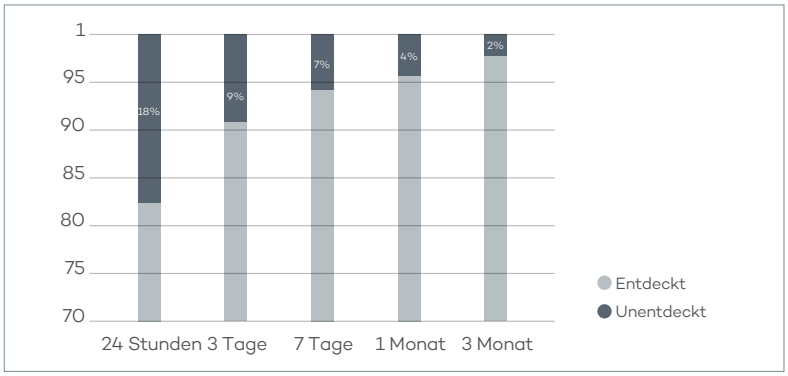
Adaptive Defense 360 Leitfaden

Antworten finden, Probleme lösen

Klassische, auf Signaturdateien basierende Antivirenprogramme können nicht zuverlässig vor Zero-Day-Angriffen, APTs oder Cryptolockern schützen.

Wir haben die passende Antwort für diese Angriffe! Der Schlüssel dazu ist die lückenlose Überwachung und Klassifizierung aller laufenden Prozesse auf den Endpoints.

Was eine signaturbasierte Antimalware Lösung nicht entdeckt



18%

der neuen Malware bleiben in den ersten 24 Stunden unentdeckt.

Nach drei Monaten sind noch immer 2 Prozent nicht entdeckt.

Wie funktioniert Adaptive Defense 360?

1 Ständige Überwachung aller Ereignisse auf den Endpoints

2 Analyse in Pandas BIG-DATA-Plattform Collective Intelligence inklusive vollständiger Klassifizierung aller ausführbaren Dateien

3 Klassifikation der Ereignisse, um deren Ausführung zu blockieren oder zu erlauben

Features von Adaptive Defense 360

ERKENNUNG UND REAKTION

- Ständige Analyse aller laufenden Anwendungen
- Zugriffskontrolle auf Anwendungsinformationen und Ereignisse, die im Netzwerk laufen
- Schutz gefährdeter Software
- Ausführliche forensische Informationen: Betroffenes Gerät / Zeitpunkt der Infektion, Route / Aktivitäten und Kommunikation der Malware

SCHUTZ

- Antivirus und Antimalware
- Schutz von Exchange Mailservern
- Webfilter (nach Kategorien)
- Firewall
- Device Control

Wie Adaptive Defense funktioniert

INSTALLATION

- Installation eines schlanken Agenten (MSI-Datei oder Installation durch Active Directory)
- Minimaler Ressourcenverbrauch auf den Endpoints (~ 5% CPU Auslastung)
- Selbstverwaltende Konsole

SCHUTZ

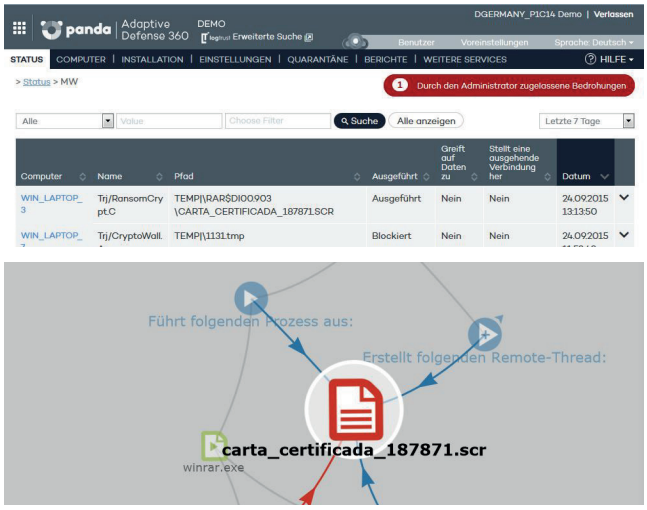
- Blockiert die Ausführung nicht klassifizierter Programme
- Zeigt die Schwachstellen von Software in Ihrem IT-Netzwerk. Webfilter (nach Kategorien)
- Registriert PUPs (Potenziell unerwünschte Programme) wie zum Beispiel Toolbars
- Schutz vor APTs (Fortgeschrittene andauernde Bedrohungen)

VERSCHIEDENE SPERRFUNKTIONEN

Audit:
Die Audit-Funktion analysiert das gesamte Netzwerk – sie sieht alles – sie blockiert nichts

Deep Hardening:
Die Deep-Hardening-Funktion sieht alles – sie blockiert das interne Netzwerk nicht – sondern blockiert externe Bedrohungen (z. B. schadhafte E-Mail- und Webdownloads)

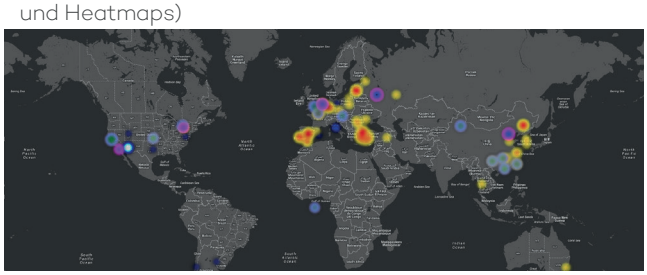
Extended:
Die Extended-Funktion blockiert alles was nicht als Goodware klassifiziert wurde – sie bietet vollständige Sicherheit



Grafische Darstellung der Malware-Aktivität

REPORTING

- Tägliche Berichte über die auf dem System ausgeführten Aktionen, sofern gewünscht
- Sofortiger Bericht über die Ortung von Malware inklusive ausführliche forensischer Informationen
- Berichte über alle gespeicherten Systemprotokolle und die Vernetzung aller Daten. (Voronoi-Diagramme und Heatmaps)



Heatmap zur Ortung der Malware

Adaptive Defense 360 in Zahlen

1 **Mehr als 8 Millionen Anwendungen** wurden in Panda Securitys BIG- DATA-Plattform klassifiziert.

2 **Unsere BIG-DATA-Plattform wird von Millionen Endpoints mit Informationen versorgt.** Pandas Collective Intelligence sammelt seit 25 Jahren Informationen.

3 In **100 Prozent der überprüften Umgebungen** wurde Malware entdeckt, unabhängig von den eingesetzten Schutzmechanismen.

4 **Mit einer Genauigkeit** von nahezu 100 Prozent (99,9991 %) **werden alle ausführbaren Dateien automatisch klassifiziert.**

Telefon:
02065 – 961 200

E-Mail:
vertrieb@de.pandasecurity.com

Web:
pandasecurity.com