# McAfee Cloud Threat Detection

## Unkomplizierte Erweiterung des Intel Security-Schutzes zur Erkennung hochentwickelter Malware und Aufdeckung von Stealth-Bedrohungen

Eine Vielzahl an neuesten Analysemöglichkeiten – einschließlich Machine Learning – erkennt Malware und setzt Erkennungen in Aktionen um, wobei die Schutzmaßnahmen auf den neuesten Stand gebracht werden, um ähnliche Angriffe in Zukunft abzuwehren.

**Wichtige Vorteile:**

- Minimierung von Risiken durch unbekannte Bedrohungen für Ihr Unternehmen
- Nutzung von Big Data und Machine Learning
- Optimale Nutzung der Sicherheitsinvestitionen
- Einfache Implementierung hochentwickelter Bedrohungsanalysen

Unternehmen befinden sich in einem ungleichen Kampf, da Malware immer wieder herkömmliche Schutzmaßnahmen umgeht. Hochentwickelte Erkennungslösungen helfen, doch wenn Sie über wenig Sicherheitspersonal und Ressourcen verfügen, dann sind diese Lösungen zu komplex und zu teuer. Zudem integrieren sie sich meist nicht in die Sicherheitsinfrastruktur, sodass das Schwachstellenfenster größer wird, während die Sicherheitsverantwortlichen hektisch Maßnahmen ergreifen.

Notwendig ist deshalb eine kostengünstige hochentwickelte Erkennungslösung, die absolut problemlos implementiert und eingesetzt werden kann: McAfee® Cloud Threat Detection. Dieser nützliche neue Service integriert sich in vorhandene Intel® Security-Lösungen, um raffinierte Malware zu überführen und Stealth-Bedrohungen aufzudecken. Als Cloud-Angebot bietet McAfee® Cloud Threat Detection enorme Rechenleistung, was den Einsatz einer Vielzahl an neuesten Analysetechniken ermöglicht. Dadurch können Sie die Erkennung verbessern und vorhandene Sicherheitsinvestitionen optimieren.

### In den Schutz integrierte Erkennung

Intel Security-Lösungen stellen Ihre erste Verteidigungslinie dar, die durch den Einsatz hochentwickelter Tools wie Emulation und Reputation bekannte sowie wahrscheinliche Malware aufspürt. Wenn jedoch nicht sicher ist, ob eine Datei als böswillig eingestuft werden muss, wird sie zur gründlichen Analyse an die Cloud übergeben.

### Maschinelle Analyse gegen neue und heimliche Malware

Bei McAfee Cloud Threat Detection werden Module zur statischen Analyse dazu eingesetzt, die Details der Datei zu extrahieren. Dank der umfassenden Abdeckung verschiedenster Dateitypen erhalten Sie die dringend erforderlichen Informationen über „graue“ Dateien, damit Sie böswillige und saubere Dateien zuverlässig trennen können. Wenn die Datei in einer Sandbox-Umgebung ausgeführt wird, kommt zusätzlich die Verhaltensanalyse ins Spiel. Jede Aktion der Malware wird erfasst, geprüft und auf böswillige Absichten untersucht.

intel Security

Legt die Datei einen zufälligen Ordner an, schreibt sie eine neue Datei hinein und löscht die ursprüngliche Datei? Verschleiert sie Verbindungen zu unbekannten oder verdächtigen URLs im Datenverkehr zu bekannten Webseiten wie Google, Amazon oder Facebook? Dies sind nur einige Beispiele für Verhalten, das der McAfee Cloud Threat Detection-Service zur Klassifizierung unbekannter Dateien hinzuzieht. Diese Prozesse decken auch die Metadaten, URLs, Dateinamen, Ordnerspeicherorte und viele weitere Informationen auf, die wir an die Kunden weitergeben, damit sie eigene Untersuchungen starten und nach weiteren kompromittierten Computern suchen können.

## Unterstütztes Machine Learning

Jeder Schritt des von McAfee Labs verwalteten und optimierten Analysevorgangs profitiert von Fachkompetenz, Big Data sowie Machine Learning. Bei der Entwicklung und dem Training umfassender Klassifizierungsmodelle in unserem Big-Data-System in der Cloud kam das Wissen aus den in mehr als 25 Jahren erhobenen Daten und 2 Milliarden Dateien zum Einsatz. Aktive Forschung und die kontinuierliche Interpretation der Untersuchungsergebnisse unterstützen das dauerhafte maschinelle Lernen, mit dessen Hilfe diese Modelle weiterentwickelt werden, da Malware-Techniken und -Verhalten sich verändern und die Forschung voranschreitet.

## Konzentration auf Genauigkeit

Aus Erfahrung wissen wir, dass ein False-Negative oder ein False-Positive schädlich und teuer werden kann. Aus diesem Grund enthalten unsere Systeme Funktionen zur Überprüfung und zum Abgleich mit den wichtigsten Systemdateien sowie Signaturzertifikaten, damit Erkennungen nicht nur schnell erfolgen, sondern auch zuverlässig sind. Während die hochentwickelte Analyse neue Bedrohungen erkennt, setzen wir Malware-Artefakte und Verhaltens- sowie Kontextattribute miteinander in Beziehung, um die Zahl von False-Positives zu minimieren. Dies ist einer der bedeutendsten Vorteile unserer Kombination aus Cloud-Analysen und umfangreichen Malware-Schutzressourcen.

## Erkennung in Aktion

Bei jedem Urteil benachrichtigt McAfee Cloud Threat Detection das ursprüngliche System, das daraufhin Richtlinien durchsetzt, z. B. die Isolierung eines Computers oder die Aktivierung geeigneter Schutzmaßnahmen zur Abwehr ähnlicher Angriffe. Detaillierte Kompromittierungsindikatoren werden zur Durchführung weiterer Untersuchungen verwendet und liefern Informationen, mit denen nach einem Angriff Behebungsmaßnahmen durchgeführt werden können. Die Erkennungen aktualisieren wiederum die Reputationsdatenbank von McAfee Global Threat Intelligence (GTI). Davon profitieren alle Unternehmen, die GTI-unterstützte Lösungen einsetzen.

## Schnell, kostengünstig und ideal für kleine Unternehmen

Die Bereitstellung dieses Cloud-basierten Services ist ganz einfach: Sie müssen lediglich einen verschlüsselten Freigabeschlüssel aus Ihrem integrierten McAfee-Produkt eingeben. Wenn Sie verteilte Systeme nutzen, müssen Sie keinen Datenverkehr zurück zum Rechenzentrum leiten, sondern können ihn einfach in die Cloud senden. Unsere Experten übernehmen die laufende Verwaltung und implementieren transparent Updates sowie Upgrades. Es sind keine Vorabinvestitionen erforderlich, da der Service mit einem volumenbasierten Abonnementmodell angeboten wird.

Weitere Informationen finden Sie unter **www.mcafee.com/de/products/cloud-threat-detection.aspx**.

**McAfee. Part of Intel Security.**
Ohmstr. 1
85716 Unterschleißheim
Deutschland
+49 (0)89 37 07-0
www.intelsecurity.com