FORCEPOINT
POWERED BY Raytheon

Solution Brief

FORCEPOINT Advanced Malware Detection

POWERED BY LASTLINE™

Forcepoint Advanced Malware Detection (AMD) leverages proven Lastline technology to detect zero-day and other advanced malware. Using Lastline's 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.

In a recent study of Breach Detection Systems (BDS) by NSS Labs, Lastline was named the most effective advanced malware detection system and was the only product to achieve **100% detection** with **zero false positives.**

NSS LABS, THE WORLD'S LEADING INDEPENDENT SECURITY PRODUCT TESTING LAB, HAS NAMED LASTLINE ENTERPRISE AS THE MOST EFFECTIVE ADVANCED MALWARE DETECTION SYSTEM.

Evaluated for comprehensive security effectiveness

NSS Labs conducted rigorous, comprehensive testing to determine how well each product detects advanced threats and attack methods. Vendor products were evaluated in numerous areas, including:

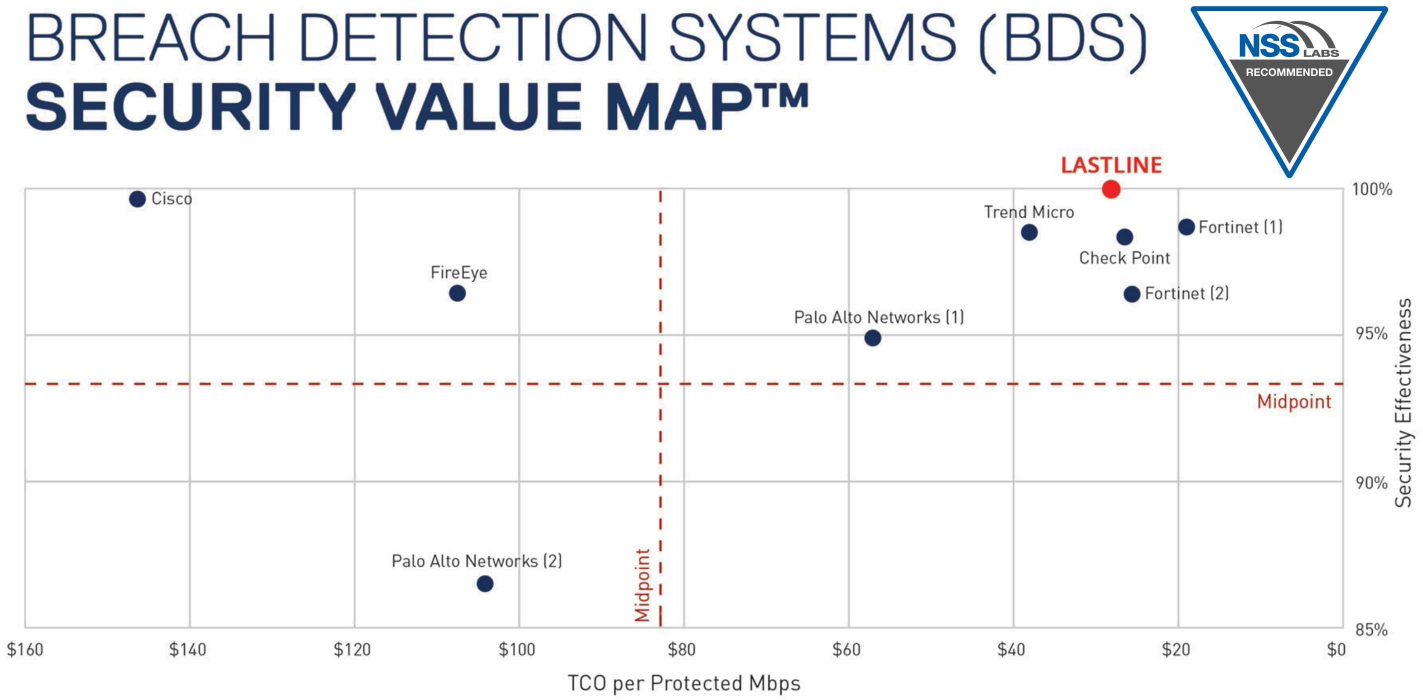
Security effectiveness

- **Detection of online infections**
- **Detection of drive-by, social, HTTP and email driven attacks**
- **Resistance to advanced evasion techniques**
- **Number of false positives**

Overall performance

- **Maximum capacity**
- **HTTP capacity with no transaction delays**
- **Real-world traffic mixes**

Total Cost of Ownership (TCO)



Lastline is #1 for overall security effectiveness

NSS Labs analyzed the security effectiveness and total costs of each product to determine the Overall Security Value Map. Lastline was identified as the solution with the greatest overall security effectiveness.

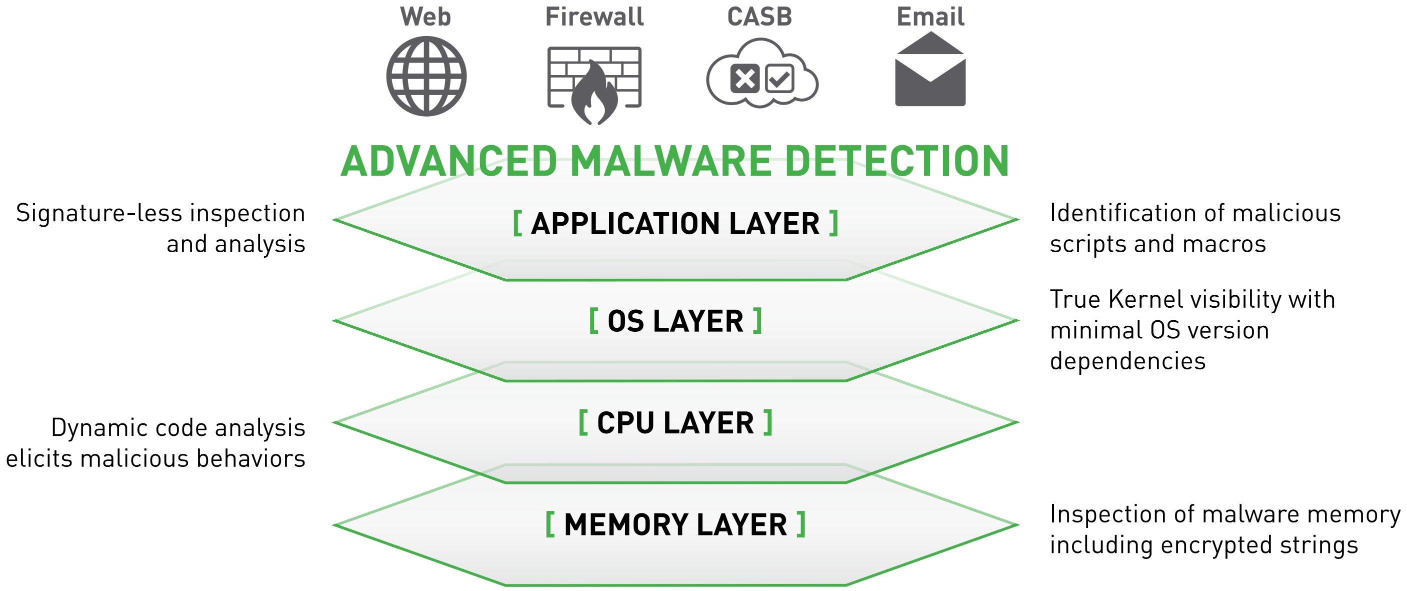
Test Result Highlights: Lastline Enterprise v7.10

FALSE POSITIVES	DRIVE-BY EXPLOITS	SOCIAL EXPLOITS	BEACH DETECTION RATE	HTTP MALWARE	STMP MALWARE	OFFLINE INFECTIONS	EVASIONS	STABILITY & RELIABILITY
0.00%	100.0%	100.0%	100.0%	100.0%	100.0%	100.0%	100.0%	PASS

The industry's best malware detection engine

Forcepoint chose Lastline as a partner for Advanced Malware Detection because of their leading malware detection capabilities (as demonstrated in the NSS Labs study). 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, Lastline'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.

THE DEEP CONTENT INSPECTION DIFFERENCE



Web

Firewall

CASB

Email

ADVANCED MALWARE DETECTION

[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

Integrated with Forcepoint defenses across all key threat vectors

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 or on-premises solution (for more cautious or otherwise cloud-adverse organizations), 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.

CONTACT
www.forcepoint.com/contact

[SOLUTION_BRIEF_FORCEPOINT_AMD_ENUS] 700006.083117