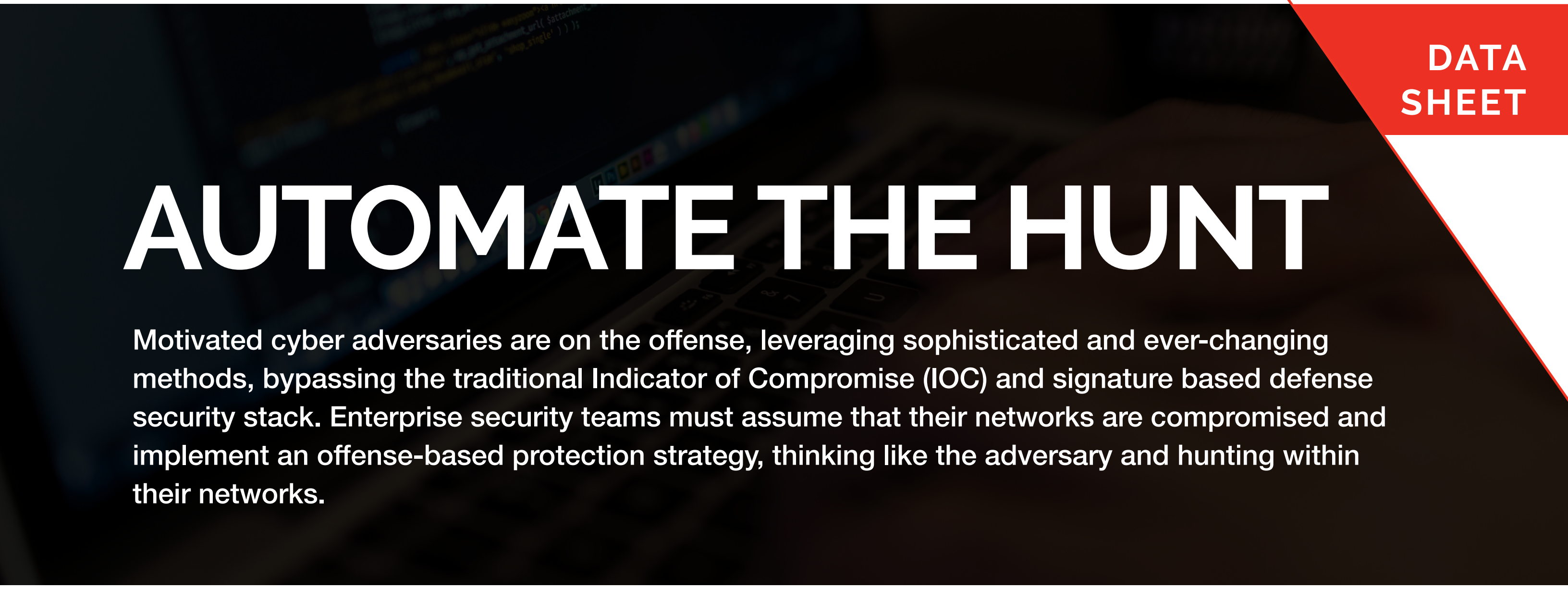


DATA SHEET

AUTOMATE THE HUNT

Motivated cyber adversaries are on the offense, leveraging sophisticated and ever-changing methods, bypassing the traditional Indicator of Compromise (IOC) and signature based defense security stack. Enterprise security teams must assume that their networks are compromised and implement an offense-based protection strategy, thinking like the adversary and hunting within their networks.

Endgame is the first and only hunt platform to detect and prevent known and never-before-seen attacks at the earliest and all stages of the kill chain. Because Endgame's early detection and prevention does not depend on IOCs, security analysts can stop damage and loss without any prior knowledge of adversary malware or attack infrastructure. Stealth at deployment, runtime and operations prevents evasion by adversaries that disable or avoid traditional security technologies. Endgame empowers hunt, IR and SOC teams with comprehensive hunt automation: built-in asset discovery, intelligent collection, one click investigation, and surgical response, ensuring rapid enterprise wide detection and remediation

> "Endgame's Hunt platform is helpful in allowing an analyst to quickly detect never-before-visible malicious behaviors on host systems, and block and remove threats at the earliest stages."
>
> *- Ryan Gurr, Information Security Manager at NuScale Power*

ENDGAME V2 FEATURES

Hardware-assisted control flow integrity (HA-CFI™) exploit protection stops the adversaries in real-time before code execution.

Endgame MalwareScore™ detects malicious files without relying on signatures, streamlining the hunt process by providing key information to focus hunters' attention.

Automated Investigation reduces the hunt from days to seconds via one-click adversary detections based on IOC-independent adversary techniques

A single lightweight stealth sensor for detection, prevention and response with on-demand and persistent deployment options across enterprise critical systems.

ENDGAME ADVANTAGES

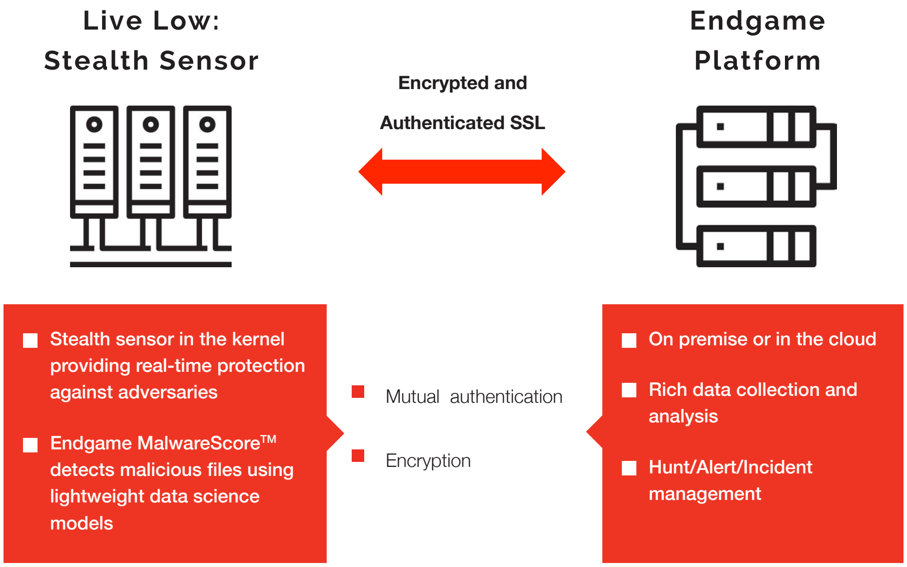
- **IOC independent detection:** Endgame rapidly detects and prevents adversaries at the earliest stages of the kill chain without relying on IOCs, by focusing on adversary techniques. By monitoring low-level chokepoints within the OS, Endgame blocks adversary techniques, such as credential dumping, process injection and token impersonation. Our HA-CFI™ exploit protection stops the adversaries before code execution. Endgame MalwareScore™ instantly detects known and never-before-seen malicious activity across critical systems.

- **Stealth Operations:** Endgame evades detection to protect hunt missions from disruption. Stealth deployment leaves no artifacts on disk. Signature diversity within and across enterprises prevents fingerprinting. Industry leading anti-tampering protections prevent disabling, protecting hunt operations from disruption.

- **Tailored and surgical response:** Adversaries often inject into critical system processes to hide from outlier analysis. Even if they're detected, this makes remediation difficult without disrupting production operation. The Endgame thread-level suspension capability provides precise and tailored response to ensure protection of compromised systems without disabling them.

- **Hunt automation:** Endgame automates the entire hunt process, from asset discovery to analyst response ensuring instant enterprise wide detection and remediation. Automated Investigations reduce the hunt from days to seconds with one-click detections of adversary techniques at scale across the network.

ENDGAME ARCHITECTURE



Live Low: Stealth Sensor

Encrypted and Authenticated SSL

Endgame Platform

- Stealth sensor in the kernel providing real-time protection against adversaries
- Endgame MalwareScore™ detects malicious files using lightweight data science models

- Mutual authentication
- Encryption

- On premise or in the cloud
- Rich data collection and analysis
- Hunt/Alert/Incident management

ENDGAME BENEFITS

Minimize Cost & Impact of IR

Hunt automation eliminates adversary dwell time reducing investigation and forensic costs.

Zero Business Disruption

Endgame prevents theft and disruption providing mission assurance.

Empower Tier 1 & Tier 2 Analysts

Predefined hunt playbooks and hunt automation, from asset discovery to analyst response improves analyst productivity.