EDR
Managed EDR

RESPOND

With Managed EDR, real-time detection and active prevention of malicious activities can prevent security breaches where they happen.

MANAGED EDR

Don't wait for a report. Stop cybercriminals in their tracks.

End users are the top entry point for cybercriminals, especially as end users work more frequently outside the safe confines of the corporate network. Additionally, the techniques for infiltrating systems have become much more sophisticated. This all makes it increasingly difficult for traditional malware detection to keep up.

Further complicating the defense against cyberattacks is the speed at which they are able to move from the initial point of entry to the rest of the environment.

These are the key challenges that Endpoint Detection and Response (EDR) is designed to address. Utilizing next generation antivirus technology, the detection of both known and unknown malicious behaviors (including zero-day attacks) can be quickly identified and addressed.

If a suspicious process is detected, an alert can be sent and/or the execution can be blocked. Our Security Operation Center will work with you to tune the security policies to ensure nothing is missed and the proper balance is struck between security and user impact.

1/3
OF CYBER ATTACKS BYPASS TRADITIONAL SECURITY SOLUTIONS, ENCRYPTING FILES IN SECONDS

77%
OF SUCCESSFUL ATTACKS UTILIZE FILELESS TECHNIQUES

RETHINK CONNECTED

EDR
Managed EDR

Customized protection to maximize security and minimize customer impact.

Visibility across endpoint landscape

Complete visibility into your endpoint security strategy.

Event prioritization

Automation and correlation to prioritize specific threats based on your business requirements.

Quick recovery

Real-time detection enabling your team to quickly remediate issues before they impact your organization.
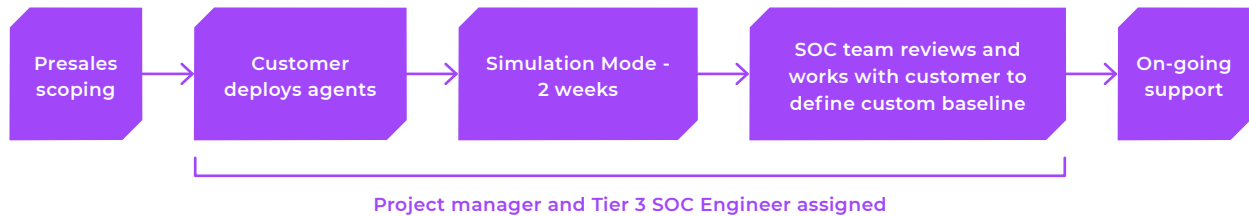
Customizable security policies

Incorporates an organization's specific customizable security policies and playbooks with the desired automated response to meet evolving threats and provide remediation.

24x7x365 Support

All security services include 24x7x365 support via our Security Operations Center (SOC), providing you experienced log analysis and reporting with actionable data to secure your organization.

Robust on-boarding process to ensure success and a quick return on investment.

Presales scoping → Customer deploys agents → Simulation Mode - 2 weeks → SOC team reviews and works with customer to define custom baseline → On-going support

Project manager and Tier 3 SOC Engineer assigned

RETHINK CONNECTED

CLOUD   CONNECTIVITY   SECURITY

1111systems.com