Extreme™
Customer-Driven Networking

Solution Brief

Extreme Defender for IoT

Simple Security for Your Critical Endpoints

The Internet of Things (IoT) is having a profound impact in every industry. According to survey data, 63% IT organizations have witnessed a 50% increase in the number of endpoints that are connecting to the network[1]. By 2020, Gartner estimates that 20.4 billion connected things will be in use by organizations worldwide[1]. Although IoT growth is really being driven by 3 main subsectors: Smart Cities (26%), Industrial IoT (24%) and Connected Health (20%)[2], there really isn't a single vertical industry that isn't experiencing growth in the number of end points that are connecting to the network.

Although IoT holds great promise in increasing efficiencies, driving down costs and enhancing customer service, these devices also widen the network attack surface, creating more routes to entry for would be hackers.

Consider the Statistics:

- Nearly 20% of organizations have observed at least one IoT-based attack in the past three years[3].
- IoT attacks increased 600% between 2016 and 2017[4]

The Challenge of Implementing IoT Security

Although the threat of attack is very real, there are many factors that make securing specific IoT devices a challenge. First, just the sheer number and diversity of endpoints, many of which might not be within IT's direct control. They might be owned by the facilitaties management team, operational teams or clinician staff within a hospital. Furthermore, many of these devices were not originally designed to be Internet-connected and lack embedded security.

Some of the Specific Security Challenges of Connected Devices Include:

- May contain older, non-supported operating systems such as Windows 95/98 and can no longer be patched.
- Lack of personal firewall, anti-virus and encryption on many devices.

[1] "Internet of Things. Preventing the next wave of Ransomware Attacks" (article) March, 2018
[2] "A round up of 2018 Enterprise Internet of Things forecasts and market estimates" (article in Enterprise CIO). Jan 2018
[3] Gartner Research Report: "IoT Solutions can't be trusted and must be separated from the enterprise networks to reduce risk." May 2018
[4] "As Internet of Things attacks increase 600% in one year, businesses need to rethink their security" (article in TechRepublic). March 2018

- In some industries (ie. healthcare) devices must go through an expensive, time consuming recertification process to remain in compliance if a change is made to the device (ie. security patch).
- In many cases, devices connecting to the wired network are more exposed. Specific issues include aging edge switches with feature disparity across the network.

"IoT security is becoming a major concern for our organization. At the same time, we are concerned that the nature of securing so many devices will be complex and expensive. The Extreme Defender for IoT solution will enhance our IoT security toolset without further complexity."

Ben Vickers, Director of IT, Promedica

Securing Devices with Extreme Defender for IoT

Extreme Defender for IoT is a unique, award-winning solution, that delivers security for end points which have limited or even no embedded security capabilities. It is especially targeted to aging wired devices, that need to roam around a room, a building or even a campus.

It complements a customer's existing security infrastructure by adding in-line defense directly at the IoT device itself. And it can be deployed over any network infrastructure to enable secure IoT management without significant network changes.

Due to its unique ability to solve a pressing need in the securityspace, under its former name, Extreme Surge, Extreme Defender for IoT won many high-profile industry awards including being named a 2017 Award Gold Winner by the internationally renowned Edison Awards™ in the category of cybersecurity.

Extreme Defender Components

Extreme Defender consists of the following components:

- **Defender Application**: A user friendly application that enables the centralized creation of security profiles for groups of IoT devices. Once profiles are created, non-technical staff can securely on-board and move their devices. They can also monitor and track their assets through intuitive dashboards and centralized inventory.
- **Defender Adapter (SA201) and the ExtremeWireless 3912i Indoor Access Point**: Provides a proxy service for the Defender application to both manage and secure IoT devices. Their specific role is to monitor traffic flows – with full Layer 2 to 7 visibility – to ensure that the device is operating according to its expected behavior. The Defender Adapter is a single port device that sits between the network and the IoT device providing in-line defense. The AP3912 is a multi-port unit that supports multiple devices in a single room.
- **ExtremeCloud™ Appliance**: Available as a hardware based or virtual-appliance, the ExtremeCloud Appliance, is a premise-based solution that provides cloud-like management and controller functionality for Extreme Smart OmniEdge™ (wired and wireless) solutions. With a full suite of rich APIs to customize applications, it is the supported platform for the Defender Application.

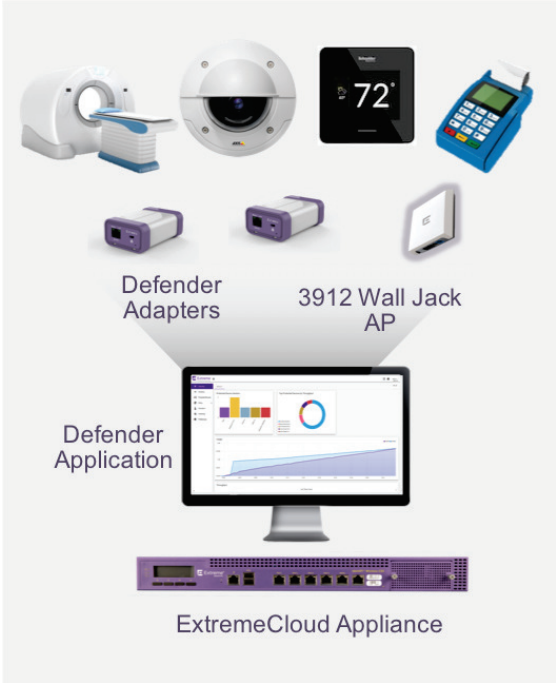

Figure 1: Extreme Defender for IoT

How Defender Secures Devices

Defender for IoT secures connected devices in a couple of ways:

- Applies profiles directly at the IoT device that ensure that the device operates according to expected behavior
- Controls IoT device attachment and access to the network
- Isolates groups of IoT devices into secure zones or network segments

According to Gartner Research, “IoT devices cannot be trusted and must be separated from the network to reduce risk." Defender for IoT provides a simple and automated approach to creating isolated segments for devices—and then provides further defense in-depth by filtering traffic flows to and from the devices. The next four sections describe the security functions of Defender for IoT.

Application of Centralized Profiles

Securing IoT devices starts with the creation of whitelist profiles. These profiles are created, managed and cataloged on the Defender Application. A single profile is typically created for each device type (i.e. IP security cameras) and then applied to all the devices that fit into that category. The profile provides a list of authorized devices and traffic flows to limit what the IoT device receives and transmits, as well as who or what the device can communicate with. A completed profile contains a group access profile with security rules and network attachment settings.

The profiles are then pushed out to the Defender Adapter and/or the AP3912 which police and monitor the traffic with full Layer 2 to 7 visibility. It ensures that traffic both to and from the IoT device is restricted to the rules contained within the profile. In doing so, the IoT device is protected and also prevented from launching an attack itself.

Creation of Profiles with Ease

Because traffic profiles can be complex to manually create, the Defender for IoT solution automates this process using an “Auto Policy Generator." The Defender for IoT solution enables adapters to mirror traffic to the Defender Application where the Auto Policy Generator can create a traffic profile for the IoT device. The IoT device operates normally with the Defender Application cataloging the traffic so the solution can learn what the expected normal behavior of the device is. When adequate time has passed in this mode (dependent on IoT device operation), mirroring can be stopped and the resultant traffic profile can be applied to the IoT device to secure its communication to the network.

Secure Device Mobility Without IT Involvement

With Defender, wired devices can be automatically moved from one network port to another. If a device needs to be relocated, a technician can simply unplug the Adapter from a room wall jack port, move the device and Adapter to a new location and plug the Adapter into a new port.

When the Adapter is unplugged, it loses its profile and network services are disabled on the old switch port. When the Adapter is reconnected, it contacts the ExtremeCloud Appliance to retrieve its profile and requests the services to be provisioned on the new port. Within a couple of minutes, the IoT device is functioning in its new location and the move has been completed quickly and safely, without network IT involvement.

Network Segmentation/Secure Zones

In addition to the policies, Defender also enables like devices to be placed in their own isolated secure zone or clinical segment. According to Gartner research only 5% of IoT devices deployed today are virtually segmented; however, by 2021 60% will be[5]. Creating secure zones reduces the attack surface and mitigates ill-intended lateral movement toward sensitive areas of the network.

Defender enables the creation of secure zones with a Fabric Connect network or over third-party IP Networks.

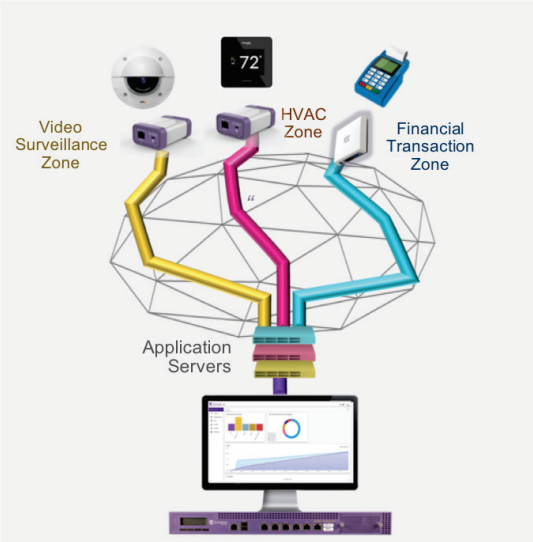

Figure 2: Clinical Segmentation and Secure Zones with Defender for IoT

Secure Zones with Fabric Connect

Extreme Defender is optimized for use with Extreme Fabric Connect, Extreme’s Campus Fabric solution. One of the main benefits of Fabric Connect is its ability to quickly and easily create secure zones at scale. Rather than complex configuration, these secure zones can be deployed very quickly and easily at the network edges. In addition, on a Fabric Connect infrastructure, an auto-attach protocol called Fabric Attach is supported on the Defender Adapter and the AP3912. This enables dynamic automatic attachment of end points as well as full network service automation so that the end to end secure zone is created dynamically as the device is on-boarded.

5. Gartner Research report: “IoT Solutions Can't Be Trusted and Must Be Separated from the Enterprise Network to Reduce Risk” – May 2018.

Secure Zones Over Third Party Networks

Extreme Defender can also be deployed on traditional IP-based networks (Extreme and third party), enabling customers to securely deploy IoT without having to make any significant network changes. The secure zones or network segments are set up using secure IPSec tunnels that segment IoT traffic from the device, across the infrastructure, to the Defender Application on the ExtremeCloud Appliance.

Automated Onboarding and Inventory Management

In addition to securing each IoT device, the sheer number of IoT devices that need to be onboarded, as well centrally tracked, can be a huge burden to already taxed IT teams. Extreme Defender simplifies securing, onboarding, and moving these devices, enabling companies to save valuable operational costs.

Specifically, the Defender Application:

- Has a streamlined User Interface that has been created to support common workflows. This makes it easy for non-technical staff and others outside the IT organization to easily on-board and apply profiles to their devices.
- Simple device on-boarding through QR codes and uploading capabilities that register devices to a centralized inventory tracking system.
- Single pane-of-glass status display of all IoT devices via their assigned APs /Adapters across all departments. It also includes location and roaming information for asset tracking purposes.
- Provides a customizable dashboard view of statistics for devices which can be useful for determining IoT device utilization and availability data.

According to research, conducted by Ponemon Institute and Shared Assessments, only 12% of organizations have a centralized inventory of all the devices connecting to the network[6]. With the Defender Application, this centralized view is now possible regardless of where the IoT device resides and what department (facilities, clinician, IT, etc.) owns and manages it.

Summary: Realize the Vision of IoT with Extreme Networks

As organizations continue to connect new devices and embrace IoT, the Extreme Networks Defender for IoT solution can help:

Secure IoT devices with a multi-layered approach consisting of secure on-boarding and attachment, traffic monitoring and filtering and the creation of end to end secure zones for isolation and protection of groups of devices and to significantly reduce the attack surface.

Achieve Greater Efficiency and Lower Costs with an automated approach to creating policies (via the learning mode) and with a simple User-Interface and small in-line device which will enable your non-technical staff to on-board and move their own devices once the profile has been created. The ability for the solution to work over any network infrastructure means that IoT security needs can be addressed without a time consuming and expensive network refresh.

For more information on Extreme Defender for IoT, please contact your Extreme representative.

Ordering Information

Ordering overview for the Defender for IoT solution:

- Activation of the Defender Application requires ordering a license for the number of protected devices being supported, as well as, ordering the desired service and subscription offer.
- The ExtremeCloud Appliance must also be ordered in advance or in conjunction with the Extreme Defender for IoT solution.
- The appropriate access hardware (the Defender Adapter (SA201) or the AP3912) must be ordered with the solution.

[6] Article TechRepublic: 97% of risk pros say IoT cyberattack would be catastrophic for their business – March, 2018

Ordering Information for the Defender for IoT Hardware

Part Number	Product Description
39505	Defender Adapter SA201 (Verify country availability before ordering) with two 10/100/1000 BASE-T ports (1 network port and 1 device port), power from POE/POE+, optional power adapter sold separately.
31025	WS-AP3912i-FCC (US, Puerto Rico, Colombia) Wall-plate Dual Radio 802.11ac/abgn, Wave 2, 2x2:2 MIMO indoor access point with four internal antenna arrays and an integrated BTLE/802.15.4 radio.
31026	WS-AP3912i-ROW (Verify country availability before ordering) Wall-plate Dual Radio 802.11ac/abgn Wave 2, 2x2:2 MIMO indoor access point with four internal antenna arrays and an integrated BTLE/802.15.4 radio.

Refer to the corresponding Defender Adapter and the AP3912 Data Sheets for details

Ordering Details for the Defender Application

Part Number	Product Description
39521	Defender License for 10 Protected End Systems
39522	Defender License for 100 Protected End Systems
39523	Defender License for 1,000 Protected End Systems
39524	Defender License for 5,000 Protected End Systems
39525	Defender License for 10,000 Protected End Systems

Note: Max application protected device capacity defined by the system capacity of the installed ExtremeCloud Appliance.
Please refer to ExtremeCloud Appliance datasheet for details.

Ordering Details for Software Subscription and Services

Service Part Number	Service Name
97003-39521	ExtremeWorks Subscription Service for 10 Protected End Systems
95603-39521	PartnerWorks Plus Subscription Service for 10 Protected End Systems
97003-39522	ExtremeWorks Subscription Service for 100 Protected End Systems
95603-39522	PartnerWorks Plus Subscription Service for 100 Protected End Systems
97003-39523	ExtremeWorks Subscription Service for 1,000 Protected End Systems
95603-39523	PartnerWorks Plus Subscription Service for 1,000 Protected End Systems
97003-39524	ExtremeWorks Subscription Service for 5,000 Protected End Systems
95603-39524	PartnerWorks Plus Subscription Service for 5,000 Protected End Systems
97003-39525	ExtremeWorks Subscription Service for 10,000 Protected End Systems
95603-39525	PartnerWorks Plus Subscription Service for 10,000 Protected End Systems
98000-39505	ExtremeWorks Premier TAC & OS for the Defender Adapter (SA201)
98001-39505	ExtremeWorks Premier Extended Warranty for the Defender Adapter (SA201)
98004-39505	ExtremeWorks Premier Next Business Day Advanced Hardware Replacement for the Defender Adapter (SA201)
98007-39505	ExtremeWorks Premier 4-hour Advanced Hardware Replacement for the Defender Adapter (SA201)
98008-39505	ExtremeWorks Premier 4-hour On-site Delivery for the Defender Adapter (SA201)
98011-39505	ExtremeWorks Premier Next Business Day On-site Delivery for the Defender Adapter (SA201)
98003-39521	ExtremeWorks Premier Subscription Service for 10 Protected End Systems
98003-39522	ExtremeWorks Premier Subscription Service for 100 Protected End Systems
98003-39523	ExtremeWorks Premier Subscription Service for 1,000 Protected End Systems
98003-39524	ExtremeWorks Premier Subscription Service for 5,000 Protected End Systems
98003-39525	ExtremeWorks Premier Subscription Service for 10,000 Protected End Systems

Extreme™
Customer-Driven Networking

http://www.extremenetworks.com/contact