

# Boost endpoint security with the Right EDR

An approach document



Synoptiq recommends



**SYNOPTIQ**  
Infosolutions

SECURITY AND INFRASTRUCTURE SOLUTIONS.  
FOR NON-STOP BUSINESS.



# How endpoint protection has progressed

AV → ATP → NGAV → EDR → MDR



Most customers  
are here



# Typical challenges with endpoint NGAV

SOC team's work increases because of **false-positives**

**Old malware and ransomware** are not detected because of lack of signatures

**MITRE-based identification** is missing in a lot of EDR solutions




There is **no rollback** to the original state possible for the end-point

There is no **automated isolation and detection** once malicious behaviour is detected

NGAV and EDR generally have **different agents**



# Typical challenges with some existing EDR Solutions

-  No good IoT Support
-  Separate agent for Cloud Security\
-  No File Integrity Monitoring



# Typical challenges with detection process

Typically, solutions follow the 1-10-60 thumb-rule

**1**

minute to  
**Detect**

**10**

minutes to  
**Respond**

**60**

minutes to  
**Remediate**



# How SentinelOne differentiates itself from all

1. Least amount of false positives
2. Single agent for EPP and EDR
3. Single agent for LT/DT/Cloud/Servers/IOT
4. Rated the best by MITRE
5. 1 Click resolution without need for scripting
6. Complete Rest API for integration

## **Operational Advantages**

- Lesser burden on SoC team because of lesser false positives

## **Remediation Advantages**

- Automated isolation & remediation

## **“Time to mitigate” Advantages**

- 0 min to detect -0 min to respond  
- 0 min to remediate



# SentinelOne

## use cases that are unique

Complete Remote shell  
access to investigate malware

Complete Device  
Control

Firewall Control

Bluetooth Control

Pre-correlated Threat  
Hunting

Context based malicious  
and exploit remediation

Static and Behavioural AI

Automated Recovery



# Why SentinelOne is timely

## BEFORE Breach

Static AI

Real-Time File  
Analysis

## DURING Breach

Behavioral AI

Behavioral Code  
Analysis

## AFTER Breach

Remediation

ActiveEDR and  
Deep Visibility







# SentinelOne add-on services

## Managed Detection and Response (MDR)



**SOC Augmentation Service**



**24/7 Global Coverage**



**Human Element Human Service**



**Peace of Mind**



**Fewer Alerts More Context**

Vigilance extends your in-house SOC expertise and provides a second set of eyes.



# SentinelOne and Gartner



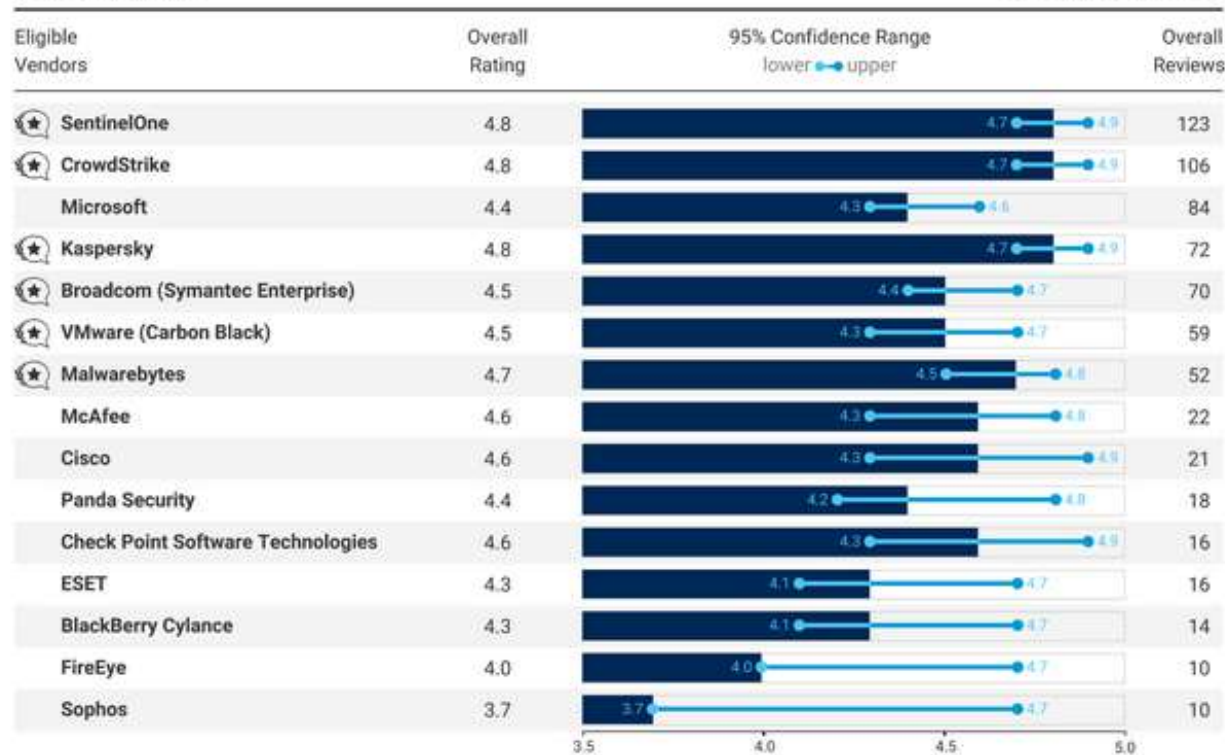
**HIGHEST RATED.  
OVERALL.**

## Gartner Peer Insights "Voice of the Customer" Endpoint Detection and Response Solutions

### Overall Ratings

As of 31 March 2020

Sorted by overall reviews



Notes: Vendors with greater than or equal to 10 eligible reviews on Gartner Peer Insights in the past one year as of 31 March 2020 are considered eligible vendors. Vendors are listed by overall reviews received for the Overall Rating. In case, two or more vendors have the same number of reviews, then they are listed alphabetically. Number of reviews and ratings as of 31 March 2020. All charts are plotted and labeled to the tenths digit for clarity.

©2020 Gartner, Inc. All rights reserved.



**Thank you!**

Synoptiq can help you by getting the respective experts to meet you! Write to us today.

Synoptiq Infosolutions  
3A, Hari OM Plaza, Opp. Borivali National Park. MG Road, Borivali  
East. Mumbai - 400066

[contact@synoptiq.biz](mailto:contact@synoptiq.biz)  
[www.synoptiq.biz](http://www.synoptiq.biz)