DATA SHEET

ENDPOINT PROTECTION PREVENT, STOP, HUNT.

Endgame prevents all attacks, stops attacks in-progress, and for the next generation of attacks, we Automate the Hunt™

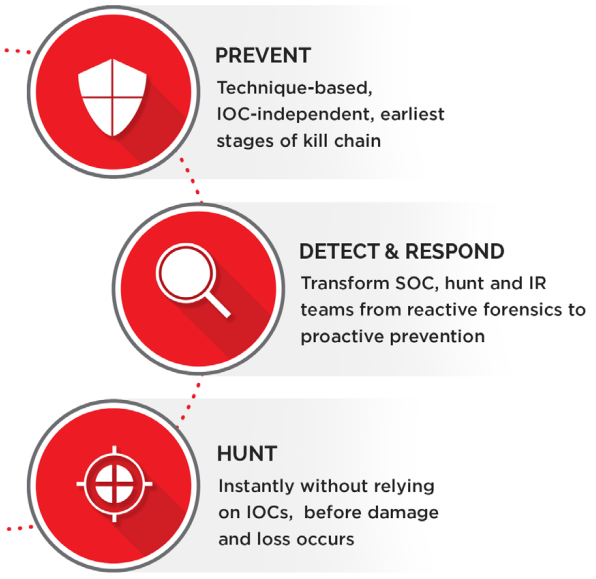
Motivated cyber attackers bypass the traditional Indicator of Compromise (IOC), signature-based defense security stack as well as next-gen prevention agents. Endgame is the only solution that prevents damage and loss from all new attacks, stops on-going attacks, and automates the hunt for the next generation of attacks.

Endgame is a centrally managed endpoint security platform that operates at the earliest and all stages of the attack life cycle. Through a single agent, Endgame transforms security operations teams and incident responders from relying on reactive response to proactive prevention, dramatically reducing time and cost associated with incident response.

Endgame prevents compromise including exploits, malware, and malware-less attacks. Our platform blocks exploits before a single attack instruction is executed, and prevents malware without signatures, and blocks malware-less attacks with patented process injection technology, prohibiting the adversary from gaining a foothold in the enterprise.

Endgame stops on-going attacks at the earliest and all stages of the attack life cycle, instantly detecting and stopping privilege escalation, defense evasion, malicious persistence, credential access, and propagation.

Endgame automates the hunt for the next generation of attacks - automating data collection for numerous data types across all endpoints in seconds, and instantly surfacing suspicious artifacts and malicious activity with pre-built whitebox analytics and act with precision to prevent disruption.



ENDGAME ADVANTAGES

- **Earliest Prevention:** Endgame prevents known and unknown threats at the earliest stages of the attack cycle without relying on IOCs, before damage and loss occur.
  - *Endgame's predictive exploit* prevention stops adversaries in real-time before they execute code by autonomously predicting changes in program control flow to pre-empt malicious execution.
  - *Endgame MalwareScore™* detects known and unknown malicious files without relying on signatures, streamlining the detection process by providing key information to focus analysts' attention.
  - *Fileless attack protection* prevents malware-less attacks with patented process injection and identifies advanced evasion techniques attackers use to hide their presence in enterprise networks.
- **Accelerated Detection:** Endgame stops attackers at the earliest stages of the attack life cycle by detecting advanced techniques across the breadth of the attacker life cycle and depth of ATT&CK matrix . By monitoring chokepoints within the operating system we detect advanced techniques such as privilege escalation, malicious persistence, credential theft, lateral movement, and in-memory attacks
- **Hunt Automation:** Automated collection, analysis and response reduce the hunt from days to seconds with one-click detections of adversary techniques at scale across the network. Whitebox analytics help analysts surface suspicious artifacts across millions of records in minutes, before damage and loss occur. Two-way API support ensures integration with workflow, external data, and existing process and reporting.
- **Uninterrupted Operations:** Endgame's single lightweight agent prevents, detects and responds to advanced threats, on-demand and persistent deployment options across the entire enterprise. Signature diversity within and across enterprises prevents fingerprinting of the agent. Industry leading anti-tampering protections prevent disabling, protecting hunt operations from disruption.

ENDGAME BENEFITS

Stop Damage and Loss

IOC-independent prevention and detection stops advanced attacks at the earliest and all stages of the kill chain.

Transform Hunt, IR and SOC teams

Automated ATT&CK matrix protections and whitebox analytics equip analysts to instantly discover anomalies and precisely respond at scale across the enterprise.

Eliminate IR and Forensic Costs

Early prevention and accelerated detection minimizes adversary dwell time eliminating investigation and forensic costs.

ENDGAME PROTECTIONS

PREVENT

EXPLOIT
- Predictive Prevention (HA-CFI™)
- Dynamic Binary Instrumentation (DBI)

MALWARE
- Signature-less MalwareScore™

MALWARE-LESS=
- Patent pending process injection

DETECT and RESPOND

ESCALATION
- Permission Theft (user mode)
- Credential Manipulation (kernel mode)

EVASION
- Fileless attack detection
- Persistence Hijacks

CREDENTIAL ACCESS
- Credential Dumping

PERSISTENCE
- MalwareScore™

PROPAGATION
- Lateral Movement Detection

HUNT

WHITEBOX ANALYTICS
IOC SEARCH AT SCALE
DIRECTED ALERT TRIAGE
INTEGRATION
- 2-way API
- SIEM

USER-CREATED RULES

ENDGAME.