

McAfee Global Threat Intelligence

Comprehensive, cloud-based threat intelligence

The cyberthreat landscape is evolving so rapidly that it is a challenge for IT to keep up. Not only has the threat growth curve shifted from a linear to an exponential one, but threats have become increasingly sophisticated and evasive. With the growth of cyberthreats putting extra pressure on your IT infrastructure and budget, your security needs to work more intelligently.

Shared Threat Intelligence

McAfee has the answer—a reputation-based system that has visibility into all types of cyberthreats from around the globe and helps an organization's security infrastructure make decisions in real time.

McAfee Global Threat Intelligence™ is a comprehensive, real-time, cloud-based threat intelligence service that enables McAfee products to protect customers against cyberthreats across all vectors—file, web, message, and network. Already integrated into your McAfee security products, McAfee Global Threat Intelligence has the broadest threat data, most robust data correlation, and most complete product integration in the market. This gives McAfee unique visibility into online dangers such as botnets, worms, DNS attacks, and even advanced persistent threats.

McAfee Global Threat Intelligence complements your on-premises or Software-as-a-Service (SaaS) McAfee products by providing them with the most up-to-date reputation intelligence so that they can take appropriate policy-based action when threats strike. McAfee Global Threat Intelligence is integrated throughout the McAfee suite of security products, creating a shared intelligence model where your security infrastructure works in concert to protect your organization.

How It Works

McAfee Global Threat Intelligence can be described using the three-part framework shown below.

At the top, the icons in the cloud represent the threat data we correlate to produce our threat intelligence. The data come from multiple sources, primarily queries from the millions of McAfee products acting as sensors that are deployed in real-world settings around the globe. With each query, our cloud system learns something new about the subject of the query. We combine that with data from other threat vectors to understand cyberthreats from all angles and identify threat relationships, such as malware used in network intrusions, websites embedded in malware code, websites hosting malware, botnet associations, and more.



Figure 1. McAfee Global Threat Intelligence framework.

McAfee Global Threat Intelligence is based on:

- More than one hundred million McAfee nodes deployed around the globe
- More than one hundred billion queries each month from all threat vectors—file, web, message, and network
- The most comprehensive set of threat intelligence services in the market—file reputation, web reputation, web categorization, message reputation, and network connection reputation

The middle tier represents the bidirectional communications that occurs between McAfee products and McAfee Global Threat Intelligence. McAfee products query the cloud, and our cloud renders the latest reputation or categorization intelligence to the products so that they can take action.

Finally, the bottom tier represents McAfee products that are integrated with McAfee Global Threat Intelligence. Not only do more McAfee products integrate McAfee Global Threat Intelligence, but those products also integrate more threat intelligence services than any other security products available today—services like file reputation, web reputation, web categorization, message reputation, and network connection reputation.

Benefits of Using McAfee Global Threat Intelligence

- Protects organizations and their users from both known and emerging cyberthreats, regardless of the source of those threats or where they propagate
- Arms your security infrastructure with shared threat intelligence, enabling security products to act in concert, based on the same robust, real-time information
- Closes the threat window with instantaneous, and often predictive, reputation-based threat intelligence, reducing the probability of attack and cost of remediation and lost downtime

Availability

McAfee Global Threat Intelligence is included in the cost of McAfee products that incorporate this service. In some products, McAfee Global Threat Intelligence is enabled by default. If not, customers may enable it easily in their McAfee product administrative interface. To learn more about how to enable McAfee Global Threat Intelligence in your product, please visit: www.mcafee.com/GTITurnItOn.

For organizations that operate environments with limited Internet access, McAfee offers the McAfee Global Threat Intelligence Server, a virtual appliance that consolidates client-to-cloud communications via a set of auditable proxy servers for McAfee-protected clients.

McAfee Global Threat Intelligence is also available as a standalone service.

Contact your McAfee account representative for more information.

