Adaptive Defense 360

Antworten finden, Probleme lösen

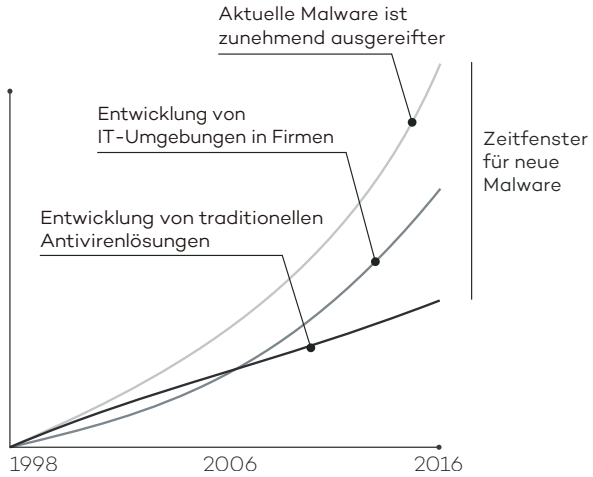
MAXIMALER SCHUTZ DURCH KOMBINATION VON EPP- UND EDR-TECHNOLOGIEN

Endpoints gegen Angriffe zu verteidigen, ist schwierig und aufwändig. Eine Schutzlösung muss eine breite Palette an Verteidigungsmaßnahmen enthalten, einschließlich traditionellem Antiviren- und Antimalwareschutz, Personal Firewall, Web- und Mail-Filter sowie Device Control. Jede Abwehr muss zusätzlichen Schutz vor schwer zu erkennenden Zero-Day- und gezielten Angriffen bieten.

Bislang mussten IT-Abteilungen eine Reihe von verschiedenen Produkten unterschiedlicher Hersteller erwerben und überwachen, um Endpoints zu schützen. **Adaptive Defense 360** ist die erste und einzige Lösung, die **Endpoint Protection Platform (EPP) und Endpoint Detection & Response (EDR) Technologien** kombiniert. Außerdem automatisiert **Adaptive Defense 360** viele Abläufe und reduziert so die Arbeitsbelastung der IT.

Adaptive Defense 360 beinhaltet Pandas modernste EPP-Lösung, die einfache und zentralisierte Sicherheit, Wiederherstellungsmaßnahmen, Echtzeitüberwachung und Reports, profilbasierten Schutz, zentralisierte Gerätesteuerung sowie Webüberwachung und -filterung bietet.

Sowohl die Malware- als auch die IT-Security-Landschaft haben sich in den letzten 20 Jahren enorm verändert. Durch das Auftreten von durchschnittlich 225.000 neuen Viren täglich (Q1/2015) und die immer komplexer und ausgereifter werdende Malware sind Netzwerke in Unternehmen anfälliger für Zero-Day- und gezielte Angriffe, sogenannte Targeted Attacks, als je zuvor.



Schutzlösungen für Endpoints, die auf Signaturdateien und heuristischen Algorithmen basieren, bieten effektiven Schutz vor bekannter Malware. Sie sind jedoch keine Verteidigung gegen Zero-Day- und gezielte Angriffe, die das „Zeitfenster für neue Malware“ ausnutzen. Dieses „Zeitfenster“ bezeichnet die Zeitspanne zwischen dem Erscheinen eines neuen Virus und der Entwicklung eines Gegenmittels durch die Sicherheitsunternehmen; eine größer werdende Lücke, die von Hackern ausgenutzt wird, um Viren, Ransomware, Trojaner und andere Arten von Malware in Firmennetzwerke einzuschleusen. Solche zunehmend verbreiteten Bedrohungen können vertrauliche Dokumente verschlüsseln, um Lösegeld zu verlangen, oder sensible Daten zum Zwecke der Industriespionage sammeln.

Adaptive Defense 360 ist Pandas Antwort auf diese Arten von Angriffen. Adaptive Defense 360 bietet einen EDR-Service, der jede in einem Unternehmen laufende Anwendung exakt klassifizieren kann, sodass nur vertrauenswürdige Prozesse ausgeführt werden. Die EDR-Fähigkeiten von **Adaptive Defense 360** resultieren aus einem Sicherheitsmodell, das auf drei Prinzipien basiert: (1) ständige Überwachung aller laufenden Anwendungen auf Firmencomputern und Servern, (2) automatische Klassifizierung durch die Collective Intelligence und (3) die Analyse nicht automatisch klassifizierter Anwendungen durch Techniker der PandaLabs. So können wir das Verhalten jeder in einem Unternehmen laufenden Anwendung überprüfen.

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 Anwendungen ausgeführt wird.

Durch die Kombination dieser EDR-Fähigkeiten mit der modernsten EPP-Lösung von Panda ermöglicht Adaptive Defense 360 Malwareschutz, der automatische Prävention, Erkennung, Forensik und Desinfektion in einer einzigen Lösung bietet.

DIE EINZIGE LÖSUNG FÜR DIE OPTIMALE SICHERHEIT ALLER LAUFENDEN ANWENDUNGEN

UMFASSENDER UND STABILER SCHUTZ

Panda **Adaptive Defense 360** 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 aller ausgeführten Aktionen** geben einen klaren Überblick über alle Ereignisse, die von der 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.

SCHUTZ FÜR GEFÄHRDETE BETRIEBSSYSTEME UND ANWENDUNGEN

Systeme wie Windows XP, die nicht länger vom Hersteller unterstützt werden und deshalb ungepatcht und ungeschützt sind, fallen Zero-Day-Angriffen und Bedrohungen der neuesten Generation leicht zum Opfer.

Zudem nutzen 90 Prozent der Malware Schwachstellen in Anwendungen wie Java, Adobe, Microsoft Office sowie in Browsern.

Adaptive Defense 360 nutzt Kontext- und Verhaltensregeln um sicherzustellen, dass Unternehmen in einer sicheren Umgebung arbeiten können, sogar wenn diese Betriebssysteme nutzen, die nicht mehr aktualisiert werden.

UMFASSENDE EPP-FÄHIGKEITEN

Adaptive Defense 360 enthält Panda Endpoint Protection Plus, die fortschrittlichste EPP-Lösung von Panda, inklusive:

- Wiederherstellungsmaßnahmen
- Zentralisierte Gerätesteuerung: Verhinderung von Malware-Eintritt und Datenverlust durch Sperren von Gerätetypen
- Webfilterung und -überwachung
- Mailfilterung und -überwachung
- Endpoint Firewall und vieles mehr

STÄNDIGE INFORMATIONEN ÜBER DEN NETZWERKSTATUS

Es werden umgehend Warnmeldungen ausgegeben, sobald Malware im Netzwerk identifiziert wird. Ein umfassender Bericht liefert Informationen zum Ort, den angegriffenen Computern und den von der Malware ausgeführten Aktionen.

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

INTEGRATION IN SIEM

A**daptive Defense 360** integriert sich in SIEM (Security Information and Event Management) Lösungen, um detaillierte Daten über die Aktivitäten aller auf dem System laufenden Anwendungen zu liefern.

Für Kunden ohne SIEM enthält **Adaptive Defense 360** optional ein komplettes SIEM-Tool zur Visualisierung und forensischen Analyse dessen, was alle Prozesse im System bzw. Netzwerk auslösen.

100 % MANAGED SERVICE

Es sind keine Investitionen in technisches Personal erforderlich, um Quarantäne, verdächtige Dateien oder infizierte Computer zu managen. **Adaptive Defense 360** klassifiziert automatisch alle Anwendungen mit Hilfe von selbstlernenden Systemen in Big-Data-Umgebungen und unter der ständigen Aufsicht von spezialisierten Technikern der PandaLabs.

TECHNISCHE ANFORDERUNGEN

Webkonsole (nur für die Überwachung)

- 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, 10
- Betriebssysteme (Server): Windows Server 2003, Windows Server 2008, Windows Server 2012
- Internetverbindung (direkt oder über Proxy)

Teilweise unterstützt (nur EPP):

- Linux, Mac OS X und Android