CHECKLIST

Top Seven Reasons to Implement an Inline Sandbox

Threat actors are increasingly waging sophisticated attacks that do not demonstrate any known indicators of compromise (IOCs) or signatures on your network, email, and endpoints. This makes it almost impossible for antivirus (AV) or firewall solutions to detect them. You need a solution that can identify, classify, and protect from zero-day and previously unknown threats in real time. Here are seven reasons why inline sandboxing is that solution:

☑ Inline, real-time analysis

Analyze suspicious files and block malicious attacks, all in real time. There should not be any traffic slowdowns or impact on business productivity.

☑ Proactive protection for top attack vectors

Move away from passive, offline, and reactive approaches. Proactively assess any file using multiple techniques across the network, email, and endpoints before they become exploits.

☑ Reduced risk and security overhead

Keep suspicious files out of the network until the analysis is complete. This will save your security team time and reduce overhead that would have been spent chasing down malicious files.

☑ Artificial intelligence (AI) and machine learning (ML)

Use both static and dynamic analysis along with deep learning to identify, classify, predict, prevent, and protect against all types of malicious threats, including zero-days and user behaviors.

☑ Global ecosystem of threat intelligence

Start with a multi-layered technology stack. But also leverage robust, real-world threat intelligence and query against a wider sandbox community to see if the threat has already been identified or if a verdict exists. If the file exhibits risky behavior or is found to contain a virus, a new virus signature should be created and added to a signature database. This intelligence and signature should also be shared with the ecosystem so all networks in the system are updated.

☑ Elimination of false positives

Filter out the noise with advanced filtering to focus only on the files that truly contain unknown threats. This saves time and money that may otherwise be spent remediating or chasing threats that pose no risk.

☑ Flexible deployment options

Choose from on-premises, cloud, hybrid-cloud, Platform-as-a-Service (PaaS), or Software-as-a-Service (SaaS) configurations. These options will fit the needs of any organization.

To learn about the FortiGuard Inline Sandbox Service, visit fortinet.com.

Copyright © 2022 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.

December 30, 2022 1:37 PM

1882316-0-0-EN