Data Sheet

McAfee Embedded Reputation SDK

McAfee enables OEM participation in the McAfee Global Threat Intelligence cloud.

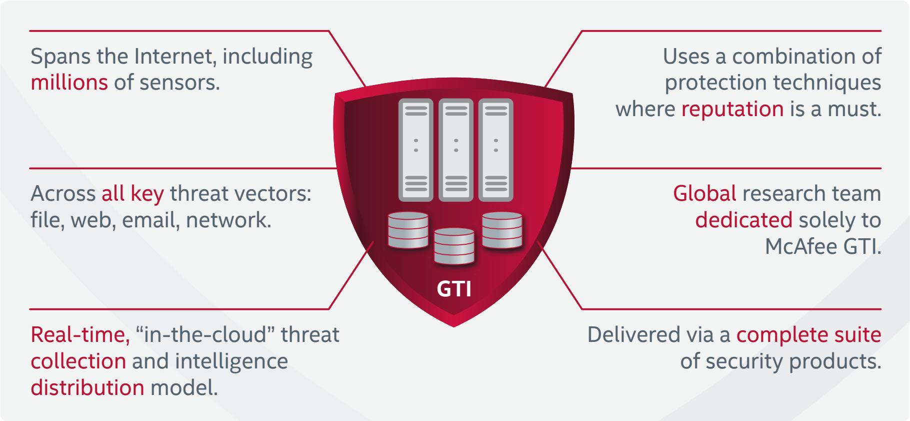
McAfee Embedded Reputation SDK

- An embeddable application programming interface (API) for C and C++ applications that lets third-party products call real-time reputation scores from the McAfee GTI cloud or resolve those queries against a local database.

McAfee Global Threat Intelligence

- The industry's most comprehensive set of threat intelligence services—web reputation, IP address reputation, message reputation, network connection reputation, and web content categorization.
- Based on real-time inquiry data from more than 100 million McAfee sensor nodes deployed worldwide.

The McAfee® Embedded Reputation SDK—now a part of the Intel® Security product offering—allows application developers and network device OEMs to boost the security and integrity of their products with the real-time protection of McAfee Global Threat Intelligence (McAfee GTI). Reputation systems have been used for years across many disciplines—from doctors diagnosing illnesses to mathematical experts rating financial instruments. Just as a weather forecaster looks at dozens of data points to determine where a storm will develop, how big it will be, and where it is headed, security vendors also need to look at thousands of data points to provide the best possible protection against today's threats.



Spans the Internet, including millions of sensors.

Across all key threat vectors: file, web, email, network.

Real-time, "in-the-cloud" threat collection and intelligence distribution model.

Uses a combination of protection techniques where reputation is a must.

Global research team dedicated solely to McAfee GTI.

Delivered via a complete suite of security products.

Figure 1. Six principles of McAfee Global Threat Intelligence.

Telemetry Scope (Sensors)

- Malware: 60 million endpoints.
- Email: 30 million nodes.
- Web: 45 million endpoint and gateway users.
- Intrusions: 4 million nodes.
- More than 100 million devices in 120 countries.
- More than 64 billion queries per day.

The Cloud Service: McAfee GTI

McAfee GTI is a comprehensive, real-time, cloud-based threat intelligence service built on a global system of more than 100 million data sensors, seven global data centers, cross-vector correlation, and more than 350 researchers. Our sensors handle more than 64 billion queries each day across all major threat vectors, including web, file, email, and network. McAfee correlates intelligence across these four primary databases to provide the latest reputation scores for IP addresses, URLs, messages, and senders. The result is a unique, real-time reputation score that reflects the moment-to-moment trustworthiness of websites, domains, hosts, IP addresses, and messages. McAfee GTI delivers unique visibility into botnets, worms, DNS attacks, advanced persistent threats, and a plague of other online perils, allowing security controls to apply policy accurately and effectively even in the absence of a known threat signature.

McAfee GTI is based on six key principles illustrated in Figure 1 that empower McAfee users to create a significantly enhanced security posture by simply activating features that already exist in their current products. That security is built into 90% of all McAfee products, and now you can build it into yours with the McAfee Embedded Reputation SDK.

The Client API: McAfee Embedded Reputation SDK

The McAfee Embedded Reputation SDK is a client-side software component—an embeddable API for C and C++ applications. The SDK allows third-party products to request real-time reputation scores from the McAfee GTI cloud or resolve queries against a local database that is updated continuously by the cloud service (see Figure 2). SSL encryption and certificate authentication secure all traffic between the application and cloud service. The SDK is available as a DLL for multiple platforms, including Microsoft Windows, Linux, OSX, and Solaris, with comprehensive developer support services.

Other SDK features include:

- A Java-native interface.
- Programmable logging interface.
- Optional support for digitally signed web database files.

Embedded Threat Intelligence Benefits

With the McAfee Embedded Reputation SDK, your application or device can leverage key features of the McAfee GTI cloud service to identify and block a wide range of threats, including targeted attacks using unknown malware with no catalogued signature. Key services include:

- **Web reputation scoring**—Reputation scores are available for millions of URLs, web domains, and DNS servers, reflecting the probability that the resource in question is a phishing site, infected with malware, or otherwise malicious. The score is based not only on the collective intelligence from sensors querying the McAfee cloud and the analysis performed by McAfee Labs researchers and automated tools, but also on the correlation of cross-vector intelligence from file, email, and network threat data. Products like McAfee SiteAdvisor® software use the McAfee Embedded Reputation SDK to provide real-time insight on the trustworthiness of websites and other online entities.
- **IP address reputation scoring**—The McAfee GTI cloud service keeps a list of IP addresses that appear to be acting as spam servers or are associated with messages that have been identified as spam. With the McAfee Embedded Reputation SDK, your application can block known spam generators and malware sources.
- **Message content reputation scoring**—Billions of individual messages are inspected daily to determine whether the content is spam or a concealed

malware payload. If a message contains many images or links to known compromised sites, the McAfee Embedded Reputation SDK will enable your product to identify it as malicious and block it at the client, server, or network gateway.

- **Connection reputation scoring**—Web reputation scores are based on an analysis of traffic originating from a host system's port 80. Connection reputation is a more holistic assessment of all traffic originating from all the open ports on a host and the probability that it is trustworthy or has been compromised. If the system in question appears to host a spam server, act as a VNC server, or host an IRC chat server, the McAfee Embedded Reputation SDK will allow your application to know before it connects.
- **Content categorization**—In addition to calculating reputation scores for web resources, IP addresses, messages, and connections, the McAfee GTI segments websites into more than 100 categories based on the types of content they host. If your product needs to block (or allow) access to certain site or content types, the McAfee Embedded Reputation SDK offers an off-the-shelf solution.

Real-Time Reputation Intelligence, Ready to Embed

For more information on the McAfee Embedded Reputation SDK and the services of the McAfee GTI cloud service, visit **www.mcafee.com/embeddedsecurity**, or contact your local McAfee representative.

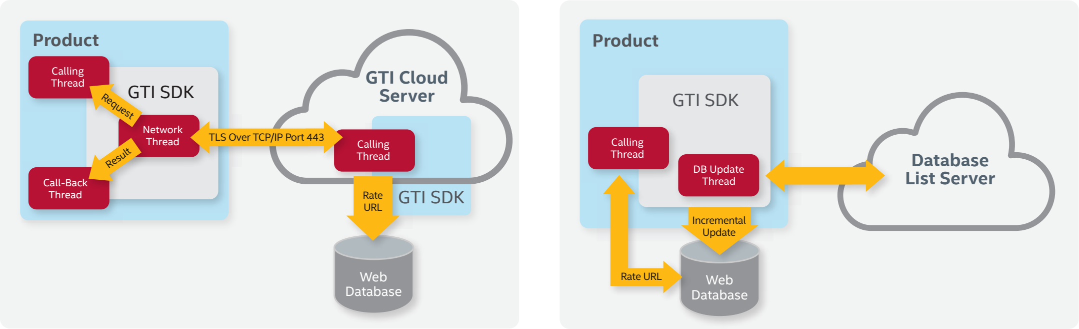


Figure 2. The McAfee Embedded Reputation SDK enables third-party devices or applications to request real-time reputation scores from either the McAfee GTI cloud service (left), or from a local database updated by the cloud service (right).

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