Einzelprodukttest

Panda Adaptive Defense 360

Dezember 2016

Letzte Überarbeitung: 12. Januar 2017

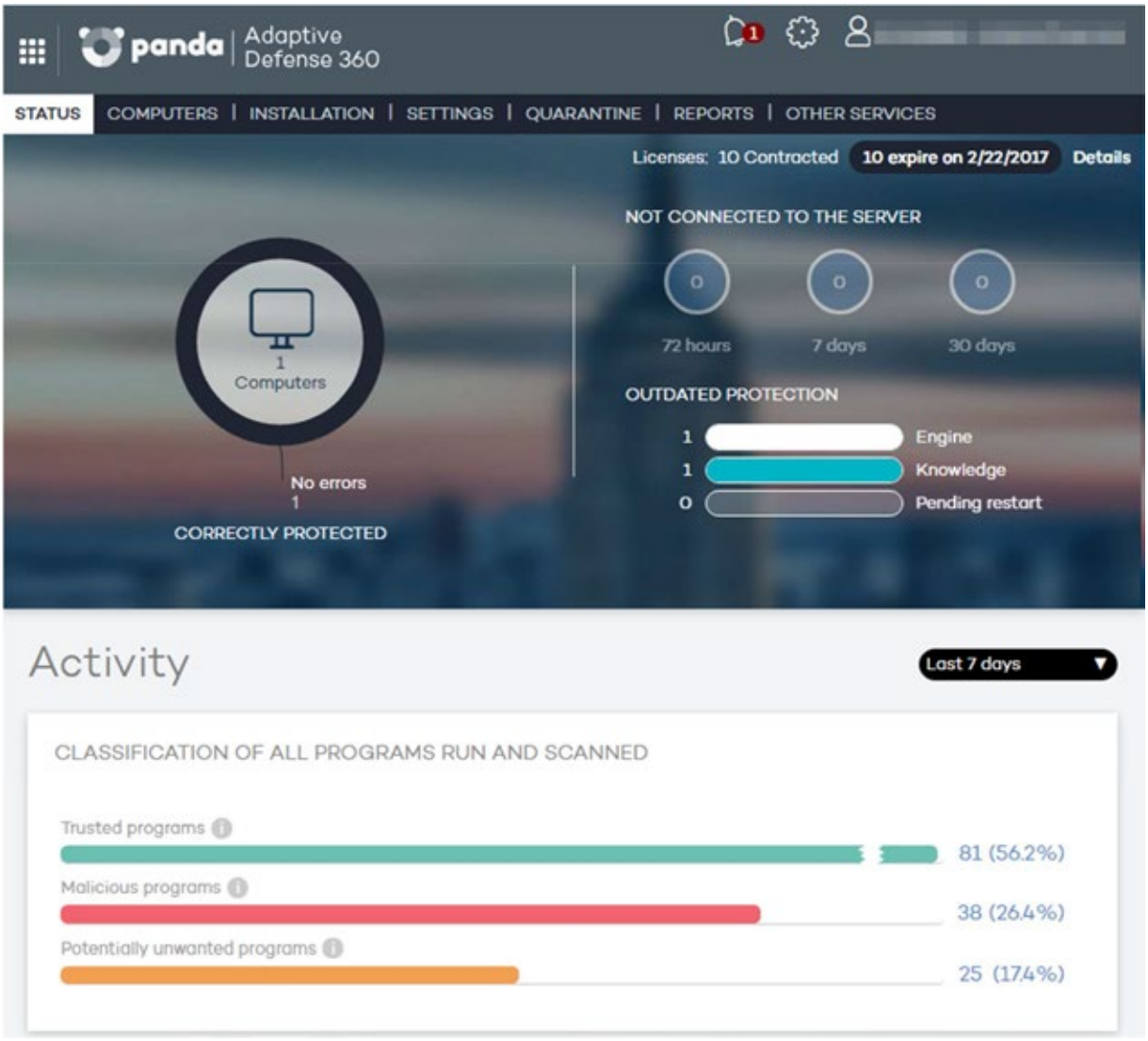
www.av-comparatives.org

Im Auftrag von Panda Security

Panda Adaptive Defense 360

Einführung

Dieser Bericht wurde von Panda Security in Auftrag gegeben.



Überblick

Überprüfte Produktversion

Adaptive Defense 360 Version 2.3.5
Windows Protection Version 7.60

Unterstützte Betriebssysteme

Windows XP SP2 und später, Windows Vista, Windows 7, 8, 8.1, 10, Windows Server 2003, 2008, 2012.
Teilweise unterstützt: Linux, Mac OS X und Android

Über das Produkt

Panda Adaptive Defense 360 bietet eine cloud-basierte, zentral gemanagte Endpoint-Security-Plattform. Sie kombiniert klassische Sicherheitsfeatures wie zum Beispiel Anti-Malware, Firewall sowie Web- und E-Mail-Filter mit einer Kombination aus Endpoint-Schutz der nächsten Generation und einer Cloud-Plattform, die einen EDR-Service bietet (Endpoint Detection and Response). Die EDR-Komponente überwacht kontinuierlich alle auf den Geräten laufenden Anwendungen innerhalb des Firmennetzwerkes und hat das Ziel, diese Geräte vor bekannten und unbekannten Bedrohungen zu schützen. Dazu nutzt EDR die automatische Klassifizierung aller laufenden Prozesse, basierend auf den aufgezeichneten Ereignissen und unter Verwendung von maschinellen Lernverfahren in einer Big-Data-Umgebung. Anwendungen, die nicht automatisch klassifiziert werden können, werden von Pandas Anti-Malware-Experten analysiert.

Die Kombination dieser Elemente stellt das Wesen des Cloud Services und der Plattform von Panda Adaptive Defense dar.

Produktseite auf der Webseite des Anbieters

http://www.pandasecurity.com/germany/intelligence-platform/solutions.htm

Beschreibung des Produktes

Panda Adaptive Defense 360 ist eine Kombination aus einer Endpoint Protection Platform (EPP), die „traditionelle“ Antivirensoftware enthält, und einer Verbindung aus einem Endpoint-Schutz der nächsten Generation und einer Cloud-Plattform, die Endpoint Detection und Response (EDR) bietet.

Die cloud-basierte Konsole gibt einen Überblick über den Status des Netzwerkes sowie aller einzelnen Endpoints und Server usw., auf denen die Lösung installiert ist.

Während EPP mithilfe von bestehenden Methoden, wie beispielsweise Signaturen und Verhaltenserkennung, Malware erkennt und blockiert, überwacht und klassifiziert der Endpoint-Schutz der nächsten Generation 100 Prozent der Prozesse, die auf den Netzwerkcomputern laufen, und generiert forensische Daten. Diese können genutzt werden, um die eigentliche Ursache, die betroffenen Geräte und die von der Malware ausgeführten Aktionen zu bestimmen, zum Beispiel: Wie die Bedrohung begonnen hat; welche Prozesse verursacht wurden und wann; geöffnete Verbindungen usw. All diese Informationen sind über die Konsole in Echtzeit verfügbar.

Alle Prozesse werden kategorisiert als entweder vertrauenswürdige Programme, schädliche Programme oder potenziell unerwünschte Programme (dies ist auf derselben Seite zu sehen, unter „Aktivitäten“). Die Listen der schädlichen und potenziell unerwünschten Programme zeigen dem Administrator, ob solche Programme erfolgreich ausgeführt wurden, ob sie externe Verbindungen aufgebaut oder auf Daten zugegriffen haben. Da diese Lösung alle ausgeführten Prozesse klassifiziert, kann sie jede Malware registrieren. Auch wenn das Produkt einen schädlichen Prozess fälschlicherweise als vertrauenswürdig klassifiziert, wird er als Malware klassifiziert, sobald aufgrund der Echtzeitüberwachung schädliche Aktivitäten erkannt werden oder verdächtiges Verhalten festgestellt wird. Wenn die Malware bereits im System war, bevor Adaptive Defense 360 installiert wurde, erkennt das Produkt die Malware, wenn sie aktiv ist, und liefert Informationen darüber, was sie seit der Installation von Adaptive Defense 360 getan hat. Adaptive Defense 360 hat ein eigenes Advanced Reporting Tool (ART), einen Service, der auf Big Data basiert und totale Transparenz und Einblicke in die Aktivitäten auf den Endpoints, die Prozesse, die Aktivitäten der Anwender sowie den Missbrauch von IT-Ressourcen liefert. Die Lösung hat auch einen SIEM-Connector, um all die Informationen in ein bestehendes SIEM (wie zum Beispiel QRADAR) einzugeben. Da Panda Adaptive Defense 360 ein gemanagter Service ist, kümmern sich Techniker von Panda um Quarantäne, verdächtige Dateien und Desinfektion.

Dokumentation

Über die Web-Management-Konsole des Produktes haben Administratoren Zugriff auf eine umfangreiche Online-Hilfefunktion sowie auf ausführliche Administrations- und Benutzerhandbücher.

Pluspunkte

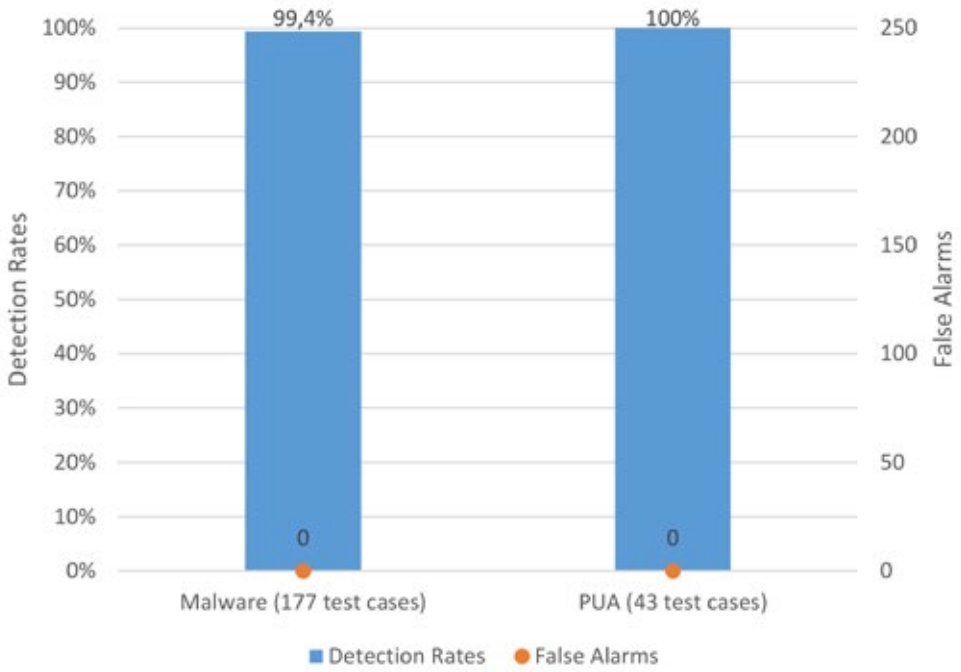
Die Management-Konsole bietet eine gut strukturierte und intuitive Benutzeroberfläche. Die von der Adaptive Defense Plattform gesammelten und angereicherten Ereignisdaten werden übersichtlich dargestellt. Aktivitätsdiagramme bieten eine intuitive Visualisierung der Ereignisse, die während jedes Sicherheitsvorfalls aufgetreten sind.

Wirksamkeitstest

Für große Anlagen empfiehlt Panda, dass Panda Adaptive Defense 360 nach seiner Installation eine Zeit lang im Audit-Modus betrieben werden sollte, sodass Adaptive Defense die normale Nutzung in der Arbeitsumgebung kennenlernen kann.

Für unseren Test nutzten wir dieselbe Methode, die Panda auch bei seinen Kunden anwendet: Der Systemadministrator installiert einen schlanken Adaptive Defense Agenten auf den Servern/ Endpoints des Unternehmens. Das Personal des Unternehmens kann ganz normal an seinen Rechnern weiterarbeiten und so lernt Adaptive Defense das normale Verhalten aller Maschinen kennen, klassifiziert laufende Prozesse usw. Also führten wir „normale“ Arbeiten auf unseren Testgeräten aus (z. B. verschiedene Anwendungen öffnen, Rechner mehrmals neustarten).

Wir haben Panda Adaptive Defense 360 in **220** Musterfällen getestet. Davon waren **177** neue **schädliche Webseiten**, die entweder auf Ransomware, Backdoors, Password-Stealer, Würmer, Viren oder andere Trojaner hindeuteten. Panda Adaptive Defense 360 blockierte alle Bedrohungen bis auf eine (ein Password-Stealer), die später aufgrund ihres schädlichen Verhaltens als Malware identifiziert wurde. Alle **43** potenziell unerwünschten Programme (PUP), die im Set enthalten waren, wurden ebenfalls von Panda Adaptive Defense 360 blockiert. Während des Testzeitraumes wurden **keine Fehlalarme** auf dem Testsystem beobachtet.

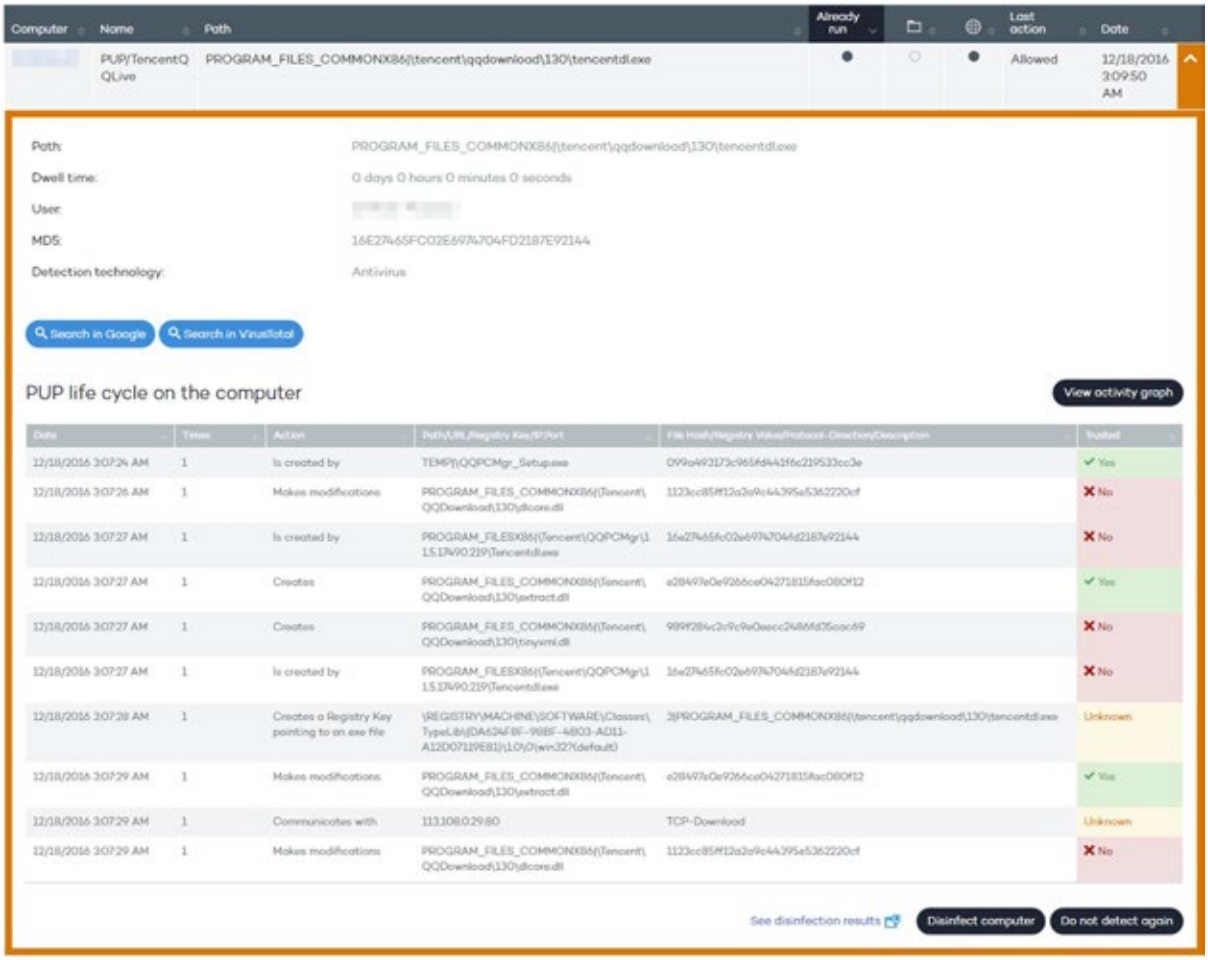


Management-Konsole

Die Web-Management-Konsole öffnet sich auf der Seite Status und gibt einen Überblick über die aufgezeichneten Aktivitäten und Entdeckungen. Die anderen Seiten der Konsole sind über das Menü ganz oben in der Konsole zu erreichen. Aufgrund der Tatsache, dass der Adaptive Defense Service alle laufenden Prozesse klassifiziert, zeigt das Dashboard die Gesamtzahl der guten Software-Anwendungen, die im vergangenen Jahr, Monat, Woche oder Tag ausgeführt wurden, zusammen mit der Gesamtmenge und dem Prozentsatz an Malware und potenziell unerwünschten Programmen, die im Unternehmen entdeckt wurden.

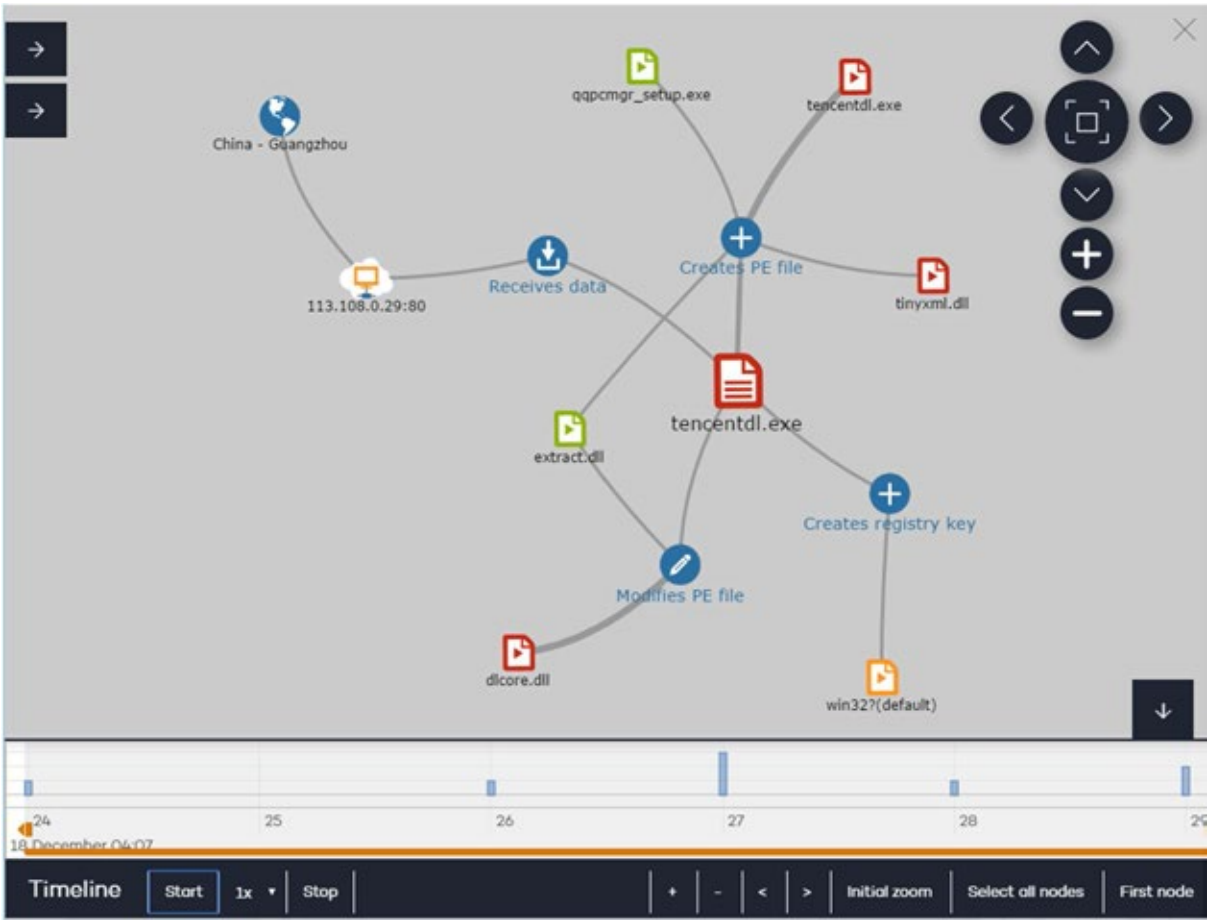
Überwachung des Netzwerkes

Der Bereich Aktivitäten auf der Seite Status gibt einen Überblick über die im Netzwerk verzeichneten Sicherheitsvorfälle. Adaptive Defense 360 zeichnet alle Ereignisse auf, die während des jeweiligen Störfalls aufgetreten sind. Dadurch können Administratoren die automatische Klassifizierung des Systems und den Vorfall als Ganzes nachvollziehen.

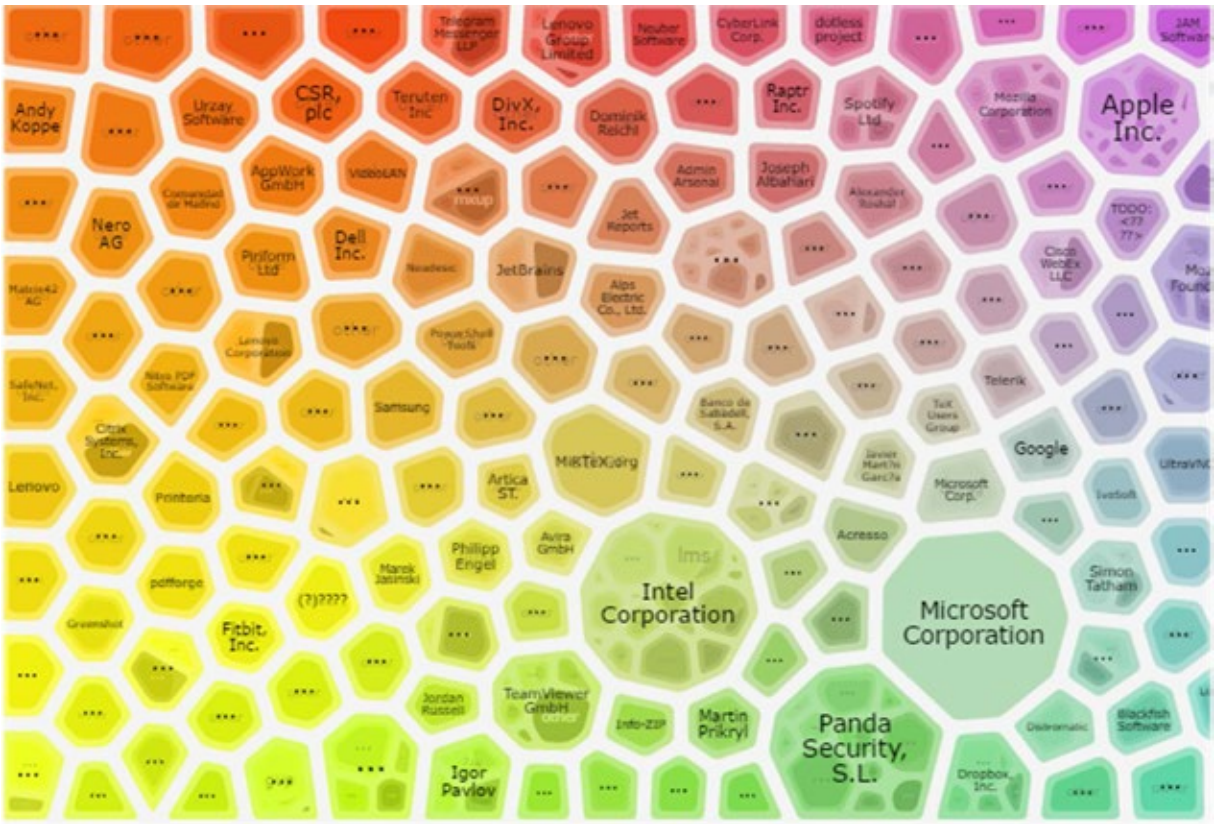


PUP-Erkennungszyklus

Diese Informationen werden zusätzlich durch ein Aktivitätsdiagramm der aufgezeichneten Ereignisse ergänzt. Das Aktivitätsdiagramm veranschaulicht die Beziehung zwischen den verschiedenen Ereignissen und ihren Akteuren während des Vorfalls. Anhand des Diagramms können Administratoren den zeitlichen Verlauf der Ereignisse auf intuitive Art nachvollziehen, indem sie das Diagramm gemäß der Vorfall-Zeitachse animieren.

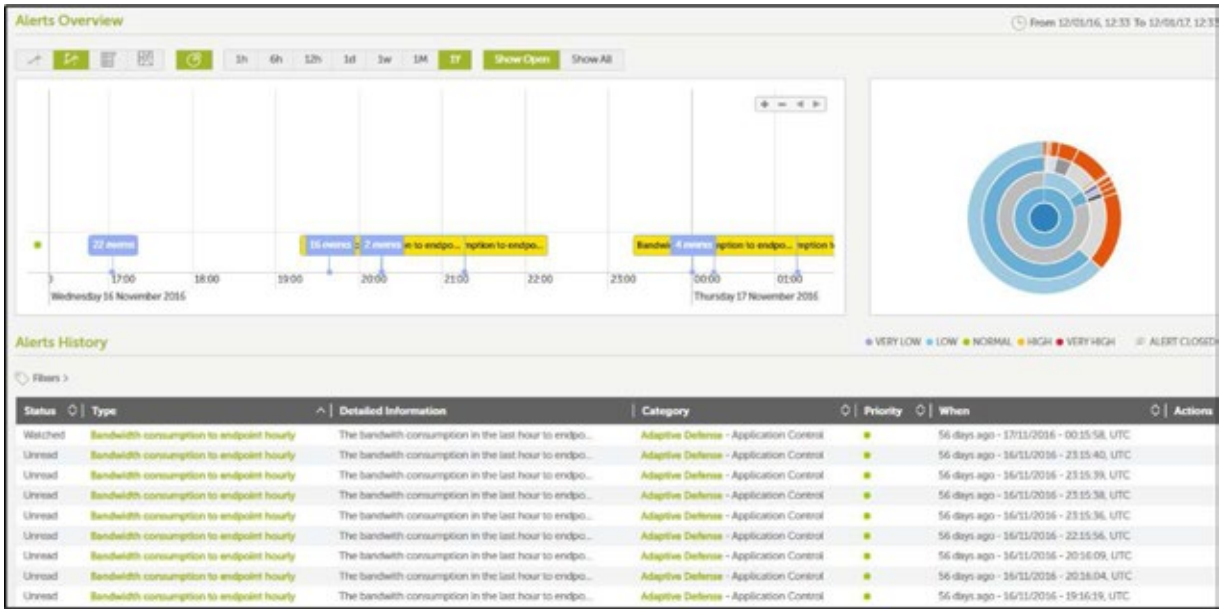


Ereignis-Zeitleiste



Dashboard - Voronoi Grafik

Dashboard - Heat Map



Alarm Übersicht

Copyright und Disclaimer

Weitere Informationen über AV-Comparatives und die Testmethoden finden Sie auf unserer Webseite.

AV-Comparatives (Januar 2017)