ENDGAME.

ENDGAME FOR LINUX

THE PROVEN LEADER IN ENDPOINT PREVENTION, DETECTION, AND RESPONSE

While the incidence of malware targeting Linux has not yet rung alarms as loudly as have attacks on Windows and now macOS, with the galloping adoption of Linux by endpoint and server providers, security teams are demanding increased visibility, control and immediate response options.

> "LINUX SHOULD BE SUPPORTED FROM THE DAY OF RELEASE. THE VENDOR MUST PROVIDE... PARITY WITH WINDOWS FOR EDR-TYPE DATA COLLECTION AND IOC SEARCH CAPABILITIES"
>
> – GARTNER, 2018

Endgame delivers protection and visibility for all major Linux distributions including RHEL, Centos, and Ubuntu as well as across Docker environments. To deliver this best in class capability on Linux, Endgame does not need to operate within the kernel. While most vendors need weeks and months to react to Linux updates, Endgame customers are able to adopt the benefits of new Linux releases, versions or patches faster than ever.

WITH ENDGAME FOR LINUX, THERE IS NO COMPROMISE.

Benefit from the same industry leading prevention and detection capabilities, tailored specifically for Linux. Your security analysts can triage alerts, investigate incidents, contain and control Linux devices in a single click, and include all Linux devices in threat hunting operations.

- ENDGAME REFLEX - Deploy custom prevention and detection rules to enforce compliance and full ATT&CK coverage
- RUNS IN USER SPACE - Kernel level visibility without constraints on kernel versioning
- FULLY FEATURED EDR AND HUNT - No disparity between Windows, macOS, and Linux investigations and response

THIRD PARTY VALIDATION

PCI DSS COMPLIANT · HIPAA COMPLIANCE · AV COMPARATIVES · amtso · Gartner · MITRE · virustotal · SE Labs · NSS LABS RECOMMENDED

ENDGAME.

ENDGAME.COM

Schedule a demo now at **endgame.com/demo**

@EndgameInc · Endgame

ENDGAME ADVANTAGES

ENDGAME PREVENTION, DETECTION, AND RESPONSE INCREASES PROTECTION: Endgame is the only security platform that makes advanced endpoint protection as simple as AV. Take advantage of proven, industry-leading prevention, detection and response, and implement advanced threat hunting capabilities with the people you already have.

- Malware and ransomware prevention: Endgame MalwareScore™ for Windows and macOS is the machine learning-powered malware prevention for known and unknown malware, with 99% block rate and zero false positives. Behavior-based ransomware prevention blocks attacks before full disk encryption.
- Phishing prevention: Picking up where email security vendors fail, Endgame includes the industry's first machine-learning based phishing prevention for Microsoft Office documents. Endgame blocks malicious macros pre-execution, achieving greater than 99% efficacy.
- Exploit and fileless attack prevention: Endgame provides full protection against memory-based attacks with patent-pending process injection prevention. MalwareScore™ prevents malicious module loads, DLL injection, and shellcode injection, preventing adversary evasion and fileless attacks.
- The only truly autonomous agent: While other vendors need time to analyze endpoint activity in their cloud, Endgame's fully autonomous agent blocks malicious activity in-line on the endpoint. This means faster, more accurate protection and detection that is always-on no matter if the endpoint is on a submarine or in Starbucks.

ENDGAME REFLEX ELIMINATES THE BREAKOUT WINDOW: The industry's first fully customizable prevention and detection engine that runs in-line on the endpoint. Organizations can define their own real-time prevention, detection and response actions within Endgame's unique autonomous agent technology. Use Endgame Reflex to move legacy SIEM searches into real-time visibility, and stop attacks in seconds across the entire enterprise with zero disruption.

- MITRE ATT&CK™ alignment brings consistency to incident information and allows for faster alert triage, assessment, and decision making.
- Full access to rule creation mode with real-time guidance and syntax. Completely avoid false positives and alert-storms with a one-click preview against your organization's data.
- Extend 100's of pre-built ATT&CK rules to fit your unique operational requirements.

ENDGAME REMOVES OPERATIONAL INEFFICIENCIES AND COMPROMISES: The single interface will streamline all administration and agent management, enhance IT operations visibility, optimize security incident response, and allow organizations of all sizes to run hunt operations across all endpoints.

- Full protection for Windows, macOS and Linux brings consistency, visibility and control across all enterprise endpoints and servers.
- Precision response actions: one-click containment empowers SOC teams to investigate incidents at enterprise scale with zero business disruption
- Endgame Cloud reduces deployment time and brings instant time-to-value. The on-premises option can combine with cloud-services to allow granular, per-endpoint data privacy controls.
- Total Attack Lookback provides 120 days retention of trusted, tamper-proof, attack data by default with no additional storage charges.

ENDGAME ARTEMIS® CLOSES THE SKILLS GAP: Endgame lowers the barrier to entry for advanced endpoint protection capabilities with the industry's first AI-powered chatbot, Artemis®.

- Alert triage assistance so analysts of all skill levels can stop targeted attacks and eliminate alert fatigue.
- Investigate and hunt using plain English questions, prioritizing threats and adversarial behaviors to instantly understand what's important.
- Endgame Resolver™ visually renders the complete incident timeline with real-time activity analysis of file, registry, user, process, network, netflow, and DNS data.
- Adversary trade-craft analytics enable real-time detection and response workflows to surface suspicious artifacts across millions of records in minutes, combined with Endgame Reflex for fully customizable adversary detection and prevention.

TECHNICAL SPECIFICATIONS

Single agent for prevention, detection and response, with always-on protection for off-network or off-line devices.

Deploys in minutes with no end user impact or reboot required

Protects privacy and secrecy across global operations with a unique flexible cloud and on-premises architecture

PERFORMANCE:

- Average CPU Usage: < 1%
- Memory Utilization: 150MB
- Disk Usage: < 500MB
- Configurable Event Storage

OS SUPPORT: Protects Windows, MacOS, Linux, and Solaris operating systems

- Windows Desktop: Windows 7, 8.1, 10
- Windows Server 2008R2, 2012R2, 2016, 2019
- Linux: RHEL 6, 7, 8 CENTOS 6, 7, 8 Ubuntu 14.04, 16.04, 18.04
- Mac: 10.11 (El Capitan), 10.12 (Sierra) 10.13 (High Sierra), 10.14 (Mojave), 10.15 (Catalina)
- Solaris 10 x86

VALIDATIONS

- "Endgame leads the pack in real-time alert generation across the kill chain." — Josh Zelonis, Forrester MITRE ATT&CK Evaluation Guide

PCI DSS COMPLIANT · amtso · AV comparatives · AICPA SOC · HIPAA COMPLIANT

MITRE · virustotal · FORRESTER · ENDGAME Endpoint Security v3.3 ADVANCED ENDPOINT PROTECTION NSS LABS RECOMMENDED MARCH 2019