Die Bedrohungslage entwickelt sich ständig weiter

Eine wirklich effiziente Lösung für Endpunktschutz zeichnet sich durch Prävention, Erkennung, Visualisierung und Adaptive Intelligence aus – vor, während und nach einem Angriff.

Adaptive Defense 360 integriert diese Elemente in einem kompakten Lösungspaket für Endpoints, das sich auf umfassende und skalierbare Verarbeitungsfunktionen in der Cloud stützt.

panda
eine Marke von WatchGuard

pandasecurity.com/business
watchguard.com

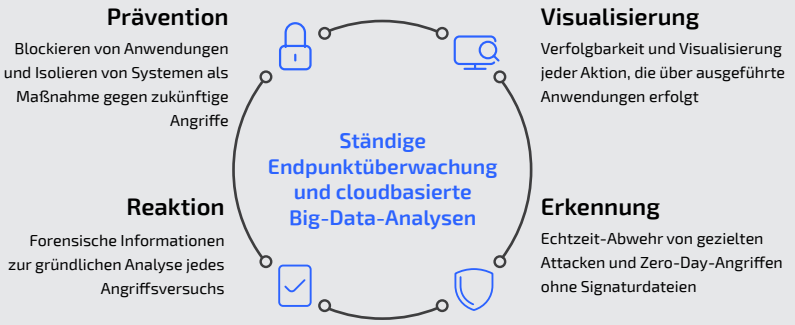
Adaptive Defense 360

Traditionelle Antiviruslösungen sind wirksam, wenn es darum geht, bekannte Malware durch Erkennungstechniken auf Basis von Signaturindizes und heuristischen Algorithmen zu blockieren. Sie eignen sich jedoch nicht zur Abwehr von Zero-Day-Angriffen und gezielten Attacken, bei denen Tools, Taktiken, Techniken und böswillige Prozesse zum Einschleusen der Malware eingesetzt werden.

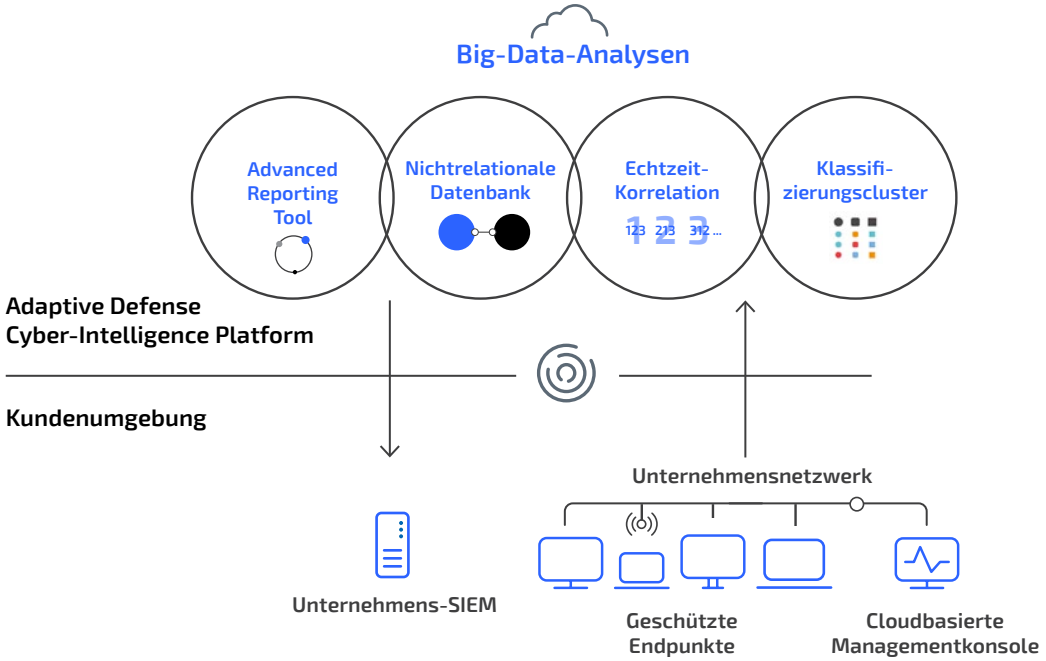
Und das Einfallstor für Malware wird immer breiter. Hacker nutzen dies aus, um Netzwerke mit Viren, Ransomware, Trojanern und anderen Arten von ausgefeilter Malware und gezielten Angriffen zu infizieren.

Garantie für die Sicherheit aller ausgeführten Anwendungen

Mit seiner Produkt- und Servicefamilie Adaptive Defense bietet Panda Security eine Lösung zur Abwehr solcher Angriffe. Der Endpoint-Detection-and-Response(EDR)-Service von Adaptive Defense ist in der Lage, jede ausgeführte Anwendung im Unternehmen genau zu klassifizieren, sodass nur vertrauenswürdige Aktionen ausgeführt werden.



Das Sicherheitsmodell für Panda Adaptive Defense basiert auf drei Prinzipien: ständige Überwachung aller Anwendungen auf Servern und Workstations, automatische Klassifizierung von Endpunktprozessen mithilfe von Big Data und Machine-Learning-Techniken in einer cloudbasierten Plattform sowie Analyse nicht automatisch klassifizierter Anwendungen durch unsere Experten.



Effektive Sicherheitslösungen kombinieren hoch entwickelte Technologien mit menschlicher und künstlicher Intelligenz. Anders ausgedrückt: Experten bestimmen, wie die Möglichkeiten des maschinellen Lernens genutzt werden. Damit eine Sicherheitslösung als Technologie der nächsten Generation eingestuft wird, muss sie durch Prävention, Erkennung, Visualisierung und Adaptive Intelligence alle Arten von Cyberangriffen ununterbrochen abwehren können.

Entscheidungsträger sollten bei der Wahl einer Endpunktsicherheitslösung auf die folgenden Kernelemente achten:

- **Ständige Überwachung**, indem alle Aktivitäten der ausgeführten Prozesse aufgezeichnet und beobachtet werden, um nicht vertrauenswürdige Software zum Zeitpunkt der Ausführung zu stoppen, moderne Bedrohungen in Echtzeit zu erkennen, in Sekundenschnelle zu reagieren und für sofortige Wiederherstellung zu sorgen.
- **Erkennung bei der Ausführung nicht vertrauenswürdiger Dateien**, um die Angriffsfläche zu verkleinern. Um das Netzwerk vor Bedrohungen zu schützen, muss die Sicherheitslösung alle auf den Geräten ausgeführten Anwendungen als vertrauenswürdig oder böswillig klassifizieren.
- **Intelligente Bedrohungserkennung,** da menschliches Eingreifen bei der Überwachung und Abwehr eines Angriffs nicht immer möglich ist. Effektive Sicherheitslösungen müssen sich eigenständig und automatisch an die äußerst individuelle Betriebsumgebung des Unternehmens anpassen können.
- **Schnelle und automatisierte Reaktion:** Unternehmenssysteme generieren eine Vielzahl von Warnungen und Ereignissen. Doch sobald ein Cyberkrimineller eingedrungen ist, können Informationen innerhalb von Sekunden gestohlen werden. Daher muss die Sicherheitslösung in der Lage sein, einen gerade stattfindenden Angriff schnell zu erkennen, Maßnahmen zur Schadensvermeidung zu ergreifen und die Systeme zu entlasten. Durch eine automatisierte Reaktion lassen sich Kosten einsparen und Aufgaben erledigen, die früher mehrere Tage in Anspruch genommen haben.

Schutzfunktionen der nächsten Generation

	Adaptive Defense 360	AV	Schutz vor Exploits	Schutz vor Ransomware	Sandboxing
SCHUTZ VOR DER DYNAMIK VON ANGRIFFEN, ZUM BEISPIEL:					
Bekannte Malware, unbekannte Malware und Zero-Day-Angriffe, einschließlich neuer Ransomware oder Variationen	●	◒			◒
Advanced Persistent Threats (APTs), gezielte Angriffe und Cyberspionage	●				
Bekannte und unbekannte Exploit-Angriffe, auch ohne Einsatz von Malware	●		●		
Botnet-Angriffe, durch die Computer in per Command-and-Control(C&C)-Server gesteuerte Rechner umgewandelt werden	●				◒
NEXT-GENERATION ENDPOINT PROTECTION (NGEP)					
Schützt vor böswilliger Software, erkennt laufende Angriffe und verhindert wiederholte Versuche	●	◒	◒	◒	
Überwacht ausgeführte Prozesse durchgängig, klassifiziert alle Anwendungen und stoppt ihre Ausführung, wenn sie nicht vertrauenswürdig sind	●				
Passt sich mithilfe von Machine-Learning-Techniken in einer Big-Data-Umgebung laufend der neuen Bedrohungsdynamik an	●	◒			◒
Langfristige Ausrichtung auf Angriffe – Erkennen und dynamisches Blockieren von Tools, Taktiken, Techniken und böswilligen Prozessen	●				
ERKENNUNG, ABSCHIRMUNG UND PROBLEMLÖSUNG					
Sie werden in Echtzeit benachrichtigt, sobald etwas Ungewöhnliches erkannt oder verdächtiges Verhalten unterbunden wird	●				
Liefert Echtzeit-Informationen über die Aktivitäten des Angreifers: Herkunft, Ursache, betroffene Ressourcen und ergriffene Maßnahmen	●				
Automatische Problemlösung, Erkennung böswilliger Dateien, Korrektur von Veränderungen und Beseitigung manipulierter Prozesse	●	◒	◒	●	◒
Zeigt operative Informationen zu im Nachhinein ausgeführten Aufgaben sowie ergriffenen Maßnahmen gegen zukünftige Angriffe an	●				
MANAGED SECURITY SERVICE					
Automatisierung mit maschinellem Lernen und Big Data, Entlastung von Sicherheitsteams und Verkürzung der Zeit zwischen Erkennung und Reaktion	●				
Experten für die Erkennung neuartiger Angriffe („Threat Hunter") werten den Service zusätzlich auf	●	◒			
Aktivitäten von Angreifern werden rund um die Uhr beobachtet und überwacht	●	◒			◒
TOOLS ZUR UNTERSUCHUNG VON VORFÄLLEN					
Chronologie von Angriffen (Dateien, Datensätze, Treiber usw.) und Informationen zu den Auswirkungen auf das Unternehmen (z. B. betroffene Ressourcen, „Zombie"-Rechner oder -Geräte)	●				
Zugriff auf detaillierte, anwenderbasierte Informationen zur Wahrung der Vertraulichkeit	●				
Vollständige Integration in andere Untersuchungstools, insbesondere SIEMs	●				
RISIKOMANAGEMENTANALYSEN					
Komplette Visualisierung aller Systeme: ausgeführte Software, anfällige Anwendungen, Anwenderverhalten, Datenverkehr usw.	●				
Suchtools zur Feststellung von Anomalien, die durch externe Angriffe, durch Insider oder durch unsachgemäße Nutzung von Unternehmensressourcen verursacht wurden	●				
Tools, die in einer cloudbasierten Big-Data-Plattform bereitgestellt werden und zur Verringerung der Betriebskosten und Reaktionszeit beitragen	●				
EINFACHE BEREITSTELLUNG UND VERWALTUNG					
Einfache Bereitstellung, Aktualisierung und Verwaltung über die Cloud, sodass Remote-Systeme ebenso gut geschützt werden können wie Systeme innerhalb des Netzwerks	●	●	●	●	◒
Umfassende Bereitstellung ohne Serviceunterbrechung, einschließlich Self-Learning und transparenter Anpassung an das Unternehmen (innerhalb weniger Stunden einsatzbereit)	●				
Perfekte Integration mehrerer Technologien, Vermeidung unnötigen Verbrauchs und Optimierung der Synergien zwischen den Technologien	●	●			
Minimale Auswirkungen auf das Netzwerk und auf geschützte Geräte, höchstens 5 % Einfluss auf die Systemleistung	●	◒	◒	◒	
Minimale Unannehmlichkeiten für Endanwender – so wird eine Überlastung von Einsatzteams vermieden, die sich stattdessen auf die Untersuchung von Vorfällen konzentrieren können	●	◒	◒	◒	
VERARBEITUNG IN ECHTZEIT					
Machine-Learning-Technologie in Big-Data-Umgebungen als exklusive Methode zur Echtzeit-Klassifizierung von Prozessen	●				
Durch Cloud- und Big-Data-Verarbeitung lässt sich das Wissen in Echtzeit vermitteln, weitergeben und exponentiell erweitern	●	◒			
Geringere Systemkomplexität und effizientes Risikomanagement durch Cloudnutzung und Data Mining ohne Begrenzung der Informationsverarbeitung	●	◒			

Schützen Sie Ihre Endpoints mit Adaptive Defense 360.
Erfahren Sie mehr auf **pandasecurity.com/business** und **watchguard.de**.

Deutschland, Österreich, Schweiz: +49 700 92229333 INTERNATIONALER VERTRIEB +1.206.613.0895 www.watchguard.de | pandasecurity.com/business