

# Combat and Mitigate Cyberattacks

Stream the latest threat data and alerts on compromised networks directly to the McAfee ePO console to block future malicious communications

## McAfee Compatible Solution

- ActiveKnowledge Signals 2.5
- ActiveTrust Resolver 2.5
- McAfee ePolicy Orchestrator 4.6

## Joint Solution Benefits

- Prevent data exfiltration by blocking known bad locations
- Optimize time and resources
- Centralize threat management
- Integrate reporting
- Dashboard alerts

Many of today's leading enterprises and government entities worldwide depend on the latest threat intelligence products and services from IID to protect their growth plans, assets, and customers from cyberattacks. Now they can stream the same threat data already being displayed in IID dashboards in real time, as well as alerts on compromised networks simultaneously to the McAfee ePolicy Orchestrator® (McAfee ePO™) console for unified control, improved visibility, streamlined workflow, and simplified threat management.

## Combat and Mitigate the Latest Cyber Threats

Cybercrime is a constantly evolving part of the Internet tapestry, and it's here to stay. An organization's ability to combat these threats is only as good as the data and tools it has on hand—which is why many of the world's largest financial services firms, government agencies, and online properties rely on IID's threat intelligence and mitigation products. Now IID's real-time threat data feeds—and alerts on compromised networks—can be viewed from within the McAfee ePO console.

### Actionable threat intelligence

IID ActiveKnowledge® Signals, powered by IID's automated threat intelligence sharing solution ActiveTrust, arms enterprise security teams with timely, actionable alerts about threatening or potentially dangerous activities occurring on internal, external, and partner networks. These alerts build on extensive and fresh knowledge about the latest malicious Internet locations and activities outside of an organization, often those related to advanced persistent threats (APTs). This actionable intelligence empowers companies to identify and quickly mitigate ongoing data exfiltration, malware infection, malicious communications, and other dangerous activities before they cause significant damage.

Data isn't always completely useful, and sources that provide inaccurate or incomplete data can ultimately lead to less-than-optimal decisions. That's why ActiveKnowledge Signals leverages one of the industry's broadest collective intelligence sources, as well as a live team that analyzes and scrubs the data to ensure it's timely, accurate, and comprehensive—in other words, actionable.

As important as it is, ActiveKnowledge Signals is also about efficiency. The data is straightforward, leaving little in the way for interpretation, and is designed for fast deployment from within an organization's McAfee ePO console. So you can spend less time wading through endless data and sources, and more time blocking threats.

### Advanced threat mitigation

IID ActiveTrust® Resolver, also powered by IID's automated threat intelligence sharing solution ActiveTrust, filters outbound DNS requests emanating from your internal networks. It redirects traffic for known bad locations to its TrapTrace server. ActiveTrust Resolver blocks communications to malware controllers, spear phishing sites, data exfiltration drop servers, and other threats—tracing these communications back to the originating system. It discovers and mitigates compromises before they can burrow deep into the network, often preventing potential problems before they happen.

Now, customers can receive the alerts from ActiveTrust Resolver in the McAfee ePO console, getting instant notifications when a compromised machine tries to access a command-and-control server or transmit sensitive data to a known drop zone. Administrators can learn immediately if users attempt to reach phishing or malware distribution sites in order to track down “spear phishing” attacks—or even just to educate employees the moment they are fooled by the latest scams. And more than just a passive alert, ActiveTrust Resolver blocks these connections, quarantines them, and traces them so you get the necessary time to pinpoint, isolate, and identify machines for immediate cleaning.

### McAfee ePO Console Integration with IID Solutions

No more digging through mountains of data to determine if your enterprise is at risk. By integrating IID’s solutions into the McAfee ePO console, organizations get real-time alerts about the latest Internet threats and compromised machines living in their network, all in one place. With this centralization and consolidation of resources, organizations can save valuable time while protecting mission- and business-critical data and communications. By doing so, organizations can concentrate more on their core business.

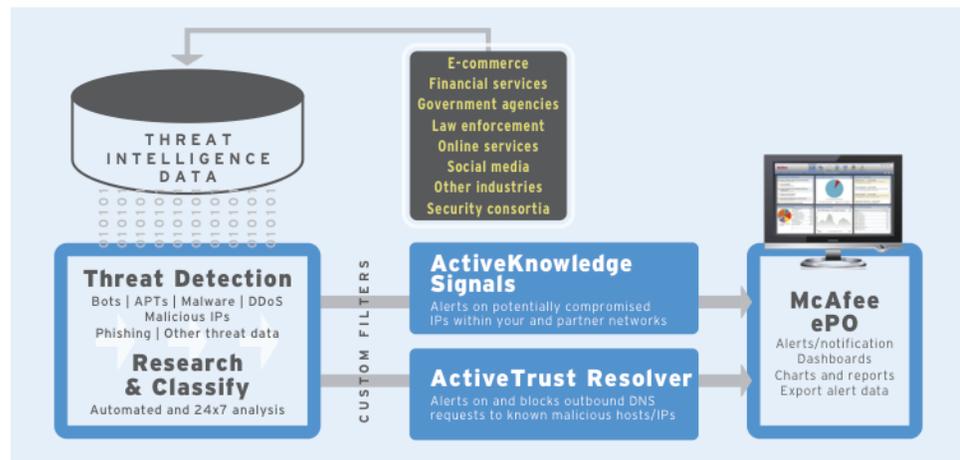


Figure 1. McAfee ePO Console integrated with IID solutions.

### About IID

IID enables trusted threat intelligence collaboration for enterprises and governments. The company aggregates widely sourced threat data and then compares this information against its own curated feeds to deliver actionable intelligence, enabling the protection of business growth, brands, and users. IID’s ActiveTrust network enables threat intelligence sharing in a trusted environment that reaches beyond limited trust groups. ActiveTrust delivers automated threat intelligence that allows network members to focus on their core business and maximize their most valuable resources, human capital and time.

For more information about IID, go to [www.internetidentity.com](http://www.internetidentity.com).

### About McAfee ePolicy Orchestrator (ePO) software

McAfee ePO is the first platform that lets enterprises and governments centrally manage security and compliance products from multiple vendors, offering unprecedented cost savings and return on investment. With more than 40,000 customers and managing more than 60 million PCs and servers, this unique platform is helping McAfee SIA partners to extend their reach and create complementary functionality.

