McAfee Cloud Threat Detection

Easily enhance McAfee® protections to convict advanced malware and expose evasive threats

An array of the latest analytics from McAfee—including machine learning—identifies malware and converts convictions into action, updating protections to thwart similar attacks in the future.

Organizations face an uphill battle as clever malware continues to evade traditional defenses. Advanced detection solutions help, but they may seem complex and expensive if you have limited security staff and resources. Most also don't integrate with protection infrastructure, so they let the vulnerability window increase as responders scramble to take action.

What's needed? Cost-effective advanced detection that's dead simple to deploy and use: McAfee® Cloud Threat Detection. This convenient new service plugs into existing McAfee solutions to convict advanced malware and expose evasive threats. As a cloud offering, it lets you easily take advantage of massive compute horsepower that operates an array of the latest analysis techniques. You can enhance detection and optimize existing security investments.

Detection Integrated with Protection

McAfee solutions provide your first line of defense, screening out known malware and likely malware using advanced tools such as emulation and reputation. But if they can't be sure a file is malicious, they can defer to the cloud for a thorough analysis.

Machines versus Emerging and Evasive Malware

With McAfee Cloud Threat Detection, static analysis engines go to work extracting file details. Comprehensive file type coverage provides much-needed context to grey files, effectively identifying both malicious and clean files. In addition, behavioral analysis engages as the file also runs in a sandbox environment. Anything the malware does is recorded, reviewed, and evaluated for malicious intent. Did the file generate a random folder, write a new file to it, and delete the original file? Did it disguise outreach to unknown or suspicious URLs between traffic to known sites like Google, Amazon, or Facebook? These are just a few examples of behaviors the McAfee Cloud Threat Detection service can use to classify an unknown file. These processes also reveal the metadata, URLs, filenames, folder locations, and more that we report back to customers so they can investigate and see if other machines have been compromised.

Key Benefits:

- Reduce risk of unknown threats damaging your business
- Harness Big Data and machine learning power
- Optimize security investments
- Simplify deployment of advanced threat analysis

Supervised Machine Learning

Managed and tuned by McAfee Labs, each step of the analysis cycle harnesses the power of big brains, Big Data, and machine learning. Insight from more than 25 years of data and 2 billion files was used to develop and train extensive classification models in our Big Data system in the cloud. Active research and the constant interpretation of inspection results feed ongoing machine learning to evolve these models as malware techniques and behaviors change and research advances.

Focus on Accuracy

Our experience has taught us that a false negative or false positive can be damaging and expensive. So the systems we use include checks and balances against the most critical system files and signing certificates to ensure convictions are timely, yet reliable. While advanced analysis detects emerging threats, we cross-reference and associate malware artifacts and behavioral and contextual attributes to minimize false positives. This is one of the distinctive advantages of our combination of cloud analysis and extensive anti-malware resources.

Detection in Action

For each verdict, McAfee Cloud Threat Detection notifies the originating system, which enforces policy such as quarantining a machine or enabling protection to thwart similar attacks. Detailed indicators of compromise (IoCs) and reports are available for further investigation and the insights required to correct and recover post-attack. And convictions update reputations in McAfee Global Threat Intelligence (McAfee GTI) to accelerate protection for all organizations with McAfee GTI-enabled solutions. Manual submission supports investigations and enables analysts to easily upload files for one-off analysis.

Fast-Acting, Affordable, and Small-Business Friendly

As a cloud-based service, you simply enter an encrypted shared key from your integrated McAfee product so provisioning is fast. If you have distributed systems, there's no need to backhaul traffic to a data center, just send it to the cloud. Our experts take care of ongoing maintenance and implement updates and upgrades transparently. Instead of up-front capital expenditures, volume-based subscription pricing that covers all integrated McAfee solutions eliminates cost-based barriers to entry.

Learn more at **mcafee.com/ctd**.

Integrated Solutions

- McAfee® ePolicy Orchestrator® Cloud
- McAfee Network Security Platform
- McAfee Threat Intelligence Exchange
  - McAfee Endpoint Protection
- McAfee Web Gateway and Web Gateway Cloud Service

McAfee
Together is power.

2821 Mission College Boulevard
Santa Clara, CA 95054
888 847 8766
www.mcafee.com