eSENTIRE®

DATA SHEET

Managed Endpoint Defense

Powered by CB Defense

Next-gen endpoint threat detection and response

DEPLOY AND HARDEN.

Rapidly deploy and optimize endpoint prevention with dedicated security experts that continuously refine and harden rules and policies that account for your unique threat landscape.

PREDICT AND PREVENT.

Block known, unknown, and file-less attacks leveraging predictive modeling with integrated threat intelligence and expert-driven continuous threat tuning.

RESPOND SWIFTLY.

Reduce mean time to response with attack chain visualization and integrated endpoint isolation capabilities that prevent lateral spread and business disruption.

THE PROBLEM

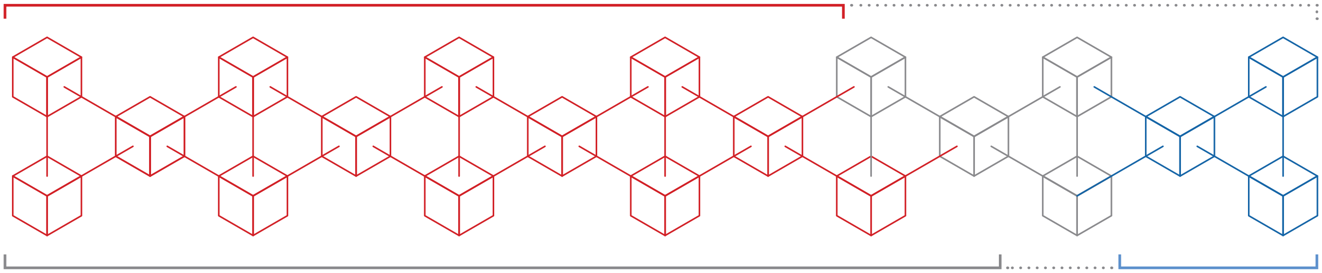
Endpoints are among the most popular targets for sophisticated threat actors. Intrusions are inevitable despite strong adoption in employee security awareness training, email security, and related solutions. A majority can be prevented with proper implementation, continuous tuning and advanced detection capabilities that account for the latest threats. However, if your company is not a large enterprise, you likely lack the resources or security staff to effectively deploy and continuously refine next-generation antivirus solutions for your unique and evolving threat landscape.

THE ANSWER

Managed Endpoint Defense, powered by CB Defense and eSentire security experts, delivers a holistic preventative endpoint solution using predictive models that continuously adapt and harden defenses to better identify and automatically block known, unknown, and file-less attacks. eSentire works with you to speed deployment and continuously tailor policies to your unique risk profile. Our security specialists deliver uncompromised protection by integrating lessons learned from years of hunting and responding to attacks that bypass preventative measures. With unified attack visualization and host isolation capabilities, organizations can rapidly identify and contain potentially compromised endpoints, preventing lateral spread and business disruption.

TRADITIONAL ANTIVIRUS IS NOT THE CURE

64% of organizations reported that they experienced one or more endpoint attacks that successfully compromised assets and/or infrastructure in the last 12 months[1]



76%

of organizations are using traditional antivirus to protect their endpoints[2]

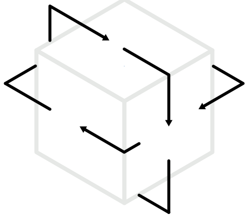
Only 15%

of organizations have replaced traditional antivirus with next-gen antivirus[3]

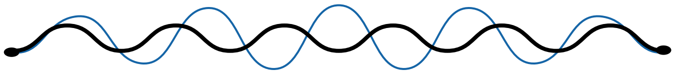
OPTIMIZED DEPLOYMENT WITH CONTINUOUS ADAPTATION IS CRITICAL

41%

of organizations say their biggest challenge with antivirus is complexity, deployment and management[4]



65% of organizations say frequency of tuning/patching is challenging or extremely challenging[5]



Only 40% of organizations believe they have ample resources to minimize IT endpoint risk due to infection or compromise6

WHAT IS MANAGED ENDPOINT DEFENSE DESIGNED TO SOLVE FOR?

- ✓ Detection limitations of traditional, signature-based antivirus solutions
- ✓ Resource limitations for deployment and initial optimization
- ✓ Limited threat visibility across endpoints
- ✓ Lack of skilled in-house resources to manage endpoint complexity
- ✓ Detection of known, unknown and file-less threats
- ✓ Resource constraints required for frequent tuning/patching
- ✓ Continuous adaptation for each organization's unique threat landscape and risk profile

[1] *Ponemon: State of Endpoint Security Risk, 2018,* [2] *Ponemon: State of Endpoint Security Risk, 2018,* [3] *Ponemon: State of Endpoint Security Risk, 2018,* [4] *Ponemon: State of Endpoint Security Risk, 2018,* [5] *Ponemon: State of Endpoint Security Risk, 2018,* [6] *Ponemon: State of Endpoint Security Risk, 2018,*

FEATURES

- **Market-leading next-generation antivirus solution**

  Full visibility into what is happening on your endpoints with advanced detection capabilities powered by CB Defense:

  - Signatures and cloud-based reputation to stop malware
  - Streaming prevention to stop advanced file-less attacks
  - Online and offline prevention
  - Flexible prevention policies
  - Customizable executive dashboard
  - Interactive attack chain visualization
  - Live Response: real-time threat remediation
  - Open APIs integrate with your security stack

- **Rapid deployment**

  Dedicated eSentire experts work with you to speed deployment and tailor initial policies contextual to your unique security requirements

- **Continuous adaptation and hardening**

  Ongoing, consultative tuning and refinement of rules and policies that results in a continuous hardened state of endpoint defense

- **Threat intelligence integration**

  Global threat intelligence integration with eSentire Managed Detection and Response that catches threats preventative technologies miss

- **Automated blocking**

  Stops advanced and file-less attacks with automated blocking to prevent business disruption

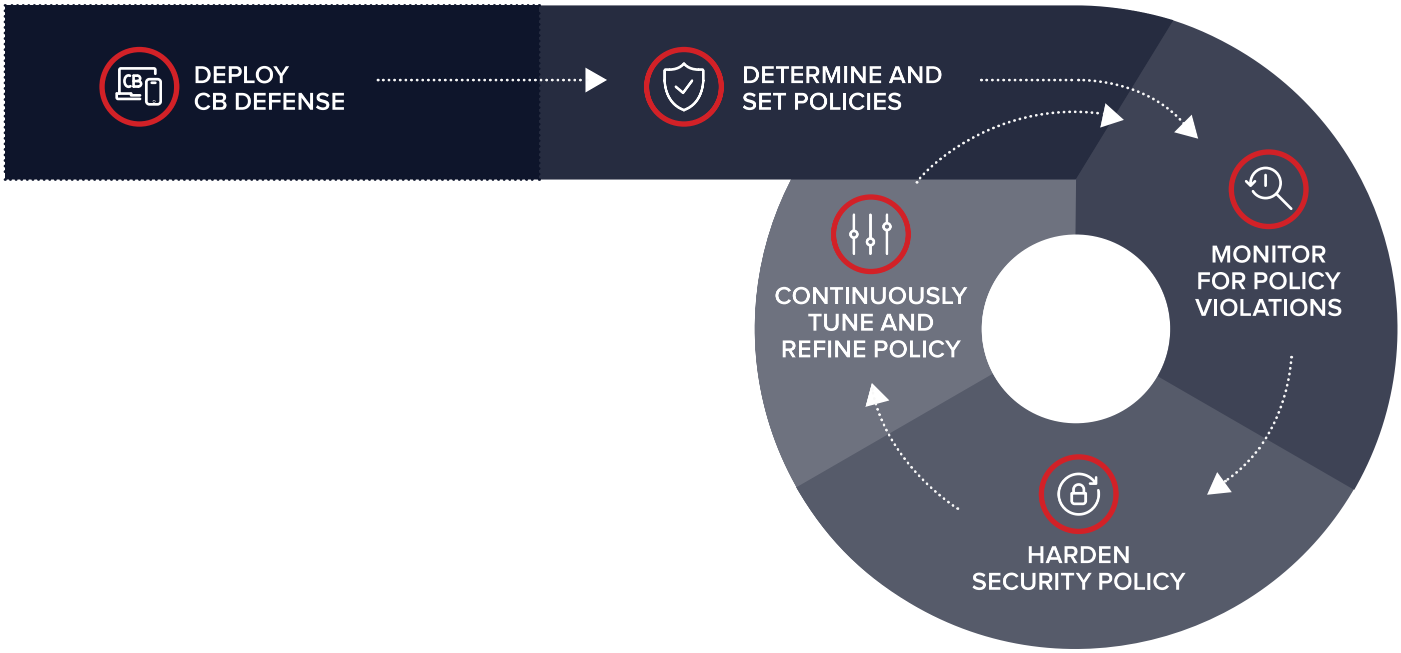
- **Integrated behavioral and cloud-based reputation**

  Identifies deceptive threats and stops suspicious behavior

- **Attack prevention**

  Locks down and isolates compromised endpoints to prevent lateral spread

HOW DOES IT WORK?



ESENTIRE VS. OTHER SECURITY PROVIDERS

	Managed Endpoint Defense		DIY	
	eSentire	Client Responsibilty/ Action Required	CB Defense Standalone	Client Responsibilty/ Action Required
Initial Agent Deployment		✓		✓
Initial Configuration (Rules and policies)	✓			✓
24x7 Monitoring	✓	✓		✓
Malware, Exploit and Ransomware Prevention	✓		✓	
Configurable Tool, Tactics and Procedure Blocking	✓		✓	
Merge and manage the signal set into a standard configuration"	✓			✓
Refinements and updates to account for client's specific environment"	✓	✓		✓
Basic Forensics Post Incident	✓			✓
DIY Quarentine and Isolation		✓		✓
Alerting of suspicious behavior	✓	✓		✓
Alerting of confirmed threats	✓	✓		✓
False positive reduction	✓		✓	
False positive elimination	✓	✓		✓
Co-managed remediation	✓	✓		✓
Host reimaging		✓		✓

MAKE THE CASE FOR ESENTIRE MANAGED ENDPOINT DEFENSE

- Rapid deployment, assisted by security experts for quicker time to value
- Full threat visibility into endpoints to close security gaps
- Optimized and hardened state of endpoint security resulting in improved protection from known and unknown attacks
- Clear alerts and prioritization of potential threats
- Easier investigation into security incidents
- Faster mean time to resolution (MTTR)
- Perpetual adaptation to your risk profile
- Continuous consultative endpoint tuning and updating of policies that accounts for your unique threat landscape
- OpEx cost reduction alleviating need for skilled and costly personnel

About eSentire:

eSentire is the largest pure-play Managed Detection and Response (MDR) service provider, keeping organizations safe from constantly evolving cyber-attacks 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 in corporate assets, 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**.

About Carbon Black:

Carbon Black (NASDAQ: CBLK) is a leading provider of next-generation endpoint security delivered via the cloud. Leveraging its big data and analytics cloud platform – the CB Predictive Security Cloud – Carbon Black consolidates prevention, detection, response, threat hunting and managed services into a single platform with a single agent and single console, making it easier for organizations to consolidate security stacks and achieve better protection. As a cybersecurity innovator, Carbon Black has pioneered multiple endpoint security categories, including application control, endpoint detection and response (EDR), and next-generation antivirus (NGAV) enabling customers to defend against the most advanced threats. More than 4,600 global customers, including one-third of the Fortune 100, trust Carbon Black to keep their organizations safe.