SOLUTION BRIEF

ENDGAME AUTOMATE THE HUNT

Enterprises are battling targeted attacks. These attacks are 100% successful because they are well planned and resourced, are human driven and have a level of sophistication that bypasses existing prevention technologies. Endgame automates the hunt for targeted attacks and all of their technologies and techniques. Our ‘flyaway’ features enable rapid hunt operations in enterprise and partner networks. Our AI mentor makes advanced hunt tradecraft accessible in simple English for analysts.

Endgame Hunt is part of the only endpoint protection platform designed to stop advanced attacks and all of their components, before damage and loss occurs, all in a single agent, at enterprise scale, with the people you already have.

RAPID HUNTING AT ENTERPRISE SCALE

With a few clicks, security analysts can discover, deploy, and hunt in minutes.

ADVERSARY TRADECRAFT ANALYTICS

Hundreds of tradecraft analytics streamline detection and response workflows to surface suspicious artifacts across millions of records in minutes.

ENDGAME ARTEMIS®

Endgame Artemis® an AI-powered security mentor, enables analysts to triage, prioritize alerts, remediating endpoints without relying on complex queries and known IOCs.

PRECISION RESPONSE

Single-click response actions, including thread level suspension, enables SOC teams to evict adversaries without business disruption.

DISSOLVABLE/PERSISTENT MODE

Built-in deployment, endpoint discovery and dissolvability options empower analysts to protect unmanaged networks in minutes across hundreds of thousands of endpoints.

> “**ENDGAME** *elevates our tier 1 analysts to operate at a tier 3 level, allowing us to spend less time and resources on incident response and compromise assessment. With Endgame, we can prevent, detect, and proactively hunt advanced attacks at the earliest possible moment, before damage and loss of critical assets.*”
>
> **Ryan Gurr, Information Security Manager, NuScale Power**

STOP MALICIOUS PERSISTENCE ACROSS 50,000 ENDPOINTS IN 5 MINUTES

CHALLENGE

Today's attackers use multiple vectors to cause enterprise-wide data theft and destruction. The majority of these attacks are completely fileless. Hidden within legitimate system processes, advanced adversaries, evade detection by IR and hunt teams. Finding fileless attacks takes a memory forensics expert hours to analyze a single system and is impossible at enterprise scale.

SOLUTION

Endgame's patent-pending fileless attack detection performs memory forensics at scale in minutes to find hidden adversaries. Endgame's adversary tradecraft and kernel-level access to the operating system elevates analysts of any skill level with the expertise of a memory forensic expert.

- One-click process hunt performs a complete inspection of system memory, identifying in-memory attacks including memory modification, memory injection, hidden modules and more. With a single pivot, analysts can perform instant malicious thread suspension, without any loss of system stability.

NEW PRODUCTIVITY WITH THE EXISTING PEOPLE

CHALLENGE

Attackers maintain persistent access to compromised systems that survive reboots by changing windows registry settings or by replacing legitimate DLLs. Because there are hundreds of unique persistence locations on an endpoint, it is impossible to detect malicious persistence at enterprise scale in time to stop damage and loss.

SOLUTION

Endgame's best-in-industry detection eliminates malicious persistence across 50,000 endpoints in minutes.

- Our persistence hunt looks for advanced techniques such as COM Hijacking, Search Order Hijacking, and Phantom DLL Hijacking to surface suspicious persistence locations in seconds.
- Endgame Malware Score® identifies malware hiding in windows registry settings.

ENDGAME VALUE

STOP TARGETED ATTACKS

Full-stack prevention, accelerated detection and response, and automated threat hunting stops attackers across the entire breadth and depth of the MITRE ATT&CK™ Matrix.

BEFORE DAMAGE AND LOSS

A single autonomous agent and a single console provides pre-execution and post-execution protection of known and unknown attacks at the earliest and all stages of the attack lifecycle at enterprise scale.

WITH THE PEOPLE YOU HAVE

Endgame elevates Tier 1 analysts and accelerates Tier 3 analysts with Endgame Resolver™ and Artemis®, an AI-powered security mentor that provides guided work flows and tradecraft analytics to instantly discover and remediate malicious activity at enterprise scale.

REDUCED OPERATIONAL COST AND COMPLEXITY

Endgame's single agent, single console platform replaces existing AV, Next-gen AV, incident response and forensic agents, eliminating cost and complexity in the enterprise security stack.