Adaptive Defense

CLOSING THE GAP IN MALWARE DETECTION

ERKENNUNGSALGORITHMEN REVOLUTIONIEREN

panda

pandasecurity.com

Kurzbeschreibung

Adaptive Defense ist ein für jeden Kunden individualisierbarer und durch Panda gemanagter Security-Service. Die auf der Panda Collective Intelligence basierende Technologie dient speziell zur Abwehr von Targeted Attacks (Datendiebstahl) und unbekannten Bedrohungen, welche u. a. in hohem Maße Sicherheitslücken in vertrauenswürdigen Programmen ausnutzen. Dabei werden alle Prozesse (PEs) auf den Endpoints kontinuierlich überwacht und klassifiziert. Die forensischen Echtzeitanalysen liefern detaillierte Informationen über alle potenziell unerwünschten und gefährlichen Aktivitäten im Unternehmen.

Aufgrund von sowohl qualitativ als auch quantitativ ständig wachsenden Bedrohungen ist der Einsatz innovativer Technologien beim Schutz sensibler Daten alternativlos.

Kriminelle und Entwickler von Sicherheitslösungen befinden sich in einem permanenten Wettstreit. Cyberkriminelle entwickeln ständig neue Angriffsszenarien, auf welche die Security-Industrie sowohl mit modernen Erkennungstechnologien als auch mit Blacklists antwortet.

Der Aufwand, den Unternehmen heutzutage betreiben müssen, um mit herkömmlichen Schutzlösungen ein kurzzeitig akzeptables Sicherheitsniveau zu erreichen, ist extrem ressourcen- und kostenintensiv. Panda Securitys Adaptive Defense schließt genau diese Lücke in der Malwarebekämpfung. Dieser revolutionäre Ansatz, weg vom Blacklisting bekannter Bedrohungen, gewährleistet für Unternehmensnetzwerke ein permanent hohes Schutzniveau bei minimalem Aufwand.

Panda Securitys innovative Technologie basiert auf drei Prinzipien:

1. Permanente Überwachung aller auf den Endpoints laufenden Prozesse.

2. Kontinuierliche Klassifizierung und Risikobewertung laufender Programme in Echtzeit.

3. Transparenz und Benutzerfreundlichkeit ohne administrativen Aufwand.

Aktuelle Bedrohungslage

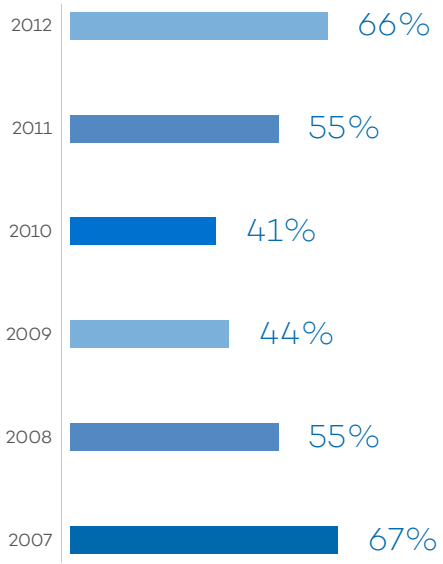
Trotz ständig steigender Investitionen in die IT-Sicherheit (2015 wurden laut Gartner weltweit mehr als 75 Milliarden Dollar in IT-Sicherheitstechnologien investiert) wird der Kampf gegen Cyberkriminalität immer komplexer und aufwändiger.

Groß angelegte Malware-Angriffe sowie bedeutende Enthüllungen über staatlich geförderte Spionageaktivitäten sorgen kontinuierlich dafür, dass das Infektionsrisiko durch Malware, speziell in Unternehmensnetzwerken, bewusster wahrgenommen wird.

Gartner hat die Gefahr erkannt: „Alle Unternehmen sollten jetzt davon ausgehen, dass sie sich in einem Zustand ständiger Gefährdung befinden." Angesichts des allgemeinen Widerwillens von IT-Abteilungen, Daten über Infizierungen und Sicherheitslücken zu veröffentlichen, lässt sich die heutige Situation mit den vergangenen Jahren nur sehr schwer vergleichen.

Niemand möchte Statistiken über seine Ausfallraten preisgeben. Laut des Verizon Data Breach Investigations Reports 2013 blieben 85 Prozent der Angriffe auf Unternehmensnetzwerke für Wochen oder sogar länger unentdeckt. 92 Prozent der Angriffe wurden von den Unternehmen selbst nicht erkannt. Es ist deshalb sehr wahrscheinlich, dass das Gesamtrisiko in der Vergangenheit auf einem ähnlich hohen Niveau war. Wie Donald Rumsfeld einmal sagte: „gibt es Dinge, von denen wir nicht wissen, dass wir sie nicht wissen."

Angriffe, die monatelang unentdeckt blieben, in Prozent



Quelle: Verizon Data Breach Investigations Report 2013.

Die Erkennungslücke

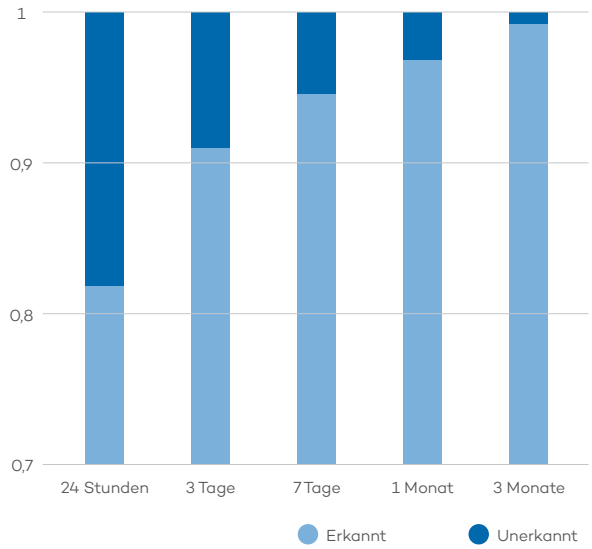
Von Januar bis Juni 2015 führte PandaLabs eine interne Studie durch. Dabei wurden alle täglich gesammelten Malware-Exemplare mit einer großen Anzahl von Antimalware-Produkten getestet.

Das erschreckende Ergebnis dieser Studie: Ein relativ hoher Anteil der veröffentlichten Malware wird nicht rechtzeitig erkannt. Fakt ist, dass auch ein Jahr nach der Entdeckung der Malware fast 1 Prozent der Exemplare immer noch unerkannt ist.

Die Ergebnisse dienen dazu, die Lücke zu veranschaulichen, die bei Produkten besteht, die sich auf Erkennung konzentrieren.

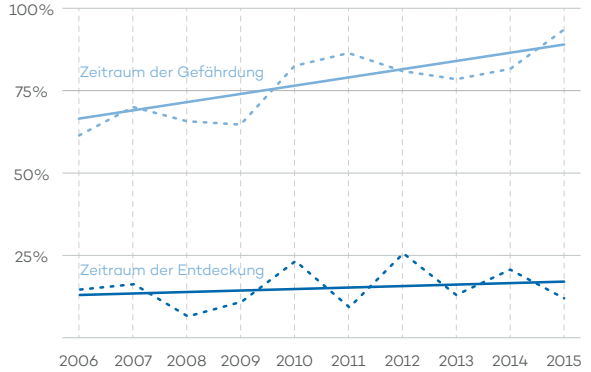
Verizon Data Breach Investigative Report 2015. Die Angreifer werden immer besser beim Eindringen in Systeme. Die Security-Industrie kann die Gefährdung kaum schnell genug entdecken. (Die Lücke wird größer.)

Von der AV-Industrie unerkannte Malware



Grafik. Erkennungslücke bei Antimalware-Produkten.

Prozentsatz der Angriffe, bei denen der Zeitraum der Gefährdung/Entdeckung einige Tage oder weniger betrug



Was ist Adaptive Defense?

Adaptive Defense ist ein Security-Service, der Malware zuverlässig erkennt, indem er alle laufenden Anwendungen automatisch überprüft. Dieser Sicherheitsservice ist speziell für Unternehmenskunden konzipiert. Er besteht aus einer agenten- und cloud-basierten Lösung sowie einer ständigen Backend-Unterstützung durch Analysten des PandaLabs.

Adaptive Defense klassifiziert transparent und mit dem höchsten Grad an Genauigkeit alle ausführbaren Programme (PE-Dateien) auf den Endpoints. Als weitere Basisschicht ermöglicht er ein Härten von Anwendungen, Daten und Betriebssystemen (Behavior Enforcement). So wird sichergestellt, dass häufig genutzte Anwendungen nicht aufgrund von Schwachstellen erfolgreich ausgenutzt werden können und dass auf sensible Bereiche des Betriebssystems nicht abnorm zugegriffen werden kann.

Des Weiteren erfolgt beim Eintreten eines Störfalles eine forensische Untersuchung, um Fragen nach dem Was, Wann, Wer und Wie des Malware-Angriffs detailliert beantworten zu können.

Adaptive Defense bietet zwei Betriebsmodi: Im Hardening-Modus dürfen alle Anwendungen laufen, die als Goodware klassifiziert wurden, sowie die Programme, die noch durch Panda Security und die automatisierten Systeme analysiert werden müssen. Alle unbekannten Programme, die aus dem Internet heruntergeladen wurden, werden jedoch blockiert. Im Lock-Modus darf ausschließlich Goodware ausgeführt werden. Im Rahmen der optional erhältlichen Service-Pakete beinhaltet Adaptive Defense u. a. einen zusätzlichen Dienst zur vollständigen Desinfektion innerhalb des Netzwerkes.

CLOUD-BASIERTE
STÄNDIGE ANALYSE

ENDPOINT-BASIERTE
STÄNDIGE ÜBERWACHUNG

Prinzipien:
Adaptive Defense basiert auf 3 Prinzipien

Ständige Überwachung

Alle Ausführungsereignisse werden überwacht und aufgezeichnet. Dies dient der Frühwarnung, der Nachverfolgbarkeit und der forensischen Störfallanalyse.

Alle Aufzeichnungen sind jederzeit verfügbar und können vollständig durchsucht werden. So können Administratoren leicht erfahren, was die Anwendungen genau tun, wie und von wem sie genutzt werden, welche Verbindungen wann und mit welchen Ländern hergestellt werden usw.

Ständige Klassifizierung laufender Programmdateien

Alle ausführbaren Dateien, die im Speicher laufen, werden mit einer Genauigkeit von nahezu 100 Prozent als Malware oder Goodware klassifiziert. Dazu nutzt Adaptive Defense sowohl lokale als auch cloud-basierte Systeme. Diese gleichen die Dateien mit lokal gesammelten Informationen sowie mit zahlreichen anderen kontextabhängigen Daten aus der Community mithilfe einer Big-Data-Analyse-Engine ab. Bei Bedarf kann auch eine manuelle Klassifizierung erfolgen.

Darüber hinaus müssen sich Programme entsprechend verhalten, um ihre Vertrauenswürdigkeit zu behalten. Die Berechnungen zur Bestimmung des Vertrauenslevels basieren auf der firmeneigenen Clustering-Technologie sowie auf den empirischen Daten aller Dateien (Malware und Goodware), die in der Vergangenheit bereits von Panda klassifiziert wurden. Sobald neue Informationen vorliegen, erfolgt eine Neuberechnung durch eine nachträgliche Analyse aller vorherigen Klassifikationen.

Transparenz/ Komfort

Weder Eingaben von Administratoren noch von Endanwendern (z. B. Erstellen von Whitelists, Konfiguration von Parametern usw.) sind für das Funktionieren des Services erforderlich.

Sobald der Agent von Adaptive Defense installiert wurde, kann er ausführbare Dateien erkennen, analysieren und klassifizieren – sowohl selbstständig als auch in Verbindung mit dem System in der Cloud. Adaptive Defense ist ein von Panda Security angebotener Managed Service, der Administratoren die Arbeit erheblich erleichtert, indem er Routineaufgaben übernimmt. Wenn Sicherheitslösungen von Drittanbietern genutzt werden, müssen Administratoren Warnmeldungen über verdächtige Aktivitäten selbst beurteilen und bearbeiten. Adaptive Defense überprüft jeden Verdacht umfassend und transparent. Administratoren erhalten anschließend Meldungen darüber, welche Anwendungen als Malware klassifiziert wurden.

Mit Adaptive Defense ist es nicht mehr erforderlich, Anwendungen auf eine Whitelist zu setzen oder Ausnahme- und Genehmigungsprozesse einzuführen, da alle ausführbaren Dateien vom System klassifiziert werden.

Hauptvorteile

Wie Adaptive Defense Unternehmen dabei hilft, das Problem eines unzureichenden Schutzes zu lösen.

Schließt die Erkennungslücke, die traditionelle Endpoint-Protection-Produkte haben.

Verkürzt die Zeit, die für die Untersuchung von Sicherheitsvorfällen aufgewendet wird. Alle Warnmeldungen von Adaptive Defense sind bestätigt.

Minimiert die Wiederherstellungskosten im Störfall. Automatisierte Desinfektion.

Beantwortet die Fragen nach dem Was, Wer, Wann und Wie von Sicherheitsvorfällen. Traditionelle Produkte können das nicht.

Reduziert die Verwaltungskosten für die Endpoint-Sicherheit.

Weitere Vorteile von Adaptive Defense

Bietet Echtzeit-Einblick in alle Aktivitäten, die auf den Endpoints stattfinden. So können Administratoren potenziell „riskante“ Ereignisse oder Verletzungen der Richtlinien leicht erkennen.

Erfordert weniger Aufwand als andere Endpoint-Protection-Produkte.

Benötigt keine Management-Infrastruktur.

Vorhandene Sicherheitslösungen müssen nicht deinstalliert werden.

Starker Schutz für virtualisierte Desktop-Umgebungen.

Technologie

Informationsquellen für Adaptive Defense:

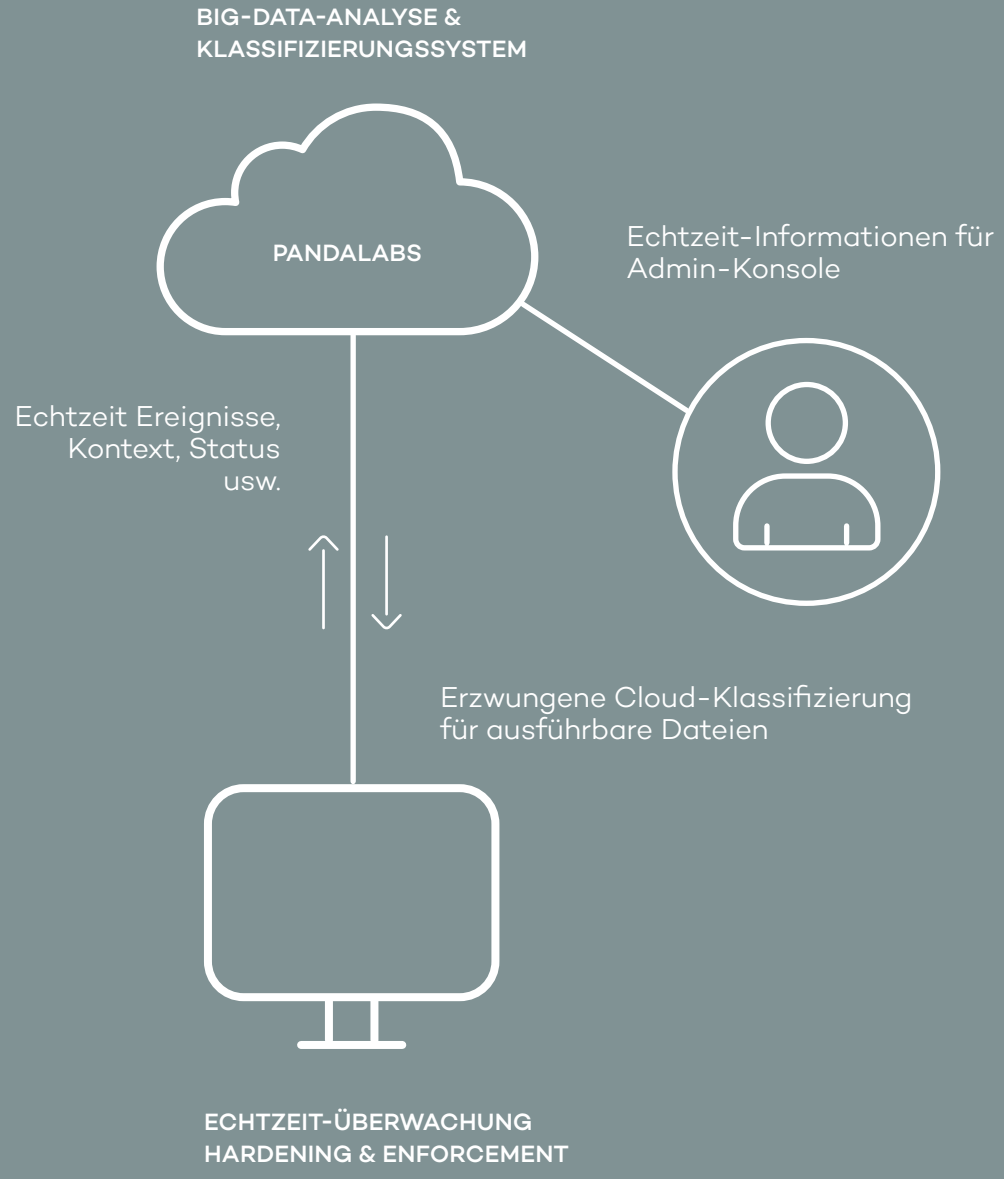
- Bedrohungen – intern (PandaLabs)
- Bedrohungen – extern
- User-Community
- Infos über Schwachstellen
- Kontext
- Software-Archiv

Echtzeit-Überwachung von Ereignissen auf Endpoints:

- Prozesse, Services, PEs
- Kommunikationen
- Registry
- Downloads
- Hooks
- Usw.

Möglichkeiten für Administratoren:

- Malware-Warnungen
- Forensische Reports
- Ereignissuche



Erkennungs-fähigkeiten

Heutzutage nutzt Malware zahlreiche Tricks, um der Entdeckung durch Sicherheitslösungen zu entgehen. Sie tarnt sich mit einem harmlosen Erscheinungsbild und führt nicht sofort verdächtige Aktionen aus, sondern nach und nach im Verlaufe von Tagen oder Wochen. Wenn also eine Programmdatei bei ihrer ersten Ausführung klassifiziert wird, werden ihre schädlichen Eigenschaften möglicherweise noch nicht enthüllt. Deshalb wird es immer wichtiger, alle Aktionen von ausführbaren Dateien ständig zu beobachten. Malware kann warten, bis sie Anweisungen erhält oder auf Bedingungen im Kontext stößt, die sie dazu bringen, ihr bösartiges Verhalten oder ihre Absichten zu zeigen. Im Übrigen können auch legitime Programme Schwachstellen enthalten, die ausgenutzt werden können, um diese Programme dazu zu bringen, schädliche Aktionen auszuführen.

Adaptive Defense überwacht sämtliche Ausführungsereignisse aller ausführbaren Dateien. Neue Verhaltensmuster oder Anomalien im Ausführungsprofil bereits klassifizierter Programmdateien lösen eine erneute Klassifizierung aus. Dabei werden nicht nur die Spuren, die das Verhalten hinterlässt, berücksichtigt, sondern ebenso der dynamische und statische Kontext der ausführbaren Datei (Elternprozess, Pfad).

Ein wesentlicher Bestandteil des Services ist, dass Kunden nur Warnmeldungen über bestätigte Malware-Ereignisse erhalten. Jede verdächtige Aktivität einer Programmdatei wird immer vollständig durch Panda geklärt, bis diese entweder ausgeschlossen oder bestätigt wird. Dies führt zu beträchtlichen Kosteneinsparungen in den Sicherheitsabteilungen, die normalerweise viele Warnmeldungen über „potenzielle“ Störfälle durchgehen müssen.

„Reaktions“-Fähigkeiten

Wenn sich ein Malware-Ereignis bestätigt, wird dem Administrator eine Warnmeldung gesendet zusammen mit allen verfügbaren forensischen Informationen, einschließlich Verweildauer (wie lange war die PE-Datei bereits im System, bis sie als Malware klassifiziert wurde), welche Rechner/User waren betroffen, was hat die Programmdatei wann getan, wie gelangte sie in das System, welche Schwachstellen hatten die auf dem Endpoint laufenden Anwendungen, auf welche Daten wurde während des Angriffs zugegriffen und wann. Im Rahmen der optional erhältlichen Service-Pakete beinhaltet Adaptive Defense u. a. einen zusätzlichen Dienst zur vollständigen Desinfektion innerhalb des Netzwerkes.

Reports und Warnmeldungen

Warnmeldungen werden an den Administrator gesendet und sind ebenfalls in einer webbasierten Konsole verfügbar, zusammen mit dem dazugehörigen forensischen Report. Für jeden Vorfall wird eine visuelle Darstellung des Angriffs angeboten, welche die Instanzen, Kommunikationen und ausgeführten Aktionen sowie die Zeitleiste der Ereignisse zeigt.

Erweiterte Suche

Alle Informationen über die Aktivitäten sämtlicher PE-Dateien, die von Adaptive Defense gesammelt und verarbeitet werden, können durchsucht, gefiltert oder als Grafiken und Diagramme dargestellt werden. Bei der detaillierten Darstellung der Ereignisse werden weitere Anwendungsfälle berücksichtigt, wie z. B. Entdeckung oder Identifizierung von laufenden Anwendungen in Echtzeit, Nutzungsdaten (welche Programme werden genutzt, von wem und wann), Geolokalisierung von Kommunikationen und potenzieller Missbrauch von Daten.

Screenshot. Visuelle Zeitleiste der von der Malware ausgeführten Aktionen.

Vier Säulen für optimale Sicherheit

Automatische Prävention

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

Automatische Erkennung

Targeted Attacks und Zero-Day-Angriffe werden in Echtzeit und ohne Signaturdateien blockiert.

Automatische Desinfektion

Entfernung von Malware mit einem Klick oder automatisch, um die Arbeitslast der Administratoren zu reduzieren.

Automatische Forensik

Forensische Informationen für die detaillierte Analyse jedes Angriffsversuchs. Nachverfolgbarkeit und Transparenz jeder Aktion, die von laufenden Anwedungen ausgeführt wird.

Quelle: Gartner, Designing an Adaptive Security Architecture for Protection From Advanced Attacks, Neil MacDonald, Februar 2014

Wie Adaptive Defense funktioniert

Den Agenten installieren:

Nach der optionalen Proxy-Konfiguration sollte der Agent (MSI-Paket oder exe-Datei) idealerweise auf allen Netzwerkgeräten installiert werden. Dabei sollen Active-Directory-Richtlinien, wenn verfügbar, angewendet werden. Mit den entsprechenden Administratorrechten kann der Agent auch mithilfe von Verteilsoftware installiert werden.

Direkt nach der Installation meldet sich der Adaptive Defense Agent beim Service an und beginnt mit dem Sammeln allgemeiner Informationen über den Rechner. Dadurch wird eine eindeutige Zuordnung von Computer, Kunde und den auftretenden Ereignissen ermöglicht.

Überwachung der Ereignisse und Erstellen von Anwendungsprofilen:

Nach der Anmeldung beginnt der Agent mit der Überwachung der Aktivitäten aller laufenden Prozesse, wie z. B.:

Dateidownloads, Softwareinstallation, URL zum Dateidownload, Modifikation der Hosts-Datei, Alter der Datei, Treibererstellung, Window hook/unhook, Prozesskommunikationen (IPs, Ports, Protokolle), PE-Erstellung, Modifikation, DLL-Last, Service-Erstellung, PE-Mapping, Datei löschen/umbenennen, Ordnererstellung, Archiverstellung/Öffnen, Registry-Key-Erstellung/Modifikation, Pfaderstellung im Remote-Prozess, Prozess beenden, Zugriff auf den Security Accounts Manager (SAM), Datenzugriff (mehr als 200 Dateiformate) usw.

Alle laufenden Prozesse werden klassifiziert. Die Klassifizierung basiert auf einer ständig aktualisierten Wissensdatenbank über Goodware und Malware sowie auf der Analyse statischer, dynamischer (lokal und durch die Community beobachtetes Verhalten) und kontextabhängiger Informationen jeder PE-Datei.

Präventive Fähigkeiten:

- Bekannte Malware wird sofort blockiert. Dazu wird eine Kombination aus dem Agenten und cloud-basierter Intelligenz genutzt.

- Häufig verwendete Applikationen wie Java, Adobe, Microsoft Office und Browser werden generell vor exploit-basierten Angriffen geschützt. Dafür werden kontextabhängige und verhaltensbezogene Regeln genutzt, welche die Ausnutzung von Schwachstellen in diesen Anwendungen verhindern.

- Daten und bestimmte sensible Bereiche des Betriebssystems werden gegen unberechtigten Zugriff durch Anwendungen von Dritten gehärtet. Der Zugriff auf legitime Applikationen, die während der Installationsphase klassifiziert wurden, ist hingegen erlaubt.

  Alle ausführbaren Dateien werden mit einer Genauigkeit von nahezu 100 Prozent (99,9999 %) klassifiziert. Programmdateien, die als Malware klassifiziert wurden, werden automatisch blockiert. Anwendungen können vor oder nach Ausführung gesperrt werden, basierend auf der Richtlinie, die vom Administrator festgelegt wurde. Das heißt, im Lock-Modus werden nicht klassifizierte PE-Dateien zum Zeitpunkt der Ausführung blockiert, bis ihre Analyse abgeschlossen ist. Im Hardening-Modus hingegen können nicht klassifizierte Programmdateien, die nicht aus dem Internet heruntergeladen wurden, laufen, bis sie klassifiziert sind. Sie werden nur blockiert, wenn bestätigt wurde, dass es sich um Malware handelt. Die Klassifizierung dauert gewöhnlich wenige Sekunden oder Minuten. Nur in Ausnahmefällen kann sie auch einige Stunden dauern.

- Legitime Programme können auch auf Grundlage einer vom Administrator festgelegten Blacklist blockiert werden, aus Produktivitätsgründen oder wegen anderer Bedenken.


panda