# McAfee Active Response

## Comprehensive endpoint detection and response

Security-conscious entities today face a threat landscape that is changing at a dramatic pace. Attacks are created and propagated at ever-faster rates. "Designer" attacks target individual organizations by using focused knowledge to improve their effectiveness and minimize detection. Attackers are more frequently penetrating preventive technologies. Forward-looking organizations therefore demand easy-to-use, integrated tools that help better detect attackers' presence and then allow rapid investigation and remediation. The best detection and response solutions increase security efficiency even as they capture increasingly more information from a growing number of systems. By providing superior out-of-the-box capabilities, automated interaction with existing security management solutions, and user-customization, McAfee® Active Response greatly narrows the window of opportunity for attackers to damage your computing assets and corporate brand.

### Key Advantages

- **Automated:** Capture and monitor context and system state for changes that may be IoAs, as well as find dormant attack components, and send intelligence to analytics, operations, and forensic teams.
- **Adaptable:** When alerted, you can adjust to changes in attack methodologies; automate data collection, alerts, and responses to objects of interest; and customize your configuration to customer workflows.
- **Continuous:** Persistent collectors activate triggers on detection of attack events, alerting you and your systems to attack activity that you have been watching.

### The Evolving Threat Landscape

Enterprises have come to the realization that they may be breached by an attacker at any time and must be prepared to effectively deal with these breaches through early detection of an attack, detection of ongoing activity, or discovery of indicators of attack (IoAs). With this realization comes the understanding that new technologies are required to address the current gaps in visibility, discovery, detection, and response.

### Limitations of Current Incident Response Approaches

When asked to investigate a suspected or known incident across an entire organization, incident responders and security administrators are typically limited by two key factors: time and scale. While a great deal of detailed information is gathered by existing systems or tools, it takes a very long time to collect and analyze that information. As speed is a critical requirement in data collection, significant compromises are made in the nature of the data collected, along with the number of systems from which it is collected. In addition, the sheer magnitude of the collected data that must be sifted through to identify key information is becoming increasingly difficult to process.

The most commonly used incident response tools are scripts written by responders themselves. These tools provide the foundation of data collection to be used in a broader analysis. This body of knowledge, along with the associated tools, is fairly mature, but the ability to leverage these at scale and speed is limited. This lack of ability to perform a live investigation on specific IoAs across an entire organization often leads responders to a myopic view in their discovery and response efforts. Typically, these efforts are artificially restricted to meet time requirements, and this can contribute to significant deficits in the incident response process. This severely handicaps responders, as their efforts are artificially limited due to the constraints of current tools.

intel Security

## System Requirements

**Minimum hardware requirements**

The server can be installed on a virtual machine if necessary. The minimum recommended hardware requirements for the McAfee Active Response server are as follows:

- 4 Intel® Xeon® CPU X5675, 3.07 GHz
- 8 GB RAM
- 120 GB solid state disk

**Required service infrastructure**

- McAfee® ePolicy Orchestrator® (McAfee ePO™) 5.1.1 or later
- McAfee Agent 5.0 extension or later
- McAfee Data Exchange Layer 2.0.0.405 broker or later

**Supported web browsers**

- Internet Explorer 9 or later
- Chrome 17 or later
- Firefox 10.0 or later

**Required client infrastructure**

- McAfee Agent 5.0.0.2710 or later for Linux endpoints
- McAfee Agent 5.0.0.2610 or later for Microsoft Windows endpoints
- McAfee Data Exchange Layer 2.0.0.405 clients or later on all managed endpoints

## Comprehensive Endpoint Detection and Response

McAfee Active Response delivers continuous detection of and response to advanced security threats to help security practitioners monitor security posture, improve threat detection, and expand incident response capabilities through forward-looking discovery, detailed analysis, forensic investigation, comprehensive reporting, and prioritized alerts and actions. Optimized to meet stringent endpoint detection and response (EDR) criteria, McAfee Active Response uses predefined and user-customizable collectors to search deeply across all systems to find IoAs that are not only present via running processes, but also may be lying dormant or may even have been deleted. Further, McAfee Active Response enables users to not only search for an IoA in the present, but also to alert and act in accordance with security objectives via triggers that give instructions should the IoA ever occur in the future.

McAfee Active Response is proof of the effectiveness of Intel Security's integrated security architecture, which is designed to resolve more threats, faster, with fewer resources in a more complex world. McAfee Active Response gives you continuous visibility and powerful insights into your endpoints so you can identify breaches faster. And it provides you with the tools you need to correct issues faster and in the way that makes the most sense for your business. All of this power is managed via McAfee® ePolicy Orchestrator® (McAfee ePO™) software leveraging McAfee Data Exchange Layer—this provides unified scalability and extensibility without the need for incremental staff to administer the product.

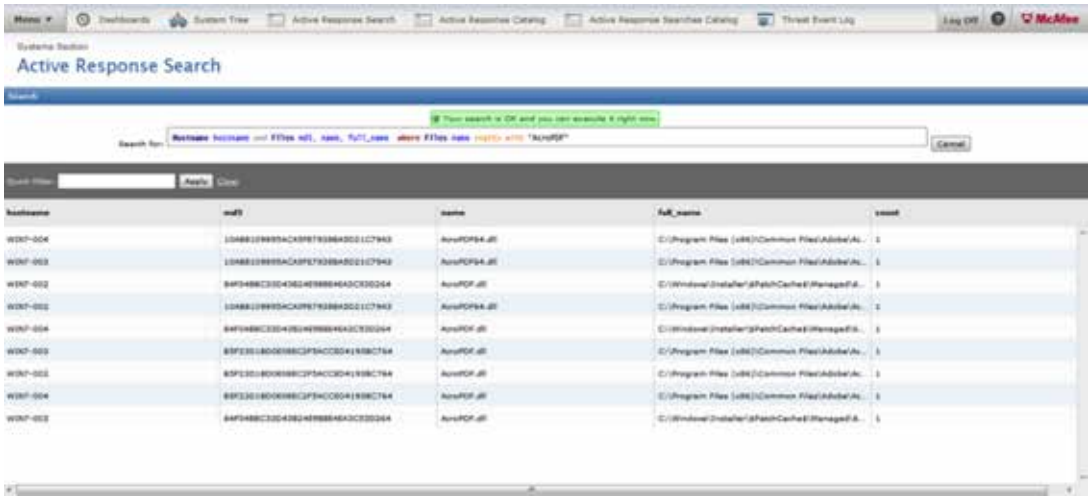


**Figure 1.** McAfee Active Response search user interface.

**Supported client operating systems**

- Microsoft Windows
  - Windows 8.0, Base, 32-bit, and 64-bit
  - Windows 8.1, Base, U1; 32-bit and 64-bit
  - Windows 2012, Server Base, R2; U1; 64-bit
  - Windows 2008 R2 Enterprise, SP1, 64-bit
  - Windows 2008 R2 Standard, SP1, 64-bit
  - Windows 7 Enterprise, up to SP1; 32-bit and 64-bit
  - Windows 7 Professional, up to SP1; 32-bit and 64-bit
- CentOS 6.5, 32-bit
- RedHat 6.5, 32-bit

| Feature | Advantage | Customer Benefits | Differentiation |
|---|---|---|---|
| **Collectors** | Collectors enable users to find and visualize data from their systems. | Collectors offer search capabilities to look deeply into systems. They provide visibility into critical breach or attack potential to collect and visualize data from these systems. Using any of several common scripting languages, users can easily customize their own collectors and responses, offering optimal configurability and adaptability. | McAfee Active Response looks beyond executable or running files into code that may be lying dormant or that may even have been deleted in an attempt to cover the attacker's tracks. McAfee Active Response can search for files, network flow, registry, and process mapping. |
| **Triggers** | Triggers enable a security practitioner to continuously monitor a critical event or state change with one set of instructions both now and in the future. | Actions are initiated by a trigger set beforehand, generating an event or executing responses. McAfee Active Response has the ability to go beyond static "peeks" and into a continuous response mode. | McAfee Active Response can see threats today and trigger actions for threats that may come tomorrow. |
| **Reactions** | Reactions provide pre-configured and customizable actions as a result of meeting the conditions of the trigger, enabling you to hunt and kill threats. | Reactions allow users to take actions, such as search for files that have been deleted from the system by file hash (MD5 and SHA1), see if any hosts are actively connected to an IP address or have connected to an IP address in the past, or search for a non-PE-based malicious file that has not been accessed or detonated on the system (search for a malicious PDF on a system where it was copied to the file system but not opened). | McAfee Active Response is preconfigured to act on search findings and accommodate custom actions prescribed by the user to meet a specific user-defined need. |
| **Centralized Management with McAfee ePO Software** | The single-console environment provides comprehensive management and automation. | Administrators can leverage McAfee ePO software as part of Intel Security's integrated security architecture to drive automated responses to triggers and searches and respond to and mitigate threats. Single-pane manageability offers greater security visibility without additional administrative burden. This simplifies operational aspects and reduces time investment for administrative staff. | Management and action via a single console is a clear differentiator. Using a single console, we uniquely protect a variety of platforms with a powerful set of security controls, including McAfee Active Response. |
| **Integrated Security Architecture** | Leverages the data exchange layer to streamline communication with other products from McAfee, a part of Intel Security. | As part of Intel Security's integrated security architecture, McAfee Active Response reduces risk and response time and lowers overhead and operational staff costs through the platform's innovative concepts, optimized processes, and practical recommendations. | |

Learn more about the benefits of McAfee Active Response at **www.mcafee.com/activeresponse**.

**McAfee. Part of Intel Security.**
2821 Mission College Boulevard
Santa Clara, CA 95054
888 847 8766
www.intelsecurity.com