

Trend Micro™

SMART PROTECTION NETWORK™

Wir spüren mehr Bedrohungen auf

Das Trend Micro Smart Protection Network ist eine cloudbasierte Sicherheitsinfrastruktur, in der neue Bedrohungen schnell und genau erfasst und erkannt werden, um diese Erkenntnisse in einen sofortigen Schutz aller Daten unabhängig vom Speicherort umzusetzen.

Kriminelle Aktivitäten im Bereich Cloud-Computing und die Konsumerisierung der IT in Kombination mit einem schnellen Zuwachs schwer zu erkennender, gezielter Angriffe machen es für Anbieter von Sicherheitslösungen dringend notwendig, nicht mehr nur die physischen Infrastrukturen ihrer Kunden zu schützen, sondern auch die virtuellen, mobilen und cloudbasierten Umgebungen.

Wir haben zu diesem Zweck eine verbesserte globale Engine für die Erfassung von Bedrohungsdaten entwickelt. Durch die Ausweitung und Vergrößerung des Smart Protection Network wird das Sammeln von Bedrohungsdaten an noch mehr Orten möglich, was für die Entwicklung effizienter Maßnahmen gegen neue Bedrohungen unabdingbar ist.

ES GEHT UM DIE DREI VS - VOLUMEN, VARIANZ UND VERARBEITUNGSGESCHWINDIGKEIT

In den Bedrohungsumgebungen von heute müssen die 3 Vs für große Datenmengen berücksichtigt werden: **Volumen, Varianz und Verarbeitungsgeschwindigkeit**. Diese drei Aspekte nehmen unaufhörlich und mit großer Geschwindigkeit zu, was auf Seiten der Anbieter von Sicherheitslösungen zu einem veränderten Umgang mit Bedrohungen geführt hat. Trend Micro sammelt über ein globales Netzwerk von Sensoren und über seine Kunden gewaltige Mengen an bedrohungsspezifischen Daten und wendet dann speziell für große Datenmengen ausgelegte Analysen an, um neue Bedrohungen zu erkennen, in Beziehung zu setzen und zu untersuchen. Dadurch entsteht ein Pool mit wertvollen Bedrohungsdaten, die wir für die unmittelbare Bereitstellung wirkungsvoller Schutzmaßnahmen über unsere bewährte Cloud-Infrastruktur nutzen.

Die Erkenntnisse fließen in alle Trend Micro Produkte und Services ein, z. B. in mobile Lösungen sowie in Endpunkt-, Server-, Netzwerk-, Messaging-, Gateway- und SaaS-Lösungen für Endverbraucher und Unternehmen jeder Größe. 48 der 50 weltweit führenden Unternehmen vertrauen heute auf die Erfassungs-, Erkennungs- und Schutzfunktionen des Smart Protection Network von Trend Micro und können sich sicher sein, dass Volumen, Varianz und Verarbeitungsgeschwindigkeit der Bedrohungsdaten wirksam und effizient verwaltet werden.

FUNKTIONSWEISE

Das Smart Protection Network lässt sich in drei Hauptaspekte unterteilen: Erfassen, Erkennen und Schützen.

ERFASSEN GROSSER DATENVOLUMEN

Das Smart Protection Network sammelt jeden Tag mehr als 6 Terabyte an Bedrohungsdaten aus der ganzen Welt, um einen Einblick in die verschiedenen Bedrohungsarten zu erlangen. Die Bedrohungsdaten werden kontinuierlich durch ein globales Netzwerk aus Honeypots, Einsendungen, Feedback-Schleifen, Web-Crawling-Technologien, Kunden, Partnern und der TrendLabs Bedrohungsforschung erfasst.

Diese Daten spiegeln die immer größere Bandbreite an Bedrohungsvektoren wider: URLs, IPs, Domänen, Dateien, Exploits, Netzwerkverkehr, Command & Control, Bedrohungsakteure, Threat-Toolkits und -Techniken und mobile Apps, um nur einige zu nennen. Die besondere Herausforderung für Anbieter von Sicherheitslösungen besteht in dem unaufhörlichen Datenstrom. Sie benötigen eine verlässliche Infrastruktur, um die ständig steigenden Mengen an Bedrohungsdaten zu bewältigen.

Dreißig Millionen neuer Angriffe werden jedes Jahr verzeichnet. Das Smart Protection Network ist darauf ausgelegt, in den riesigen Datenmengen die Daten ausfindig zu machen, die beim Erkennen dieser Angriffe helfen.



In Zahlen

Jede Sekunde:

- Cyberkriminelle lösen eine neue Bedrohung aus

Jedes Jahr:

- 30 Millionen neue Angriffe

Jeden Tag, durch das Trend Micro Smart Protection Network:

- Herstellen von Beziehungen zwischen über 16 Milliarden URLs, E-Mails und Dateiabfragen
- Analysieren von mehr als 6 Terabyte Bedrohungsdaten
- Erkennen und Blockieren von mehr als 200 Millionen Bedrohungen
- Mehr als 1.000 Sicherheitsexperten kümmern sich um die Überwachung und Abwehr von Bedrohungen.

ERKENNEN DER VARIANZ AN DATEN

Als wir vor etwa sieben Jahren mit dem Aufbau des Smart Protection Network begannen, waren wir Pioniere im Bereich der Analyse großer Datenmengen zur Erfassung von Bedrohungsdaten. Inzwischen hosten wir Tausende von Ereignis-Feeds, streamen Milliarden von Ereignissen in unseren Rechenzentren und sind zu Experten bei der Auswertung der Vielzahl an Bedrohungen und Angriffen geworden.

Wir setzen z. B. angepasste Werkzeuge ein, um die kritischen Beziehungen zwischen den Komponenten eines Angriffs aufzudecken und das Verhalten von Cyberkriminellen und der von ihnen verwendeten Umgebungen modellhaft nachzuvollziehen, sodass ein Angriff schnell von einem harmlosen Phänomen unterschieden werden kann. Die mit diesen Werkzeugen erstellten Modelle helfen uns beim schnellen Aufspüren neuer Bedrohungen in den Datenströmen mithilfe von verhaltensbasierten Erkennungsmethoden. Durch die Verknüpfung globaler Bedrohungsdaten für viele Bedrohungsvektoren bieten wir Schutz vor den vielfältigen Angriffen von heute.

SCHUTZ DURCH EINE HOHE VERARBEITUNGSGESCHWINDIGKEIT

Im Schnellfeuer der Angriffe kommt dem Tempo der Abwehr eine entscheidende Rolle zu. Über unsere bewährte Cloud-Infrastruktur können wir die erfassten Informationen zu Bedrohungen schnell an physische, virtuelle, cloudbasierte und mobile Umgebungen weitergeben, um alle Daten unabhängig vom Speicherort zu schützen. In unabhängigen Tests werden uns immer wieder kurze Reaktionszeiten bei der Abwehr von Angriffen bescheinigt.

Da Bedrohungsdaten in der Cloud statt auf einzelnen Computern verarbeitet werden, schonen wir die Systemressourcen und benötigen keine zeitaufwändigen Signatur-Downloads. Höhere Leistung und weniger Wartungsaufwand senken gleichzeitig die Betriebskosten.

VERFÜGBARKEIT

Das Trend Micro Smart Protection Network stellt allen Trend Micro Produkten und Services globale Bedrohungsdaten bereit und geht in die Kosten dieser Lösungen ein. Es bietet eine umfassende, beispiellose Unterstützung für Privatanwender, kleine, mittelständische und große Unternehmen sowie Partner in Form von Lösungen für mobile Geräte, Endpunkte, Server (physisch und virtuell), Netzwerke, Messaging, Gateways und Cloud-Plattformen.

Für Unternehmen mit begrenzter Bandbreite oder strengen Datenschutzrichtlinien bieten wir den Smart Protection Server an, bei dem Kommunikation und Abfragen im lokalen Netzwerk verbleiben.

Großen Unternehmen, Regierungsbehörden und anderen speziellen Partnern stehen die neuen Trend Micro Threat Intelligence Services zur Verfügung. Diese Services ermöglichen Unternehmen den direkten Zugriff auf den aufschlussreichen Bedrohungsdatenpool des Smart Protection Network, sodass sie ihre Sicherheitsinfrastruktur noch besser gegen Datenschutzverletzungen oder andere potenzielle Bedrohungen schützen können.

Weitere Informationen erhalten Sie bei Ihrem Trend Micro Ansprechpartner oder Channel-Partner, oder Sie besuchen folgende Website: <http://www.trendmicro.de/technologie-innovationen/technologie/smart-protection-network/>

Vorteile des globalen Bedrohungsdatenpools des Smart Protection Network

- Erfassung einer großen Menge an Bedrohungsdaten über ein robustes, globales Sensornetz, um Kunden vor den zahlreichen und vielfältigen Bedrohungen von heute zu schützen, wie z. B. mobile und gezielte Angriffe
- schnelle Erkennung neuer Bedrohungen durch fein abgestimmte, benutzerdefinierte Data-Mining-Tools, die die sekundlich entstehenden riesigen Datenmengen durchforsten
- Schutz durch eine bewährte cloud-basierte Infrastruktur, die neue Bedrohungen schnellstmöglich abwehrt, um die mit einem Angriff verknüpften Risiken zu minimieren



Securing Your Journey to the Cloud

© 2012 Trend Micro, Incorporated. Alle Rechte vorbehalten. Trend Micro, das Trend Micro T-Ball-Logo und Smart Protection Network sind Marken oder eingetragene Marken von Trend Micro Incorporated. Alle anderen Firmen- bzw. Produktnamen sind Marken oder eingetragene Marken ihrer jeweiligen Eigentümer. Die in diesem Dokument enthaltenen Informationen können sich ohne vorherige Ankündigung ändern. [DSOI_SPN_120716DE]