Extreme™
Customer-Driven Networking

Solution Brief

Extreme Defender for IoT

Einfache Sicherheit für Ihre kritischen Endgeräte

Das Internet der Dinge (IoT) hat großen Einfluss auf alle Branchen. Laut Umfragedaten haben 63% der IT-Organisationen einen Anstieg der Anzahl der Endgeräte, die sich mit dem Netzwerk verbinden, um 50% festgestellt[1]. Gartner schätzt, dass Unternehmen weltweit bis 2020 20,4 Milliarden vernetzte Geräte nutzen werden. Auch wenn das IoT-Wachstum tatsächlich von 3 wichtigen Teilbereichen getragen wird, nämlich Smart Cities (26%), Industrial IoT (24%) und Connected Health (20%)[2], so gibt es doch keine einzige vertikale Branche, die kein Wachstum bei der Anzahl der Endgeräte verzeichnet, die sich mit dem Netzwerk verbinden.

Das IoT verspricht zwar Effizienzsteigerungen, Kostensenkungen und einen verbesserten Kundenservice – aber gleichzeitig vergrößern diese Geräte auch die Angriffsfläche des Netzwerks und schaffen mehr Zugangswege für Hacker.

Die Statistiken:

- Fast 20% der Unternehmen waren in den letzten drei Jahren mindestens einem IoT-basierten Angriff ausgesetzt[3]
- Zwischen 2016 und 2017 stiegen die IoT-Angriffe um 600%[4]

„Sicherheit im Bereich IoT wird für unser Unternehmen immer wichtiger. Gleichzeitig befürchten wir, dass die Absicherung so vieler Geräte sehr komplex und teuer sein wird. Die Extreme Defender for IoT-Lösung wird unser IoT-Sicherheitstoolset ohne zusätzliche Komplexität verbessern.“

Ben Vickers,
Director of IT, Promedica

Herausforderungen bei der Implementierung von Sicherheit im Bereich IoT

Die Gefahr eines Angriffs ist sehr real – und es gibt viele Faktoren, die die Sicherung bestimmter IoT-Geräte zu einer Herausforderung machen. Erstens ist es allein die bloße Anzahl und Vielfalt der Endgeräte, von denen viele möglicherweise nicht unter der direkten Kontrolle der IT-Abteilung stehen. Sie können sich im Besitz des

2„A round up of 2018 Enterprise Internet of Things forecasts and market estimates“ (Artikel in Enterprise CIO) Januar 2018
3 Gartner Research Report: „IoT Solutions can't be trusted and must be separated from the enterprise networks to reduce risk.“ Mai 2018
4 „As Internet of Things attacks increase 60 0% in one year, businesses need to rethink their security“ (Artikel in TechRepublic) März 2018

Facility-Management-Teams, unterschiedlicher Betriebsteams oder des Klinikpersonals innerhalb eines Krankenhauses befinden. Darüber hinaus waren viele dieser Geräte ursprünglich nicht als internetfähige Geräte konzipiert und verfügen daher über keine integrierte Sicherheit.

Zu den speziellen Sicherheitsherausforderungen verbundener Geräte gehören unter anderem:

- Die Geräte arbeiten möglicherweise mit älteren, nicht mehr unterstützten Betriebssystemen wie Windows 95/98 und können nicht mehr gepatcht werden.
- Fehlende eigene Firewall, Virenschutz und Verschlüsselung auf vielen Geräten.
- In einigen Branchen (z.B. im Gesundheitswesen) müssen Geräte bei einer Änderung am Gerät (z. B. einem „Security Patch“) einen teuren, zeitaufwändigen Prozess zur Neuzertifizierung durchlaufen, um die Compliance zu wahren.
- In vielen Fällen sind Geräte, die per Kabel mit dem Netzwerk verbunden sind, stärker gefährdet. Spezifische Probleme bereiten hier veraltete Edge-Switches mit unterschiedlichen Funktionen im gesamten Netzwerk.

Absicherung von Geräten mit dem Extreme Defender for IoT

Der Extreme Defender for IoT ist eine einzigartige, preisgekrönte Lösung, die Sicherheit für Endgeräte bietet, die nur über eingeschränkte oder gar keine integrierten Sicherheitsfunktionen verfügen. Die Lösung zielt vor allem auf ältere kabelgebundene Geräte ab, die innerhalb eines Raumes, eines Gebäudes oder sogar auf einem Campus verschoben werden müssen.

Die Lösung ergänzt die bestehende Sicherheitsinfrastruktur eines Kunden durch eine Inline-Verteidigungslinie direkt am IoT-Gerät. Außerdem kann die Lösung über jede Netzwerkinfrastruktur hinweg bereitgestellt werden und gewährleistet so ein sicheres IoT-Management ohne wesentliche Änderungen am Netzwerk.

Komponenten von Extreme Defender for IoT

Der Extreme Defender for IoT besteht aus folgenden Komponenten:

- **Defender-Anwendung:** Eine benutzerfreundliche Anwendung, die die zentrale Erstellung von Sicherheitsprofilen für Gruppen von IoT-Geräten ermöglicht. Sobald die Profile erstellt sind, können auch nicht-technische Mitarbeiter ihre Geräte sicher „onboarden“ und verschieben. Sie können ihre Assets auch über intuitive Dashboards und eine zentrale Inventarisierung überwachen und verfolgen.
- **Defender-Adapter (SA20 1) und der ExtremeWireless 3912i Indoor Access Point:** Diese bieten einen Proxy-Service für die Defender-Anwendung zur Verwaltung und Sicherung von IoT-Geräten. Die spezifische Aufgabe besteht darin, den Verkehrsfluss zu überwachen – mit voller Sichtbarkeit der Layer 2 bis 7 – um sicherzustellen, dass das Gerät entsprechend seinem erwarteten Verhalten arbeitet. Der Defender-Adapter ist ein Single-Port-Gerät, das sich zwischen dem Netzwerk und dem IoT-Gerät befindet und eine Inline-Verteidigungslinie bietet. Der AP3912 ist eine Multi-Port-Einheit, die mehrere Geräte innerhalb eines Raumes unterstützt.
- **ExtremeCloud™ Appliance:** Die ExtremeCloud Appliance, die als Hardware-basierte oder virtuelle Appliance erhältlich ist, ist eine Standort-basierte Lösung, die Cloud-ähnliche Management- und Steuerungsfunktionen für Extreme Smart OmniEdge™ Lösungen (kabelgebunden oder drahtlos) bereitstellt. Dank einer umfassenden Palette umfangreicher APIs zur Anpassung von Anwendungen bildet sie die unterstützte Plattform für die Defender-Anwendung.

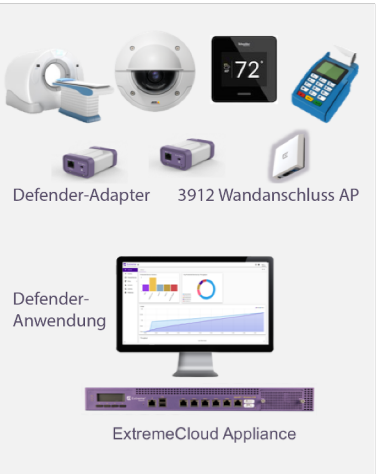

Abbildung 1: Extreme Defender for IoT

So schützt Extreme Defender for IoT Ihre Geräte

Der Extreme Defender for IoT schützt angeschlossene Geräte wie folgt:

- Profile, die sicherstellen, dass das Gerät gemäß dem erwarteten Verhalten arbeitet, werden direkt auf das IoT-Gerät angewendet.
- Der Extreme Defender for IoT steuert die Anbindung von IoT-Geräten und den Zugriff auf das Netzwerk.
- Die Lösung isoliert Gruppen von IoT-Geräten in Sicherheitszonen oder Netzwerksegmenten.

Laut Gartner Research „sind IoT-Geräte nicht vertrauenswürdig und müssen vom Netzwerk getrennt werden, um das Risiko zu reduzieren“[5]. Der Extreme Defender for IoT bietet einen einfachen und automatisierten Ansatz zur Erstellung isolierter Segmente für Geräte – und bietet dann eine weitergehende Verteidigungslinie, indem die Verkehrsströme zu und von den Geräten gefiltert werden. Die nächsten vier Abschnitte beschreiben die Sicherheitsfunktionen der Extreme Defender for IoT-Lösung.

Anwendung zentralisierter Profile

Die Absicherung von IoT-Geräten beginnt mit der Erstellung von Whitelist-Profilen. Diese Profile werden auf der Defender-Anwendung erstellt, verwaltet und katalogisiert. Typischerweise wird für jeden Gerätetyp (z.B. IP-Sicherheitskameras) ein einzelnes Profil erstellt und dann auf alle Geräte angewendet, die in diese Kategorie passen. Das Profil enthält eine Liste der autorisierten Geräte und Verkehrsströme und grenzt damit ab, was das IoT-Gerät empfängt und sendet mit wem das Gerät kommunizieren kann. Ein vollständiges Profil enthält ein Gruppenzugriffsprofil mit Sicherheitsregeln und Einstellungen für Netzwerkverbindungen.

Die Profile werden dann an den Defender-Adapter und/oder den AP3912 weitergeleitet, der den Verkehr mit voller Sichtbarkeit über die Layer 2 bis 7 regelt und überwacht. Damit wird sichergestellt, dass der Datenverkehr sowohl zum als auch vom IoT-Gerät durch die im Profil enthaltenen Regeln beschränkt wird. Dadurch ist das IoT-Gerät geschützt – und es wird außerdem daran gehindert, selbst einen Angriff zu starten.

Einfaches Erstellen von Profilen

Da Verkehrsprofile manchmal zu komplex sind, um sie manuell zu erstellen, automatisiert die Extreme Defender for IoT-Lösung diesen Prozess mit einem „Auto Policy Generator“. Die Extreme Defender for IoT-Lösung ermöglicht es den Adaptern, den Datenverkehr zur Defender-Anwendung zu spiegeln, in der der Auto Policy Generator dann ein Verkehrsprofil für das IoT-Gerät erstellen kann. Das IoT-Gerät arbeitet normalerweise mit der Defender-Anwendung zusammen, die den Datenverkehr katalogisiert, so dass die Lösung das zu erwartende normale Verhalten des Geräts erlernen kann. Sobald in diesem Modus genügend Zeit vergangen ist (abhängig vom Betrieb des IoT-Geräts), kann die Spiegelung gestoppt und das resultierende Verkehrsprofil auf das IoT-Gerät angewendet werden, um seine Kommunikation mit dem Netzwerk abzusichern.

Sichere Gerätemobilität ohne Einbindung der IT

Mit der Extreme Defender for IoT-Lösung können kabelgebundene Geräte automatisch von einem Netzwerkport zu einem anderen verschoben werden. Wenn ein Gerät verschoben werden muss, kann ein Techniker den Adapter einfach von einem Raum-Wandanschluss trennen, das Gerät und den Adapter an einen neuen Ort verschieben und den Adapter an einen neuen Port anschließen. Wenn der Adapter vom Stromnetz getrennt wird, verliert er sein Profil und die Netzwerkdienste werden auf dem alten Switch-Port deaktiviert. Wird der Adapter wieder verbunden, kontaktiert er die ExtremeCloud Appliance, um sein Profil abzurufen, und fordert die Bereitstellung der Dienste auf dem neuen Port an. Innerhalb weniger Minuten arbeitet das IoT-Gerät am neuen Standort – der Umzug kann schnell und sicher ohne Eingriffe der IT-Abteilung abgeschlossen werden.

Netzwerksegmentierung / Sichere Zonen

Zusätzlich zu den Richtlinien ermöglicht der Extreme Defender for IoT auch die Platzierung ähnlicher Geräte in einer eigenen isolierten Sicherheitszone oder einem klinischen Segment. Laut Gartner-Forschung sind nur 5% der heute eingesetzten IoT-Geräte praktisch segmentiert, bis 2021 werden es jedoch 60% sein[5]. Die Schaffung von Sicherheitszonen reduziert die Angriffsfläche und

[5]Gartner Research Report: „IoT Solutions Can't Be Trusted and Must Be Separated from the Enterprise Network to Reduce Risk“ – Mai 2018.

Abbildung 2: Klinische Segmentierung und sichere Zonen mit dem Extreme Defender for IoT

verhindert böswillige Ausweichbewegungen in Richtung empfindlicher Bereiche des Netzwerks. Der Extreme Defender for IoT ermöglicht die Einrichtung von Sicherheitszonen mit einem Fabric Connect-Netzwerk oder über IP-Netzwerke von Drittanbietern.

Sichere Zonen mit Fabric Connect

Der Extreme Defender for IoT ist für den Einsatz mit Extreme Fabric Connect optimiert, der Campus Fabric-Lösung von Extreme. Einer der Hauptvorteile von Fabric Connect ist seine Fähigkeit, schnell und einfach eine große Anzahl sicherer Zonen zu erstellen. Statt einer komplexen Konfiguration können diese Sicherheitszonen sehr schnell und einfach an den Netzwerkrändern eingesetzt werden. Darüber hinaus wird in einer Fabric Connect-Infrastruktur ein Auto-Attach-Protokoll namens Fabric Attach auf dem Defender-Adapter und dem AP3912 unterstützt. Dies ermöglicht eine dynamische und automatisierte Ankopplung von Endpunkten sowie eine vollständige Automatisierung der Netzwerkdienste, so dass die End-to-End-Sicherheitszone dynamisch erstellt wird, während das Gerät „onboarded“ wird.

Sichere Zonen über Netzwerke von Drittanbietern

Der Extreme Defender for IoT kann auch in traditionellen IP-basierten Netzwerken (Extreme oder Drittanbieter) eingesetzt werden, so dass Kunden IoT-Geräte sicher einsetzen können, ohne wesentliche Änderungen am Netzwerk vornehmen zu müssen. Die sicheren Zonen oder Netzwerksegmente werden mittels sicherer IPSec-Tunnel eingerichtet, die den IoT-Verkehr vom Gerät über die gesamte Infrastruktur bis zur Defender-Anwendung auf der ExtremeCloud Appliance segmentieren.

Automatisiertes Onboarding und Inventarisierung

Zusätzlich zur Sicherung jedes IoT-Gerätes kann die bloße Anzahl der IoT-Geräte, die sowohl „onboarded“ als auch zentral verfolgt werden müssen, eine enorme Belastung für IT-Teams darstellen, die schon am Limit arbeiten. Der Extreme Defender for IoT vereinfacht die Sicherung, das Onboarding und die Verlagerung dieser Geräte und ermöglicht es Unternehmen, wertvolle Betriebskosten zu sparen.

Die Defender-Anwendung bietet:

- Eine optimierte Benutzeroberfläche, die zur Unterstützung gängiger Arbeitsabläufe entwickelt wurde; dies erleichtert es nicht-technischem Personal und anderen Personen außerhalb der IT-Organisation, ihre Geräte problemlos einzubinden und mit Profilen zu belegen.
- Einfaches Onboarding der Geräte durch QR-Codes und Upload-Funktionen, die die Geräte in einem zentralen Inventarisierungssystem registrieren.
- Statusanzeige aller IoT-Geräte über die ihnen zugeordneten APs/Adapter in allen Abteilungen auf einen Blick; diese Anzeige enthält auch Standort- und Roaming-Informationen für die Bestandsverfolgung.
- Eine anpassbare Dashboard-Ansicht der Geräte-Statistiken, die für die Ermittlung der IoT-Geräteauslastung und der Verfügbarkeitsdaten nützlich sein können.

Laut Untersuchungen von Ponemon Institute and Shared Assessments verfügen nur 12% der Unternehmen über eine zentrale Inventarisierung aller Geräte, die mit dem Netzwerk verbunden sind[6]. Mit der Defender-Anwendung ist diese zentrale Ansicht nun unabhängig davon möglich, wo sich das IoT-Gerät befindet und welche Abteilung (Einrichtungen, Klinikärzte, IT usw.) es besitzt und verwaltet.

[6]Artikel in TechRepublic: „97% of risk pros say IoT cyberattack would be catastrophic for their business“ – März, 2018

Zusammenfassung: IoT – von der Vision zur Realität mit Extreme Networks

Wenn Unternehmen immer mehr neue Geräte anschließen und IoT einsetzen, kann die Extreme Defender for IoT-Lösung von Extreme Networks in folgenden Bereichen dabei helfen:

IoT-Geräte mit einem mehrschichtigen Ansatz abzusichern, bestehend aus sicherem Onboarding und Anbindung, Verkehrsüberwachung und -filterung sowie der Schaffung von End-to-End-Sicherheitszonen zur Isolierung und zum Schutz von Gerätegruppen und zur deutlichen Reduzierung der Angriffsfläche.

Eine höhere Effizienz und niedrigere Kosten zu erzielen– mit einem automatisierten Ansatz zur Erstellung von Richtlinien (über den Lernmodus) und mit einer einfachen Benutzeroberfläche sowie einem kleinen Inline-Gerät, das es Ihren nicht-technischen Mitarbeitern ermöglicht, ihre eigenen Geräte zu „onboarden“ und zu verschieben, sobald das Profil erstellt wurde. Da die Lösung über jede beliebige Netzwerkinfrastruktur hinweg funktioniert, können die IoT-Sicherheitsanforderungen ohne zeitaufwändige und teure Netzwerkaktualisierung erfüllt werden.

Weitere Informationen zum Extreme Defender for IoT erhalten Sie von Ihrem Vertriebspartner oder Ihrem Ansprechpartner bei Extreme Networks.

Bestellinformationen

Überblick über die Bestelloptionen für die Extreme Defender for IoT-Lösung:

- Die Aktivierung der Defender-Anwendung erfordert die Bestellung einer Lizenz für die Anzahl der unterstützten zu schützenden Geräte sowie die Bestellung des gewünschten Service- und Abonnement-Angebots.
- Die ExtremeCloud Appliance muss ebenfalls im Voraus oder in Verbindung mit der Extreme Defender for IoT-Lösung bestellt werden.
- Die entsprechende Zugangshardware („Defender Adapter“ (SA20 1) oder AP3912)) muss zusammen mit der Lösung bestellt werden.

Bestellinformationen für die Extreme Defender for IoT-Hardware

Bestellnummer	Produktbeschreibung
39505	Defender Adapter SA201 (vor Bestellung Verfügbarkeit für Ihr Land prüfen) mit zwei 10/100/1000 BASE-T Ports (1 Netzwerk-Port und 1 Geräte-Port), Stromversorgung über POE/ POE+, optionales Netzteil kann separat bestellt werden.
31025	WS-AP3912i-FCC (USA, Puerto Rico, Colombia) Montageelement Dual Radio 802.11ac/abgn, Wave 2, 2x2:2 MIMO Indoor Access Point mit vier internen Antennen-Arrays und einer integrierten BTLE/802.15.4 Funkverbindung.
31026	WS-AP3912i-ROW (vor Bestellung Verfügbarkeit für Ihr Land prüfen) Montageelement Dual Radio 802.11ac/abgn Wave 2, 2x2:2 MIMO Indoor Access Point mit vier internen Antennen-Arrays und einer integrierten BTLE/ 802.15.4 Funkverbindung.

Einzelheiten dazu finden Sie in den dazugehörigen Datenblättern für den Defender Adapter und den AP3912.

Bestellinformationen für die Defender-Anwendung

Bestellnummer	Produktbeschreibung
39521	Defender-Lizenz für 10 geschützte Endgeräte
39522	Defender-Lizenz für 100 geschützte Endgeräte
39523	Defender-Lizenz für 1.000 geschützte Endgeräte
39524	Defender-Lizenz für 5.000 geschützte Endgeräte
39525	Defender-Lizenz für 10.000 geschützte Endgeräte

Hinweis: Die maximale Anzahl geschützter Endgeräte der Anwendung hängt von der Systemkapazität der installierten ExtremeCloud Appliance ab. Einzelheiten dazu finden Sie im dazugehörigen Datenblatt für die ExtremeCloud Appliance.

Bestellinformationen für Software-Abonnements und Services

Service-Bestellnummer	Servicebezeichnung
97003-39521	ExtremeWorks Subscription-Service für 10 geschützte Endgeräte
95603-39521	PartnerWorks Plus Subscription-Service für 10 geschützte Endgeräte
97003-39522	ExtremeWorks Subscription-Service für 100 geschützte Endgeräte
95603-39522	PartnerWorks Plus Subscription-Service für 100 geschützte Endgeräte
97003-39523	ExtremeWorks Subscription-Service für 1.000 geschützte Endgeräte
95603-39523	PartnerWorks Plus Subscription-Service für 1.000 geschützte Endgeräte
97003-39524	ExtremeWorks Subscription-Service für 5.000 geschützte Endgeräte
95603-39524	PartnerWorks Plus Subscription-Service für 5.000 geschützte Endgeräte
97003-39525	ExtremeWorks Subscription-Service für 10.000 geschützte Endgeräte
95603-39525	PartnerWorks Plus Subscription-Service für 10.000 geschützte Endgeräte
98000-39505	ExtremeWorks Premier TAC & OS für den Defender Adapter (SA201)
98001-39505	ExtremeWorks Premier Extended Warranty für den Defender Adapter (SA201)
98004-39505	ExtremeWorks Premier Next Business Day Advanced Hardware Replacement für den Defender Adapter (SA201)
98007-39505	ExtremeWorks Premier 4-Stunden Advanced Hardware Replacement für den Defender Adapter (SA201)
98008-39505	ExtremeWorks Premier 4-Stunden On-site Delivery für den Defender Adapter (SA201)
98011-39505	ExtremeWorks Premier Next Business Day On-site Delivery für den Defender Adapter (SA201)
98003-39521	ExtremeWorks Premier Subscription-Service für 10 geschützte Endgeräte
98003-39522	ExtremeWorks Premier Subscription-Service für 100 geschützte Endgeräte
98003-39523	ExtremeWorks Premier Subscription-Service für 1.000 geschützte Endgeräte
98003-39524	ExtremeWorks Premier Subscription-Service für 5.000 geschützte Endgeräte
98003-39525	ExtremeWorks Premier Subscription-Service für 10.000 geschützte Endgeräte

Extreme™
Customer-Driven Networking

https://de.extremenetworks.com/kontakt/