ENDGAME.

SOLUTION BRIEF

Endgame Detection & Response

Endgame is the only endpoint protection platform that has the scope to stop targeted attacks, the speed to prevent damage and loss, and the simplicity to get the job done with the people you already have. Our single-agent solution for IT Operations, SOC, and Hunt teams, replaces multiple agents, including AV, Next-gen AV, Exploit Protection, Incident Response, and IOC-based agents. Endgame's autonomous agent provides online and offline protection, without requiring any connectivity to the internet.

ENDGAME'S SINGLE AGENT PROVIDES

Automated EDR & Tailored SOC Operations

AUTOMATED DETECTION & RESPONSE

Endgame Resolver™
Intuitive attack visualization leveraging file, registry user, process, network, netflow, and DNS data.

Endgame Artemis™
An AI-powered, natural language understanding security chatbot for plain English investigations.

Precision Response
Restore endpoint operations and conduct advanced forensic analysis with zero business disruption.

TAILORED SOC OPERATIONS

Endgame Arbiter™
Automate malware sandboxing and advanced attack analysis for prioritization and IOC extraction.

Automated Hunt with Adversary Tradecraft Analytics
Hundreds of tradecraft analytics streamline detection and response and automated hunt workflows.

User Defined Policy
Across the breadth and depth of the MITRE ATT&CK™ Matrix.

WITH ENDGAME

STOP TARGETED ATTACKS

85% MITRE ATT&CK™ COVERAGE*

99% EFFECTIVE AGAINST APT EXPLOITS

99.5% EFFECTIVE AGAINST KNOWN & UNKNOWN MALWARE

WITH THE PEOPLE YOU HAVE

97% REDUCTION IN TIME TO DETECT

5X INCREASED ANALYST PRODUCTIVITY

10 MIN MEMORY ANALYSIS AT ENTERPRISE SCALE

REDUCE OPERATIONAL COSTS

1 AGENT REPLACES FIVE

< 1% OVERALL SYSTEM IMPACT

1 SOLUTION FOR ALL ENTERPRISE ENDPOINTS (WIN, MAC, LINUX, SOLARIS)

*85% COVERAGE IN THE APT3 EVALUATION BY MITRE

THIRD PARTY VALIDATION

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

Oil & Gas

STOPPING FILELESS ATTACKS ON ONLINE AND OFFLINE ASSETS

CHALLENGE

A leading oil and gas company with offshore subsea drilling services has diverse, disconnected endpoints located across multiple geographies. The company was targeted by fileless attacks, a rising attack vector, that bypassed their existing endpoint security tools. Also, their most high-value assets were often not connected to the internet and needed offline protection.

SOLUTION

Endgame's patent-pending fileless attack technology prevents techniques like shellcode injection and DLL injection. Kernel-level analysis, performed on every executing thread, stops fileless attacks before an adversary can gain a foothold in memory. Endgame addressed the company's

Large Education

WITH THE PEOPLE YOU ALREADY HAVE

CHALLENGE

A large educational institution with over 20 IT departments, serving 11 universities, 7 stand-alone 'operating units', including healthcare providers, research institutions with US DoD projects, and multiple state government agencies were looking to reduce the time to detect and to remediate threats within their network. They had a small team who dealt with increased workloads and were exposed to alert fatigue. Because experts are difficult to hire and retain, while nimble, the team was made of mostly junior analysts with limited experience handling targeted attacks.

SOLUTION

Endgame elevated the capabilities of their tier 1 analysts, and accelerated tier 3 analysts. Endgame Resolver™ attack visualization instantly renders the the origin, extent, and timeline of an attack. This context combined with Endgame Artemis®, an AI-powered security mentor, guides SOC analyst to prioritize, triage, and remediate alerts, before damage and loss occurs without relying on complex queries and known IOCs.

Federal Customer

AUTOMATED HUNTING

CHALLENGE

A large U.S. Department of Defense (DoD) customer has cyber protection teams (CPT) that are constantly battling nation-state adversaries. The CPTs were in need of a protection technology that could rapidly hunt and respond to targeted attacks, without any business disruption. The platform had to be easy to use without additional training and protected against nation-state techniques such as persistence, fileless attacks, lateral movement, and broader coverage across the attacker techniques and tactics.

SOLUTION

Endgame's single agent solution stops known and unknown attacker techniques across the breadth and depth of the MITRE ATT&CK™ matrix. Endgame leverages knowledge of hundreds of adversary tradecraft and sequential analytics to streamline detection and response and automated hunt workflows. Data collection, investigations, and alert triage are performed at enterprise scale to surface suspicious artifacts in seconds. Endgame's precise scalable response enabled CPTs to restore endpoint operations across the enterprise and conduct advanced forensic analysis with zero business disruption.

ENDGAME.

Endgame.com

Schedule a demo now with demo@endgame.com

@EndgameInc EndgameInc Endgame