CAYUGA NETWORKS

DECISIS DATA SHEET

Next-Generation Web App Attack Detection Delivers 100% Actionable Intelligence

Managed service warns of only credible, critical and imminent threats

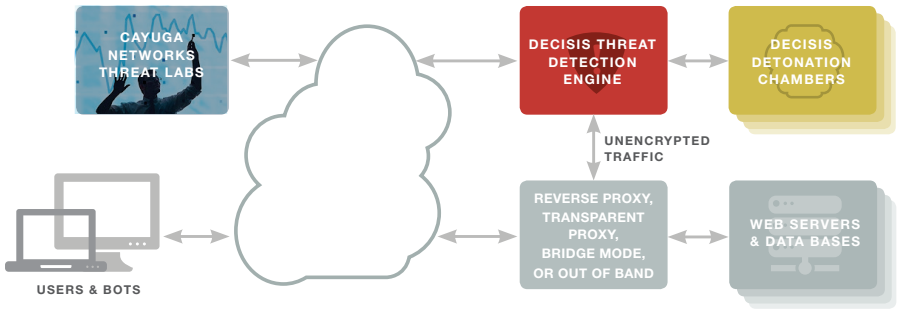
Cayuga Networks Decisis™ Next-Generation Web App Attack Detection protects enterprises from the huge deluge of attacks hitting today's web application attack surfaces. It not only spots indicators of attacks that otherwise go unnoticed in the web request stream, but also intelligently assesses the potential severity of threats and delivers early warnings of credible threats.

This 100% actionable intelligence provides huge benefits to today's busy, resource-constrained security teams, such as eliminating false alarms. The fused machine/human managed service only warns customers when it determines that bad actors on the Internet know an app vulnerability exists and are actively probing or attacking it. Additionally, when the service does issue an alert, it provides a highly contextual report that enables security teams and owners of the app to quickly remediate the vulnerability.

Allowing security teams to focus their effort where it matters most

Essentially a layered defense in a box, the Cayuga Networks Decisis threat detection engine combines multiple algorithms, machine learning, and active defenses. Its multiple statistical modules track and correlate hundreds of indicators of attacks in real time and at web scale, while unique Cayuga Networks code flow analysis (CFA™) spots hidden attack code.

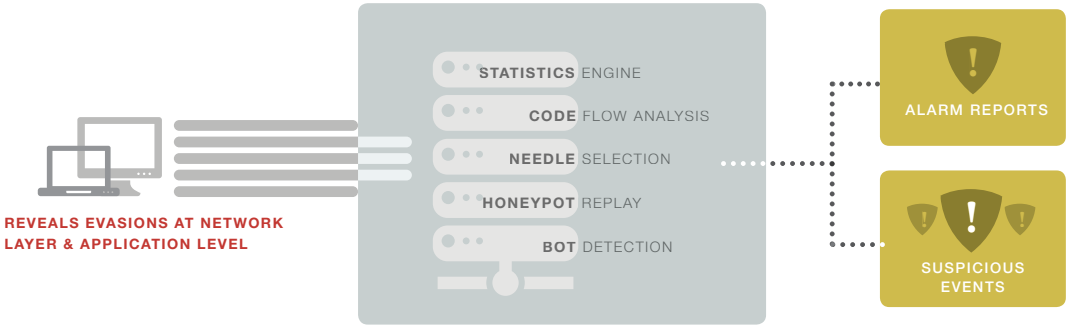
When these automated defenses accumulate enough statistical evidence to suggest a high-risk event, the engine elevates it to an Anomaly. The software modules then perform additional automated analysis routines to confirm that the Anomaly is significant enough to be 'actionable.' In other words, they confirm that a vulnerability exists and the attack either worked or could have worked had the hacker made minor modifications.



To further prevent false alarms and provide reporting with the rich context required to quickly fix vulnerabilities, threat experts at Cayuga Investigation Central (CIC) can also perform various forensics on the suspicious code. This investigation may include replaying it in sandboxed detonation chambers to determine if the malicious code is effective or possibly a zero-day attack.

Machine/Human detection catches threats that evade other defenses

This fused Machine/Human detection, which is delivered as a managed service, works better than either approach applied alone. It not only catches threats that other defenses miss but also delivers only alerts that matter—highly actionable reports with complete context. As a result, enterprise security teams can more quickly—and more cost-effectively—remediate vulnerabilities by applying resources to only critical, credible and imminent attacks.



INFERENCE ENGINE AGGREGATES EVENTS OF INTEREST AND PRIORITIZES ANOMALIES

Finding needles in a rapidly moving haystack

A very fast detection engine inspects, analyzes and decodes packets at line speed before delivering them to the statistical analysis modules.

Statistics Modules

The detection engine employs numerous statistical analysis modules to correlate interesting web events. It continuously calculates statistics on hundreds of types of suspicious indicators to determine Anomaly Scores.

Network Code Flow Analysis

Code detection is critical because code found in HTTP requests is highly indicative of an attack. The detection engine employs CFA technology to inspect inbound network traffic and sessions. When CFA finds an indication of hidden attack code, it analyzes the grammar of the suspect string across multiple languages—in parallel across the whole packet stream at web speed—to identify the likely language and verify that the transitions are grammatically allowed in the observed language. Using machine learning, it infers if the request stream contains valid code in the respective languages until it can confidently confirm or deny that it is valid code.

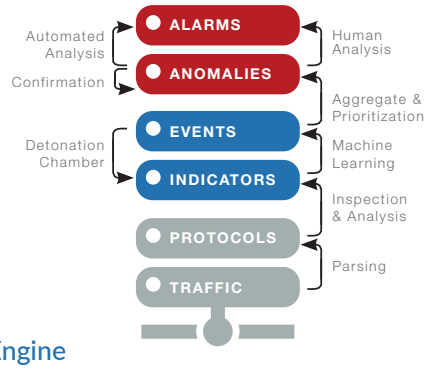
Detonation Chambers Catch Zero Day Attacks

Optionally, the detection engine automatically sends the snippet into a sandboxed detonation chamber that has a clone of the customer's application stack components. The orchestrator then safely replays the code to see what it does and whether or not it poses a credible threat.

Needle and Bot Detection

Needle Detection enables custom or ad hoc inspections and rapid deployment of defenses against newly discovered attack vectors.

Bot Detection offers an important clue to the nature of the web visitor. Techniques employed include verifying browser behavior, checking cookie support, and examining the headers for bot indicators.



Inference Engine

Machine learning does the heavy lifting in determining which anomalies to prioritize. The Inference Engine then centralizes the suspicious incidents, correlating indicators of attack across detection modules, and determines which incidents are most interesting and merit additional investigation.

Enterprise Size	Small	Medium	Large
Specifications	**vDecisis**	**Decisis**	**Decisis XL**
Dimensions	Virtual	1U	2U
Performance	Trial Only	1Gbps	10Gbps
Network Interfaces	Virtual	4 x 1Gbps	1 10 Gbps Napatech card
Processors	2	16: 2 CPUs x 8 cores	28: 2 CPUs x 14 cores
Storage	Temporary	3 x 1TB disks	14 x 1.2TB + 2 x 300GB disks
Power	N/A	2 x 495W	Dual Hotplug Redundant 1+1 1100w

CAYUGA NETWORKS

317 N. Aurora St.
Ithaca, NY 14850
607.216.9636
info@cayuganetworks.com
cayuganetworks.com