DATA SHEET:

esENDPOINT

Prevent the Predictable. Hunt the Elusive.

PREVENT THE PREDICTABLE

Identify suspicious behavior using predictive threat modeling to automatically block expected, unexpected and fileless attacks.

DETECT THE ELUSIVE

Find threats built to circumvent prevention with a zero-trust approach, leveraging proprietary machine learning and advanced analytics.

HUNT AND ISOLATE BEFORE DISRUPTION

Minimize threat actor dwell time with elite eSentire threat hunters that identify, lock down and isolate compromised endpoints on your behalf.

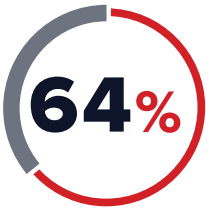
HARDEN AGAINST FUTURE ATTACKS

Determine root cause and eradicate threat actor presence across your environment with full incident lifecycle support.

esENDPOINT, powered by CrowdStrike and Carbon Black and built on zero trust, protects your assets 24x7x365 no matter where users or data reside. esENDPOINT is a single agent that combines our elite threat hunting with endpoint protection platform (EPP) and endpoint detection and response (EDR) capabilities to eliminate blind spots traditional prevention misses.

Our team of experts uses predictive threat modeling and proprietary machine learning to continuously tune the latest detection measures to prevent known attacks and identify potential unknown and zero day threats.

For the most elusive of threats, an elite team of eSentire threat hunters rapidly investigate and neutralize compromised endpoints on your behalf, preventing lateral spread. Supporting the full incident response lifecycle, we work alongside your security team to determine root cause and corrective actions, ensuring your environment is hardened against future business disruption.



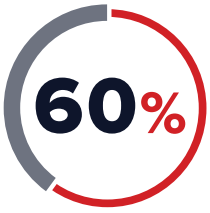
of organizations experienced one or more successful endpoint attacks in the last year[1]

- **10%** increase year-over-year
- **76%** of those attacks were unknown or zero days

of organizations state traditional antivirus does not provide adequate protection[2]

Current endpoint adoption:

- **76%** traditional AV
- **30%** EDR
- **23%** next-generation AV



of organizations state they lack ample resources to minimize IT endpoint risk due to an infection[3]

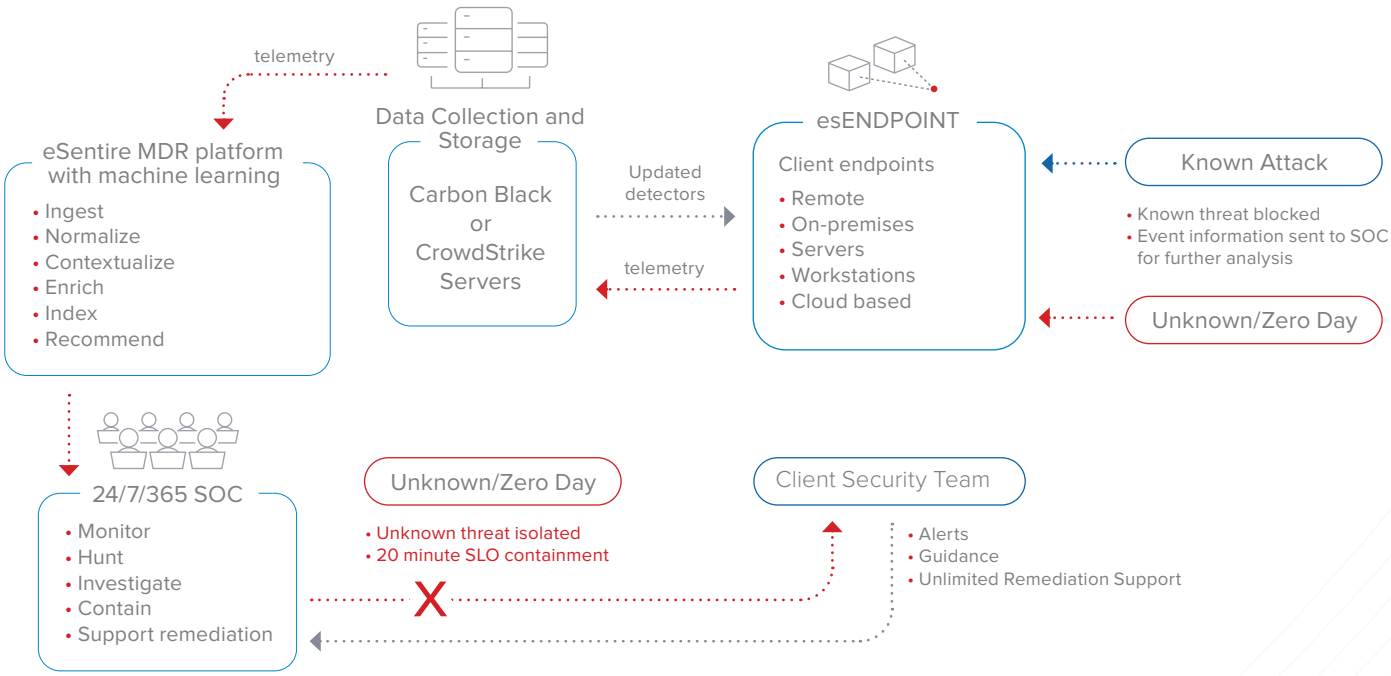
- **47%** of organization say lack of in-house resources
- **36%** say it is too complex to manage
- **50%** say lack of in-house expertise
- **24%** say it is too costly to manage

[1,2,3]Ponemon: 2018 State of Endpoint SecurityRisk

WHAT DOES esENDPOINT DETECT?

- Malware
- Known attacks
- Suspicious activity
- Abnormal behavior
- File-less attacks
- Advanced persistent threats
- Lateral movement
- Zero-day attacks

HOW IT WORKS



FEATURES

24x7x365 Coverage

Monitors endpoints on and off the network around the clock with eSentire's global Security Operations Centers (SOCs).

Zero Trust

Assumes the suspicious is malicious sending all endpoint activity that has not been seen before to an elite team of threat hunters.

Industry-Leading Technologies

Eliminates blind spots under a singular solution powered by market leaders CrowdStrike and Carbon Black.

Single Agent

Reduces complexity and management with a single lightweight agent that collects all endpoint data without sacrificing operational performance.

Endpoint Anywhere Visibility

Protects your endpoints anywhere users and data reside–across cloud, mobile, virtual and physical environments.

Endpoint Activity Recording

Accelerates forensic investigation, acting as a "black box" flight recorder that continuously records, centralizes and retains vital endpoint activity.

Automated Blocking

Prevents known, unknown and fileless attacks using predictive threat modeling and behavioral analysis.

Advanced Detection of Unknown and Zero Days

Catches what prevention misses with proprietary machine learning layered with attack pattern and behavioral analytics.

Integrated Expertise

Speeds deployment and continuously adapts and hardens endpoints, alleviating resource constraints.

Elite Threat Hunting

Pursues elusive threat actors and performs rapid forensic investigation, enabling timely containment and root cause determination.

Remote Managed Containment

Locks down and isolates threat actors on your behalf preventing lateral spread and potential business disruption.

Full Incident Lifecycle Support

Eradicates threat actor presence with co-managed remediation from initial detection to confirmation of hardening and monitoring for reentry.

THE esENDPOINT DIFFERENCE

	Other EDR	esENDPOINT
24x7 continuous monitoring, recording and centralizing of activity	✓	✓
Continuous management, tuning and refinement of detection platform	Varies (May Require Add-on to Service)	✓
Singular agent	Varies	✓
Prevention of known attacks	✓	✓
Detection of unknown attacks using machine learning and advanced analytics	Limited	✓
Active threat hunting	Limited (May Require IR Retainer)	✓
Alerting of confirmed threats and suspicious behavior	✓	✓
Full forensic analysis to confirm threat and eliminate false positives	Varies (May Require IR Retainer)	✓
Tactical threat containment on customer's behalf via host isolation to stop lateral spread	Varies	✓
Root cause determination	Varies (May Require IR Retainer)	✓
Remediation and hardening recommendations	✓	✓
Full incident lifecycle support	Requires IR Retainer	✓

MAKE THE CASE FOR esENDPOINT

- Rapid deployment and quick time to value
- Optimized and hardened state of endpoint defense
- Elimination of physical and virtual endpoint blind spots
- Blocking of known, unknown and fileless attacks
- Detection of elusive attackers and zero-day threats
- Isolation of compromised endpoints, preventing lateral spread
- Reduction in operating expenditure cost and resource demands
- Minimized incident recovery timeframe
- Improvement in overall security posture
- Mitigation of potential business disruption
- Satisfaction of compliance requirements

eSENTIRE®

About eSentire:

eSentire, Inc., the global leader in **Managed Detection and Response (MDR)**, keeps organizations safe from constantly evolving cyberattacks that technology alone cannot prevent. Its 24x7 Security Operations Center (SOC), staffed by elite security analysts, hunts, investigates, and responds in real-time to known and unknown threats before they become business disrupting events. Protecting more than $6 trillion AUM, eSentire absorbs the complexity of cybersecurity, delivering enterprise-grade protection and the ability to comply with growing regulatory requirements. For more information, visit **www.esentire.com** and follow **@eSentire**.