JEDES GERÄT UND JEDE VERBINDUNG SEHEN.

AGENTLESS SECURITY FOR THE ENTERPRISE OF THINGS

Die meisten Unternehmen können 40 % der Geräte in ihrer Umgebung nicht sehen. Sie haben Schwierigkeiten, gemanagte und ungemanagte Geräte in ihrer Umgebung zu identifizieren und sich entsprechend zu schützen. Armis findet alle Geräte und die damit verbundenen Risiken in Ihrer Umgebung, erkennt Bedrohungen und handelt automatisch, um Ihre kritischen Systeme und Daten zu schützen – insbesondere ungemanagte Geräte.

EINE RASANTE ZUNAHME VON VERNETZTEN GERÄTEN

Wir beobachten eine rasante Zunahme ungemanagter Geräte am Arbeitsplatz – eine digitale Transformation, die größer ist als die Einführung von PCs und Mobilgeräten zusammen. Von traditionellen Geräten wie Laptops und Smartphones zu neuen, ungemanagten Geräten wie Smart-TVs, Sicherheitskameras, intelligenter Beleuchtung, digitalen Assistenten, HLK-Systemen, medizinischen Geräten, Fertigungsgeräten und mehr.

Jedes Jahr wächst die Anzahl ungemanagter Geräte in Unternehmen um fast 31 %. Bis 2021 werden bis zu 90 % davon ungemanagte und IoT-Geräte sein. Obwohl diese verbundenen Geräte zu einer höheren Produktivität beitragen, stellen sie auch ein größeres Risiko dar.

Die überwiegende Mehrheit dieser Geräte ist nicht gesichert, schwer oder unmöglich zu aktualisieren, und Unternehmen haben keine Möglichkeit, sie zu sehen oder zu managen. Herkömmliche Firewalls, Netzwerksicherheit und Endpunktsicherheitsprodukte reichen dafür nicht aus. All das stellt Ihr Sicherheitsteam vor ein großes Problem.

DIE SICHERHEITSPLATTFORM VON ARMIS

Armis ist die erste agentless Enterprise-Class-Sicherheitsplattform, die die neue Bedrohungslandschaft ungemanagter und IoT-Geräte adressiert. Wir erkennen jedes gemanagte, ungemanagte und IoT-Gerät innerhalb und außerhalb Ihres Netzwerks, analysieren das Verhalten dieser Geräte, um Risiken oder Angriffe zu identifizieren, und schützen Ihre kritischen Geschäftsinformationen und -systeme. Die Armis-Plattform ist agentless, d. h. eine Installation von Software (Agenten) auf den Geräten ist nicht erforderlich, und lässt sich ganz einfach in Ihre vorhandenen Sicherheitsprodukte integrieren.

DIE ARMIS-PLATTFORM

UMFASSEND

Erkennt und klassifiziert alle Geräte in Ihrer Umgebung, innerhalb oder außerhalb Ihres Netzwerks.

AGENTLESS

Nichts auf Geräten zu installieren, keine Konfiguration, keine Störung des laufenden Betriebs.

PASSIV

Keine Auswirkung auf das Netzwerk Ihres Unternehmens. Kein Scannen von Geräten.

REIBUNGSLOS

Installiert sich in wenigen Minuten unter Verwendung der bereits vorhandenen Infrastruktur.

Wir überwachen passiv den kabelgebundenen und drahtlosen Verkehr in Ihrem Netzwerk und in Ihrem Luftraum, um alle Geräte zu identifizieren und das Verhalten jedes einzelnen Geräts zu verstehen – ganz ohne Unterbrechungen. Dann analysieren wir diese Daten in unserer Risiko-Engine. Die Engine nutzt Geräteprofile und -eigenschaften aus der Armis Device Knowledgebase, um jedes Gerät zu identifizieren, seine Risiken zu bewerten, Bedrohungen zu erkennen und Gegenmaßnahmen einzuleiten.

WICHTIGE GERÄTEEINBLICKE

Die Armis Device Knowledgebase analysiert über 280 Millionen Geräte.

Asset-Management

Sichtbarkeit. Sie ist ein wesentlicher Bestandteil jeder Sicherheitsstrategie für jedes Unternehmen. Wenn Ihr Unternehmen Frameworks wie PCI, HIPAA, NIST oder die CIS Critical Security Controls erfüllen muss, dann müssen Sie ein akkurates Inventar der Assets in Ihrer Umgebung führen. Das ist leichter gesagt als getan.

Armis erkennt und klassifiziert alle gemanagten, ungemanagten und IoT-Geräte in Ihrer Umgebung, einschließlich Server, Laptops, Smartphones, VoIP-Telefone, Smart-TVs, IP-Kameras, Drucker, HLK-Steuerungen, medizinische Geräte, industrielle Steuerungen und vieles mehr. Armis kann sogar netzfremde Geräte in Ihrer Umgebung identifizieren, die Wi-Fi, Bluetooth und andere IoT-Protokolle verwenden – eine Funktion, die kein anderes Sicherheitsprodukt ohne zusätzliche Hardware bietet.

Das umfassende, von Armis generierte Geräteinventar umfasst kritische Informationen wie Gerätehersteller, Modell, Seriennummer, Standort, Benutzername, Betriebssystem, installierte Anwendungen und im Laufe der Zeit hergestellte Verbindungen.

Zusätzlich zur Erkennung und Klassifizierung eines Geräts berechnet Armis seinen Risikowert auf der Grundlage von Faktoren wie Schwachstellen, bekannten Angriffsmustern und dem beobachteten Verhalten jedes Geräts in Ihrem Netzwerk. Dieser Risikowert hilft Ihrem Sicherheitsteam, die Angriffsfläche zu verstehen und die Einhaltung gesetzlicher Rahmenbedingungen zu erfüllen, die die Identifizierung und Priorisierung von Schwachstellen erfordern.

Risikobewertung

Armis geht über die Identifizierung von Geräten und Risiken hinaus. Die Armis Threat Detection Engine überwacht kontinuierlich das Verhalten jedes Geräts in Ihrem Netzwerk und in Ihrem Luftraum auf Verhaltensanomalien. Anhand unserer Device Knowledgebase vergleicht Armis das Echtzeitverhalten jedes Geräts mit folgenden Kriterien:

- Historisches Verhalten des Gerätes
- Verhalten von vergleichbaren Geräten in Ihrer Umgebung
- Verhalten von vergleichbaren Geräten in anderen Umgebungen
- Bekannte Angriffstechniken
- Informationen von Threat Intelligence Feeds

Aufgrund der detaillierten Kenntnisse zu Geräten und deren Verhalten ist Armis bestens positioniert, um Bedrohungen und Angriffe zu erkennen.

Erkennung und Reaktion

Wenn Armis eine Bedrohung erkennt, kann Ihr Sicherheitsteam alamiert werden oder es werden automatische Gegenmaßnahmen eingeleitet, um einen Angriff zu stoppen. Durch die Integration mit Ihren Switches und Wireless LAN-Controllern, mit Firewalls von Cisco, Check Point oder Palo Alto Networks sowie Network Access Control (NAC)-Produkten wie Cisco ISE und Aruba ClearPass kann Armis den Zugang beschränken oder verdächtige oder bösartige Geräte unter Quarantäne stellen. Dank dieser Automatisierung können Sie sicher sein, dass ein Angriff auf ein Gerät – ob gemanagt oder ungemanagt – auch dann gestoppt wird, wenn Ihr Sicherheitsteam gerade an anderen Prioritäten arbeitet.

Reibungslose Integration

Armis erfordert weder den Einsatz von Agenten noch von zusätzlicher Hardware, sodass sie innerhalb von Minuten bis Stunden einsatzbereit ist. Armis lässt sich nicht nur in Ihre Firewall oder Ihre NAC integrieren, sondern auch in Ihre Sicherheitsmanagementsysteme wie SIEM, Ticketing-Systeme und Asset-Datenbanken. Damit können diese Systeme und Ihre Sicherheitsteams bei Vorfällen die reichhaltigen Informationen nutzen, die Armis zur Verfügung stellt.

ÜBER ARMIS

Armis ist die erste agentless Enterprise-Class-Sicherheitsplattform, die die neue Bedrohungslandschaft ungemanagter und IoT-Geräte adressiert. Fortune 1000-Unternehmen vertrauen auf unsere einzigartige Out-of-Band-Sensortechnologie, um alle gemanagten, ungemanagten und IoT-Geräte zu erkennen und zu analysieren – von herkömmlichen Geräten wie Laptops und Smartphones bis zu neuen ungemanagten Smart-Geräten wie Smart-TVs, Webcams, Druckern, HLK-Systemen, Industrierobotern, medizinischen Geräten und mehr. Armis erkennt Geräte innerhalb und außerhalb des Netzwerks, analysiert kontinuierlich das Verhalten der Endpunkte zur Identifizierung von Risiken und Angriffen, und schützt kritische Informationen und Systeme, indem verdächtige oder böswillige Geräte identifiziert und unter Quarantäne gestellt werden. Armis ist ein Unternehmen in Privatbesitz und hat seinen Hauptsitz in Palo Alto, Kalifornien.

ARMIS

1.888.452.4011
armis.com