

## Seculert: Advanced Threat Protection

### Eine umfassende und zukunftsweisende Plattform zum Schutz vor modernen Angriffen

Seculert bietet Cloud-basierte Lösungen an, die Organisationen vor moderner Schadsoftware (Malware) einschließlich APTs (Advanced Persistent Threats= komplexe, andauernde, zielgerichtete und effektive Angriffe auf kritische IT-Infrastrukturen und vertrauliche Daten von Behörden, Groß- und Mittelstandsunternehmen) schützen können.

Seculert nutzt die Leistungsfähigkeit der Cloud-Dienste, um die Unternehmen vor den sich ständig ändernden Bedrohungslandschaften zu schützen. Mit diesen kostengünstigen Lösungen lassen sich komplexe Malware Angriffe erfassen, stoppen und beseitigen. Seculert vereint dabei mehrere Schlüsselerkennungs- und Schutz-Technologien in einer einfach und bequem zu verwaltenden Cloud-basierten Anwendung, die bereits pro-aktiv neue Bedrohungen identifizieren kann.

### Features:

- **Botnet-Überwachung** zur Erfassung von noch nicht identifizierten, unbekanntem Bedrohungen, die bereits Mitarbeiter, Partner und Kunden des Unternehmens über interne oder externe Wege angegriffen haben, aber von ihrer aktuellen Perimeter-Security nicht erkannt wurden.
- **Automatisierte Traffic-Logfile Analyse** zur Überprüfung von verdächtigem Dateicode, der bereits innerhalb der Organisation identifiziert wurde, oder zur Blockade von potentiellen Botnet-Infizierungsversuchen.
- **Integration von Seculert via API** mit vorhandenen Perimeter-Security Einrichtungen, um identifizierte Bedrohungen automatisch stoppen zu können.
- **Big Data Analyse** zur Überprüfung von Zehntausend Malware-Profilen pro Tag und Überwachung des Datenverkehrs und der Kundenprotokolle im Petabyte-Bereich, um mögliche APTs zu erkennen.
- **Machine Learning Technologie** zur Identifikation unbekannter Malware über verhaltensbasierte Methoden, um mit Volumen- und Änderungsraten der Malwarevarianten mithalten zu können.
- **Intuitives Dashboard** zur sofortigen Information bei erkannten Bedrohungen.
- **Volle Erfassung** aller Remote- und Mobile-Nutzer inkl. aller BYODs an allen Endpunkten.
- **Kostengünstiger Cloud-Service** bedeutet: keine Installation, schnelle Ergebnisse und geringer TCO (Gesamtbetriebskosten)

### Funktionsweise

Seculert liefert die erste Cloud-basierte Lösung, die einen sofortigen Schutz vor moderner Schadsoftware und APTs bietet. Ab dem Zeitpunkt der Aktivierung identifiziert Seculert bestehende Infektionen und unbekanntem Malware, sowohl innerhalb als auch außerhalb Ihres internen Netzwerks, sowie in angebundenen Standorten und mobilen Geräten. Mit der patentierten Botnet-Überwachung, der Elastic Sandbox-Technologie und der Big Data Analyse, nutzt Seculert die volle Leistungsfähigkeit der heutigen Cloud, um moderne Bedrohungen bekämpfen zu können.

## **Botnet-Überwachung**

Seculert einzigartige Botnet-Abhörtechnik sucht sowohl innerhalb als auch außerhalb Ihres internen Netzwerks nach möglichen Malware-Infektionen Ihrer Computer. Dabei agiert Seculert als sog. Doppelagent, der einerseits die Botnet-Kommunikation beobachtet und andererseits kompromittierte Systeme aufspürt.

## **Elastic Sandbox**

Die Elastic Sandbox untersucht und profiliert bereits gefundene oder verdächtige Malware im Unternehmen. Dabei simuliert Seculert, unabhängig von Zeit und Raum, verschiedene Umgebungsarten, einschließlich geografische Regionen und unterschiedliche Betriebssysteme, um dabei das Verhalten der Malware zu beobachten.

## **Automatische Big Data Traffic-Protokoll-Analyse**

Durch das eingehende Fachwissen von Seculert über fortgeschrittene Lernalgorithmen bei Maschinen, konnte eine sehr robuste und performante Big Data Protokollanalyse entwickelt werden. Seculert untersucht täglich Terabytes an Log-Dateien, um das Vorhandensein von Malware auf einem Netzwerk erkennen zu können.

## **Application Programming Interface (API)**

Seculert arbeitet nahtlos mit Ihrer bestehenden Sicherheitslösung über ein einfaches API zusammen. Dadurch können sie erkannte Malware sofort automatisch blockieren. Durch die Ergänzung Ihrer vorhandenen Sicherheitseinrichtungen mit dieser Lösung, verwandelt Seculert Ihre heutige Netzwerksicherheit zu einer leistungsfähigen und zukunftsweisenden Sicherheitsplattform zum Schutz gegen moderne Bedrohungen und Angriffe.

**Weitere Informationen finden Sie unter**

<http://info.seculert.com/apt-detection-seculert-netuse-lp>