DATA SHEET

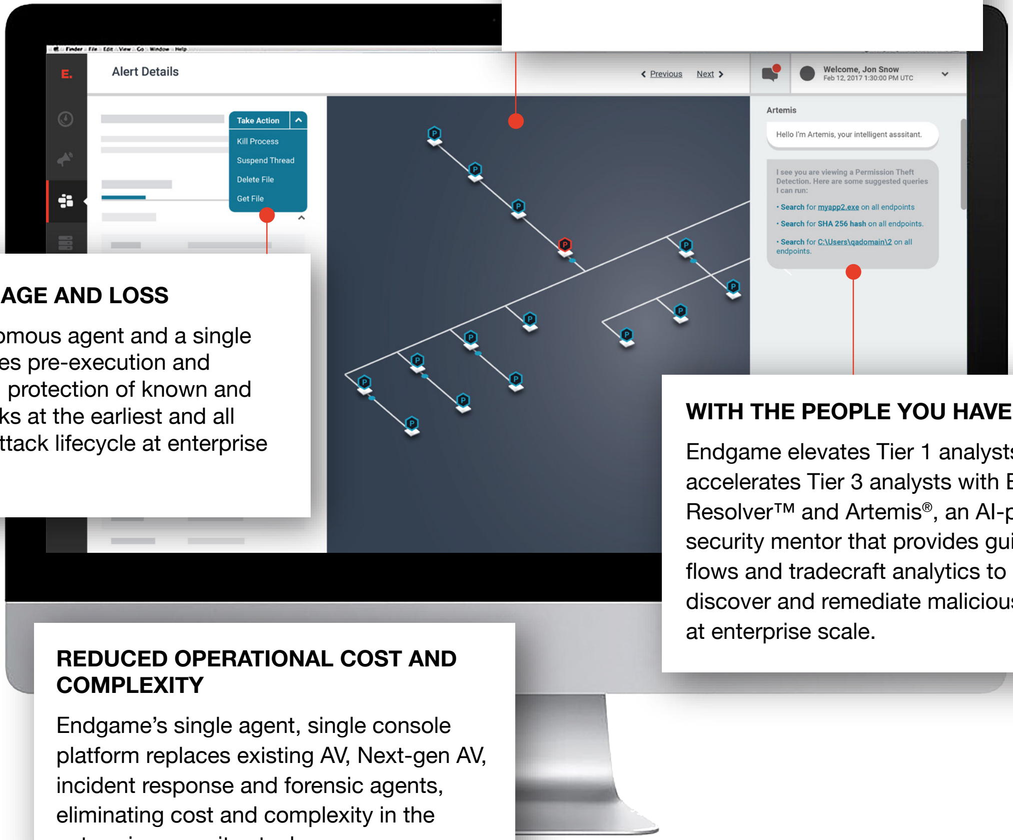
ENDGAME PLATFORM:
Zero Breach Tolerance

Endgame is the only endpoint security platform that stops targeted attacks and all of their technologies and techniques, before damage and loss occurs, with the people you already have. Our single-agent solution for IT Operations, SOC, and Hunt teams, replaces multiple agents for prevention, detection and response, and threat hunting, providing full stack protection at the earliest and all stages of the attack lifecycle.

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.



Hello I'm Artemis, your intelligent asssitant.

I see you are viewing a Permission Theft Detection. Here are some suggested queries I can run:

- Search for myapp2.exe on all endpoints
- Search for SHA 256 hash on all endpoints.
- Search for C:\Users\qadomain\2 on all endpoints.

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.

STOP TARGETED ATTACKS

Full-stack prevention, accelerated detection and response, and automated hunting stops targeted attacks across the breadth and depth of the MITRE ATT&CK™ matrix.

- ***Exploit Prevention:*** Patent-pending Hardware Assisted Control Flow Integrity (HA-CFI™) and enhanced Dynamic Binary Instrumentation (DBI) blocks zero-day exploits before malicious code execution.
- ***Malware Prevention:*** Machine learning powered signature-less malware prevention, Endgame MalwareScore®, certified by SE Labs and AV-Comparatives and running in VirusTotal, prevents execution of known and unknown malware with 99.5% efficacy.
- ***Fileless Attack Prevention:*** Patent-pending process injection prevention and MalwareScore® prevents malicious module loads, dll injection, and shellcode injection to stop adversary evasion and fileless attacks.
- ***Malicious Macro Prevention:*** Heuristic-based macro prevention blocks malicious macros embedded in commonly targeted applications such as MS Office applications.
- ***Ransomware Prevention:*** Behavior-based ransomware prevention is effective against ransomware families such as BadRabbit, Petya, WannaCry, Locky, etc. Our ransomware prevention monitors all process activity to stop ransomware attacks before encryption.
- ***Technique-focused protection*** expands across the breadth and depth of the MITRE ATT&CK™ matrix stopping ongoing attacks such as malicious persistence, credential dumping, malwareless attacks, and privilege escalation by leveraging Endgame's knowledge of adversary tradecraft.

BEFORE DAMAGE AND LOSS

Earliest protection with a single autonomous agent and single console to stop targeted threats

- ***Autonomous agent*** provides 24x7 online and offline protection with no round-trip time to cloud or the platform.
- ***Precision and scalable response*** empowers SOC teams to restore endpoints at enterprise scale with zero business disruption.
- ***Tradecraft analytics and Outlier analysis*** streamlines detection and response workflows to surface suspicious artifacts across millions of records in minutes.

WITH THE PEOPLE YOU HAVE

Elevate Tier 1 analysts and Accelerate Tier 3 analysts to stop targeted attacks.

- ***Endgame's AI-powered security mentor, Artemis***®, uses natural language understanding to automate data collection, investigation, and alert triage at enterprise scale.
- ***Endgame Resolver***™ attack visualization instantly renders the origin, extent and timeline of an attack by leveraging real-time data collection and analysis for file, registry, user, process, network, netflow, and DNS data.
- ***Endgame Arbiter®,*** automates advanced attack analysis to determine file reputation, attack type, and other attributes, extracting IOCs to reveal previously unknown threats across the entire enterprise.

demo@endgame.com

TECHNICAL FEATURES

1 **Single Dissolvable or Persistent agent** provides 24x7 online and offline protection

2 **Built-in deployment in minutes** across the enterprise to protect unmanaged networks

3 **On-premise and cloud deployment,** hosted by Endgame or by the customer

4 **Robust two-way API support** for integration with existing workflows including orchestration, ticketing, and reporting tools

5 **Protects Windows and Linux** operating systems

Windows CentOS redhat LINUX ubuntu

6 **Validations**
First to be validated against the MITRE ATT&CK™ matrix

virustotal

AV comparatives Approved Business Product 2017

SE Labs

MEMBER amtso Anti-Malware Testing Standards Organization

ENDGAME.