ALERT LOGIC®

SOLUTION BRIEF:

ALERT LOGIC ESSENTIALS

EXTENDED ENDPOINT PROTECTION

Security and IT directors in mid-size companies spend a significant part of their time and budget on breach prevention and access control technology and processes. But attacks can consist of multiple techniques that try to compromise endpoints, gain access to resources, and detonate payloads.

Malware has typically used files that it makes resident on a target machine to carry out an attack. But another class of malware called "fileless" does the opposite. The attack this malware causes does not touch the disk of the target, but instead loads the malware instructions into memory.

Malware attacks can be difficult to prevent and with ever-changing signatures or, in the case of fileless attacks, no detectable signature, malware can bypass the effectiveness of some antimalware protection services or whitelists.

In reports[1], respondents predicted over 62% of attacks targeting respondents' companies in 2019 would be file-based while 38% would be fileless attacks. And, 77% of successful breaches involved fileless techniques.

62%

of attacks are caused by malware files

77%

of breaches are caused by fileless techniques

But traditional approaches to protect against malware involve solutions that use machine learning to generate models every 4 to 6 months to identify malicious files before they execute. The problem with this approach is that businesses must manage decreasing accuracy over time and deal with false positives.

Alert Logic Extended Endpoint Protection Uses Machine Learning Differently.

Alert Logic extended endpoint protection automatically gathers, analyzes, and integrates, thousands of samples a day. As a result, customers get the best protection, transparently receiving new models that improve coverage and accuracy.

[1] *2017 and 2018 Ponemon Institute State of Endpoint Security Risk*

FEWER FALSE POSITIVES

GATHER AND ANALYZE DAILY

LOOK FOR PATTERNS OF BEHAVIOR

RULES FOR FILE-LESS MALWARE

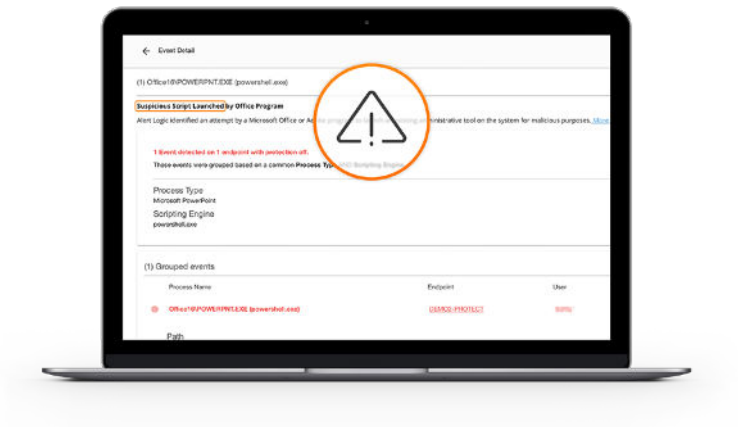
TRAINED FOR CUSTOMER'S SOFTWARE

This organization-specific approach results in fewer false positives because the model has already been trained with the specific software that customers are running.

- We gather and analyze, thousands of samples a day
- We look for patterns of behavior that fuels our behavioral protection
- We create rules for file-less malware that have no file to scan
- Models are trained with the software that customers are running

This approach enables Alert Logic to:

- Thwart multiple attack techniques that try to compromise endpoints, gain access to resources, and detonate payloads
- Achieve multi-vector attack monitoring and isolation that recognizes techniques and stops them early before any damage is done
- Work alongside existing anti-virus tools to provide an additional layer of defense



Requirements for Alert Logic Extended Endpoint Protection:

OPERATING SYSTEMS	SERVERS	HARDWARE	LANGUAGE SUPPORT
Windows 7	Windows Server 2008 R2	64-bit operating systems running on 64-bit processors	US English
Windows 8.1	Windows Server 2012	Windows 7 32-bit operating systems	UK English
Windows 10	Windows Server 2016	Intel processors	Spanish
MacOS 10.2 and higher	Windows Server 2019	AMD processors	German

Learn more at https://www.alertlogic.com/solutions/extended-endpoint-protection

ALERT LOGIC®