Solution Brief

# Monitor Continuously. Respond Swiftly.

**McAfee® Active Response enhances ATA detection and remediation.**

Every day last year, 2,803,036 data records were lost or stolen as a result of a data breach—and research indicates that the numbers are climbing at an alarming rate. Data breaches totaled 1,540 last year, up 46% from the previous year.[1] Most security-conscious organizations are quickly coming to the realization that traditional set-and-forget endpoint solutions are ill-equipped to handle the daily barrage of zero-day and advanced targeted attacks (ATAs). Security teams need uninterrupted visibility into endpoint activity, rather than just alerts from security products after something has already gone wrong. Endpoint detection and response (EDR) is an indispensable supplement to current defenses. As Gartner points out, "Organizations investing in EDR tools are purposefully moving from an 'incident response' mentality to one of 'continuous monitoring' in search of incidents that they know are constantly occurring."[2]

## The Defense Deficit in Most Endpoint Solutions

Instead of taking a proactive approach, most incident response teams currently take a reactive approach. Often, threats are not even discovered until long after the damage has been done. After bypassing your defenses, low-lying ATAs have a prolonged "dwell time," which enables them to proliferate throughout your infrastructure, eventually causing a breach.

Traditional endpoint solutions with signature-based antivirus, data loss prevention, host intrusion prevention, and other key capabilities offer limited visibility into what is actually going on with your endpoints across your entire infrastructure. This is especially true if multiple tools from different vendors are in place. This patchwork, siloed approach makes search and analysis of threat activity difficult and costly. Security teams have had to rely on scheduled scans to get a picture of their company's security posture, but these occasional glimpses are far from adequate—especially when you consider that more than 307 new threats appear every minute, or more than five appear every second, according to the McAfee Labs' *November 2014 Threats Report*.[3] In addition to the onslaught of zero-day malware, scheduled scans miss dormant, multivector threats that might have crept into your infrastructure undetected, waiting to unleash their fury.

intel Security

In general, security teams are unable to keep abreast of malicious activity because resources are scarce, practitioners have limited time, and rigid incident response processes don't necessarily scale well enough to handle the big attacks. As more endpoints are added to the infrastructure—laptops, desktops, mobile devices, and servers—IT is faced with the challenge of managing these systems and extracting relevant security and threat intelligence.

## Why Everyone Needs McAfee Active Response

EDR will soon become an essential component of everyone's cybersecurity defense strategy and practice. As security consultant John Reed Stark suggests, "EDR tools improve a company's ability to detect and respond to outsider and insider threats; enhance a company's speed and flexibility to contain any future attack or anomaly; and help a company manage data threats more effectively overall."[4]

McAfee Active Response completes your layered security strategy and enhances not only your endpoint protection, but your overall security posture as well. It is a critical element of a comprehensive solution set that includes essential endpoint security technologies, such as antivirus, application control, local threat intelligence, and more. As part of Intel Security's integrated and connected architecture, McAfee Active Response provides continuous visibility and insights into endpoint activity to help you act more quickly to remediate issues in a way that works best for your business.

Administrators, investigators, and responders get an uninterrupted view of activity across your infrastructure—enabling them to respond appropriately to threats that may be lying in wait, may have been deleted to avoid detection, or may be propagating throughout your network. Built-in, customizable triggers help your security team discover today's and tomorrow's indicators of attack (IoAs) and act on that information swiftly.

The power of intelligent discovery, detailed live and interactive investigation and analysis, comprehensive reporting, and prioritized alerts and actions are harnessed by the McAfee® ePolicy Orchestrator® (McAfee ePO™) management platform. Intel Security unifies **Protect, Detect, and Correct** through the McAfee ePO platform into an adaptive feedback loop, enabling security to evolve and learn in an iterative cycle that improves over time. McAfee Active Response is the **Detect** and **Correct** component of this threat defense lifecycle, helping organizations identify compromises more effectively and implement quick remediation. McAfee ePO software enables scalability, extensibility, and unified, continuous monitoring across your infrastructure. It helps you keep costs down too, as additional technical staff or management agents are not required for administration.

### McAfee Active Response

- Persistently monitor critical events and state changes at endpoints.
- Use continuous collectors to find and visualize all files—executable and dormant.
- Set traps, triggering automatic or customized responses.
- Manage the entire solution from a single console.

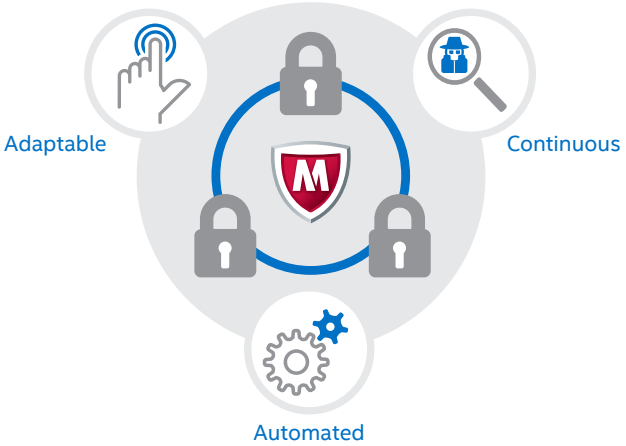


**Figure 1.** Automated, adaptable, and continuous protection against ATAs with McAfee Active Response.

McAfee Active Response has the three ingredients that are essential for an effective EDR:

- **Automation:** Triggers or traps can be set based on various parameters. They tell all the endpoints in your environment to look for specific types of IoAs. When a particular type of IoA is discovered, triggers automatically set in motion a user-definable reaction, such as "reboot system." Unlike other EDR solutions that only collect information constantly, McAfee Active Response automatically applies logic to invoke a specified reaction under certain conditions.
- **Adaptability:** When administrators receive an alert, McAfee Active Response adapts the response according to the attack methodologies at play. Customized or standard searches can be done across your organization to gain a more thorough understanding of IoAs and align the proper remediation efforts and resources.
- **Continuous monitoring:** McAfee Active Response operates persistently. Triggers set off alerts or responses when attack events occur—and you can adjust this to monitor systems for future attack activity.

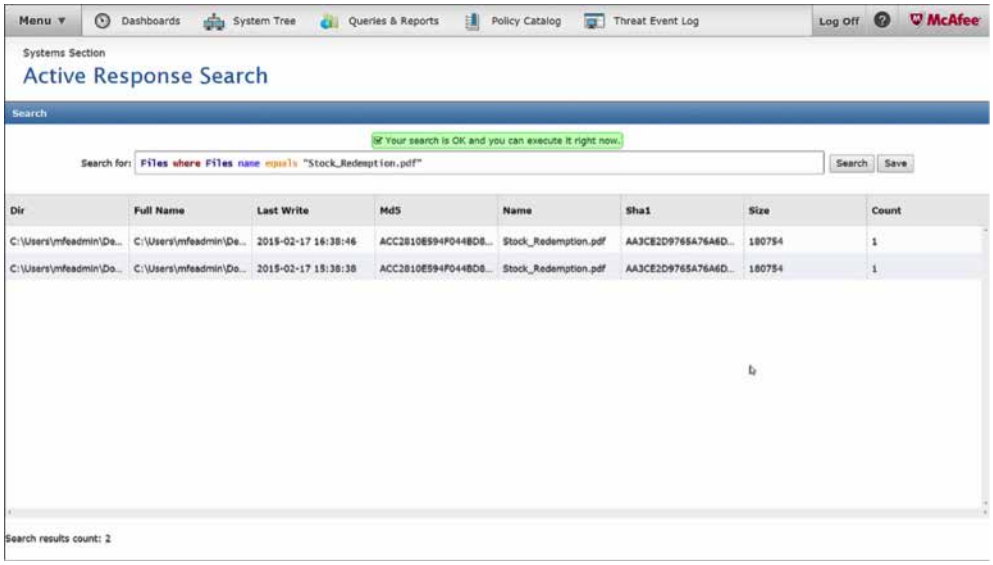


**Figure 2.** McAfee Active Response search results.

**Precise data collection uncovers breach potential.**
Collectors are a key component of McAfee Active Response. Built-in search capabilities allow users to take a deep dive into systems to discover and visualize insightful data that can offer clues about lurking malware or suspicious activity. Collectors are like detectives who can look beyond the obvious, examining program executables, running processes, and dormant or deleted files and objects.

McAfee Active Response collectors enable optimal configurability, adaptability, and accuracy. You have the option of either using the provided catalog or writing and importing your own scripts using McAfee Data Exchange Layer to run them. You can then search across traditional data sources or black holes—where data packets may be destroyed or discarded without your knowledge—to find the exact combination of characteristics that correspond to IoAs you are interested in tracking.

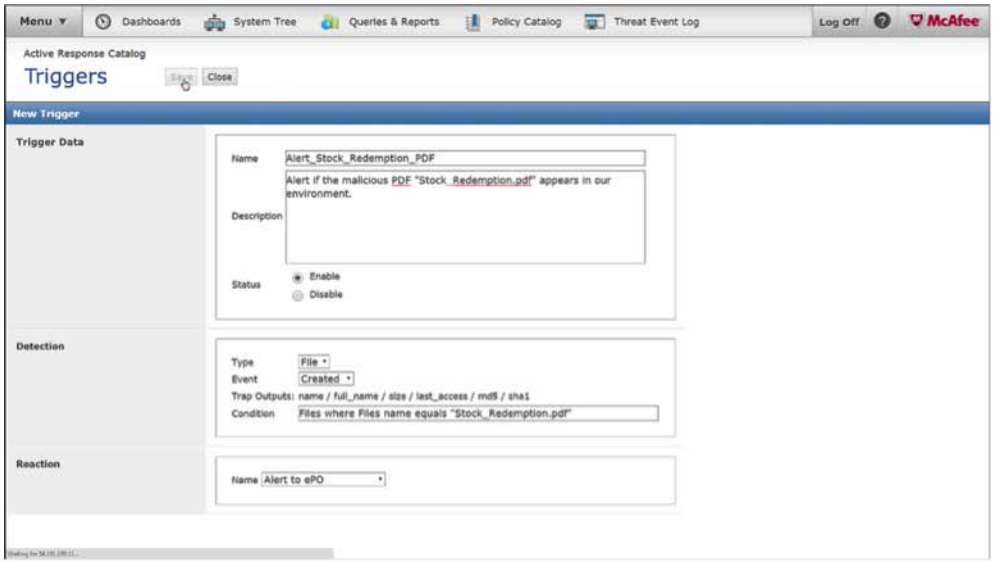


**Figure 3.** Setting a trigger and specifying a reaction in McAfee Active Response.

**Triggers and reactions provide automated, continuous response.**
With just a single set of instructions, triggers help you continuously monitor and respond to security events or state changes today and tomorrow. After you define the set of potential attack behaviors or details you wish to monitor, you set a trigger to automatically generate an alert or execute a reaction when those IoAs are present. In one simple step, your security team can efficiently and effectively detect and remediate emerging threats. Gartner recommends this type of EDR capability in its 2015 report, *Best Practices for Detecting and Mitigating Advanced Persistent Threats:* "... automatic responsive capabilities for threat detection events when using EDR solutions, such as 'kill process,' delete file, or clear memory, to avert data losses and disrupt an active 'kill chain.'"[5]

## McAfee Active Response in the Intel Security Architecture

The Intel Security framework unifies and integrates multiple products, services, and partner solutions for centralized, efficient, and effective mitigation of security risk. It helps you respond more rapidly when ATAs threaten your environment. At the core of Intel Security's integrated, connected architecture is the McAfee ePO management platform, which you use to deploy and manage McAfee Active Response. Since McAfee Active Response is so tightly integrated with the McAfee ePO management platform, it works seamlessly with other advanced Intel Security technologies, including McAfee Threat Intelligence Exchange, McAfee Complete Endpoint Protection suites, and McAfee Enterprise Security Manager.

**How it works.**

Once the McAfee Active Response client is installed on the endpoint, it integrates with the McAfee Agent and populates a file hash cache, a network flow cache, and a registry cache. These are instantly and continuously updated whenever there is any endpoint activity. The always-on collector captures the type of information specified by your instructions about the malicious files (even if they are dormant) or suspicious activity. This data is stored and indexed locally on the endpoint and then served up in the McAfee ePO software interface. There's no need for a separate data storage appliance or for cloud storage. Persistent collection runs low and slow, so there's never a spike in resource consumption on the endpoint. Users can continue their work uninterrupted.

If you receive an alert from a security product or want to hunt down a newly discovered threat that you just learned about through intelligence sharing, you can do a search, which works much like a Google search. When administrators initiate a search from the McAfee ePO management platform, the McAfee Active Response client examines the caches. Results are returned in just 10 to 20 seconds—you get an accurate picture of the current state of your environment in real time.

Triggers and reactions then come into play. Triggers act like sentries, continuously monitoring endpoints for IoAs. If a particular IoA is present, the trigger activates and then automatically responds with a reaction, which you can customize according to your specific objectives. Typical reactions include sending an alert, deleting a bad file, killing a malicious process, or doing a more detailed forensic analysis.

## McAfee Active Response in Action

There's nothing better than real-world use cases to drive home the importance of EDR. Here are some examples of how McAfee Active Response can help detect and respond to threats under different circumstances.

**Undetonated "land mines"**

As mentioned above, McAfee Active Response works in concert with McAfee Threat Intelligence Exchange, which enables sharing of relevant threat data in real time across security components in the Intel Security architecture, enabling them to act as a unified, collaborative security infrastructure. McAfee Threat Intelligence Exchanges helps you block unknown or emerging "gray" files that slip past antivirus programs. It offers better visibility and control over these types of files and pinpoints where the attempted or actual file execution takes place. McAfee Threat Intelligence Exchange then sends out the first alert on the McAfee Data Exchange Layer. From there, security teams can turn to McAfee Active Response to survey the environment for the file hash and determine whether dormant land mines have been planted elsewhere. All these activities are conducted swiftly and efficiently through the McAfee ePO management platform.

**Malware hidden in documents**

Increasingly, zero-day threats or code used to distribute malware is inserted into documents, such as .ZIP files, image files, .PDFs, Adobe Flash files, or .PNG files. These stealthy attacks are often undetectable by standard antivirus. You can use McAfee Active Response to perform a search for these types of files based on certain attributes. For example, let's say a suspicious document file shows up on your assistant's laptop. Your team can use McAfee Active Response to set a trigger, which will keep an eye out for this type of file on all the endpoints in your organization and then wipe it before it does any damage.

## Learn More

Automated, adaptable, and continuous, McAfee Active Response is a critical part of Intel Security's integrated approach to defeating the growing number and complexity of ATAs in today's threat landscape rapidly and successfully. To learn more about how McAfee Active Response complements Intel Security's current portfolio, visit:

- **McAfee Active Response**
- **McAfee ePolicy Orchestrator**
- **McAfee Threat Intelligence Exchange**
- **McAfee Complete Endpoint Protection suites**

1. **http://breachlevelindex.com/pdf/Breach-Level-Index-Annual-Report-2014.pdf**
2. **https://www.gartner.com/doc/2738017/market-guide-endpoint-detection-response**
3. **http://www.mcafee.com/us/about/news/2014/q4/20141209-01.aspx**
4. **http://www.cybersecuritydocket.com/2015/05/08/edr-the-future-of-cybersecurity-and-incident-response/**
5. **https://www.gartner.com/doc/2589029/best-practices-mitigating-advanced-persistent**



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