Cisco AMP für Endpunkte

Entdecken Sie das gefährlichste 1 % der Bedrohungen, das Ihnen bislang entgangen ist. Innerhalb von Stunden – statt Tagen oder Monaten.

Nahezu alle Sicherheitslösungen für Endpunkte versprechen, 99 % sämtlicher Malware zu blockieren. Doch was ist mit dem 1 % der Bedrohungen, das ihnen entgeht? Das gefährlichste 1 % der Bedrohungen wird in Ihrem Netzwerk immense Schäden anrichten. Wenn Sie sich ausschließlich auf herkömmliche Point-in-Time-Technologien verlassen, beispielsweise Antivirus, können diese Bedrohungen im Schnitt bis zu 200 Tage unentdeckt bleiben. Sie können sich über Monate hinweg einschleichen und sich lateral in Ihrem Netzwerk bewegen. Dabei verursachen sie durch heimliche Malware-Kampagnen Schäden, ohne dass Sie es bemerken – bis es zu spät ist.

Schneller Schutz von Benutzern mit höchster Präzision

Die moderne Malware hat sich weiterentwickelt, sodass es nun schwieriger ist und länger dauert, sie zu erkennen und einzudämmen. Cybersecurity-Teams haben mit einer überwältigenden Anzahl an Warnungen zu kämpfen. Sie verbringen sehr viel Zeit mit der Prävention, Erkennung von und Reaktion auf Bedrohungen. Dabei müssen sie sich immer noch auf manuelle Prozesse verlassen und eine Vielzahl schlecht integrierter Tools verwenden. Der Schutz von Benutzern ist heute wichtiger denn je, aber muss er wirklich bedeuten, dass man mit übermäßigen Mengen an Warnungen kämpfen muss und dabei Zeit verliert, die man mit seiner Familie verbringen könnte? Wer seine Benutzer vor den heutigen komplexen Bedrohungen schützen will, benötigt eine Endpunkt-Sicherheitslösung der nächsten Generation, die Genauigkeit, Geschwindigkeit und Effizienz bietet.

Endpunkt-Sicherheit der nächsten Generation

Endpunkt-Sicherheit der nächsten Generation bedeutet die Integration von Präventions-, Erkennungs- und Reaktionsfunktionen in einer einzigen Lösung, die das Potenzial von Cloud-basierter Analytik voll ausschöpft. Cisco® Advanced Malware Protection (AMP) für Endpunkte ist ein übersichtlicher Connector, der auf Ihren Windows-, Mac-, Linux-, Android- und iOS-Geräten verwendet werden kann. Er kann in der Public Cloud verwendet oder als Private Cloud bereitgestellt werden. AMP überwacht und analysiert alle Aktivitäten von Dateien und Prozessen in Ihrem Netzwerk kontinuierlich, um das riskanteste 1 Prozent aller Bedrohungen aufzuspüren und automatisch zu beseitigen, das anderen Lösungen entgeht. AMP verliert nie den Überblick, wohin eine Datei verschoben wird oder was sie tut. Wenn eine Datei, die bei der ersten Untersuchung als unbedenklich eingestuft wurde, jemals zum Problem wird, kann AMP auf den gesamten Verlauf der Bedrohungsaktivität zurückgreifen, um eine Bedrohung beim ersten Anzeichen schädlichen Verhaltens zu erkennen, einzudämmen und zu beseitigen.

Vorteile

Cisco AMP für Endpunkte bietet schnell maximalen Schutz vor den komplexesten Angriffen, sodass Sie Ihre Zeit wieder gezielt für Innovationen nutzen können. Es verhindert Sicherheitsverletzungen und blockiert Malware beim Eintritt, es erkennt schnell komplexe Bedrohungen, die die erste Verteidigungslinie durchbrochen haben, dämmt sie ein und beseitigt sie.

- **Verhindern:** Stärken Sie Ihre Abwehr mithilfe von branchenführender, weltweit erfasster Threat-Intelligence und blockieren Sie dateilose und dateibasierte Malware in Echtzeit.
- **Erkennen:** Überwachen Sie fortlaufend alle Dateiaktivitäten und zeichnen Sie sie auf, um getarnte Malware schnell aufzuspüren.
- **Reagieren:** Beschleunigen Sie Untersuchungen und beseitigen Sie Malware automatisch auf PCs, Macs, Linux-Rechnern, Servern und Mobilgeräten (Android und iOS).

Nächste Schritte

Sprechen Sie mit einem Vertriebsmitarbeiter von Cisco oder einem unserer Channel-Partner darüber, wie AMP für Endpunkte Sie beim Schutz vor hochentwickelten Cyber-Angriffen unterstützen kann. Weitere Informationen finden Sie auf unserer Website.

C45-731874-13 01/19

Malware stoppen

AMP für Endpunkte nutzt einen Cloud-basierten Ansatz für Threat-Intelligence und Dateianalysen. Die AMP-Cloud wird laufend mit Informationen von Talos™ und Cisco Threat Grid aktualisiert. Dank des Zugriffs auf die branchenweit größte Sammlung von globalen Echtzeit-Threat-Intelligence-Feeds wird die Zeit, die Sie selbst für Bedrohungsforschung aufbringen müssen, drastisch verkürzt. Anhand dieses Cloud-basierten Ansatzes kann AMP Dateien gegen die aktuellsten Threat-Intelligence-Daten analysieren, um Sie vor der sich stetig weiterentwickelnden Malware von heute zu schützen.

Mit 15 integrierten Schutz- und Erkennungsmechanismen, die verhindern, dass Bedrohungen sich auf Ihre Geschäfte auswirken, übernimmt AMP den Großteil der Arbeit für Sie. Dazu zählen unter anderem der Schutz vor schädlichen Aktivitäten, um Ransomware aufzuhalten, Prävention von Exploits mit dateiloser Malware, Machine-Learning-Analysen neuer Bedrohungen und Sandboxing. Wenn sich eine Datei als sauber genug erweist, um alle Mechanismen zu bestehen, wird sie von AMP durchgelassen und daraufhin kontinuierlich auf schädliches Verhalten überwacht und analysiert.

„Blinde Flecken“ beseitigen

Cisco AMP für Endpunkte bietet einen ganzheitlichen Überblick über Ihre Endgeräte, unabhängig vom Betriebssystem. Darüber hinaus bietet AMP Einblick in ungewöhnlichen Datenverkehr auf vernetzten Geräten im Internet of Things (IoT), auf denen kein Connector bereitgestellt werden kann – darunter Drucker, Thermostate und Sicherheitskameras –, um proaktiven Schutz vor fortschrittlichen Bedrohungen in allen denkbaren Vektoren zu bieten.

Cisco weiß, dass Cyberkriminelle sich nur selten auf einen Angriffsvektor beschränken. AMP für Endpunkte teilt Threat-Intelligence in Ihrer gesamten Umgebung und vereinheitlicht somit die Sicherheit für alle Endgeräte, Netzwerke, E-Mails, die Cloud und das Internet. Dank dieser Integrationen ist es möglich, dass AMP eine Bedrohung in einem Bereich Ihrer Umgebung erkennt und diese daraufhin an allen anderen Orten blockiert, an denen sie in Erscheinung tritt. AMP korreliert automatisch Dateien, Telemetriedaten, Verhalten und Aktivitäten, um Untersuchungen zu vereinfachen und die Problemlösungs- und Eindämmungszeit zu verkürzen.

Unbekannte Bedrohungen erkennen

Die integrierte Sandboxing-Technologie von AMP analysiert das Verhalten von verdächtigen Dateien und korreliert es mit anderen Informationsquellen. Die Dateianalyse liefert detaillierte Informationen, damit Sie besser nachvollziehen können, wie der Outbreak eingedämmt und zukünftige Angriffe blockiert werden können. Zusätzlich sorgt AMP für Klarheit, da es dem Sicherheitspersonal ermöglicht wird, die Kontrolle über seine Zeit zurückzugewinnen, indem Ihre Endgeräte vor den anspruchsvollsten Bedrohungen geschützt werden – und das in kürzerer Zeit und mit weniger Aufwand und geringeren Kosten.

Wenn eine Datei als schädlich eingestuft wird, reduziert AMP den Zeit- und Ressourcenaufwand für die Untersuchung deutlich. Es zeigt automatisch, was passiert ist, wie die Malware eindringen konnte, an welchen Stellen sie gefunden wurde, was sie gerade tut und wie sie gestoppt werden kann.

Mit nur wenigen Klicks kann die Datei über die browserbasierte Managementkonsole von AMP blockiert und so verhindert werden, dass sie auf allen Endpunkten ausgeführt wird. Da AMP jedes Endgerät kennt, das die Datei erreicht hat, kann es die Datei für alle Benutzer unter Quarantäne stellen. Mit AMP gleicht die Beseitigung von Malware einem chirurgischen Eingriff. Es entstehen keine weiteren Schäden an den IT-Systemen und Beeinträchtigungen der Geschäftsabläufe werden vermieden.