, only relevant information is shared with those that may be impacted by the attack. Controls shared are in real time, relevant, and actionable; the application of these controls can also be automated.

The time interval between the time a threat is stopped by one customer to the time controls can be applied by the HIVE to prevent that attack at another customer can be as low as 90 seconds. In the HIVE, **an attack on one is defense for all.**

About Fortinet

Fortinet (NASDAQ: FTNT) secures the largest enterprise, service provider, and government organizations around the world. Fortinet empowers its customers with intelligent, seamless protection across the expanding attack surface and the power to take on ever-increasing performance requirements of the borderless network—today and into the future. Only the Fortinet Security Fabric architecture can deliver security without compromise to address the most critical security challenges, whether in networked, application, cloud, or mobile environments. More than 450,000 customers worldwide trust Fortinet to protect their businesses. Learn more at http://www.fortinet.com.

Copyright © 2020 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.

February 11, 2020 5:53 AM

597655-0-0-EN

D:\Fortinet\Solution Briefs\grey solution briefs\Smart Hive\sb-FA-fortinet-and-smart-hive-integrated-defense