

MANAGED ENDPOINT DETECTION AND RESPONSE

Detect and Respond to Threats 24x7x365

When battling threats in your environment, time is of the essence. Today's attackers can compromise systems within minutes of an attack. To reduce risk, leading organizations often rely on a next-generation endpoint solution for continuous monitoring and automatic threat detection. However, these organizations may fall short in their internal threat analysis capabilities and incident handling, limiting the value these next-generation technologies can deliver. As a result, organizations struggle with an inability to triage suspicious samples and respond to threats quickly with appropriate measures, defenses and controls.

Optiv's Managed Endpoint Detection and Response (MEDR) service augments your next-generation endpoint solution's detection capabilities by continuously monitoring incidents and shortening your response times. Optiv's experts serve as an extension of your team by using advanced tools and techniques to accelerate response times and contain the spread of malware. Our experts identify the real threats in your environment and provide context and actionable steps to help you mitigate threats 24x7x365.

Endpoint Detection and Response



Optiv's MEDR service is offered to clients in multiple tiered options. Clients may elect to receive a monitoring only option, a monitoring plus endpoint management option or a monitoring plus endpoint management plus incident management option.

How Do We Do It?

- ALERT INVESTIGATION AND INCIDENT NOTIFICATION:**
Optiv monitors, collects, prioritizes, classifies, tracks, and escalates alerts 24x7x365 to identify malicious activity in your environment.
- SAMPLE ANALYSIS:**
Optiv conducts static, dynamic and interactive analysis to examine a sample's code and behavior.
- THREAT HUNTING:**
Hunts are executed when relevant threat intelligence is received, or in response to an active incident investigation.
- INTELLIGENCE INTEGRATION:**
Optiv ensures newly generated intelligence is automatically integrated into your environment, while providing reports and advisories highlighting threat protection techniques.
- ENDPOINT AND INCIDENT MANAGEMENT:**
Depending on the service tier selected, Optiv will manage your endpoint technology and provide reactive and/or proactive incident management.

Extend Beyond Alerts

Enhanced situational awareness above getting an alert to drive an informed response in your environment.

Accelerate Analysis and Response

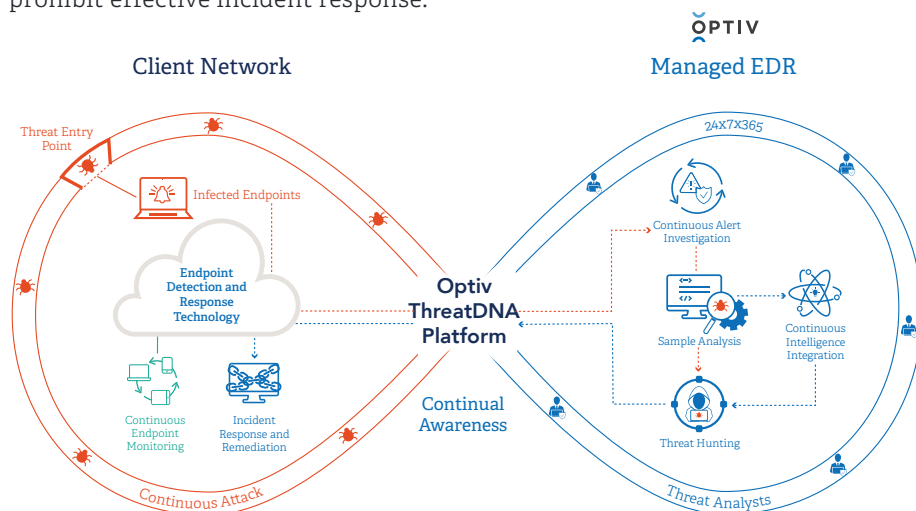
Reduce the amount of time it takes to respond to known and unknown threat activity by accelerating analysis and response.

Enhance Investigation

Leverage trained experts and integrated intelligence that uses multiple sandbox technologies to investigate threats.

Say Goodbye to Alert Overload

Having endpoint detection and response (EDR) technology deployed is more powerful when combined with Optiv experts and processes. The result will be an integrated state of continual detection and response to the threats you're facing. You'll no longer deal with issues such as alert overload that would otherwise prohibit effective incident response.



Service Tiers

Optiv provides flexible bundling and pricing options based on your needs.

<p>Monitoring</p> <ul style="list-style-type: none"> • Alert Monitoring • Alert Investigation • Incident Notification • Sample Analysis • Threat Hunting • Intelligence Integration 	<p>Monitoring + Device Management</p> <p>Monitoring +</p> <ul style="list-style-type: none"> • Configuration Management • Change Management • Problem Management • Release Management 	<p>Monitoring + Device Management + Incident Management</p> <p>Monitoring + Device Management +</p> <ul style="list-style-type: none"> • Incident Response • Readiness Assessment • Playbook Development • Tabletop Exercises
--	--	--

The Optiv Advantage

Optiv can help businesses in every industry connect information security policies, procedures and practices with business goals. Our security leadership experts, backed by our team of consultants, can provide the experience you need to take your program to the next level.



Expert Minds

Optiv's security professionals are dedicated to helping you achieve results and realize value. Our team of 1,000+ highly skilled client managers and security practitioners work hard to deliver superior results and cutting-edge research to solve your complex, real-world security problems.

Leading Best Practices

Our knowledge of leading best practices helps Optiv formulate security recommendations tailored to meet your specific business objectives.

Client-First Culture

Optiv's passion for security and our commitment to quality results means we focus on the right solutions to meet your specific needs.

Proven Methodologies

Optiv has developed proven methodologies to help ensure superior outcomes for your projects and programs.



1125 17th Street, Suite 1700
Denver, CO 80202

800.574.0896 | www.optiv.com

Optiv is a market-leading provider of end-to-end cyber security solutions. We help clients plan, build and run successful cyber security programs that achieve business objectives through our depth and breadth of cyber security offerings, extensive capabilities and proven expertise in cyber security strategy, managed security services, incident response, risk and compliance, security consulting, training and support, integration and architecture services, and security technology. Optiv maintains premium partnerships with more than 350 of the leading security technology manufacturers. For more information, visit www.optiv.com or follow us at [www.twitter.com/optiv](https://twitter.com/optiv), www.facebook.com/optivinc and www.linkedin.com/company/optiv-inc.

© 207 Optiv All Rights Reserved. Optiv is a registered trademark of Optiv Security Inc.