DATA SHEET

wedge networks
securing the cloud connected world

WEDGE SECURITY OPERATIONS CLOUD™

MALWARE ANALYZER™

CHARACTERIZE UNKNOWN MALWARE, ELIMINATE FALSE POSITIVES

OVERVIEW

With an average of more than a million new variants of malware created daily, new, previously unknown malware routinely evades real-time detection by conventional security systems to deliver Ransomware and other threats. WedgeAMB™ introduced cutting edge AI detection of new malware with industry leading speed and accuracy. Wedge Malware Analyzer™ (WedgeMA™) is a value-added service available to WedgeAMB™ users to automatically execute, analyze, and characterize files that are suspicious but unconfirmed as malware, to provide additional threat intelligence. Additional threat intelligence derived from these analyses is automatically fed back to WedgeAMB systems, to further improve threat detection speed and accuracy.

> *"WedgeAMB™ blocks conventional and advanced malware in real-time, using AI enhanced static analysis for superior threat detection with imperceptible latency."*

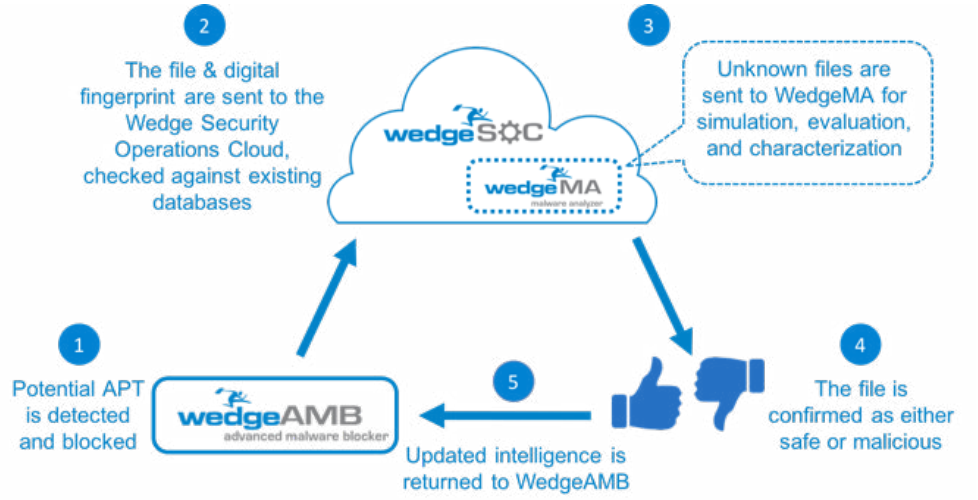
wedgeAMB
advanced malware blocker

> *"WedgeMA™ characterizes suspicious files that are blocked by WedgeAMB™, using AI enhanced behavioral analysis technologies for increased threat intelligence ."*

wedgeMA
malware analyzer

Simple and Highly Efficient Operations

WedgeMA™ is a cloud-based subscription service. There are no platforms to purchase or maintain, and no software to update. Simply subscribe to the service and pay a monthly fee for the incremental service. Unlike more conventional sandbox services which analyze all content that is not whitelisted, WedgeAMB systems will only forward content which has a verdict of "suspicious but unconfirmed" as malware. Suspicious content is then analyzed by WedgeMA and discarded immediately afterwards.



Simple and Effective Accelerated Learning

WedgeMA is hosted in the Wedge Security Operations Cloud (WedgeSOC). WedgeAMB users have the option to subscribe to the service and allow their WedgeAMB appliances to automatically forward blocked web content or files that are suspected of containing malware, but unconfirmed as malware (1).

WedgeMA immediately compares the content and digital fingerprint against the WedgeSOC database for possible prior verdicts (2). The verdict of recognized, known files are immediately returned to the WedgeAMB appliance and automatically added to its local database for future analyses.

If the content is unrecognized, WedgeMA executes the suspicious content using a multi-stage data analysis process with machine learning, behavioral analysis, and other techniques to characterize and confirm previously undiscovered malicious content (3).
Typically, this multi-stage analysis includes:

- Static Analysis: applying continuously updated rules and signatures to look for known threats.
- Payload Analysis: leveraging an intelligent sandbox array to gain deeper understanding of malware behavior by detonating suspicious web and file content, which would otherwise target Windows, OSX, or Android endpoint devices.
- Machine Learning and Behavioral Analysis: applying cutting edge technologies to recognize the latest threat behaviors (such as multi-component attacks over time) and quickly detecting previously unknown threats.
- Verdict Classification: the content is either confirmed as malware or safe for consumption (4).
- Malware Reputation Analysis: results from the analysis are compared with similar known threats to determine whether the new threat is a variant of an existing known threat or something completely original.

Updated threat intelligence is recorded in the WedgeSOC database and is also returned to the issuing WedgeAMB system and added to the local database for immediate detection as part of the initial WedgeAMB analysis (5). This feedback loop enables a bypass of multi-stage scanning for identical web content and files that are encountered by WedgeAMB in the future.