paloalto NETWORKS | Cybersecurity Partner of Choice

Das Ziel dieser anbieterunabhängigen Request for Information (RFI) Informationsanfrage) ist es, unsere Kunden bei der Evaluierung verschiedener IoT-Sicherheitslösungen zu unterstützen, damit sie effektive Maßnahmen zum Schutz nicht verwalteter Endpunkte innerhalb ihres Netzwerks ergreifen können.
Dazu das Ziel, geeigneten Angebots an verfügbaren Lösungen haben viele Organisationen Schwierigkeiten mit der Wahl der richtigen IoT-Sicherheitslösung, die den unternehmensspezifischen Anforderungen nachkommt. Das heißt konkret, dass Sie als Entscheidungsträger bestimmen müssen, ob die diversen, am Markt verfügbaren Lösungen für die IoT-Sicherheit die Funktionen bieten, die in Ihrer Organisation am wichtigsten sind.

Diese RFI-Checkliste führt wichtige Features und Funktionen auf, die geschäftliche Entscheidungsträger verschiedener Unternehmen und Branchen berücksichtigen sollten, bevor sie sich für die perfekte Lösung zum Schutz aller nicht verwalteten IoT-Geräte in ihrem Netzwerk entscheiden.

Die Checkliste deckt folgende zehn Kernbereiche ab:

1. Architektur und zugrunde liegende Technologie von IoT-Lösungen
2. Transparenz und Kontextdaten von nicht verwalteten Assets
3. Risikobewertung und Richtlinienempfehlungen für IoT-Geräte
4. Von der Lösung generierte Arten von Alarmen
5. Funktionen für die Threat Prevention
6. Funktionen für die Bedrohungsabwehr
7. Dashboard und Berichterstellung
8. Integration in vorhandene Infrastruktur und zukünftige IT- und Sicherheitslösungen
9. Compliance
10. Vorteile des Anbieters und Kundenservice

Projekttitel	**Angefordert von:**
Projektnummer	**Angefordert am:**
Projektbeschreibung	

ANLEITUNG

1) Identifizieren Sie, welche der in den Spalten „Kernbereich" und „Feature" angeführten Anforderungen Ihre Organisation stellt.

2) Überlegen Sie im Anschluss, ob die einzelnen, von Ihnen in Erwägung gezogenen Anbieter diese Anforderungen erfüllen. Wenn ja, tragen Sie in der Spalte des jeweiligen Anbieters auf der rechten Seite eine „1" ein. Wenn nicht, tragen Sie jeweils eine „0" ein.

3) Evaluieren Sie die Ergebnisse der einzelnen Kernbereiche, indem Sie die Gesamtzahl der pro Anbieter erzielten RFI-Punkte vergleichen.

	KERNBEREICH	FEATURE	PALO ALTO NETWORKS	ANBIETER 2	ANBIETER 3
1	ARCHITEKTUR UND TECHNOLOGIE: BEREITSTELLUNG UND VERWALTUNG	Die Lösung benötigt keine Sensoren.			
2		Der Sensor unterstützt physische, virtuelle und Cloud-Umgebungen.			
3		Die Lösung bietet On-Premises-Management.			
4		Die Lösung bietet eine Verwaltung in der Cloud.			
5		Die Gerätekennung erfolgt in Echtzeit.			
6		Die Gerätekennung kann gepatcht werden.			
7		Die Lösung ist so skalierbar, dass pro Bereitstellung die Zentralebene Campus abgedeckt wird.			
8		Die Lösung ist so skalierbar, dass pro Bereitstellung die Filialen/Außenstellen abgedeckt werden.			
9		Um IoT-Geräte zu erkennen, erhält der IoT-Sensor Informationen zum Netzwerkdatenverkehr aus folgenden Quellen:			
10		DHCP-Datenverkehr			
11		NetFlow			
12		SNMP			
13		TAP			
14		Die Lösung pflegt per Crowdsourcing eine Wissensdatenbank für Geräte.			
15		Die Lösung unterstützt die folgenden Protokolle zur Benutzerverwaltung:			
16		Rollenbasierte Zugriffskontrolle			
17		Multi-Faktor-Authentifizierung (MFA)			
18		Single Sign-On (einmaliges Anmelden, SSO)			
19		Bei der Bereitstellung der Verwaltung können je nach Standort, Subnetz oder Organisationsbereich unterschiedliche Sets an Anmeldedaten genutzt werden.			
20		Für die zur Erkennung genutzten Zugangsdaten sind keine lokalen Administratorrechte auf den Zielgeräten notwendig.			
21	ARCHITEKTUR UND TECHNOLOGIE: DATENSICHERHEIT UND -SCHUTZ	Der Anbieter nutzt NIST-definierte Protokolle für die Datensicherheit.			
22		Der Anbieter übermittelt Daten in der Cloud sicher zur Analyse.			
23		Die Daten sind DSGVO-konform.			
24		Die IoT-Lösung verwaltet den Benutzerzugriff durch:			
25		Rollenbasierte Zugriffskontrolle			
26		SSO			
27		MFA			
28		Gemäß den Richtlinien für Datenschutz und -sicherheit ermöglicht die Lösung das Löschen aller auf eine einzelne Person bezogenen, gespeicherten Daten.			
29		Die Lösung speichert nur notwendige Daten.			
30		Die geräte- und benutzerbezogenen Daten werden regelmäßig und automatisch gelöscht.			
31		Die Lösung erkennt Geräte, ohne dafür ein Konto mit erweiterten Zugriffsrechten zu benötigen.			
32	ARCHITEKTUR UND TECHNOLOGIE: ASSETIDENTIFIZIERUNG	Die Lösung ist auf passiven Gerätekennung getätigt, ohne Auswirkungen auf die Zielgeräte			
33		Die Lösung nutzt Signaturen oder Fingerabdrücke zur Identifizierung und Klassifizierung von Geräten.			
34		Die Lösung nutzt maschinelles Lernen (ML) zur Identifizierung und Klassifizierung von Geräten.			
35		Die Lösung erkennt Geräte per Bluetooth.			
36		Die Lösung erkennt Geräte per WLAN.			
37		Die Lösung erkennt Geräte über andere Protokolle mit niedriger Frequenz (z. B. Zigbee oder Z-Wave)			
38		Die Lösung erkennt private Bring-Your-Own-Device(BYOD)-Geräte.			
39		Die Lösung nutzt manuelle Scans für die Erkennung von Geräten.			
40		Die Lösung kann automatisierte (gezielte) Scans für die Erkennung von Geräten durchführen.			
	GESAMTZAHL DER RFI-PUNKTE FÜR DEN KERNBEREICH: ARCHITEKTUR UND TECHNOLOGIE		0	0	0
41	NICHT VERWALTETE ASSETS – TRANSPARENZ UND KONTEXT	Erkennung und Meldung von Datum und Uhrzeit der letzten Sichtung von IoT-Geräten			
42		Erkennung und Meldung von Datum und Uhrzeit der letzten Aktivität von IoT-Geräten			
43		Erkennung und Ermittlung des Normalverhaltens von IoT-Geräten			
44		Erkennung des Patchstatus von Geräten			
45		Erkennung und Meldung von Änderungen der Gerätekonfiguration			
46		Erkennung und Meldung von Anwendungen, inklusive Informationen zu Namen und Version			
47		Erkennung und Meldung von Anwendungen, inklusive Informationen zu Datum und Uhrzeit von Aktivitäten			
48		Erkennung und Meldung des Status von Sicherheitssprache			
49		Erstellung einer Stückliste, inklusive Informationen zu auf Geräten ausgeführter Software			
50		Erkennung und Meldung der Softwareversion von Anwendungen			
51		Erkennung und Meldung der Gerätekennzeichnung			
52		Erkennung und Meldung von internen und externen Verbindungstypen			
53		Erkennung und Meldung der Benutzerzuteilung – Identifizierung der Benutzer, die sich bei IoT-Geräten anmelden			
	GESAMTZAHL DER RFI-PUNKTE FÜR DEN KERNBEREICH: NICHT VERWALTETE ASSETS – TRANSPARENZ UND KONTEXT		0	0	0
54	RISIKOBEWERTUNG: COMPLIANCE DER GERÄTE	Vergleich der Konfiguration mit der anderer Geräte im Netzwerk			
55		Vergleich der Konfiguration mit der anderer Geräte in der durch Crowdsourcing generierten Gerätedatenbank			
56		Überwachung von Fehlkonfigurationen auf Geräten			
57		Überwachung, ob unzulässige Software auf IoT-Geräten ausgeführt wird			
58	RISIKOBEWERTUNG: SICHERHEITSLÜCKEN	Überwachung von sich mit der Cloud oder dem Netzwerk verbindenden Geräten			
59		Überwachung genutzter Standardkennwörter			
60		Überwachung nicht mehr unterstützter Geräte, Betriebssysteme und Anwendungen			
61		Überwachung, ob sich ein Gerät mit einem weniger sicheren Gerät verbindet			
62		Erkennung, ob das Betriebssystem gepatcht wurde oder nicht			
63		Erkennung, ob Software gepatcht wurde oder nicht			
64		Nachverfolgung ehemaliger Sicherheitslücken von IoT-Geräten			
65		Überwachung von CVEs			
66		Überwachung der Sicherheit gespeicherter Daten			
67		Erkennung, ob IoT-Geräte ICS-CERT-konform sind			
68	RISIKOBEWERTUNG: ANOMALIEN	Vergleich des Verhaltens eines Geräts mit dem von Vergleichsgeräten			
69		Überwachung von Anwendungen, die die Netzwerkleistung mindern			
70		Überwachung des Normalverhaltens			
71		Erkennung, ob ein Gerät kontinuierlich DHCP-Fehler erzeugt			
72		Erkennung der unverschlüsselten Übertragung großer Datenmengen			
73		Erkennung der Übertragung großer Datenmengen			
74		Erkennung von Richtlinienverstößen			
75		Erkennung ungewöhnlichen Datenverkehrs zwischen Geräten			
76		Erkennung, ob sich eigentlich stationäre Geräte bewegen			
77	RISIKOBEWERTUNG: BEDROHUNGEN	Erkennung von Anomalien, die auf Bedrohungen hinweisen			
78		Erkennung von Geräten, die sich mit schädlichen Domains verbinden			
79		Erkennung von Bedrohungen auf BYOD			
80		Erkennung bekannter IoT-Bedrohungen auf Geräten			
81		Erkennung unbekannter IoT-Bedrohungen auf Geräten			
82		Erkennung von Bedrohungen basierend auf omnifaceter, kontextreicher Bedrohungsforschung			
83	RISIKOBEWERTUNG: EXPLOITS	Erkennung geschwächter Brute-Force-Angriffe auf Felder			
84		Erkennung einer Verbindung zwischen einem privaten Gerät und zahlreichen anderen Geräten, die auf einen Exploit hinweist			
85		Erkennung signaturbasierter Alarme von NGFWs, EPP etc.			
86		Erkennung einer unzulässigen Netzwerkbrücke			
87		Erkennung ungewöhnlicher Verbindungsaufbauten			
88	RISIKOBEWERTUNG: MONITOR	Lassen sich verlorene Assets mit der Lösung nach gewisser Zeit automatisch entfernen?			
89		Automatische Richtlinienempfehlungen zur Risikoreduzierung auf Grundlage der Risikobewertung			
	GESAMTZAHL DER RFI-PUNKTE FÜR DEN KERNBEREICH: RISIKOBEWERTUNG UND RICHTLINIENEMPFEHLUNGEN FÜR IOT-GERÄTE		0	0	0
90	ALARME	Alarme aufgrund von Schwachstellen			
91		Alarme aufgrund von nicht konformen Geräten			
92		Alarme aufgrund von Bedrohungen			
93		Alarme aufgrund von Exploits			
94		Unterschiedliche Schweregrade für Alarme: hoch/mittel/niedrig			
95		Die Alarme bieten wichtige Informationen: wie Datum, Uhrzeit, Typ und Details zu den auslösenden Aktivitäten.			
96		Anpassbares Risikoniveau für Alarme			
97		Benutzerdefiniertes Risikoniveau zur Anpassung an bestehende Risikoframeworks von Kunden			
98		Inhalts- und Kontextbasierte Alarme			
99		Unterdrückung der Alarmmeldungen von bestimmten Alarmtypen			
100		Erstellung personalisierter Alarme			
101		Automatische Erstellung von Alarmtickets in Ticketsystemen – CMMB bzw. ITSM			
102		Erstellung automatischer Reaktionen auf Alarme, z. B. Isolierung von Geräten, in NAC-System			

0		Unterstützung von starren ob einheitlicher, geschlossener Kreislauf vom Dashboard aus		
		GESAMTZAHL DER RFI-PUNKTE FÜR DEN KERNBEREICH: ALARME	0	0
0	THREAT PREVENTION	Der IoT-Sensor umfasst Funktionen zur Threat Prevention.		
0		Threat Prevention erfordert die Integration mit einer Drittanbieterlösung.		
0		Virtuelle Segmentierung von Geräten		
0		Aktive Schadensbegrenzung dank NAC-Lösungen (z. B. Cisco ISE, Aruba ClearPass etc.)		
0		Empfehlungen für Netzwerkrichtlinien		
0		Netzwerksegmentierung		
0		Virtuelles Patching von risikobehafteten Geräten		
0		Threat Prevention für bekannte Bedrohungen		
0		Bedrohungserkennung und -eindämmung für unbekannte Bedrohungen		
0		Eingebaute Funktionen für das Schwachstellenmanagement		
0		Verwaltung von Schwachstellen mit Integrationen von Drittanbietern		
		GESAMTZAHL DER RFI-PUNKTE FÜR DEN KERNBEREICH: THREAT PREVENTION	0	0
0	BEDROHUNGSABWEHR	Maßnahmen zur Bedrohungsabwehr ausgehend von der IoT-Lösungskonsole		
0		Verhaltensbasiertes Blockieren		
0		Auf Richtlinien basierte Isolierung risikobehafteter oder infizierter Geräte		
0		Auf Sicherheitsrichtlinien basierte Blockierung oder Zulassung von Geräten		
0		Isolierung infizierter Geräte zur weiteren Untersuchung		
0		Automatische Richtlinienaktualisierung vom Sensor aus		
0		Abwehr von Zero-Day-Bedrohungen vom Sensor aus		
		GESAMTZAHL DER RFI-PUNKTE FÜR DEN KERNBEREICH: BEDROHUNGSABWEHR	0	0
0	DASHBOARD UND BERICHTERSTELLUNG	Darstellung der Gerätestandorte im Netzwerk, um Segmentierungsrichtlinien zu verfeinern		
0		Änderung von Richtlinien über das Dashboard		
0		Personalisierte Dashboards für verschiedene Benutzer		
0		Regelmäßige Berichtserstellung		
0		Berichtserstellung auf Anfrage		
0		Vorgefertigte, vorkonfigurierte Berichte		
0		Benutzerdefiniertes Reporting		
0		Berichtserstellung für einzelne Gerätegruppen		
0		Anzeige von Berichten basierend auf Geräteprofilen		
0		Berichte über neu erkannte Geräte		
0		Berichte über Asset/Schwachstellen		
0		Berichte über Assetcompliance		
0		Berichte über Richtlinien- und Validierung angewandter Sicherheitskontrollen		
0		Berichtserstellung basierend auf Priorisierung von Risiken		
0		Berichtserstellung zur VLAN-Zusammensetzung		
		GESAMTZAHL DER RFI-PUNKTE FÜR DEN KERNBEREICH: DASHBOARD UND BERICHTERSTELLUNG	0	0
0	INTEGRATION UND INTEROPERABILITÄT MIT VORHANDENER INFRASTRUKTUR	Eingebaute Integration für die Firewall zur Durchsetzung von Richtlinien und Segmentierung		
0		Eingebaute Integration für NAC zur Durchsetzung von Richtlinien und Segmentierung		
0		Eingebaute Integration für Switches zur Segmentierung		
0		Eingebaute Integration für drahtlose Infrastruktur (WLC) zur Segmentierung		
0		Eingebaute Integration für die Konfigurationsmanagementdatenbank (Configuration Management Database, CMDB) zur Verwaltung von Assets und zur Asset-Lebenszyklusverwaltung		
0		Eingebaute Integration für Lösungen für die Ressourceneplanung (Enterprise-Resource-Planning, ERP)		
0		Eingebaute Integration für das IP-Adressenmanagement (IPAM)		
0		Eingebaute Integration für das IT-Servicemanagement (ITSM)		
0		Eingebaute Integration für LDAP/Active-Directory (AD)		
0		Eingebaute Integration für System zur Echtzeitlokalisierung (Real-Time-Locating System, RTLS)		
0		Eingebaute Integration für Security-Information-and-Event-Management(SIEM)-Lösungen		
0		Eingebaute Integration für Sicherheitsorchestrierung, -automatisierung und -reaktion (SOAR)		
0		Eingebaute Integration für das Schwachstellenmanagement (Qualys, Rapid7, Tenable etc.)		
0		Eingebaute Integration von Ressourcen für Sicherheitslücken (HHS-ACI, ICS-CERT, MDISS etc.)		
0		Offene API zur Integration mit Drittanbieterlösungen		
		GESAMTZAHL DER RFI-PUNKTE FÜR DEN KERNBEREICH: INTEGRATION UND INTEROPERABILITÄT MIT VORHANDENER INFRASTRUKTUR	0	0
0	COMPLIANCE	Befolgung gesetzlicher Normen und Vorschriften (z. B. FDA, ECRI, ISO, NIST, ICS-CERT)		
0		Erfüllung von SP-800-121-Compliance (Richtlinien für die Bluetooth-Sicherheit)		
0		Unterstützung von Compliance mit PCI-DSS (Payment Card Industry Data Security Standard)		
0		Unterstützung von Compliance mit SWIFT CSP (SWIFT Customer Security Program)		
		GESAMTZAHL DER RFI-PUNKTE FÜR DEN KERNBEREICH: COMPLIANCE	0	0
0	MEHRWERT DES ANBIETERS UND KUNDENSERVICE	Der Anbieter der Lösung ist seit über zehn Jahren in der Branche tätig.		
0		Der Anbieter der Lösung kann Fallstudien zu bestehenden Kunden zur Verfügung stellen.		
0		Mindestens 75 % der Fortune 100 vertrauen auf den Anbieter der Lösung.		
0		Der Anbieter der Lösung ist weltweit tätig.		
0		Der Anbieter der Lösung wird in Analystenberichten zum Thema IoT-Sicherheit (Gartner, Forrester etc.) aufgeführt.		
0		Der Anbieter der Lösung stellt professionelle Services zur Verfügung, die die Planung und Bereitstellung erleichtern.		
0		Der Anbieter der Lösung bietet regelmäßige und auf Abruf verfügbare Schulungen zu Produkten.		
0		Der Anbieter der Lösung bietet rund um die Uhr Supportservices.		
0		Der Anbieter der Lösung stellt einen dedizierten Account Manager zur Verfügung, der zudem Beratung in Sicherheitsfragen bietet.		
0		Der Anbieter der Lösung bietet von dem Kauf an eine Gratisversion von den Produkten		
		GESAMTZAHL DER RFI-PUNKTE FÜR DEN KERNBEREICH: MEHRWERT DES ANBIETERS UND KUNDENSERVICE	0	0
		GESAMTZAHL DER RFI-PUNKTE - VERGLEICH	0	0