Why Traditional Threat Hunting and Investigations are Flawed.

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 suspected, navigate the impacts. This can take days, weeks, even months, as you collect and sift through mountains of data investigating an incident.

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.6

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

But what about that skills shortage?

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.

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.

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.

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

The Symantec 2019 Internet Security Threat Report shows...