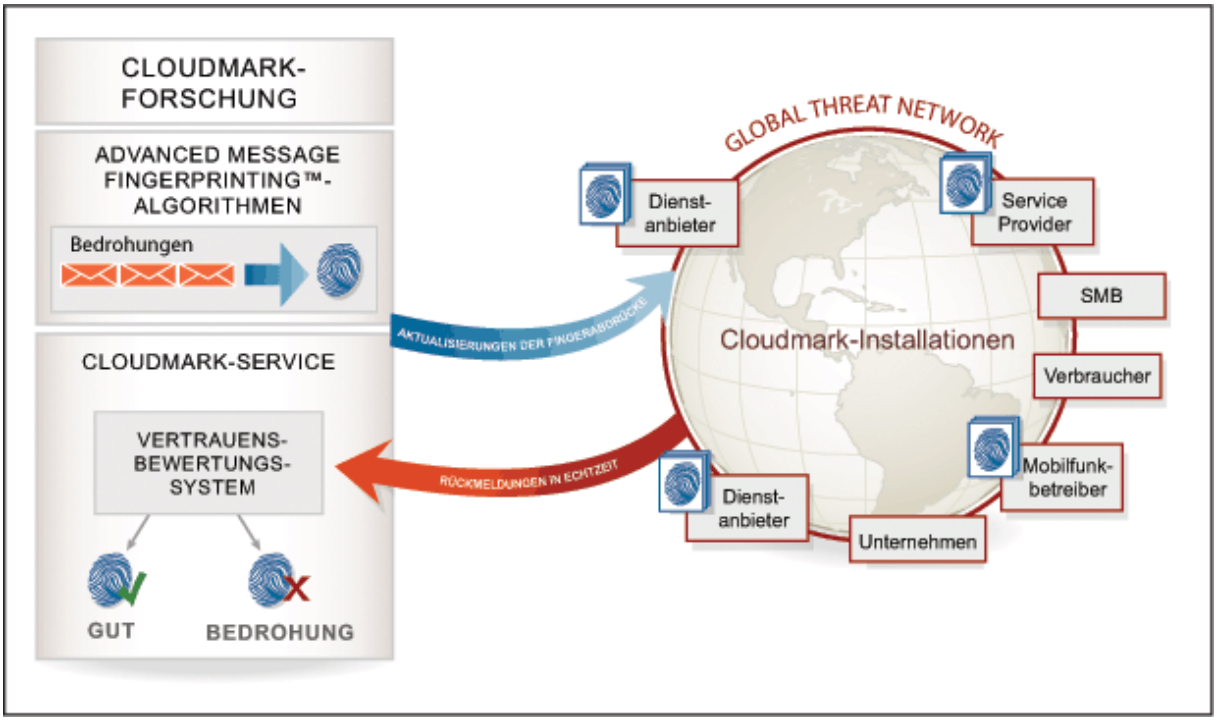
Cloudmark-Technologie

Cloudmark nutzt von Anwendern gesammelte Informationen, das Zusammenspiel aus Advanced Message Fingerprinting™, Benutzermeldungen und automatisierter Datenanalyse sorgt für unübertroffene Erkennungsraten und die schnellsten verfügbaren Reaktionszeiten auf neue Bedrohungen.

Die Technologien von Cloudmark wurden von Experten für Messaging-Sicherheit mit drei zentralen Zielen entwickelt:

- Gegenwärtig verbreitete Angriffe automatisch aufhalten, einschließlich ihrer polymorphen Varianten
- Neuen Angriffsvektoren einen Schritt voraus sein
- Große Datenströme mit hoher Effizienz und Skalierbarkeit filtern

Der Ansatz von Cloudmark



Advanced Message Fingerprinting

Die Advanced Message Fingerprinting-Algorithmen von Cloudmark bilden den Kern des Cloudmark-Ansatzes und ermöglichen die automatische Erkennung von Bedrohungen der Messaging-Systeme. Die Fingerabdruck-Algorithmen von Cloudmark richten sich auf verschiedene, in Nachrichten eingebettete Attribute von Bedrohungen. Beim Empfang der einzelnen Nachrichten erzeugen diese Algorithmen "Fingerabdrücke", die eindeutige Aspekte jeder Nachricht darstellen. Nachdem die Übereinstimmung eines Fingerabdrucks mit einem bestätigten Spam-, Phishing- oder Viren-Angriff festgestellt wurde, werden alle aktuellen und zukünftigen Nachrichten mit diesem Fingerabdruck sofort blockiert. So kann Cloudmark Mutationen und Varianten praktisch in Echtzeit erkennen. Weitere Informationen zum Advanced Message Fingerprinting

Global Threat Network™

Bei neuen Ausbrüchen bietet Cloudmark dank seines Global Threat Network, dem größten und ausgereiftesten Netzwerk der Branche, extrem kurze Reaktionszeiten. Mit Cloudmark ist die

Bedrohungsüberwachung nicht auf eine einzige Abteilung in einem Unternehmen beschränkt, sondern wird durch ein weltweites Netzwerk mit 850 Millionen Berichtsquellen in mehr als 190 Ländern gebildet. Das Global Threat Network setzt sich aus den Teams zur Bekämpfung von Missbrauch bei Dienstanbietern, Systemadministratoren, Honeypots und vertrauenswürdigen Benutzern zusammen. Die Rückmeldungen dieser Quellen erlauben es Cloudmark, die neuesten Bedrohungen innerhalb von Minuten nach Beginn des Angriffs zu blockieren.

Dienste von Cloudmark und das Trust Evaluation System™

Alle Rückmeldungen aus dem Global Threat Network werden über das Trust Evaluation System von Cloudmark analysiert und überprüft. Das System verfolgt den Ruf der Quelle und klassifiziert Fingerabdrücke anhand dieses Rufs sowie der Anzahl der Meldungen. Ein Absender erreicht nur mit der Zeit und durchgängig richtigen Rückmeldungen einen guter Ruf oder "Vertrauenswürdigkeit". Das System erhält die Integrität der Berichte und ist dadurch in der Erkennung äußerst genau. Rückmeldungen werden fortlaufend überprüft, und alle Fehlklassifizierungen von Nachrichten, wie zu unrecht als Spam klassifizierte legitime Nachrichten und der umgekehrte Fall, werden ohne manuelles Einschreiten berichtigt. Kein anderes System überprüft Rückmeldungen mit derselben Kontinuität und Schnelligkeit.

Das Trust Evaluation System bildet eine Schlüsselkomponente des Cloudmark-Dienstes, der die Backend-Analyse durchführt und festlegt, ob eine Nachricht legitim oder bedrohlich ist, Bedrohungen nach ihrer Art einordnet und Informationen zu Bedrohungen an die Kunden von Cloudmark verteilt.

Cloudmark-Forschung

Das Forschungsteam von Cloudmark setzt sich aus führenden Innovatoren der Bekämpfung von Nachrichtenmissbrauch zusammen. Die Forschung von Cloudmark entwickelt neue Fingerabdruck-Algorithmen und Prozesse für die Backend-Analyse, damit Bedrohungen der Messaging-Systeme in allen ihren Spielarten bekämpft werden können. Für die optimale Wirksamkeit der Lösung von Cloudmark gegen die neuesten Arten von Nachrichtenmissbrauch analysiert und prognostiziert die Cloudmark-Forschung fortlaufend die globalen Trends beim Missbrauch der Messaging-Systeme.