Extreme™
Customer-Driven Networking

Solution Brief

Extreme Defender for IoT

Securing Medical and other Connected Devices with Ease

The Internet of Things (IoT) is having a profound impact in every industry and healthcare is no exception. From remote monitoring systems to smart sensors to medical device integration, connected technologies have become more pervasive in healthcare. And this is for good reason. IoT has the potential to deliver better patient care, improve operational efficiency and drive down healthcare costs. However, at the same time, IoT poses the challenge of needing new requirements for cybersecurity and patient data privacy.

Consider the statistics:

- Nearly 60% of healthcare organizations have introduced IoT devices into their facilities
- 87% of healthcare organizations plan to implement IoT technology by 2019[1]
- Nearly 20% of organizations have observed at least one IoT-based attack in the past three years.

The Challenge of Implementing IoT Security in Healthcare Organizations

Although the threat of attack is very real, there are many factors that make securing specific IoT devices within healthcare a challenge. First, the sheer number of IoT endpoints significantly widens the attack surface – creating more routes to entry to the network for would-be hackers. To make matters worse, some of these devices, in particularly older medical devices, have little embedded security and are therefore vulnerable to hacking.

"Legacy medical devices that were not designed to be internet-accessible are now being connected to the internet as part of healthcare initiatives, increasing risks and the attack surface." Gartner Research 2017: Top Three Security and Privacy Impacts of Connected Medical Devices on Healthcare Providers[2]

1 Internet of Things in Healthcare: What are the possibilities and Challenges? Ray Parker, Jan 2018

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

"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

Some of the specific challenges of older medical devices include:

- May contain older, non-supported operating systems such as Windows 98, 2000, and XP, contain no personal firewall, and are difficult to patch against vulnerabilities.
- May fall outside the control of the IT department and are managed by clinician staff or even the medical device manufacturer itself.
- Many of these devices attach to legacy PCs to perform their function and therefore, widen the attack surface even further.
- Typically, the web consoles used to control the medical devices don't encrypt data.
- Upgrades to medical devices means that they must go through an expensive, time consuming recertification process to remain in compliance. If the clinical function is performing well, there is a "if it isn't broken, why fix it attitude."
- Many of these medical devices (i.e. Infusion Pumps, MRI machines) are mobile and transported as needed around the hospital or clinic.

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; especially medical devices, that need to roam around a room, a building or even a campus.

It works with a customer's existing security infrastructure (NAC, firewalls, etc.) to provide multi-layered security directly at the IoT device. 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 healthcare space, 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:** Provides security management plus traffic and application visibility of connected end devices. Enables the centralized creation of policies that define network and security settings for groups of IT devices.
- **Defender Adapter and the 3912 Wall Jack AP:** Provides a proxy service for the Defender application to both manage and secure IoT devices. Their specific role is to analyze traffic flows – with full Layer 2 to 7 visibility – and identify and block anomalies. The Defender Adapter can be paired 1:1 with a medical/IoT device, supporting full device mobility, whereas, the 3912 Wall Jack AP supports multiple devices in a single room – each with its own profile.
- **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 one: Extreme Defender for IoT

How Defender Secures Devices

Defender for IoT secures medical and other 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 clinical segments

According to Gartner Research, "IoT devices cannot be trusted and must be separated from the network to reduce risk."[3] 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/medical 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. Infusion Pumps) and then applied to all the devices that fit into that category. The profile provides a list of approved 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 3912 Wall Jack AP 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. Any anomalies are blocked and reported to the Defender Application.

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 Extreme Cloud 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.

Clinical Segmentation and 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[4]. 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.

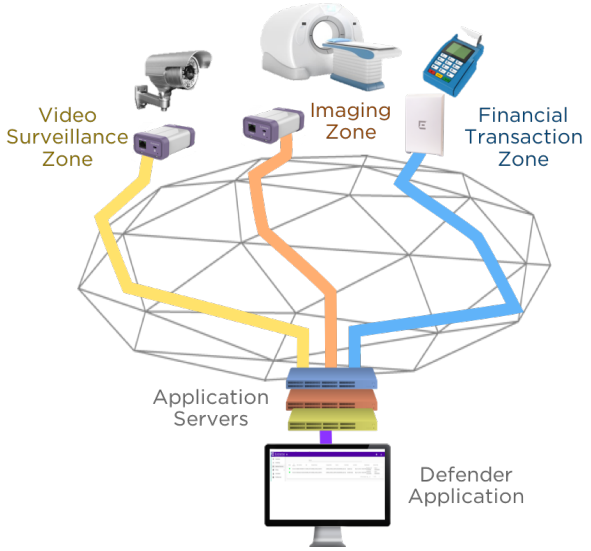

Figure 2: Clinical Segmentation and Secure Zones with Defender for IoT

3,4 Gartner Research report: "IoT Solutions Can't Be Trusted and Must Be Separated from the Enterprise Network to Reduce Risk" – May 2018.

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. This enables dynamic automatic attachment of medical devices and other end points as well as full network service automation so that the end to end secure zone clinical segment is created dynamically as the device is on-boarded.

Secure Zones over Traditional IP 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 clinical 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. In fact, in an independent study, Nemertes research found that the Extreme Defender for IoT solution significantly reduced the costs of onboarding and moving IoT devices.

Specifically, the Defender Application:

- Has a Healthcare Defined User Interface that has been created in conjunction with large healthcare companies to support common healthcare centric workflows. This makes it easy for clinical 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.
- Provides a single pane-of-glass status display of all IoT devices via their assigned APs Adapters across all departments.
- 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[5]. 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 healthcare organizations continue to connect new devices and embrace IoT, the Extreme Networks Defender for IoT solution can help your organization:

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

Achieve Greater Efficiency and Lower Costs with an automated approach to creating policies (via the learning mode) and with a simple healthcare-centric UI which will enable your clinical staff and others to on-board and move their own devices once the profile has been created. The automated creation of secure zones end-to-end with Fabric Connect also isolates and protects devices without the complexity of creating network segments in traditional networks.

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

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