SOLUTION BRIEF

# Managed Endpoint Detection and Response Service

## Remote investigation, managed threat hunting, and pre-authorized containment

Symantec™

## At A Glance

- Symantec SOC analysts assigned to every customer
- Powered by Symantec Endpoint Detection and Response
- Advanced investigations on-premises and in the cloud
- Proactive, managed threat hunting of emerging IoCs, TTPs, and MITRE ATT&CK tactics
- Pre-authorized containment of compromised endpoints
- Big data analytics and Symantec Global Intelligence Network correlation
- Rapid, no-cost onboarding and continuous customer engagement

## Consider your team's ability to:

- Hunt for emerging IoCs and sophisticated adversary TTPs
- Investigate suspicious threat activity across on-premises and cloud endpoints
- Verify attacks and immediately contain compromised endpoints 24 hours a day
- Use endpoint detection and response tools effectively in-house

## Introduction

To stay ahead of sophisticated attackers, you must evolve your cyber security strategies beyond prevention-only technologies and reactive processes. Actively hunting for emerging indicators of compromise (IoCs) and tactics, techniques, and procedures (TTPs) digs deeper and detects stealthy threats that often go unnoticed. Even with advanced tools, organizations struggle with:

- **Inadequate detection capabilities**—Threats go unnoticed unless your defense incorporates global threat trends and evaluates emerging IOCs, and your teams chase down every alert.
- **Gaps in in-house skillsets**—Endpoint detection and response (EDR) tools are ineffective when used by a team that lacks experience in advanced investigations and threat hunting, especially in a cloud environment.
- **Too few, under-resourced staff**—Other security projects are delayed and stifled when your teams are absorbed in time-consuming investigations, which typically require off-hours commitment.

Symantec Managed Endpoint Detection and Response can help.

## Overview

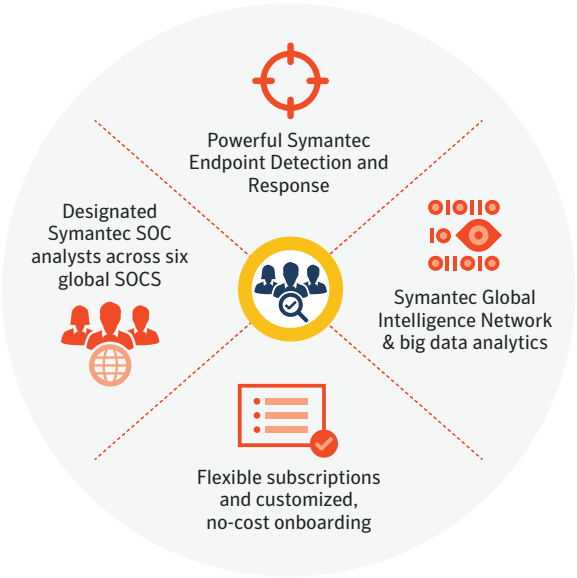
### Designated Symantec SOC analysts extend your team.

- Address in-house skills gaps with expert SOC teams trained in advanced investigations and complex cloud environments.
- Address critical off-hour attacks with 24x7 coverage across six global SOCs (United States, United Kingdom, India, Singapore, Australia, and Japan).

### Managed threat hunting detects threats that would go unnoticed.

- Detect stealthy and previously unknown attacks faster by automatically processing security logs through dynamic, big data analytics engines and correlation with the Symantec Global Intelligence Network.
- Hunt for threats continuously and automatically based on emerging IoCs and TTPs using the MITRE ATT&CK framework—all enhanced with human analysis.

# Key components: Symantec Managed Endpoint Detection and Response Service




## Expert investigations and pre-authorized containment immobilize attacks.

- Symantec SOC analysts expertly investigate critical indicators of an attack across on-premises and complex cloud environments to quickly understand and act on threats.
- Symantec SOC analysts disrupt attacks by containing compromised endpoints via pre-authorized measures (using Symantec EDR* via a single agent with Symantec Endpoint Protection*).

## Fast onboarding and ongoing engagement deliver top value.

- Interact with your dedicated Symantec Service Manager and SOC team at any time via phone, portal, email and online chat.
- Receive Emerging Threat Reports and Symantec SOC team insights as soon as they become available.

*Containment is available to customers with both Symantec Endpoint Protection 14.x and Symantec Advanced Threat Protection: Endpoint 3.x/Symantec Endpoint Detection and Response 4.x. Containment support for Symantec Endpoint Protection 15 is expected in the first half of calendar year 2019.

# Conclusion

Adversaries are using sophisticated and pervasive TTPs to exploit vulnerabilities within organizations. The latest endpoint detection and response tools enable teams to better detect, investigate, and respond to threats; however, if your organization lacks the appropriate manpower and advanced skillsets, these tools are underutilized at best. Symantec Managed Endpoint Detection and Response combines market-leading Symantec EDR, big data analytics, the Symantec Global Intelligence Network, and designated teams of highly trained Symantec SOC analysts to actively hunt, investigate, and contain threats when your team can't.

**To learn more about Symantec Managed Endpoint Detection and Response Service, please visit us at go.symantec.com/MEDR**

## About Symantec

Symantec Corporation (NASDAQ: SYMC), the world's leading cyber security company, helps organizations, governments and people secure their most important data wherever it lives. Organizations across the world look to Symantec for strategic, integrated solutions to defend against sophisticated attacks across endpoints, cloud and infrastructure. Likewise, a global community of more than 50 million people and families rely on Symantec's Norton and LifeLock product suites to protect their digital lives at home and across their devices. Symantec operates one of the world's largest civilian cyber intelligence networks, allowing it to see and protect against the most advanced threats. For additional information, please visit www.symantec.com or connect with us on Facebook, Twitter, and LinkedIn.

Symantec™

350 Ellis St., Mountain View, CA 94043 USA | +1 (650) 527-8000 | +1 (800) 721-3934 | www.symantec.com



19C208298_SB_MEDR_SERVICE_EN