Leitfaden für Käufer:
IoT Security

Fünf unverzichtbare Merkmale einer erstklassigen IoT-Sicherheitslösung

Inhalt

IoT-Nutzung in den Unternehmen steigt

Unternehmen, die das Internet der Dinge (Internet of Things, IoT) erfolgreich in ihre Geschäftsmodelle integrieren, profitieren von enormen Vorteilen für ihre internen Abläufe, ihre Mitarbeiter und ihre Kunden.

Am offensichtlichsten sind höhere Effizienz und Produktivität bei geringeren Kosten. Doch immer mehr Unternehmen nutzen das IoT auch als eine hervorragende Quelle von Informationen darüber, wie ihre Produkte sich auf das Leben von Mitarbeitern und Kunden auswirken.

Das liegt daran, dass der wichtigste Vorteil von IoT in Unternehmen in den gelieferten Daten liegt. Aus IoT-Daten gewonnene Erkenntnisse sind für Entscheidungsträger von unschätzbarem Wert.

Mehr als 30 % aller mit dem Unternehmensnetzwerk verbundenen Endgeräte sind heute IoT-Geräte. Es versteht sich von selbst, dass der Trend weiter nach oben geht – und mobile Geräte sind in diesen Zahlen noch nicht berücksichtigt. Laut Prognosen von Gartner wird die Zahl der IoT-Geräte in diesem Jahr auf 5,81 Milliarden ansteigen.

Quellen:

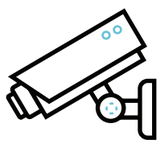
1 – Gartner: „Scenarios for the IoT Marketplace“, 2019
2, 3, 4 – 451 Research's Voice of the Enterprise: „Internet of Things, Budgets and Outlook“, 2019

46 %
Unternehmen, die bereits IoT einsetzen (inkl. bezahlter Pilotprojekte)[2]

23 %
Unternehmen, die gerade eine IoT-Machbarkeitsstudie durchführen[3]

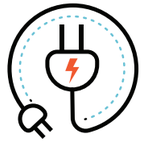
18 %
Unternehmen, die IoT in den nächsten zwei Jahren einführen möchten[4]

UNTERNEHMENSSEGMENTE MIT DEM GRÖSSTEN WACHSTUM 2020



PHYSISCHE SICHERHEIT

1,09 Mrd.
IoT-Geräte 2020



VERSORGUNG

1,37 Mrd.
IoT-Geräte 2020

UNTERNEHMENSSEGMENTE MIT DER STÄRKSTEN NUTZUNG 2020

42 % Gebäude-automatisierung

31 % Automobil-industrie

29 % Gesundheits-wesen

IoT- und OT-gestützte Geschäftsmodelle bieten hervorragende Gelegenheiten für die digitale Transformation. Doch wer ihre Vorteile voll ausschöpfen will, benötigt modernste Sicherheitstechnologie zum zuverlässigen Schutz des IoT.

Wachstum bringt neue Sicherheitsrisiken mit sich

Der zunehmende Einsatz von IoT-Geräten in Unternehmen wirft insbesondere für Sicherheitsteams eine Reihe neuer Herausforderungen auf.

Sie sind bereits für den Schutz von IT-Endgeräten verantwortlich, die mit dem Unternehmensnetzwerk verbunden sind. In der neuen Normalität – die insbesondere durch viel versprechende neue IoT-Konzepte charakterisiert ist – müssen sie sich auch mit Herausforderungen auseinandersetzen, die sich aus der zunehmenden Anzahl von IoT-Geräten ergeben, die zwar mit dem Unternehmensnetzwerk verbunden, aber typischerweise nicht verwaltet werden.

Einzigartige IoT-Sicherheitsrisiken, denen sich die Sicherheitsteams von Unternehmen gegenübersehen

BESTAND

Mangelnder Überblick darüber, welche IoT-Geräte im Netzwerk vorhanden sind und wie neue Geräte gefunden und verfolgt werden sollten

DATENVOLUMEN

Mangelnde Kontrolle über die riesigen Mengen von Daten, die von verwalteten und nicht verwalteten IoT-Geräten generiert werden

VIELFALT

Enorme Vielfalt an IoT-Geräten mit unzähligen Funktionen

RISIKEN

Unzureichende Sicherheitsvorkehrungen in den Betriebssystemen von IoT-Geräten, die zudem schwer oder unmöglich zu patchen sind

ZUSTÄNDIGKEIT

Neue Risiken bei der Verwaltung von IoT-Geräten durch verschiedene Teams innerhalb des Unternehmens

BETRIEB

Das Dilemma: IoT-Geräte sind zum einen kritisch für den Kernbetrieb, zum anderen aber nur schwer in die Kernsicherheitslösungen zu integrieren

Aktuelle Lösungen sind den Herausforderungen nicht gewachsen

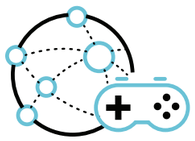
Die vorherrschenden Sicherheitsmechanismen sind für die Sicherung des Internetverkehrs im Unternehmen nicht ausreichend.

Immer mehr praktisch unsichtbare IoT-Geräte werden zu festen Bestandteilen in Unternehmensnetzwerken. Von Gebäude- und Straßenbeleuchtungssensoren, Strömungsmonitoren und Überwachungskameras bis hin zu IP-Telefonen, Kassensystemen, Konferenzraumtechnik und vielem mehr sind IoT- und OT-Geräte in Netzwerken und Unternehmen zu finden. Diese Geräte vergrößern die Angriffsfläche des Unternehmens erheblich. Derzeitige Schutzsysteme am Netzwerkperimeter können dem Zustrom dieser Geräte und den daraus resultierenden Sicherheitsproblemen nur schwer begegnen.

Gängige, aber unzureichende Lösungen

Schwachstellenanalyse

Sie ist für IoT-Geräte von Natur aus komplizierter, weil die Hardware, Software und Kommunikationsprotokolle so vielfältig sind. Zudem können potenzielle Schwachstellen mit dieser Methode zwar bis zu einem gewissen Grad erkannt, aber nicht behoben werden.



NAC oder Netzwerkzugriffskontrolle

Solche Lösungen lassen sich nicht auf IoT skalieren. Sie sind nicht in der Lage, IoT-Geräte zu erkennen und vor noch unbekannten Bedrohungen zu schützen. Im besten Fall können sie Maßnahmen zum Schutz vor bekannten Gefahren durchsetzen.

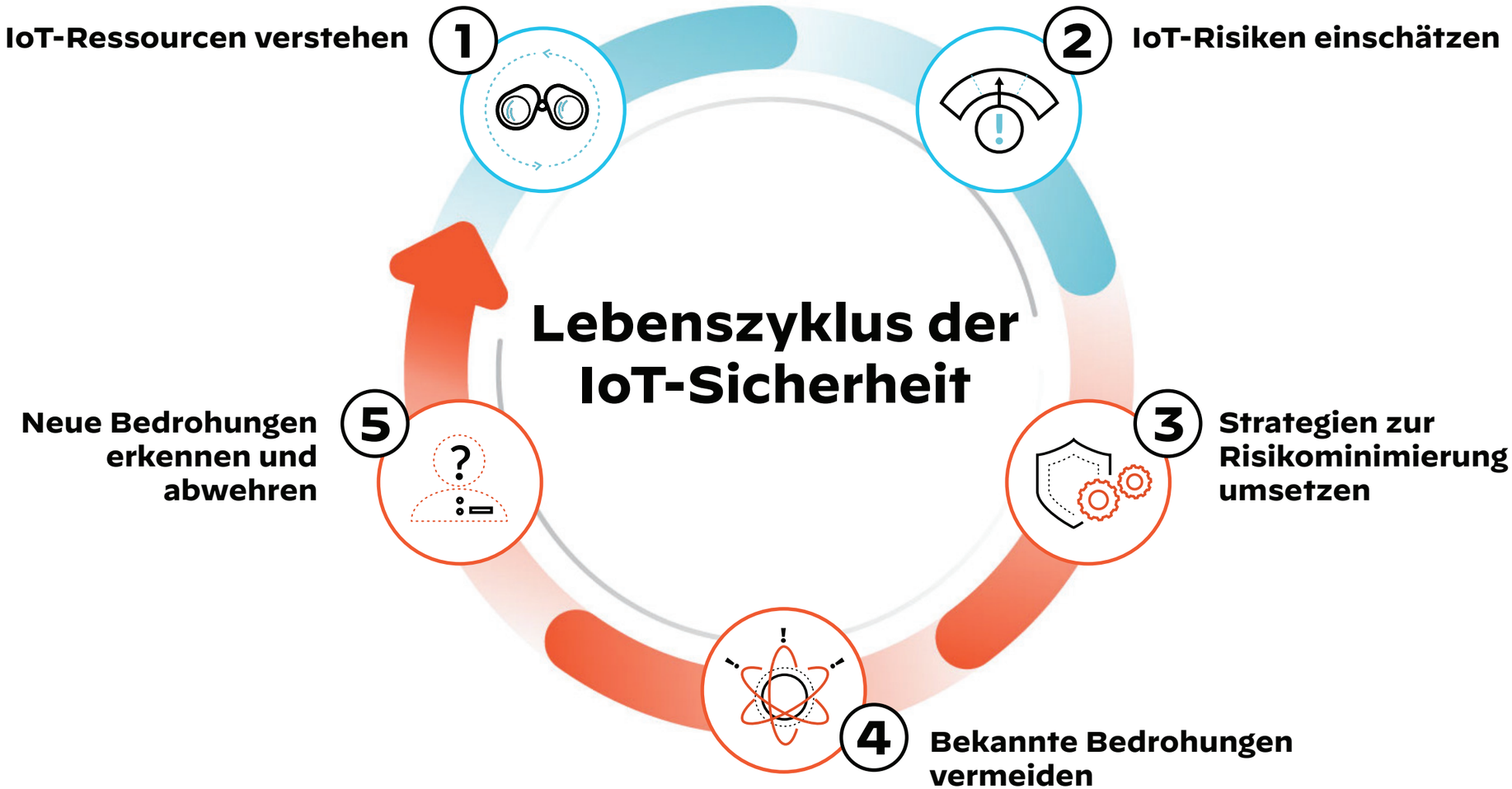
Punktlösungen für IoT-Sicherheit

Sie sind aufgrund der nötigen Implementierung von Einzwecksensoren, der Integration in bestehende Systeme und der erforderlichen Einarbeitung zu aufwendig.

CISOs sollten einen lebenszyklusbasierten Ansatz in Betracht ziehen, um ihre IoT-Sicherheitsstrategie zu verbessern.

Lebenszyklusbasierter Ansatz

Ein lebenszyklusbasierter Ansatz für die Sicherung der IoT- und OT-Geräte ist ein Muss. Eine ideale IoT-Sicherheitslösung unterstützt und verbindet alle Phasen des IoT-Lebenszyklus nahtlos, von der Erkennung der Geräte und der mit ihnen verbundenen Risiken bis hin zu Sicherheitsmaßnahmen zu ihrem Schutz vor bekannten und unbekannten Bedrohungen.



Für einen wirksamen IoT-Sicherheitslebenszyklus sollte Ihre IoT-Sicherheitslösung *fünf unbedingt erforderliche Merkmale aufweisen.*

Ihre IoT-Sicherheitslösung muss Folgendes bieten

1

Vollständige Transparenz über alle mit dem Unternehmen verbundenen IoT-Geräte

Bevor Sie sich für eine Sicherheitsstrategie entscheiden, sollten Sie sich einen umfassenden Überblick über **alle IoT-Angriffsflächen verschaffen.** Damit beginnt Ihr IoT-Sicherheitslebenszyklus. Nutzen Sie Geräteerkennung, um sich einen vollständigen Überblick über Ihre IoT-Ressourcen zu verschaffen. Ihre IoT-Sicherheitslösung sollte die genaue Anzahl der mit Ihrem Netzwerk verbundenen Geräte ermitteln können – und zwar aller Geräte, von denen Sie bereits wissen, sowie aller Geräte, von denen Sie nichts wissen oder die Sie vergessen haben. So lässt sich ein aktuelles Inventar aller IoT-Geräte erstellen. Außerdem sollte die Lösung wesentliche Gerätemerkmale aufzeigen, um umfassende Transparenz über jedes Gerät zu liefern.

Die Lösung sollte:

- Mehrzwecksensoren nutzen, die sich in die bestehende Infrastruktur integrieren lassen.
- wesentliche IoT-Gerätemerkmale (wie Hersteller, Modell, Betriebssystem, Firmware, Ports, Anwendungen, VLAN, Subnetz, Virenschutzsoftware usw.) erkennen und anzeigen.
- neue, zum ersten Mal erkannte Geräte ohne menschliche Unterstützung oder ständige Signaturupdates erkennen können.
- neu angeschlossene Geräte innerhalb weniger Minuten erkennen.
- mindestens 80 % der Geräte in sichtbaren Segmenten innerhalb von 48 Stunden erkennen.
- nicht verwaltete IoT-Geräte von verwalteten IT-Geräten unterscheiden können.
- eine Liste aller IT-Geräte führen, damit Sicherheitsteams auch nicht verwaltete IT-Geräte erkennen können.

Ihre IoT-Sicherheitslösung muss Folgendes bieten

2

Proaktive Überwachung von IoT-Geräten zur kontinuierlichen Erkennung riskanten Verhaltens

Um die Anforderungen der **IoT-Risikoeinschätzungsphase** im Sicherheitslebenszyklus zu erfüllen, muss Ihre Lösung IoT-Geräte jederzeit aktiv überwachen. Unternehmen benötigen für den Umgang mit den Risiken durch IoT-Geräte zwingend Überwachung, Berichte und Warnmeldungen in Echtzeit. Herkömmliche Endpunktlösungen können IoT-Geräte nicht schützen, da sie Softwareagenten erfordern, für die IoT-Geräte nicht ausgelegt sind. Durch die Einschätzung der Risiken in Ihrem IoT-Sicherheitslebenszyklus können Sie einen besseren Ansatz nutzen. Implementieren Sie eine Echtzeitüberwachungslösung, die kontinuierlich das Verhalten aller mit dem Netzwerk verbundenen IoT-Geräte analysiert, um Ihr Netzwerk kontextbezogen zu segmentieren und so eine granulare Kontrolle über die laterale Bewegung des Datenverkehrs zwischen IT- und IoT-Geräten (und deren Workloads) zu ermöglichen.

Die Lösung sollte unbedingt Folgendes bieten:

- ✓ Integration mit mehreren Bedrohungsdatenfeeds, damit Risiken den IoT-Geräten präzise zugeordnet werden können
- ✓ Erkennung und Meldung von Anomalien im IoT-Geräteverhalten, die zu einer Änderung des Risikos führen könnten
- ✓ Nachverfolgung von Veränderungen der IoT-Geräterisiken und Protokollierung der vollständigen Risikoentwicklung für Compliancezwecke
- ✓ Berechnung von Risikowertungen für IoT-Geräte und Gerätekategorien
- ✓ Integration in Risikomanagementsysteme für ein zentralisiertes IoT-Risikomanagement
- ✓ Integration mit den IoT-Geräteherstellern zur Bereitstellung von Daten an Sicherheitsteams

Ihre IoT-Sicherheitslösung muss Folgendes bieten

3

Automatisierte risikobasierte Empfehlung von Sicherheitsrichtlinien und deren Durchsetzung

Ihre IoT-Sicherheitslösung sollte einfach und ohne zusätzliche Infrastruktur oder Investitionen zu implementieren sein. Finden Sie eine Lösung, die Ihre vorhandene Firewall einbezieht, um eine umfassende und integrierte Sicherheitsinfrastruktur aufzubauen. Die Lösung sollte die Funktionen Ihrer Firewall **nutzen und automatisch Sicherheitsrichtlinien empfehlen und durchsetzen,** die für das Risikoniveau und das Ausmaß des bei Ihren IoT-Geräten erkannten nicht vertrauenswürdigen Verhaltens angemessen sind.

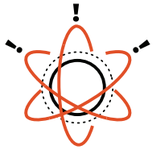
Da Vertrauen im Grunde eine Schwachstelle ist, sollte Ihre IoT-Lösung einen Zero-Trust-Ansatz verfolgen und Richtlinien nach dem Least-Privilege-Prinzip anwenden. Dadurch werden die Möglichkeiten für Angreifer – ganz gleich, ob sie sich nun innerhalb oder außerhalb Ihrer Organisation befinden – erheblich reduziert und Ihre kritischen IoT-Ressourcen geschützt.

Die Lösung sollte:

- Verhaltensweisen von IoT-Geräten automatisch in Richtlinien umwandeln, um nur vertrauenswürdiges Verhalten zuzulassen.
- die mehrschichtige Durchsetzung von Richtlinien für Gerätegruppen zulassen.
- sowohl Zulassungs- als auch Sperrlisten unterstützen.
- Geräte und Anwendungen verfolgen, um Richtlinien überall im Netzwerk durchzusetzen.
- einmal definierte Richtlinien automatisch aktualisieren, damit nicht bei jeder Änderung manuelle Aktualisierungen nötig sind.

Ihre IoT-Sicherheitslösung muss Folgendes bieten

4



Schnelle Abwehr bekannter Bedrohungen

Durch die Vielfalt der IoT-Geräte wird Ihr Netzwerk zu einer sehr heterogenen Umgebung mit zahlreichen potenziellen Einfallstoren. Erfolgreiche Sicherheitsmaßnahmen in Phase 4 des IoT-Sicherheitslebenszyklus erfordern verwertbare Erkenntnisse über die **Erkennung und Prävention bekannter** Bedrohungen für Ihre IoT-Geräte, damit Sie schnell auf Bedrohungen reagieren können. Suchen Sie nach einem Mechanismus zur Bedrohungsabwehr, der komplexe Bedrohungen auf Ihren IoT-Geräten mittels inhaltsbasierter Signaturen blockiert. Dadurch wird die aktuellste Verteidigung gegen bekannte Bedrohungen gewährleistet. So können Sie schnell und in Echtzeit auf Schwachstellen von IoT-Geräten und Schwachstellen in Ihrem gesamten Netzwerk reagieren und die Sicherheitsteams nicht mit unnötigen Erkennungswarnungen überlasten.

Prüfen Sie, ob die Lösung Folgendes bietet:

- ✓ Selektive Aktivierung von Schutzmaßnahmen auf Grundlage der Risikosituation der IoT-Gerätegruppe
- ✓ Erkennung und Abwehr bekannter Bedrohungen von Malware, Spyware und Exploits
- ✓ Abwehr von IoT-Angriffen über schädliche URLs und Websites
- ✓ Abwehr von IoT-Angriffen, bei denen DNS für Command-and-Control-Kommunikation oder Datendiebstahl missbraucht wird
- ✓ Blockierung von unbekannten, in Datenpaketen eingeschleusten IoT-Bedrohungen

Ihre IoT-Sicherheitslösung muss Folgendes bieten

5

Schnelle Erkennung und Abwehr unbekannter Bedrohungen

Bei der **Erkennung und Abwehr wirklich unbekannter Bedrohungen** isolieren alte Ansätze die Bedrohungsdaten, die jede Organisation erhält und erzeugt. Das erzeugt Silos und erschwert die Prävention. Um die Anforderungen des letzten Schritts im IoT-Sicherheitslebenszyklus zu erfüllen, sollte Ihre IoT-Sicherheitslösung einen neuen Ansatz nutzen, der sich auf eine kollektive Engine für Bedrohungsdaten stützt, die in Echtzeit Malware analysiert und vor Zero-Day-Angriffen auf Ihre IoT-Geräte schützt. Die Nutzung von durch Crowdsourcing in einer globalen Community generierten Daten bietet nicht nur kollektive Immunität. Sie spart Ihrem IT-Sicherheitsteam auch wertvolle Zeit, da die gesammelten IoT-Identitätsinformationen, Risikobewertungen, Schwachstellendaten und Verhaltensanalysen genutzt werden können, um unbekannte, nur in Ihrer IoT-Umgebung auftretende Bedrohungen von der ersten Erkennung an zu untersuchen. Dieser letzte Schritt deckt auch potenzielle Bedrohungen auf, die in früheren Phasen übersehen wurden, und führt Sie in einen Kreislauf zur kontinuierlichen Verbesserung.

Achten Sie darauf, dass die Lösung Folgendes bieten:

- ✓ Erkennung von ungewöhnlichem Verhalten auf verschiedenen Ebenen – auf Ebene der Gerätekategorie, dann des Herstellers/Modells und schließlich der Geräteinstanz
- ✓ Verwertung von per Crowdsourcing gewonnenen Daten, die mithilfe von maschinellem Lernen und Bedrohungsmodellen genutzt werden, um unbekannte Bedrohungen zu erkennen und proaktiv auf sie zu reagieren
- ✓ Integration in Sicherheitsorchestrierung, -automatisierung und -reaktion (SOAR) für prozessgestützte Ablaufskripte
- ✓ Zusammenarbeit mit aktiven IoT-Sicherheitsteams, um neue IoT-Bedrohungen zu erkennen

Die IoT-Sicherheitslösung von Palo Alto Networks

weist alle fünf Merkmale auf

Unsere IoT-Sicherheitslösung kombiniert maschinelles Lernen mit unserer patentierten App-ID-Funktion der Next-Generation Firewall, um Ihnen den genauesten und detailliertesten Überblick über Ihre IoT- und OT-Geräte zu bieten. Die Lösung versetzt Sicherheitsteams in die Lage, Bedrohungen proaktiv zu verhindern, das Geräterisiko zu überwachen, Anomalien zu erkennen und Richtlinien zu empfehlen und durchzusetzen.

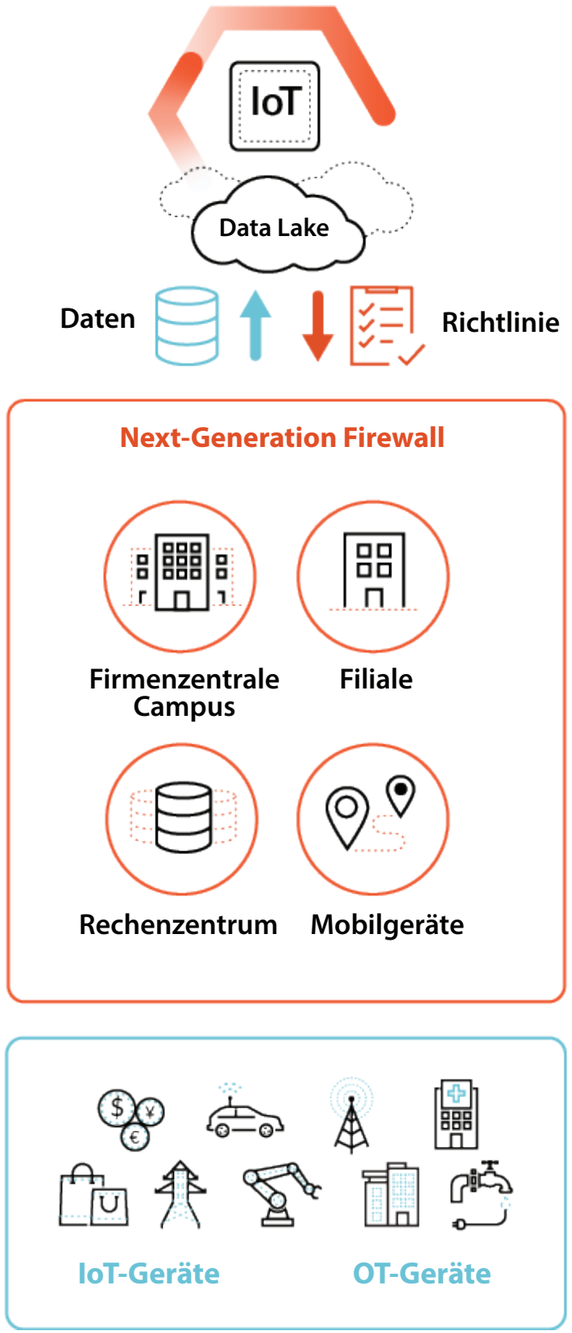
IoT Security ist eine abonnementbasierte Lösung, die einfach und ohne Einzwecksensoren oder Infrastrukturinvestitionen bereitgestellt werden kann. Sie brauchen das Abonnement nur auf Ihrer ML-gestützten Next-Generation Firewall von Palo Alto Networks zu aktivieren, um Ihre bisher nicht verwalteten IoT- und OT-Geräte umfassend zu schützen.

Wenn Sie noch nicht Kunde von Palo Alto Networks sind, dient unsere ML-gestützte Next-Generation Firewall auch als Sensor und Durchsetzungspunkt für IoT Security. Der Preis der Lösung kann sich mit Silolösungen für die IoT-Sicherheit an nicht von Firewalls abgedeckten Stellen messen.

In Kombination mit den leistungsstarken App-ID- und User-ID-Sicherheitsfunktionen, die bereits in unsere ML-gestützte Next-Generation Firewall integriert sind, setzt unsere Lösung automatisch Richtlinien zur Risikominderung durch (und zwar jetzt mit einem **neuen** Richtlinienkonzept auf Basis der Geräte-ID), um nur vertrauenswürdiges Verhalten von IoT-Geräten im Netzwerk zuzulassen.

Diese einzigartige Kombination von Funktionen gewährleistet eine kontextsensitive Segmentierung Ihres Netzwerks und minimiert so das Risiko, das von sich lateral ausbreitenden Exploits ausgeht. Darüber hinaus wendet die Lösung unsere führenden Abonnements zur Abwehr netzwerkbasierter Bedrohungen an, um Ihre IoT-Geräte vor bekannten und unbekannten Gefahren zu schützen.

Sichern Sie Ihre nicht verwalteten IoT- und OT-Geräte jetzt mit Palo Alto Networks.



Vorteile für Ihr bestehendes Sicherheitsteam

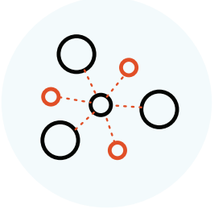
Ohne ein neues Team bilden zu müssen, können Sie neue Infrastrukturen bereitstellen oder vorhandene Abläufe ändern

Transparenz und Schutz ohnegleichen

- ML-gestützte IoT-Geräteerkennung
- Automatisierte Risikobewertung
- Native Richtliniendurchsetzung
- Kontextbewusste Netzwerksegmentierung

Einfache Bereitstellung mit flexiblen Optionen

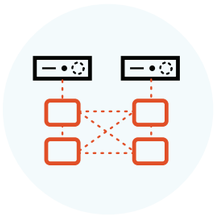
- Hardware-Firewalls der PA-Series
- Virtualisierte Firewalls der VM-Series
- Cloudbasiert mit Prisma Access SASE



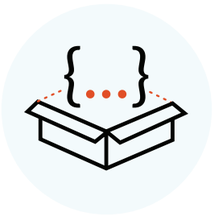
Umfassende Abdeckung von IoT- und OT-Geräten

- Verbraucher- und Enterprise-IoT-Geräte
- Geschäftskritische OT-Geräte
- Alte, nicht verwaltete Systeme

Stärken Sie die Sicherheit mit Abonnements für erweiterte Bedrohungsabwehr



Skalieren Sie die Lösung mühelos dank flexibler Cloud-Infrastruktur



Nutzen Sie ein funktionsreiches Set an Integrationen für Produkte anderer Hersteller für Geräteinventare, Protokollierung und Richtliniendurchsetzung

IoT Security heißt
Palo Alto Networks

Wir haben uns das Ziel gesetzt, zum bevorzugten Cybersicherheitspartner für Unternehmen zu werden und gemeinsam mit ihnen unseren digitalen Lebensstil zu schützen. Palo Alto Networks schützt die Clouds, Netzwerke und Mobilgeräte Zehntausender Unternehmen. Dazu gehen wir durch kontinuierliche Innovation die größten Herausforderungen rund um die Cybersicherheit an, mit denen Unternehmen derzeit konfrontiert sind. Dabei kommen die neuesten Forschungsergebnisse aus den Bereichen der künstlichen Intelligenz, Analysen, Automatisierung und Orchestrierung zum Einsatz.

Palo Alto Networks wurde 2005 gegründet und hat seinen Hauptsitz im kalifornischen Santa Clara. Zur Betreuung unserer Kunden haben wir zudem Niederlassungen auf der ganzen Welt.

Das sagen unsere Kunden

> *Innerhalb weniger Stunden fanden und identifizierten wir Tausende von Geräten, darunter auch einige, die uns einen kritischen Einblick gaben, sodass wir vorbeugende Maßnahmen ergreifen konnten.*

Weitere Informationen erhalten Sie unter : www.paloaltonetworks.com

Sie möchten mehr erfahren?

Demo ansehen

BayCare Medical Group

www.paloaltonetworks.de

Oval Tower, De Entrée 99-197
1101 HE Amsterdam, Niederlande

Zentrale: +1.408.753.4000
Vertrieb: +1.866.320.4788
Support: +1.866.898.9087