Security Connected Reference Architecture
Technology Blueprint

Combatting Advanced Targeted Attacks: DETECT

Part II of the Combatting Advanced Targeted Attacks Blueprint Trilogy

intel Security

Intel® Security recommends a three-pronged approach for disrupting advanced targeted attacks. This document covers advanced monitoring to identify anomalous, outlier behavior to perceive low-threshold attacks that would otherwise go unnoticed. As you uncover evidence, your system should share findings to enrich decision-making throughout your security infrastructure. To see the rest of the story, read the companion **Protect** and **Correct** blueprints.

Discover Advanced Threats Before They Do Damage

The Situation

Compromises and active attacks can persist for months without being detected, resulting in breaches that go unexposed for months or years. And when you learn about the data loss, it's usually because a third party, such as your own customer or law enforcement, has informed you. This scenario may not have happened to you yet, but you know it's only a matter of time, unless you make some changes in the way you approach incident detection. How can you find out as soon as possible that you have been compromised? You and your team gather to find the best answer to that question.

Driving Concerns

The biggest concern is the ability to answer the question "Are the bad guys in my environment right now?" Detecting attacks and incidents has proven to be a challenging task, even for highly trained security personnel. Here are some reasons why.

- **Limited visibility.** Security solutions have traditionally been siloed. Each product has a piece of the puzzle but no one knows what the big picture looks like. That makes it difficult and time consuming for security teams to gather the data required to clearly identify advanced attacks. If the team suspects something, it can take hours or even days for the security analysts to log into multiple consoles and retrieve the necessary data, or reach out to the different teams that hold part of the information.
- **Too much noise.** Security data grows exponentially and log collection has left us inundated with an ocean of data. Every day we generate millions of events from point products and applications that make up our environment. If you get an alert every time you get an event, you become prone to alert fatigue and will potentially miss or ignore key signals. However, discarding too many events might lead you to miss an attack altogether.
- **Attack sophistication.** Most advanced targeted attacks are intended to be stealthy, making them hard to detect. They can use multiple vectors of infection, advanced evasion techniques, and morphing mechanisms to stay below the radar. The indicators of compromise (IoCs) can be subtle and hard to detect. And just because you detected one IoC does not mean that you detected all of the hidden threats, or that it won't be back tomorrow in a slightly different form.
- **Time plays against you.** There is a clear correlation between the time it takes to detect an attack and the amount of damage the attacker can perpetrate. This is why time is of the essence when detecting a breach. The sooner you detect an attack, the faster you can start responding to it. Detecting a breach during the 'Golden Hour,' the hour following the initial breach, is essential to disrupting and containing the attack before damage occurs. Unfortunately, most security teams fail to detect breaches in a timely manner with the solutions they currently use. Instead of detecting incidents as soon as they occur, it takes days, weeks, or even months.

Solution Description

Visibility, security intelligence, and continuous monitoring are the keys to detecting advanced targeted attacks before damage is done. This is why you need a solution that can continuously provide full visibility of the events taking place in your environment and apply the latest security intelligence to that data. To maximize timely detection, the solution should enable that process to happen automatically and in real time as events occur in your environment. But it should also allow you to be proactive, so you can either check your environment against new threat intelligence anytime you want, or have the systems automatically do it for you.

To achieve this, you first need to gain visibility. We advocate collecting data about your environment in a central location that includes data from both security and non-security products, such as logs and events, network flows, applications, email, web traffic, and identities. The more data you collect, the more complete and accurate picture you can potentially gain.

But collecting data is not enough. The data is only valuable if you are able to use it. To transform the data from noise to valuable information, you need real-time advanced analytics capabilities. Ideally, the analysis process will sift through all the data, separate the important from the trivial, correlate related events from different sources into an incident, reduce noise, and elevate visibility of significant incidents so only what matters is brought up to the surface. When that process is fully automated, it has the ability to detect attacks in real time. But the quality of the detection—not missing incidents, not generating false positives, and not creating alert fatigue—also depends on the solution's ability to know what to look for. This is why the capability of accessing threat intelligence is critical. The quality, accuracy, and speed of the detection depend on it.

That intelligence can come from third parties, such as industry feeds and security vendors. But, for faster results, and especially in the case of advanced targeted attacks, the threat intelligence should also come from your own internal solutions. We call that local threat intelligence. Local Intelligence should encompass the understanding of what constitutes normal activity for your organization, context about your specific environment, and indicators of compromise that are known or generated by your security solutions. For example, if your sandbox technology generates a list of IoCs for malware that it analyzes, the solution should consume and share those IoCs so you can immediately start detecting the presence of that malware in your environment.

Because you've only detected an attack today does not mean that an attacker has not already tried or succeeded in the past. This is why the solution also needs to give you the ability to start looking for indicators of attack (IoAs) without having to wait for an alert to be triggered. Proactive detection is critical when suspicion is raised, which happens when you are observing unusual events, or when information about a new threat emerges in the news or through security feeds. In that case, the solution should allow you to hunt proactively for indicators of existing footholds, so you can verify that you have not already been compromised by that new threat.

Decision Elements

These factors could influence your architecture:

- Scalability: how big is the environment you need to monitor?
- Can you staff a security incident team 24x7 to detect breaches?
- Where do you currently store event and log data?
- How many events per second does your environment generate?
- What logs and data are you currently collecting?

Technologies Used in Our Solution

To build such a solution, innovative Intel Security technologies integrate with each other and help you evaluate the past, present, and future to detect and monitor for targeted attacks. The modular McAfee® Enterprise Security Manager—our security information and event management (SIEM) platform, McAfee Advanced Threat Defense, McAfee Active Response, and McAfee Threat Intelligence Exchange constitute the framework necessary to automatically detect advanced targeted attacks before damage is done. The four solutions are natively designed and pre-integrated to work together, offering the most unique, efficient, and comprehensive abilities. But each part of the solution can also be deployed individually to integrate with other existing security solutions, both homegrown and third-party. Additionally, integration with other Intel Security products will extend visibility and threat intelligence throughout your infrastructure.

McAfee Enterprise Security Manager resides at the heart of the solution. First the SIEM solution provides full visibility. It performs the data collection necessary to gain full situational awareness. The analysis of that data, which is the next step required to detect incidents, is also performed on the SIEM solution using advanced correlation modules.

The McAfee Advanced Threat Defense then boosts the SIEM's analytical abilities with deeper insights into the contents and intent of payloads collected by endpoint and gateway countermeasures, or input via RESTful APIs. McAfee Advanced Threat Defense provides McAfee Enterprise Security Manager with the most accurate and current threat intelligence, including intelligence that comes from malware found at your site—potentially from files targeted at your company and users. When Advanced Threat Defense convicts zero-day malware, it generates a list of IoCs matching the malware attributes and listing the changes and actions the malware would perform if run. McAfee Enterprise Security Manager will automatically receive that information from Advanced Threat Defense.

The BackTrace feature of the Enterprise Security Manager will then sift through past events looking for events matching the IoCs, letting you know if a similar attack has previously taken place in your environment. Looking towards the future, the solution's Alarm feature keeps an eye open for those IoCs, in case it encounters one in the future, immediately alerting you if the attacker comes back.

McAfee Active Response complements the McAfee Enterprise Security Manager solution by proactively searching your environment for IoCs. Active Response also uses the intelligence provided by Advanced Threat Defense so you can search for existing malware footholds. Once Advanced Threat Defense has generated a list of IoCs, incident response teams and administrators can use Active Response to look for malicious zero-day files that lay dormant on systems, which can be the case if the user has downloaded the file prior to its detection by Advanced Threat Defense, and has not run it yet. Active Response also looks for active processes in memory and many other IoCs. In addition to searching for IoCs on the fly, McAfee Active Response uses persistent collectors to continuously monitor your endpoints for specific IoCs. You will then be automatically alerted as soon as an IoC transpires somewhere in your environment.

Finally, the McAfee Threat Intelligence Exchange with the Data Exchange Layer (DXL) transmits threat intelligence in real time between all the other components. For example, using the DXL layer, Threat Intelligence Exchange instantly informs the SIEM solution and other components when Advanced Threat Defense convicts previously unknown malware in the environment. Sharing threat intelligence in real time is crucial since it ensures that all your security solutions can detect an attack as soon as information about that attack is generated.

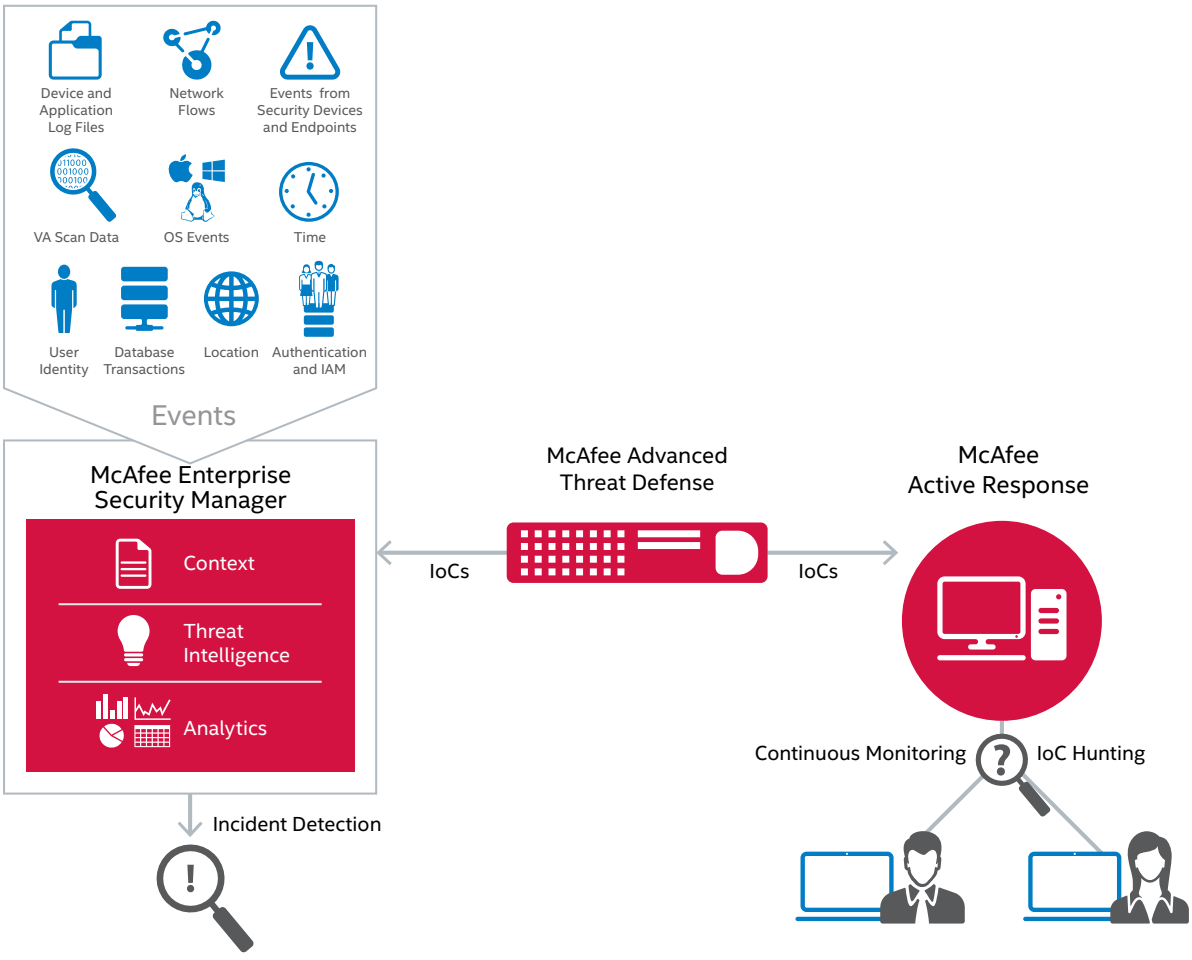


Figure 1. Technologies used in Intel Security solutions.

- **McAfee Enterprise Security Manager provides complete visibility and centralized intelligence**. It detects advanced targeted attacks by automatically collecting all of the necessary events and data from products in your environment and by analyzing and correlating that data to detect threats.

  First, the McAfee Enterprise Security Manager solution provides full visibility—it automatically collects, normalizes, and aggregates events from disparate sources. It then enriches that data with context that is not in the original event sent by the upstream data source, such as user information or host location information.

  It then analyzes that data to detect incidents using rule-based event correlation. For maximum effectiveness, the correlation engine gets its intelligence from multiple sources.

1. **From IoCs:** The Cyber Threat Manager in McAfee Enterprise Security Manager allows you to retrieve IoCs from remote sources and quickly assess related IoC activity in your environment. You can set up ongoing consumption of IoC feeds such as industry feeds (FS-ISAC) via STIX/TAXII, McAfee Advanced Threat Defense, and third-party web URLs, feeding the data into watchlists, alarms, and reports. You can then use dedicated dashboards for real-time monitoring. As part of the IoC ingestion workflow, the BackTrace feature of McAfee Enterprise Security Manager will look back up to 60 days to hunt for indicators in any network or system data it has retained. For example, it can reveal internal systems that have previously communicated with newly identified malware sources to help you reconstruct and contain an attack. Integrations with McAfee Threat Intelligence Exchange can also identify any managed endpoint that has previously accessed/executed files learned through IoC artifacts to be malicious.
2. **From the McAfee Global Threat Intelligence (McAfee GTI):** The McAfee GTI watchlist automatically provides the SIEM solution with reputation information about IP addresses, URLs, and malware.

In addition to the built-in correlation rules, the correlation engine then uses the following analytics methods.

1. **From content packs published by Intel Security:** These provide sets of correlation rules, alarms, watchlists, and dashboards for specific use cases such as malicious activity, malware, reconnaissance, and suspicious activity.
2. **From baselines:** McAfee Enterprise Security Manager can establish a baseline of what is normal in your environment, so any deviation can be used as an IoC. For example, if your users normally access websites located in North America, and you suddenly observe a spike in communication to sites in Eastern European countries where you don't do business and at a time when that user does not usually work, it could be a red flag indicating that some systems were compromised and are communicating with attackers.
3. **From customized rules:** Our Enterprise Security Manager provides you with the ability to create your own custom correlation rules to match your specific needs and risk tolerance. You could, for example, write your own correlation rule to be alerted when more than 10 viruses in less than an hour are detected for a user, followed by their system executing a file that has never been seen before. This usually would be a telltale sign that the user's credentials have been compromised, and someone is trying to set a foot hold on their system.

With that security information and its powerful analytics engine, McAfee Enterprise Security Manager is able to perform correlations to automatically detect and prioritize current, past, or future attacks.

- **McAfee Active Threat Defense detects zero-day malware and generates local threat intelligence**. When McAfee Threat Defense analyzes a file and convicts it of being malicious, it will generate a list of IoCs matching that malware. In addition to performing a dynamic analysis by letting the file run in a sandbox, McAfee Advanced Threat Defense performs a static code analysis by unpacking and fully reviewing the source code of the file. It analyzes both the original payload and any nested payloads that could be present in the code. This gives Advanced Threat Defense a unique ability to generate a comprehensive list of IoCs associated with that malware. The information includes the name, hash (MD5 or SHA-1), and severity of the convicted file, system that first detected it, the message that carried it, the source and destination systems, and the source URL if applicable. McAfee Advanced Threat Defense produces a report formatted in the industry standard Structured Threat Information eXpression (STIX). These details on malware and open formats enable you to understand malware intent and share the findings with other security applications, such as the Cyber Threat Manager of McAfee Enterprise Security Manager, which will then incorporate this threat intelligence in its analysis.

- **McAfee Active Response proactively looks for indicators of compromise on the endpoints.** McAfee Active Response gives you continuous visibility into your endpoints so you can identify breaches faster. It features persistent collectors that trigger upon detection of attack events, alerting you and your systems to attack activity you've been monitoring. It is highly automated, allowing you to capture and monitor events and changes that may indicate an attack as well as attack components that are lying dormant on the endpoints.
- **McAfee Threat Intelligence Exchange enables collaboration between security solutions.** The DXL is the protocol used between security solutions to exchange information about threats that are newly discovered. McAfee Enterprise Security Manager listens on the DXL, so it can benefit from any product that sends new information on the DXL. If the McAfee Threat Intelligence Exchange publishes information on the DXL about a brand-new malicious file, McAfee Enterprise Security Manager will be able to use that information immediately to create incidents if that file is also reported by other security countermeasures. A partnering Network Access Control solution listening to the DXL could also benefit from that information, by checking systems, including bring-your-own-device (BYOD) systems, for the presence of that new malicious file before granting them access to the network.

Optional Integrations

Product	Data Source for SIEM solution	McAfee Threat Intelligence Exchange	McAfee Advanced Threat Defense	McAfee ePolicy Orchestrator® (McAfee ePO™) software	Detection Example
McAfee Application Control	√			√	• Execution of unauthorized application.
McAfee Data Loss Prevention	√	√		√	• Sensitive data exfiltration. • Unapproved application accesses sensitive data. • Unapproved storage devices.
McAfee Endpoint Intelligence Agent	√			√	• Abnormal application makes outbound network connection.
McAfee Network Security Platform/ McAfee Intrusion Prevention System	√	√	√		• C2 (botnet) traffic detected. • Communication with malicious IP address.
McAfee Web Gateway	√	√	√	√	• C2 (botnet) traffic detected. • Malicious website accessed. • Unauthorized website accessed.
McAfee Database Application Monitor	√			√	• Privileged database access detected. • Database threat detected.
McAfee Application Data Monitor	√				• Sensitive data is transmitted. • Use of unauthorized applications.
McAfee Database Event Monitor	√				• Sensitive database data and policy violations. • Loss of database data through authorized channels.
McAfee Change Control	√			√	• Unauthorized system changes.
McAfee Host Intrusion Prevention	√			√	• Malware detected. • Abnormal firewall activity.
McAfee VirusScan® Enterprise software	√	√		√	• Malware detected.
McAfee SiteAdvisor® Enterprise	√	√		√	• Unauthorized website accessed. • Malicious website accessed.

Table 1. Additional integration with other Intel Security products will extend visibility and threat intelligence.

Impact of the Solution

The McAfee Enterprise Security Manager offers full visibility by consolidating each piece of the puzzle in one central location and one single-pane-of-glass console, allowing you to see the big picture and gain valuable insight into your security posture. It makes it easy for your security team to quickly gather the data required to clearly detect advanced targeted attacks. If they suspect something, the security analysts can retrieve the necessary data in minutes, saving precious time to respond to the attack.

The centralized intelligence provided by McAfee Enterprise Security Manager allows you to cut through the noise created by the millions of events generated in your environment. Its intelligence allows it to make sense of those events automatically and present you with only the incidents that matter, making sure that you do not miss key signals without falling victim to alert fatigue.

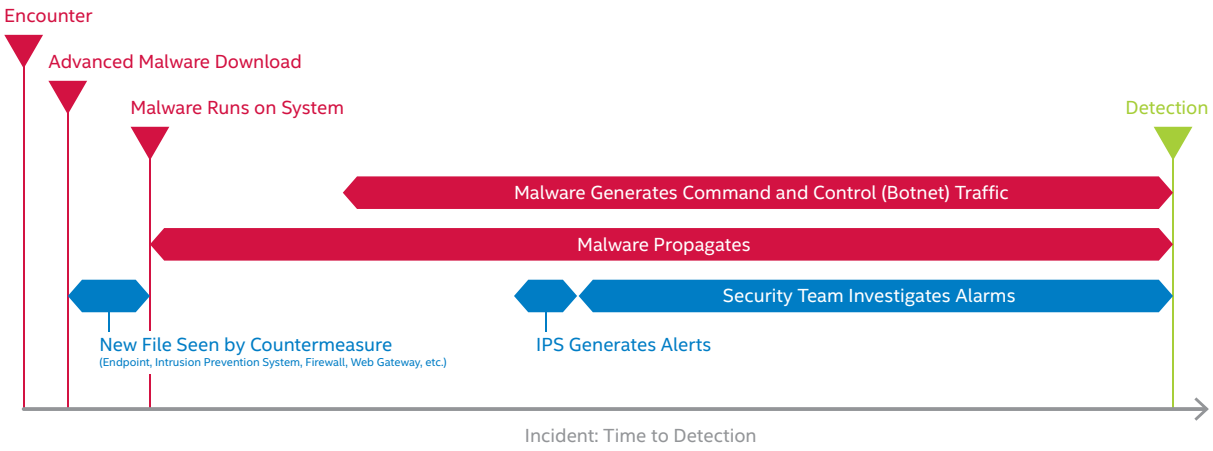
The powerful combination of Intel Security products will help you catch subtle and hard-to-detect IoCs that result from sophisticated advanced targeted attacks. With McAfee Advanced Threat Defense generating a list of IoCs, McAfee Threat Intelligence Exchange helping with their distribution, and McAfee Enterprise Security Manager and McAfee Active Response searching the past, the present, and the future for those IoCs, you tremendously increase your ability to detect hidden threats while reducing the time to find them.

Overall, the solution makes time work in your favor rather than against you. This product combination gives you the ability to detect attacks as soon as they occur, instead of days, weeks, or even months later. This Intel Security solution helps you drive toward detecting advanced targeted attacks during the Golden Hour, the essential hour that follows the initial breach, when you still have a chance to disrupt the attack before damage is done.

Ultimately, it allows you to free up and better use your security resources, so they can focus on responding and remediating the incident instead of spending their effort on detecting the incident.

Our solution for detecting advanced targeted attacks enables you to continuously monitor your environment to detect attacks in real time. It considerably reduces detection time, allowing you to take action immediately to limit the damage attackers can perpetrate. Through the unique use of local threat intelligence, it enables you to detect threats that only exist in your environment, so you don't have to rely on external sources to identify zero-day attacks against you.

Legacy Solutions



Intel Security Solutions

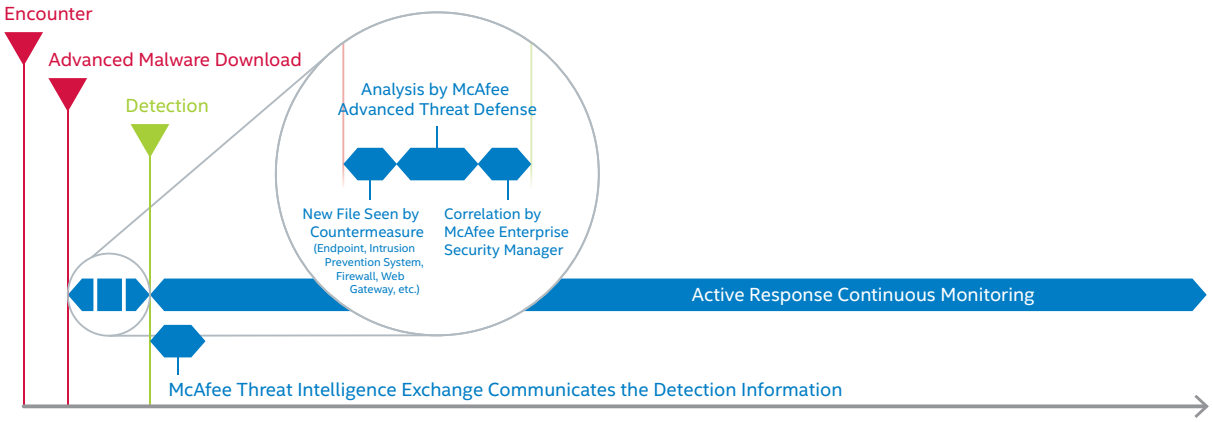


Figure 2. Incident time-to-detection.

Q&A

Does the solution work only with Intel Security products?

McAfee Enterprise Security Manager solution can collect events from most sources of data, including other security solutions and third-party services. We would recommend enriching its intelligence with information coming from McAfee Threat Intelligence Exchange and other unique Intel Security solutions.

In addition, more than 130 technology partners are available through the McAfee Security Innovation Alliance. Their tools snap directly into our Security Connected framework. The Security Innovation Alliance enables you to leverage investments you've already made, bringing strategic tools together, and augmenting them where necessary.

Finally, the platform supports a range of open standards including STIX/TAXII, IoCs, and RESTful APIs. Our products support open standards wherever reasonable.

Most SIEM solution vendors say they can do the same thing. What's so special about McAfee Enterprise Security Manager?

Ours goes beyond a SIEM solution. Even though McAfee Enterprise Security Manager solution is at the heart of the solution, it's completed by McAfee Advanced Threat Defense intelligence, McAfee Threat Intelligence Exchange/DXL, and the ability to immediately communicate threat data to other components of your defense, and McAfee Active Response's ability to search for IoCs in real time. This ability to generate its own local threat intelligence and share and use it in real-time is what makes the Intel Security solution unique and powerful. This ability is crucial to ensure that all your security solutions can detect an attack as soon as any bit of information about it is uncovered by one of the security products, instantly making the entire system stronger. In addition, the BackTrace feature of McAfee Enterprise Security Manager looks for indicators that have been encountered in the past, allowing you to know if you have previously been exposed to a specific attack.

I have my own helpdesk solution to manage alerts and incidents; Can your solution work with it?

Absolutely. The McAfee Enterprise Security Manager integrates with third-party ticketing systems, such as Remedy, and can forward alerts to them.

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

62344bp_detect_0416_pb