Symantec.

Why Traditional Threat Hunting and Investigations are Flawed.

And what you can do about it…

Complexity prevents productivity

Uncovering the signs of new, unknown or zero-day threats has typically fallen on the shoulders of your team. It's up to you to piece together what's happening and, if an attack is uncovered, resolve the impacts. This can take days, weeks, even months, as you collect and sift through mountains of data investigating an incident.

Attacks are growing in volume and sophistication. Malicious PowerShell usage was up 1,000% in 2018.[1]

It takes too long to detect and respond to threats. It takes, on average, 191 days for an attacker to be detected inside the network.[2]

The competition is fierce to hire and retain advanced security staff. Four in five cyber security decision makers reported feeling 'burnt-out,' and just under two thirds think about quitting their job or leaving the industry.[3]

Incomplete, un-integrated tools increase cost and complexity. 64% of organizations agreed their ability to detect and respond to threats is limited because it requires too many manual processes.[4]

Endpoint devices are increasingly diverse. Mobile endpoints can make up 50% of the endpoints that access corporate data in a given organization.[5]

[1] Symantec 2019 Internet Security Threat Report
[2] By Ponemon Institute
[3] Source: High Alert: Tackling Cyber Security Overload in 2019, Symantec
[4] ESG Threat Detection & Response Survey
[5] Frost & Sullivan

There's a better way

What's needed is a way to see the full picture so attack activity stands out and is fully understood. Here's how Symantec Endpoint Detection and Response (EDR) tools and services remove complexities and enable you to find attacks and stop them. Fast.

1 Detect and Expose

- Reduce time to breach discovery and quickly expose scope
- Apply Machine Learning and Behavioral Analytics to detect and prioritize incidents
- Automatically identify and create incidents for suspicious scripts and memory exploits
- Expose memory-based attacks with analysis of process memory

2 Investigate and Contain

- Increase incident responder productivity and ensure threat containment
- Gain full endpoint visibility with continuous recording of system activity
- Hunt for threats by searching for indicators of compromise across all endpoints
- Contain potentially compromised endpoints during investigation with endpoint quarantine

3 Resolve

- Rapidly fix endpoints and ensure the threat does not return
- Delete malicious files and associated artifacts on all impacted endpoints
- Blacklist and whitelist files at the endpoint
- Enhanced reporting allows any table to be exported for incident resolution reports

4 Integrate and Automate

- Unify investigator views, orchestrate data and work flows
- Easily integrate incident data and actions into existing SOC infrastructure
- Replicate best practices and analysis of skilled investigators with automated incident playbook rules
- Gain in-depth visibility into endpoint activity with automated artifact collection

But what about that skills shortage?

We know that **two thirds of cyber security decision makers (65%) feel they are being put in a position where they are set up for failure.** If this rings true with your team, Symantec's award-winning Cyber Security Services can help strengthen your defenses.

65%

Fortify your team with our experts

The Symantec Managed Endpoint Detection and Response (MEDR) Service provides 24x7 managed threat hunting, remote investigation, and pre-authorized remediation delivered by expert Symantec SOC analysts who actively detect, validate, and remediate stealthy attacks.

500+
Cyber Experts

Supported by leading experts in incident response, security monitoring, and threat intelligence with backgrounds in private and public sectors.

15 Years
Experience Delivering Monitoring and Response

Our teams have years of experience, hold multiple industry certifications, and are skilled in cyber security, forensic investigation, data science, and more.

Global Visibility & Local Expertise

Every customer is assigned a designated global team of analysts who are stationed across 6 global security operations centers to provide 24x7 coverage.

Try Symantec EDR for 30 days free of charge

Symantec.