Extreme™ Customer-Driven Networking | SentryWire PACKET CAPTURE PLATFORM

Solution Brief

Highlights

Using simple and scalable network segmentation combined with advanced packet capture and analytics Extreme Networks and SentryWire make managing everywhere-access practical while significantly minimizing damage caused by breaches.

> *"There are two types of organizations in today's world, those that have been hacked and those that just don't know it yet."*

Intro

In the past, the hard edges of the firewall were enough to protect an organization against outside access. Today, supporting Internet of Things (IoT), visitors and remote workers, personal devices, and more have fragmented the traditional network perimeter. These trends make it nearly impossible to determine where the organization's perimeter lies... Is it the branch? The campus edge? A user device? An IoT device? An external cloud? An internal cloud? The answer is that there is no longer a rigid perimeter; there is only an everywhere-perimeter.

Protecting the Enterprise by Providing a Higher Level of Security

Discover Network Breaches and Mitigate Data Loss Faster with Extreme Networks and SentryWire

Securing the Everywhere-Perimeter

Defending an everywhere perimeter calls for fundamentally new capabilities to today's security model. Organizations must find ways to automate the increasingly tedious task of securely onboarding thousands of devices, servers, users, and applications to the network and ensure safe transport of data seamlessly across the network.

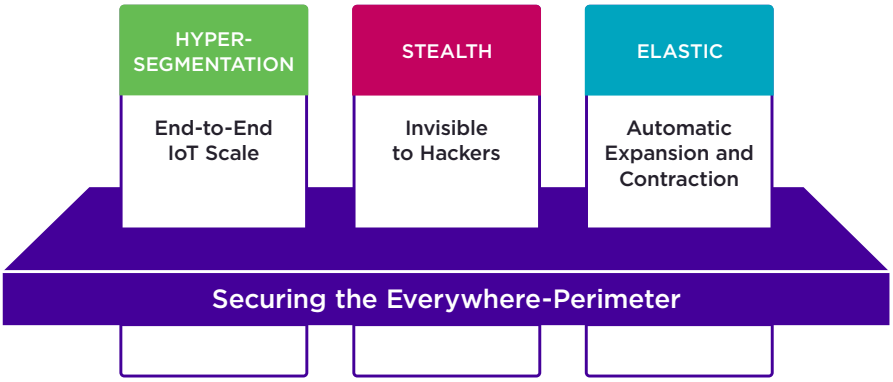

Figure 1: *Fabric Connect Network Virtualization Technology*

Extreme's capabilities do not replace the various security layers employed today, but provides a foundational layer directly at the network to enhance them. This foundational layer is comprised three synergistic capabilities which are inherent within its Fabric Connect network virtualization technology: Hyper-Segmentation, Native Stealth, and Automated Elasticity.

Hyper-Segmentation

Greatly improving upon traditional network segmentation, Extreme's hyper-segmentation offers massive scalability and enables the network to be segmented end to end from the data center to the device. Once Hyper-segments are created organizations experience a reduction in the attack surface, a quarantine function if a segment is breached, simplified anomaly scanning, and greater firewall efficiency.

Native Stealth

Hyper-segmentation is combined with another capability that we call native stealth. What stealth really means is by limiting the visibility of the network we can reduce attack opportunities. With Fabric Connect, because forwarding is based on Ethernet Switched Paths, the network topology is invisible from an IP perspective. Because there are no inherent hop-by-hop IP paths, the network topology cannot be traced using common IP scanning tools.

The other aspect to stealth networking is that in a Fabric Connect network aggregation and core nodes do not have visibility to the service layer. Services are encapsulated at the network edge. What hackers cannot see, they cannot attack!

Automated Elasticity

Extreme has pioneered the concept of network elasticity as an enabler for securing the Everywhere-Perimeter. An elastic hyper-segment automatically stretches services to the edge, only as required and only for the duration of a specific application session. As applications terminate, or end-point devices close down or disconnect, the now-redundant networking services retract from the edge. In deleting network configuration that isn't required anymore, it eliminates any back door entry points to the network.

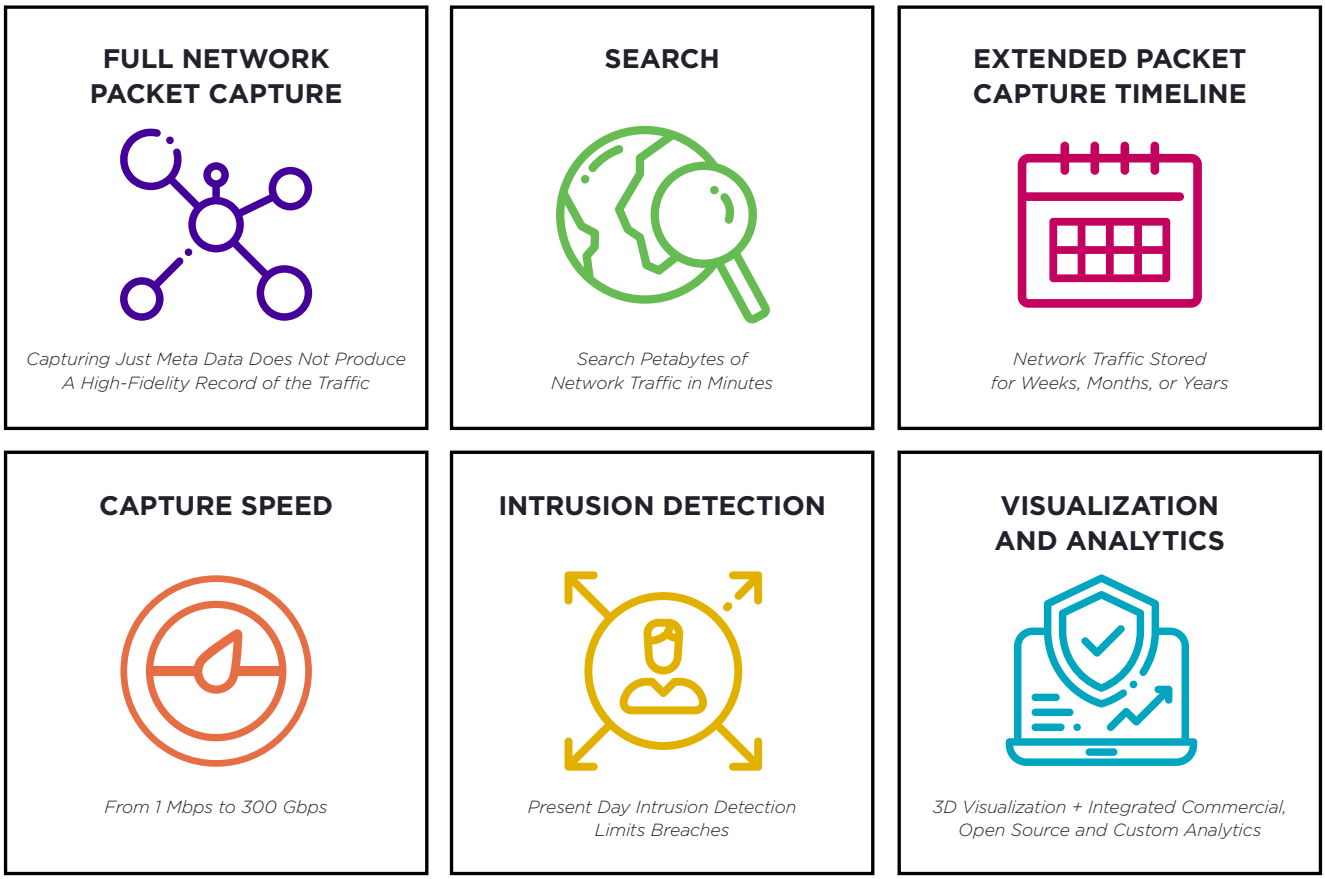

Figure 2: *Situational Awareness — Full Network Packet Capture, Search, Extended Packet Capture Timeline, Capture Speed, Intrusion Detection, Visualization and Analytics.*

A Higher Level of Security Situational Awareness

As a natural complement to Extreme's networking capabilities (hyper-segmentation, stealth and elasticity), SentryWire can quickly analyze, diagnose, solve and even determine when the network has had an attempted breach.

SentryWire is the next generation platform for network packet capture that is based on a unique capture and storage architecture which breaks the performance, scalability and expense barriers of existing frameworks. The system supports capture rates from 1Mbps to 100Gbps, while providing real-time filtering, and allowing retention of network traffic for months and even years at price points that can be as little as 20% of the cost of other systems.

SentryWire allows an extended timeline of traffic to be recorded and analyzed at commodity prices using new or existing analytics. Why is it important to have an extended timeline of packet traffic stored? Because we know on average it takes 240 days to detect certain nation-state intruders in a network and without a high fidelity recording of the network traffic enterprises cannot make an authoritative determination of when intruders got in, how they got in or exactly what data was exfiltrated.

What's Possible with SentryWire

Full Network Packet Capture with Simultaneous IPFix Netflow — Line rates 1Mbps to 100Gbps, lossless and continuous capture and storage of all the network traffic so it can be filtered against known signatures, and, be continuously inspected and analyzed for signatures that materialized after the traffic was filtered, collected and stored. Simultaneously producing netflow feeds to provide more granular situational awareness.

Search — Because of the architecture, searches occur over smaller data stores, dramatically increasing search results, incredibly fast!

Extended Packet Capture Timeline — Forensics for incident response and post-breach activities.

Capture Speed — Capture rates, as well as the rates the packets move around inside the appliance and the cluster nodes, have been architected and engineered to continuously capture, even the burstiest traffic, and can scale to the fastest current market bandwidths (100Gbps).

Intrusion Detection — Includes open source, SNORT and Suricata as IDS options, leveraging the rich intrusion visualization capabilities of many frontends by instrumenting our filtered data flows so that the various frontends have the best data feeds for their intended purposes.

Visualization — Extensive visualization capabilities, pivoting around the Mitre ATT&CK framework and correlating network activities to adversary tactics and their associated techniques, along with a RESTful API connection to existing visualization platforms, allows for exponentially faster hunt results. For log correlation and aggregation visualization solutions, fast and seamless access to our metadata logs.

Analytics — Pre-analytics and real-time filtering, with a RESTful API allowing for integration with existing analytic tools and platforms. SentryWire uses BPF syntax and primitives to filter large amounts of data down to a very manageable size so that customers can run additional tools, such as SIEMs, NextGen Firewalls, eGRC platforms, ELSA, Splunk, and other log correlation tools… to uncover deeper insights regarding potential threats.

Where SentryWire Meets Extreme Fabric

The combined bulletproof solution can quarantine, track, and stop Advanced Persistent Threats (APT's) before any harm is done.

Extreme™
Customer-Driven Networking

http://www.extremenetworks.com/contact / Phone +1-408-579-2800