ENDGAME.

SOLUTION BRIEF

Endgame Prevention

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 UNIFIED PREVENTION STOPS

Pre & Post-Execution Attacker Techniques

PRE-EXECUTION

Exploit Prevention
Patent-pending HA-CFI and enhanced Dynamic Binary Instrumentation (DBI)

Malicious Macro Prevention
Heuristic-based prevention for macros embedded in Microsoft Office

Malware & Ransomware Prevention
Machine-learning, signatureless

POST-EXECUTION

Ransomware Behavioral Prevention
2nd layer of ransomware prevention
Dynamic, behavior based

MITRE Technique Focused Prevention
Across the breadth and depth of the MITRE ATT&CK™ Matrix

Fileless Attack Prevention
Patent-pending process injection prevention

WITH ENDGAME

STOP TARGETED ATTACKS

85%
MITRE ATT&CK™ COVERAGE*

99%
EFFECTIVE AGAINST APT EXPLOITS

99.5%
EFFECTIVE AGAINST KNOWN & UNKNOWN MALWARE

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

Financial Services

PREVENT EXPLOITS & MACROS BEFORE THEY RUN

CHALLENGE

A top 10 global financial services company has 100,000+ endpoints, 215,000 servers, and sprawling network infrastructure. Their business processed millions of transactions per minute and any disruption resulted in significant losses. The SOC team was looking for a solution to stop exploitation of vulnerabilities, malicious macros, and comprehensive coverage of multiple attack vectors.

SOLUTION

Endgame blocks exploits and malicious macros before attacker code execution. Unlike any other solution, our patent-pending HA-CFI™ and enhanced DBI prevents zero-day exploits before malicious code execution. Our heuristic-based macro prevention blocks malicious macros embedded in commonly targeted applications. Endgame's exploit and macro prevention technology achieves greater than 99% effectiveness against all active exploit kits and APT samples.

Healthcare

BLOCKING RANSOMWARE & MALWARE ATTACKS

CHALLENGE

A regional healthcare organization required to protect critical electronic patient health information (ePHI) ensuring compliance with HIPAA (Health Insurance Portability and Accountability Act) and PCI DSS are met. This means they must have the ability to prevent ransomware and malware based attacks across their Windows and Mac endpoints.

SOLUTION

Endgame platform protects the healthcare organization's critical data by blocking malware on mac and Windows endpoints. Our signature-less machine learning model, Endgame MalwareScore™, stops known and unknown malware with 99.5% efficacy. Our dynamic behavior-based protection blocks ransomware attacks and protects against critical data loss. Endgame monitors all processes to stop ransomware attacks, including BadRabbit, NotPetya, WannaCry, and Locky before they cause damage.

Oil & Gas

STOPPING FILELESS ATTACKS ON ONLINE & 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 adversaries using fileless attacks, a rising attack vector, that bypassed their existing endpoint security tools. Many of their high-value assets were not connected to the internet yet they still 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.