ENDGAME.

SOLUTION BRIEF

ENDGAME DETECTION & RESPONSE

Endgame is the only endpoint protection platform that includes trade craft protection techniques covering the complete MITRE ATT&CK™ Matrix, stopping targeted attacks at any stage before damage and loss occur, with the people you already have today. A single interface provides all administration and agent management and is designed to streamline incident response and hunt operations. A single agent can replace multiple endpoint agent products, including AV, Next-gen AV, Exploit Protection, Incident Response, and IOC-based sensors. Endgame's Cloud-first platform provides instant time to value by reducing deployment time and resources. The on-premises option can combine with cloud-services to allow granular, per-endpoint data privacy controls. Endgame combines complete on-line and off-line protection against exploits, phishing, malware, ransomware, fileless attacks. What's more, Endgame goes beyond malware to detect and block known and unknown attacks in minutes across the enterprise with zero disruption.

ENDGAME'S SINGLE AGENT PROVIDES

AUTOMATED EDR & EFFICIENT SOC OPERATIONS

INTELLIGENT EDR ANALYSIS & INVESTIGATION

ENDGAME RESOLVER™
Intuitive attack visualization leveraging file, registry user, process, network, netflow, and DNS data

ENDGAME ARTEMIS®
An AI-powered security mentor with natural language understanding answers to plain English questions and empowers analysts of all skill levels

AUTOMATED HUNT
Hundreds of tradecraft analytics streamline high-fidelity detections across the MITRE ATT&CK Matrix, with automated hunting and rapid response workflows

HIGHLY EFFICIENT SOC OPERATIONS

ALERT DASHBOARD
Prioritizes threats and adversarial behaviors to simplify what's important and eliminate alert fatigue

ENDGAME REFLEX™
The first language and development environment for behavioral security and compliance policy enforcement

RAPID, ACCURATE RESPONSE
Restore endpoint operations and conduct advanced forensic analysis with zero business disruption

WITH ENDGAME

STOP TARGETED ATTACKS

85%
MITRE ATT&CK™ COVERAGE*

99%
EFFECTIVE AGAINST APT EXPLOITS

99.5%
EFFECTIVE AGAINST KNOWN & UNKNOWN MALWARE

CLOSE THE SKILLS GAP

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 LABS 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 challenge of protecting their disconnected high-value assets with our lightweight autonomous agent that provides protection for online and offline systems.

HIGHER 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.