FORCEPOINT
POWERED BY Raytheon

Datasheet

Advanced Malware Detection

DETECT AND STOP THE MOST EVASIVE ADVANCED MALWARE THREATS

Forcepoint Advanced Malware Detection (AMD) accurately identifies today's evasive malware—with zero false positives —to focus incident response teams on actual threats and prevent breaches that take advantage of the human point.

UNRIVALED EVASIVE MALWARE THREAT DETECTION

Identifying the malware components of advanced threats has become increasingly difficult due to the evolution of evasion tactics and technology by criminal and nation-state threat actors.

Unrivaled Accuracy

Forcepoint AMD technology delivers proven, industry-leading security accuracy. Even highly evasive threats are revealed through deep content inspection of activity at multiple levels, dormant code, and other indicators often overlooked by traditional sandbox technologies.

Zero-False Positives

Eliminate the distraction of False Positive results with AMD. This means your incident response team can spend its valuable time responding to actual threats, not chasing down false positives or searching for indicators of compromise (IOCs).

Global Threat Intelligence

Your team automatically receives threat intelligence updates containing the malware characteristics, behaviors and associated IOCs of every malicious object curated and analyzed within the global service. This means faster identification of known threats, new threats that reuse objects, and streamlines the analysis, detection and response to previously unknown threats.

MORE THAN SANDBOXING – DEEP CONTENT INSPECTION

Like sandboxing, Forcepoint AMD provides a simulated environment for malware execution. But that's where the similarity ends.

A Complete Environment

Traditional sandboxes only have visibility down to the operating system level. 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 the malware to observe all the actions a malicious object might take within this complete environment, and even identifies dormant code for special analysis.

Intelligent Malware Interaction

Because Forcepoint AMD interacts with malware, it can observe every action that a malicious object might take, even when those actions are delegated to the operating system or other programs. But we also identify potentially malicious dormant code that does not execute. In contrast, sandbox-only solutions provide a relatively static environment, limiting the types of malicious behavior they may uncover.

Extensive Malware Detail Exposure

A comprehensive solution must do more than just stop advanced malware—it must prioritize it. Correlated incident information helps prioritize the most significant threats in your network without having to search through massive log files. And full attack chain visibility helps your incident response team to quickly understand the nature of the attack, making your valuable security resources more efficient.

CROSS-CHANNEL SUPPORT

Threat actors have demonstrated their flexibility to find and exploit any available point of entry. Forcepoint AMD integrates with other defenses, complimenting their security capabilities to frustrate an attacker's efforts across multiple channels. The resulting shared intelligence improves overall visibility and strengthens each point of defense.

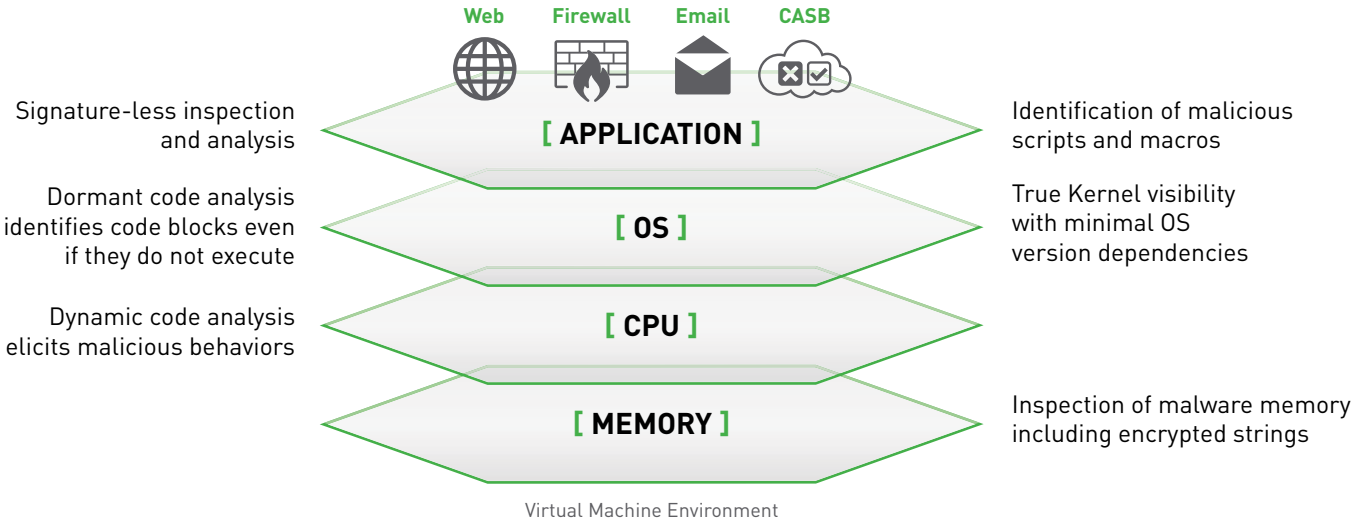
Web Security

Forcepoint Web Security is a cloud- or hybrid-deployed Secure Web Gateway that stops advanced threats from getting in and sensitive data from getting out—wherever and however your users access it. Forcepoint AMD integrates with Web Security as an additional defense against zero-day and other advanced, evasive malware.

Its cutting-edge classification engine, global threat intelligence, advanced malware detection and enterprise-class DLP work together to make world-class security easy to deploy. It delivers real-time web protection for increasingly mobile workforces and can share policies and context with Email Security to stop advanced, coordinated web and email attacks with complete inbound and outbound defenses.

Email Security

Forcepoint Email Security stops the spam and phishing emails that introduce ransomware and other advanced threats before they can infect systems with malware. Forcepoint AMD integrates with Email Security as an additional defense against zero-day and other advanced, evasive malware.



Deep Content Inspection Delivers Unmatched Visibility

Comprehensive defenses integrate highly effective analytics, URL Wrapping, Phishing Education and Forcepoint AMD for inbound protection, as well as integrated DLP as an outbound control and email encryption for secure communications.

Operating on the industry's most secure cloud infrastructure, Forcepoint Email Security delivers unparalleled phishing, malware and DLP protection for Microsoft Office 365™ and other popular email systems.

NGFW

Forcepoint Next Generation Firewall (NGFW) connects and protects people and the data they use throughout your offices, branches and the Cloud—all with the greatest efficiency, availability and security. It applies multiple scanning techniques to files found in network traffic, allowing granular levels of security to be tailored to the specific needs of each connection. Forcepoint AMD integrates with Forcepoint NGFW as an additional defense against zero-day and other advanced, evasive malware.

With Forcepoint, you can deploy, monitor and update thousands of firewalls, VPNs and IPSs from a single console—cutting network operating expenses up to 50%. You can eliminate more downtime with our high-availability clustering and Multi-Link networking. And, you can block attacks and manage encrypted traffic without hurting performance. As the pioneer in Advanced Evasion Technique defenses and proxy technologies for mission-critical applications, Forcepoint gives you security without compromise.

CASB

Forcepoint CASB delivers visibility and control over cloud applications to bolster security and compliance. It quickly discovers unsanctioned cloud applications and assesses their associated risks while simultaneously ensuring complete control over how sanctioned cloud applications such as Office 365, Google Suite, Salesforce, Box, Dropbox and others are used in order to prevent the loss of critical intellectual property.

With Forcepoint CASB, organizations can truly embrace the cloud by preventing users from engaging in risky behaviors, but without slowing them down.

CONTACT

www.forcepoint.com/contact

ABOUT FORCEPOINT

[DATASHEET_ADVANCED_MALWARE_DETECTION_ENUS] 100060.061417