PROTECTING THE ENTERPRISE

PROVIDING A HIGHER LEVEL OF SECURITY

Discover Network Breaches and Mitigate Data Loss Faster with Avaya and SentryWire

Using software-defined and identity technologies to automate onboarding and access from users, devices, networking nodes, and servers, Avaya makes protecting and managing everywhere-access practical.

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

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.

Securing the Everywhere-Perimeter

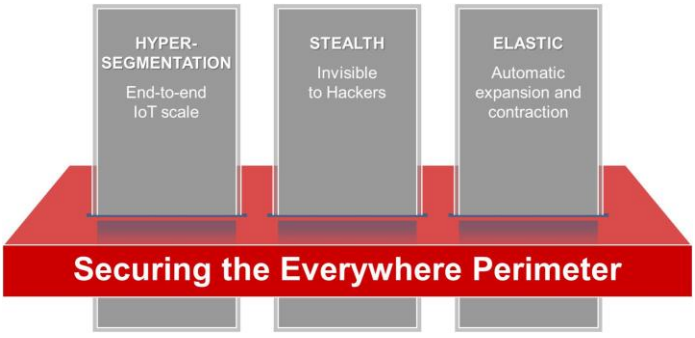
Defending an everywhere perimeter calls for fundamentally new capabilities to today's security model. Organizations must find ways to automate the increasingly tedious task of securely onboarding thousands of devices, servers, users, and applications to the network and ensure safe transport of data seamlessly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

Avaya's capabilities do not replace the various security layers employed today, but provides a foundational layer to enhance them. This foundational layer is comprised three synergistic capabilities:

Hyper-Segmentation: Greatly improving upon traditional segmentation, Avaya's hyper-segmentation scales to millions and seamlessly spans the entire organization from data center to device. Once Hyper-segments are created organizations experience a reduction in the attack surface, a quarantine function if a segment is breached, improvement of anomaly scanning, and greater firewall efficiency.

Native Stealth: Unlike traditional technology, Avaya delivers hyper-segments that are not exposed to the vulnerabilities of Internet Protocol (IP). What this means is that in the event the organization is breached, for example, through the HVAC or an IoT network segment—the hacker is unable to see anything outside that segment, keeping them contained. And because intermediate networking nodes are ignorant of the content, and do not rely upon IP-based reachability, these cannot be used as launch points for exploiting a breach.

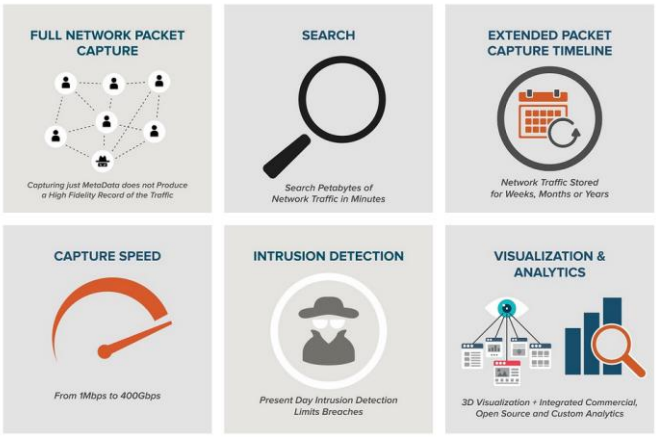
Automated Elasticity: Avaya has pioneered the concept of network elasticity as an enabler for securing the Everywhere-Perimeter. An elastic hyper-segment automatically stretches services to the edge, only as required and only for the duration of a specific application session. As applications terminate, or end-point devices close down or disconnect, the now-redundant networking services retract from the edge. It simplifies deployment of hundreds of segments for tens of thousands of endpoints.



Where SentryWire meets Avaya Fabric: The combined bulletproof solution can quarantine, track and stop Advanced Persistent Threats (APT's) before harm is done.

About Avaya

Avaya is a leading, global provider of customer and team engagement solutions and services available in a variety of flexible on-premise and cloud deployment options. Avaya's fabric-based networking solutions help simplify and accelerate the deployment of business critical applications and services. For more information, please visit **www.avaya.com**.



A higher level of security situational awareness

As a natural complement to Avaya's Stealth architecture, when Advanced Persitent Threats are attempted, SentryWire can quickly analyze, diagnose, solve and even determine when network security has 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 - 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.

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, SNORTand 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 – Bundled open source visualization capabilities, including a 3-D interface that allows engineers and users to isolate anomalous activity, along with a RESTful API connection to existing visualization platforms. 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 Avaya Fabric: The combined solution can quarantine, track and mitigate Advanced Persistent Threats (APT's) before harm is done.

Learn More

To learn more please contact your Avaya account manager, Avaya authorized Partner or visit us at www.avaya.com