Cynet
Advanced Threat Detection & Response

TOP 10 TIPS FOR EFFECTIVELY IMPLEMENTING ENDPOINT DETECTION & RESPONSE

Evolving attack methods have made traditional security approaches that rely on solutions like anti-viruses insufficient in protecting the enterprise. An endpoint detection and response (EDR) solution that provides visibility into endpoint activity for quick detection and mitigation of advanced threats before they reach and jeopardize data enterprise-wide, is now essential for proper enterprise threat protection.

As you navigate through the growing EDR solutions landscape, be sure to address these **10 important considerations** for effectively implementing EDR in the enterprise:

1 EASE OF DEPLOYMENT

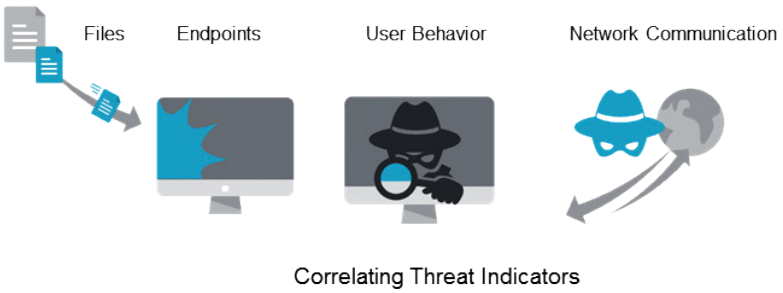
The ideal enterprise EDR solution will require only a few hours to deploy across thousands of endpoints, minimizing interruption to work. Deployment should be smooth across all device types and operating systems, protecting every OS version in use within the enterprise and ensuring protection for future OS versions.

2 EASE OF MANAGEMENT

An in-house or contract security expert should not be required for managing the EDR solution. The solution should be straight-forward enough for technical personnel such as IT people to manage thousands of endpoints with minimal, if any, added burden.

3 PART OF A BROAD SECURITY PLATFORM

The EDR solution should be part of a broader security platform that includes monitoring of files, users and networks, in addition to endpoints. Only this type of platform provides the complete visibility into the enterprise environment that's necessary for advanced threat protection.
As an added benefit, an EDR solution that's part of a broader platform significantly reduces false positives, increasing IT efficiency and eliminating the need for the enterprise to engage in the complicated and time-consuming activity of correlating between multiple silo solutions.



4 DETECTION, REMEDIATION AND PREVENTION

The EDR solution must go beyond detection and remediation and also provide a prevention layer, in order to protect the enterprise against immediate attacks such as ransomware. The ideal solution also includes deception capabilities, providing insight into the activity of attackers and the methods they use to gain access to organizational systems.

5 BEHAVIORAL (HEURISTIC) ANALYSIS

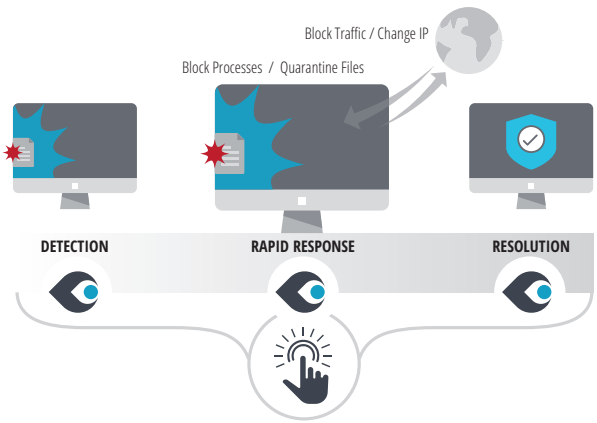
Behavioral analysis, which goes beyond only the known indicators to provide a full picture of endpoint activities, is a must-have. Only by leveraging heuristic analysis will an organization be protected against unique, previously unknown threats

6 NEAR-ZERO FALSE POSITIVES

An EDR solution trusted by the enterprise should provide near-zero false positives. The greatest likelihood of achieving near-zero false positives is through an EDR solution that employs both machine learning and behavioral analysis on endpoint behavior, as well as on network traffic, file and user behaviors.

7 AUTOMATED REMEDIATION

The EDR solution should offer the option to employ automated remediation actions and rules defined by the security team in response to threats as they are detected. This crucial capability enables the enterprise to build on existing knowledge without increasing vulnerability due to a lack of quick action.



8 ADVANCED INVESTIGATION AND FORENSIC CAPABILITIES

The solution should be equipped with advanced forensic capabilities revealing threat evidence on an endpoint and associating this data with related processes, users and network traffic. It should offer investigative insights that make it possible to see the full picture of a threat and threat operation.

9 CONNECT THREAT INTELLIGENCE FEEDS

The EDR solution should enable the organization to correlate behavioral and interaction indicators and anomalies from every available intelligence feed, in order to provide accurate and timely alerts.

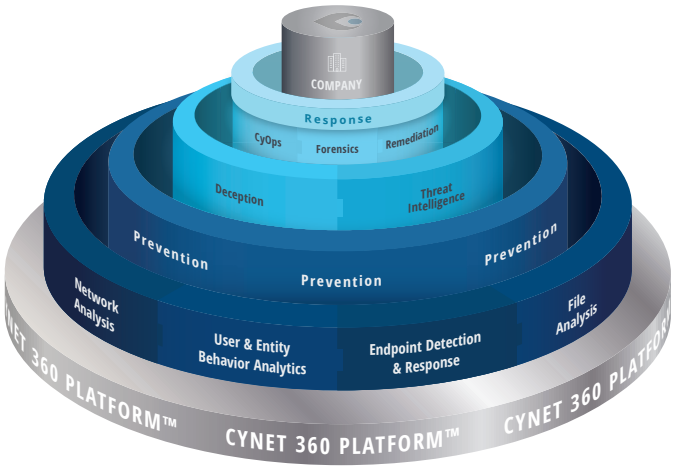
10 24/7 EXPERT SECURITY ASSISTANCE

Beyond freeing the enterprise from the need to have an in-house security expert at their disposal, the EDR solution should include access to a team of cyber threat analysts who can assist the organization with any situation they might encounter. Without the support of a SOC team, issues can take months or even years to resolve.

ONE PLATFORM FOR COMPLETE VISIBILITY, FULL PROTECTION

While an effective endpoint detection and response solution is integral to protecting the organization, the enterprise reaps additional benefits when EDR is part of a broader solution, such as the Cynet cyber security platform, encompassing EDR, UEBA, network traffic analysis, file analysis, and more.

The power of machine learning and heuristic analysis, backed by full visibility into the enterprise environment, provides the security team with the most complete picture available. Anomalies and threat indicators can then be accurately identified across thousands of endpoints, protecting the enterprise from even the most advanced and never-seen-before threats.



The Cynet 360 Platform

SIMPLIFY
YOUR
SECURITY

About Cynet

Cynet is a pioneer and leader in advanced threat detection and response. Cynet simplifies security by providing a scalable, easily deployable protection platform that delivers prevention, precise findings and automated response to advanced threats with near-zero false positives, shortening the time from detection to resolution and limiting damage to an organization.

To learn more visit: www.cynet.com

Cynet
Advanced Threat Detection & Response

www.cynet.com.