Forcepoint

Solution Brief

Forcepoint Advanced Malware Detection

Detect even the most evasive zero-day malware to prevent crippling breaches

Challenge

- Threat actors will find and exploit any available point of entry.
- Traditional sandboxes have visibility down to the operating system level only, but a comprehensive solution must stop advanced malware while enabling full attack chain visibility.

Solution

- Forcepoint Advanced Malware Detection (AMD) integrates with Forcepoint CASB, NGFW, Web Security and Email security solutions, complimenting their own security capabilities and sharing intelligence to improve overall visibility and strengthens each point of defense.
- Deep Content Inspection interacts with malware to observe all the actions it might take within this complete environment and even identifies 'dormant code' for special analysis to improve situational awareness.

Outcome

- Increase protection for your organization with proven security effectiveness.
- Enable improved situational awareness for incident response teams.
- Achieve better and faster ROI with integrations.

Forcepoint Advanced Malware Detection (AMD) leverages proven technology to detect zero-day and other advanced malware. Using Deep Content Inspection technology, Forcepoint AMD emulates an entire host, interacting with malware to expose and observe a malicious object's possible actions. These include advanced evasion techniques, O/S or application specific threats, dormant code analysis and even CPU and in-memory activity.

Powered by the industry's best malware detection engine

Forcepoint Advanced Malware Detection provides leading malware detection capabilities. The sandbox is based on a unique architecture that emulates and analyzes the activity of an entire host, including the CPU, system memory and all input/output devices. Often missed by other security technologies, AMD's Deep Content Inspection provides visibility into the behavior of malicious code by emulating a complete operating system and hardware environment. Emulation eliminates the clues that malware often uses to evade detection in more traditional, virtualized sandboxes.

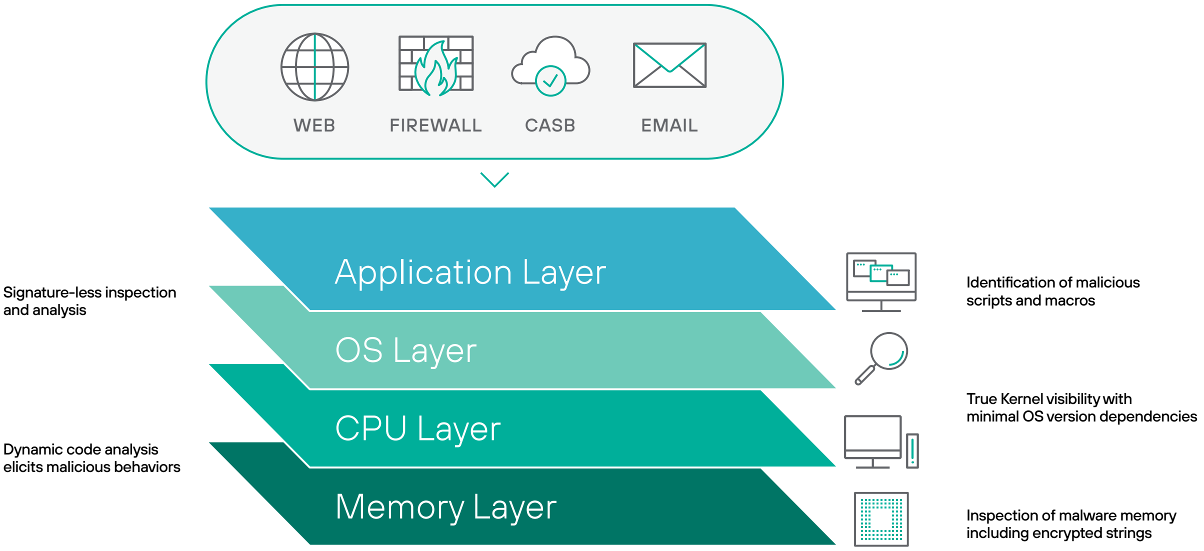
Integrated with Forcepoint defenses across all key threat vectors

Threat actors will find and exploit any available point of entry. Forcepoint Advanced Malware Detection integrates with other defenses, complementing their own security capabilities to frustrate attacker efforts across multiple channels. The resulting shared intelligence improves overall visibility and strengthens each point of defense. AMD is available as a fully integrated option for Forcepoint CASB, NGFW, Web Security and Email Security. In this integration, Forcepoint's core solutions first assess the broader context of an internet transaction for potential indicators of compromise. After performing static analysis of suspicious files, AMD can be called upon to perform the deep behavioral analysis necessary to identify zero-day threats and other modern malware.

Available as a cloud service for high availability, scalability, low maintenance and other SaaS benefits, on-premises for cloud-adverse organizations, or even deployed as an air gapped solution with Forcepoint NGFW for physically isolated network requirements. Forcepoint AMD is the perfect complement to your Forcepoint CASB, NGFW, Web Security or Email Security solution. It provides unparalleled threat detection, as well as consistent threat forensic information, to optimize incident response teams.

Forcepoint AMD will give you all the information you need—regardless of the threat vector—while 'zero-false positives' means you'll spend your valuable time working against true threats. Regardless of your size or industry, Forcepoint provides the comprehensive security solutions you need to challenge today's fast evolving, highly evasive threats.

The deep content inspection difference


WEB
FIREWALL
CASB
EMAIL
Application Layer
OS Layer
CPU Layer
Memory Layer
Signature-less inspection and analysis
Dynamic code analysis elicits malicious behaviors
Identification of malicious scripts and macros
True Kernel visibility with minimal OS version dependencies
Inspection of malware memory including encrypted strings

Deep content inspection—a step beyond sandboxing

As with sandboxing, Forcepoint Advanced Malware Detection provides a simulated environment for malware execution; that is where any similarity ends.

A complete environment

Traditional sandboxes have visibility down to the operating system level only. Forcepoint offers a unique isolation and inspection environment that simulates an entire host including the CPU, system memory and all devices. Deep Content Inspection interacts with malware to observe all the actions it might take within this complete environment and even identifies 'dormant code' for special analysis.

Malware interaction

Sandbox-only solutions provide a relatively static environment, limiting the malicious 'behavior' they may uncover. Because Forcepoint Advanced Malware Detection interacts with malware, it observes every action that it might take, even when those actions are delegated to the operating system or other programs.

In addition, this tool identifies potentially malicious 'dormant code' that the malware does not execute.

Extensive malware detail exposure

A comprehensive solution must do more than just stop advanced malware. Correlated incident information prioritizes the most significant threats in your network without combing through massive log files. Full attack chain visibility enables your incident response team to quickly understand the nature of the attack, making your scarce security resources more efficient.

Powered by the industry's best malware detection engine

Forcepoint Advanced Malware Detection provides leading malware detection capabilities and offers top rated security efficacy. This enables unmatched accuracy and eliminates false positives, so your incident response team can focus on actual threats.

forcepoint.com/contact

© 2020 Forcepoint. Forcepoint and the FORCEPOINT logo are trademarks of Forcepoint.
All other trademarks used in this document are the property of their respective owners
[Forcepoint-Advanced-Malware-Detection-Solution-Brief-EN] 3AUG2020