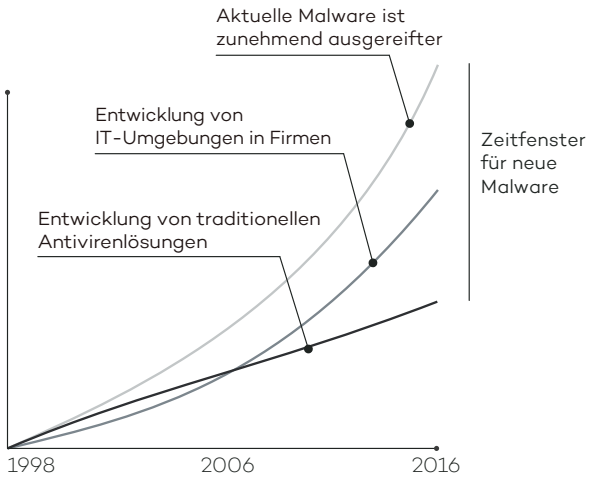
Adaptive Defense
Individueller Managed Security Service

panda

WIR SCHLIESSEN DIE LÜCKE IN DER MALWARE-ERKENNUNG

Die IT-Sicherheitslandschaft hat sich hinsichtlich des Umfangs und der Ausgereiftheit der Malware grundlegend verändert. Die Anzahl der im Umlauf befindlichen Viren steigt kontinuierlich exponentiell an. Neue Techniken, mittels derer Malware die Schutzmaßnahmen umgehen und sich verstecken kann, ermöglichen es dem Schadcode, über lange Zeit in Firmennetzwerken unentdeckt zu bleiben.



Gleichzeitig sind die IT-Umgebungen viel komplexer geworden, was ihre Verwaltung schwieriger und die Systeme anfälliger macht.

Traditionelle Antivirenlösungen halten nicht Schritt mit der Realität. Ihre lineare Entwicklung nutzt weiterhin veraltete Erkennungstechniken, die auf Signaturdateien und heuristischen Algorithmen basieren. Dies bedeutet, dass die Ergebnisse ungenau sein können. Die Malware kann so unter Umständen unerkannt bleiben oder es gibt False Positives.

Diese Diskrepanz hat zu dem geführt, was wir das ‚**Zeitfenster für neue Malware**' nennen: die Zeitspanne zwischen dem Auftauchen einer neuen Bedrohung und der Entwicklung eines Gegenmittels durch die Sicherheitsunternehmen. Diese immer größer werdende Lücke wird von Hackern ausgenutzt, um Viren, Ransomware, Trojaner und andere Arten von Malware in Firmennetzwerke einzuschleusen. Solche zunehmend verbreiteten Bedrohungen können beispielsweise vertrauliche Dokumente verschlüsseln, um „Lösegeld" zu verlangen, oder sensible Daten zum Zweck der Industriespionage stehlen.

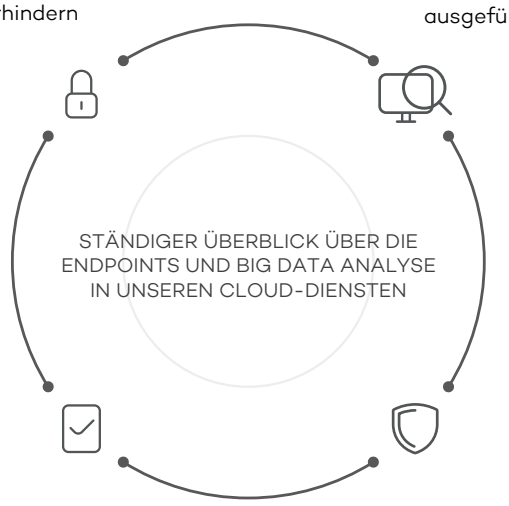
Regierungen, Banken und andere große Unternehmen leiden stark unter den Angriffen, die von traditionellen Antivirenlösungen einfach nicht rechtzeitig entdeckt werden. Unsere Forschungsabteilung hat Millionen von Viren sowie die besten auf dem Markt erhältlichen Antivirenprodukte analysiert. Dabei kam heraus, dass 18 Prozent der Malware in den ersten 24 Stunden nach der Infektion unentdeckt bleibt. Sogar nach drei Monaten sind diese herkömmlichen Lösungen immer noch nicht in der Lage, zwei Prozent der Malware zu erkennen.

Die Lösung für dieses Problem bietet **Adaptive Defense**: ein Panda Security Service, der jede laufende Anwendung in Ihrem Unternehmen ganz genau klassifizieren kann und nur vertrauenswürdige Programme zulässt.

Um dies zu erreichen, haben wir intensiv an einem **neuen Sicherheitsmodell** gearbeitet, das auf drei Prinzipien basiert: ständige Überwachung aller Anwendungen auf Firmencomputern und Servern, automatische Klassifizierung mit Hilfe unserer Big-Data-Plattform in der Cloud und die Analyse nicht automatisch klassifizierter Anwendungen durch unsere Experten.

PRÄVENTION
Blockiert Anwendungen und isoliert Systeme, um zukünftige Angriffe zu verhindern

TRANSPARENZ
Nachverfolgbarkeit und Transparenz jeder Aktion, die von laufenden Anwendungen ausgeführt wird



REAKTION
Forensische Informationen für die gründliche Analyse jedes Angriffsversuchs

ERKENNUNG
Gezielte und Zero-Day Angriffe werden in Echtzeit und ohne Signaturdateien blockiert

GARANTIERTE SICHERHEIT FÜR ALLE LAUFENDEN ANWENDUNGEN

UMFASSENDER UND STABILER SCHUTZ

Panda **Adaptive Defense** bietet zwei Betriebsmodi:

• **Hardening-Modus:** Es dürfen alle Anwendungen laufen, die als Goodware klassifiziert wurden, sowie die Programme, die noch durch Panda Security und die automatisierten Systeme analysiert werden müssen. Jedoch werden alle unbekannten Programme, die aus dem Internet heruntergeladen wurden, blockiert.

• **Lock-Modus:** Es darf ausschließlich Goodware ausgeführt werden. Dies ist die beste Schutzform für Unternehmen, die einen „Nullrisiko"-Ansatz bei der Sicherheit haben.

FORENSISCHE INFORMATIONEN

• **Übersichten über ausgeführte Aktionen** geben einen klaren Überblick über alle Ereignisse, die von Malware verursacht wurden.

• **Heatmaps** geben visuelle Informationen über die geografische Herkunft der Malware-Verbindungen, erstellte Dateien und vieles mehr.

• Software mit bekannten Schwachstellen, die im Netzwerk installiert wurde, wird lokalisiert.

KOMPATIBEL MIT TRADITIONELLEN ANTIVIRENLÖSUNGEN

Adaptive Defense kann gleichzeitig mit traditionellen Antivirenlösungen installiert sein. Es übernimmt dann die Rolle eines **Unternehmenstools**, das **alle Arten von Malware blockiert,** die von herkömmlichen Lösungen nicht entdeckt werden, **einschließlich gezielter und Zero-Day Angriffe**.

SCHUTZ FÜR GEFÄHRDETE BETRIEBSSYSTEME UND ANWENDUNGEN

Systeme wie Windows XP, die nicht länger durch Entwickler unterstützt werden und deshalb ungepatcht und ungeschützt sind, fallen Zero-Day-Angriffen und neuen Bedrohungen leicht zum Opfer. Zudem werden Schwachstellen in Anwendungen wie Java, Adobe, Microsoft Office sowie in Browsern von 90 Prozent der Malware ausgenutzt.

Adaptive Defense bietet ein Schutzmodul für solche Schwachstellen. Dieses nutzt Kontext- und Verhaltensregeln um sicherzustellen, dass Unternehmen in einer sicheren Umgebung arbeiten können, auch wenn ihre Systeme nicht mehr gepatcht werden.

STÄNDIGE INFORMATIONEN ÜBER DEN NETZWERKSTATUS

• Sofortige Ausgabe von Warnmeldungen, wenn Malware im Netzwerk identifiziert wird. Dazu gibt es einen umfassenden Bericht mit Informationen zum Ort, den infizierten Computern und den von der Malware ausgeführten Aktionen.

• Automatisierte Berichte über die täglichen Service-Aktivitäten werden per E-Mail versandt.

INTEGRATION IN SIEM (Sicherheitsinformations- und Ereignismanagement)

Adaptive Defense integriert sich in SIEM-Lösungen, um detaillierte Daten über die Aktivitäten aller auf dem System laufenden Anwendungen zu liefern.

Für Kunden ohne SIEM, bietet **Adaptive Defense** optional ein eigenes System zum Speichern und Verwalten von Sicherheitsereignissen, um alle in Echtzeit gesammelten Informationen zu analysieren.

100 % MANAGED SERVICE

Es sind keine Investitionen in technisches Personal erforderlich, das sich mit Quarantäne oder verdächtigen Dateien beschäftigt oder infizierte Computer desinfiziert und wiederherstellen. **Adaptive Defense** klassifiziert alle Anwendungen in unseren Big-Data-Umgebungen automatisch unter der ständigen Aufsicht der Panda Labs Experten.

TECHNISCHE ANFORDERUNGEN

Webkonsole

- Internetverbindung
- Internet Explorer 7.0 oder höher
- Firefox 3.0 oder höher
- Google Chrome 2.0 oder höher

Agent

- Betriebssysteme (Workstations): Windows XP SP2 und später, Vista, Windows 7, 8 & 8.1
- Betriebssysteme (Server): Windows Server 2003, Windows Server 2008, Windows Server 2012
- Internetverbindung (direkt oder über Proxy)