DATA SHEET

ENDGAME. ENTERPRISE

Instant Detection. Active Response.

KEY BENEFITS

REDUCE DAMAGE AND LOSS

Guided advisories enable timely discovery of compromised or targeted hosts before assets are stolen or business operations are disrupted.

IMPROVE OPERATOR PRODUCTIVITY

Automated analysis and advanced visualization eliminates time spent aggregating data, writing queries, or interpreting results.

STREAMLINE FORENSIC INVESTIGATIONS

Continuous access to rich host intelligence reduces the need for disruptive and costly forensic appliance deployments.

KEY FEATURES

ADVANCED THREAT INTELLIGENCE

Live network of global sensors ensures early detection of evolving attacks and their technology, industry, and geographic targets.

ENTERPRISE VISIBILITY

Broad range of sensors for legacy, virtual, and cloud infrastructure tunable to meet operational requirements.

INSTANT DETECTION

Behavioral analysis, attack chain modeling, and intelligence are applied to perform early identification of malicious behavior.

ACTIVE RESPONSE

Endgame Advisories provide precise details on targeted and compromised systems, enabling containment and remediation actions.

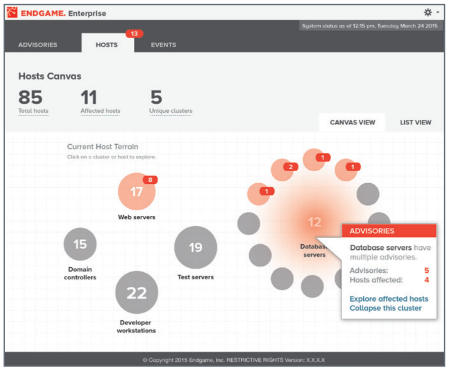
INSTANT DETECTION AND ACTIVE RESPONSE TO ADVANCED THREATS WITH ENDGAME ENTERPRISE

Adversaries consistently demonstrate their ability to slip past the most hardened perimeters. They have moved beyond exploiting known vulnerabilities and using known malware. To identify new attack vectors, they perform reconnaissance on your people, technology, and supply chain. Dynamic techniques enable them to obtain malicious access, impersonate authorized users, and hijack approved software. Once inside, they dwell undetected and have ample time to locate your most valuable assets.

Endgame Enterprise is the industry's first endpoint detection and response (EDR) platform that delivers early warning, instant detection, and active response to advanced threats missed by traditional defenses.

ENTERPRISE VISIBILITY

Endgame's approach starts with Endgame Sensors, lightweight software that resides on monitored hosts – covering bare metal, virtualized, and cloud environments. Integration with enterprise infrastructure ensures that dynamically provisioned hosts are monitored. Endgame Sensors inventory thousands of host activities and attributes, including user, system, application, file, and network connections, with minimum system performance impact.



System status as of 12:15 pm, Tuesday March 24 2015

Hosts Canvas

85 Total hosts

11 Affected hosts

5 Unique clusters

Current Host Terrain

Click on a cluster or host to explore.

17 Web servers

15 Domain controllers

19 Test servers

22 Developer workstations

12 Database servers

ADVISORIES

Database servers have multiple advisories.

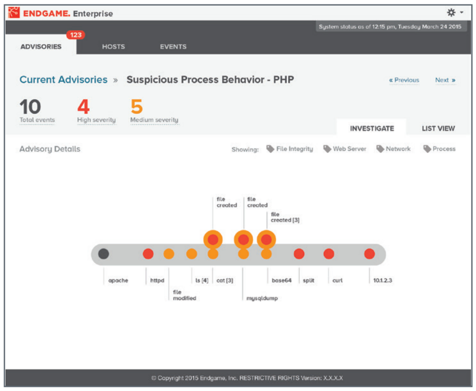
Advisories: 5

Hosts affected: 4

© Copyright 2015 Endgame, Inc. RESTRICTIVE RIGHTS Version: X.X.X.X

Host Map

Visualize suspicious changes to host populations.



System status as of 12:15 pm, Tuesday March 24 2015

Current Advisories » Suspicious Process Behavior - PHP

10 Total events

4 High severity

5 Medium severity

Advisory Details

Showing: File Integrity, Web Server, Network, Process

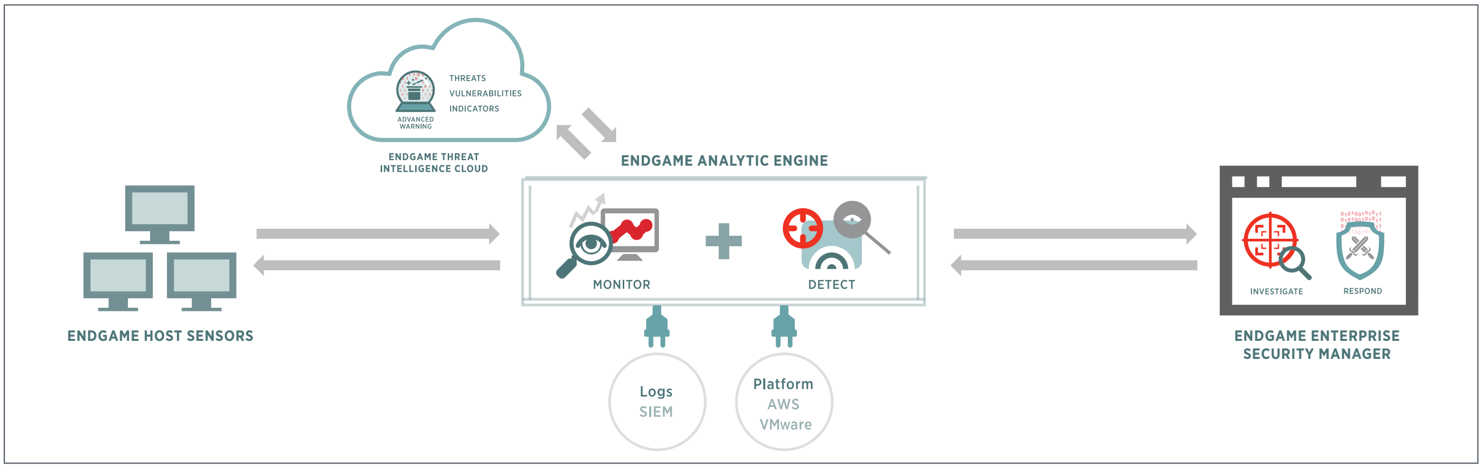
© Copyright 2015 Endgame, Inc. RESTRICTIVE RIGHTS Version: X.X.X.X

Investigator View

Traces an evolving attack and enables an operator to respond quickly.

INSTANT DETECTION

Endgame's cloud-based Analytic Engine aggregates application, network, file, and configuration details from all Sensors. Using context-based behavioral analysis and attack chain modeling, suspicious behavior is quickly identified and tracked in real time as it evolves. Kill chain visualization identifies malicious behavior, and compromised or targeted hosts, enabling an operator to act in time. Full event details are provided to confirm the results of automated analysis.



KEY COMPONENTS

ENDGAME HOST SENSORS

reside on monitored endpoints, collecting high-fidelity application, network, file, and configuration details with minimum impact on host performance.

ENDGAME ANALYTIC ENGINE

applies context-based behavioral analysis and attack chain modeling to host data and threat intelligence, identifying malicious behavior and compromised or targeted hosts.

ENDGAME ENTERPRISE SECURITY MANAGER

provides analysts and operators with a comprehensive view of suspicious behavior and tools that accelerate investigation and response.

ENDGAME THREAT INTELLIGENCE CLOUD

is a live global network that identifies evolving threats and the technology, industry, and geographies they target, giving customers unique advanced warning.

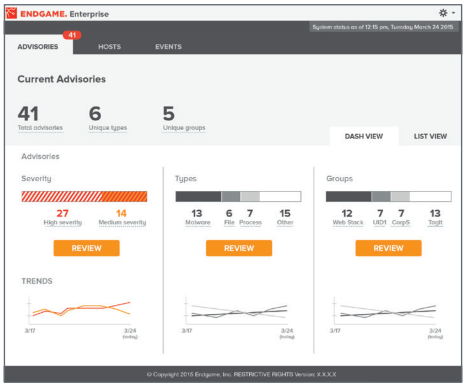
Supported Platforms

Current Linux Support: CentOS 6.x, RHEL 6.x, and Ubuntu 12.x & 14.x Upcoming Windows Desktop and Server Support

Endgame Enterprise consists of four components: Host Sensors, Analytic Engine, Enterprise Security Manager, and Threat Intelligence Cloud.

ACTIVE RESPONSE

Endgame Enterprise Security Manager guides your security team with Advisories that enable fast, effective investigation and response without requiring expert-level skills and knowledge. It produces guidance that dramatically reduces the signal-to- noise ratio, empowering security teams to take control in real-time. This is a stark contrast from the volume of meaningless alerts generated by traditional security products.



Advisory summary gives rapid access to the reasons behind the ratings.

ADVANCED THREAT INTELLIGENCE

Endgame Enterprise is powered by our proprietary intelligence feed, the Endgame Intelligence Cloud. Our vulnerability and threat researchers leverage a global network of sensors to identify evolving threats, giving our customers the earliest warning of new techniques and the technology stacks they are targeting by industry and geography. This intelligence is used by the Endgame Analytic Engine to identify and prioritize known and unknown threats that evade traditional defenses.

ABOUT ENDGAME

Endgame is leveling the playing field against adversaries by protecting national security and commercial interests from the most advanced cyber threats. Using its deep knowledge of the adversary, Endgame helps customers understand their defenses from the perspective of the attacker. This new approach allows organizations to instantly detect and actively respond to advanced threats, preventing damage and loss. Endgame's technology and techniques are proven in the most extreme environments—from defending U.S. national security interests to protecting the world's critical infrastructure.

Endgame Enterprise is available now in the form of a limited release beta for Linux platforms. For more information, or to request access to our beta program, contact Endgame at enterprisesales@endgame.com

info@endgame.com www.endgame.com
Washington, DC · San Francisco · San Antonio · Melbourne

ENDGAME.
Take Control.