

# Managed Next-Gen Antivirus

## Stop attacks before they start

Today's increasingly complex, rapidly expanding threat landscape makes stopping attacks earlier in the kill chain more important than ever. Discovering malicious behavior and malware before compromise lets you defuse many of the tools and techniques deployed by sophisticated, elusive cybercriminals.

As customers look for pragmatic approaches to address the challenges posed by a dynamic threat environment, Rapid7 remains committed to investments that drive greater security operations efficiency. Rapid7's **Managed Next-Gen Antivirus (NGAV)** service delivers a new level of security: high-fidelity prevention against both known static threats and suspicious behavior to block attacks before they execute and do damage.

## Mitigate Risk and Gain Efficiencies With Managed NGAV

### Accelerate containment and eliminate breach impact

Rapid7 [Managed Threat Complete](#) offers customers 24x7x365 expert monitoring and XDR coverage across their entire modern environment. With Managed NGAV, customers extend this coverage to neutralize attacks before deployment by:

- Blocking known and unknown threats early in the kill chain
- Stopping malware built to bypass existing security controls
- Maximizing efficiency with the Rapid7 universal Insight Agent

## Block known and unknown threats early in the kill chain

Moving beyond traditional antivirus, NGAV can block diverse attacks, including fileless malware, across the entire endpoint ecosystem. Blocking malware (IOCs, virus signatures, IPs, file hashes, URLs) and malicious activity across the environment versus addressing a single endpoint or taking down a device that's part of critical infrastructure avoids potentially significant financial and reputational damage to the business. With the help of our MDR experts, we ensure high-fidelity prevention that you can trust to block real threats—without disrupting your business.

## Rapid7 Managed NGAV Customer Benefits

- Gain deeper visibility into endpoint activity
- Prevent threats earlier
- Get ahead of emerging attacks
- Elevate security posture
- Consolidate tools
- Maximize ROI of security investments

## Stop malware built to bypass security controls

Rely on best-in-class, prevention-first NGAV designed to address modern attacks:

### Memory Injection Prevention

- Blocks attempts by fileless threats to avoid execution of code from the file system
- Stops attempts to inject and hide malicious code in a legitimate process

### Malicious Documents Prevention

- Breaks or otherwise disarms malicious documents that try to abuse features such as macros, scripts, and built-in tools
- Allows users to benefit from the full capabilities of modern applications without worrying about infections

### Living-off-the-Land Prevention:

- Interferes with attempts to misuse tools built into the system to cause damage without using classic forms of malware
- Prevents threats from “trampolining” off such tools to infect the endpoint or cause damage

### OS Credential Dumping Protection:

- Blocks attempts to steal credentials

## Maximize efficiency with the Rapid7 universal Insight Agent

Our Managed NGAV solution can be implemented quickly using the universal Insight Agent, expediting the path to keeping organizations safe from pervasive cyberattacks. This is the same agent that powers high-fidelity endpoint detections, telemetry collection, and DFIR in Rapid7's [Managed Threat Complete](#) services, as well as vulnerability scanning and containment actions. This lightweight software has a smaller footprint but drives big insights. Rapid7 maintains versioning, and it auto-updates, so customers realize new capabilities immediately—without more work to manage on their end.

**Get Complete Support  
From Your Trusted  
SecOps Partner**

Rapid7's Managed Threat Complete with NGAV instantly extends your team with an elite SOC for uninterrupted eyes on your environment. Consolidation of the security stack helps teams stop wasting time navigating between siloed solutions. Increase efficacy, productivity, and ROI by unifying your security operations with fewer tools, fewer agents, and a single trusted partner for endpoint security.

**Learn more** about how to execute comprehensive Managed NGAV capabilities as part of a pragmatic, results-oriented security infrastructure.



#### PRODUCTS

Cloud Security  
XDR & SIEM  
Threat Intelligence  
Vulnerability Risk Management

Application Security  
Orchestration & Automation  
Managed Services

#### CUSTOMER SUPPORT

Call +1.866.380.8113

To learn more or start a free trial, visit: <https://www.rapid7.com/try/insight/>