HOWARD™
TECHNOLOGY SOLUTIONS

Sentriant™ Security Appliance

For more information visit www.Howard.com or call us at 888.912.3151.

Sentriant detects and mitigates rapidly propagating threats in seconds.

Features

- Defends against threats without interfering with network traffic
- Delivers fast detection with a network of virtual decoys creating an early warning system that fires an alert when a virtual target is contacted
- Allows valid machines to hide in the white noise of virtual decoys
- Isolates attackers and prevents them from communicating with the remainder of the network, allowing mission-critical data to continue to flow normally

Target Applications

- Protection against Denial of Service attacks such as Smurf, Ping of death, Ping sweep, Ping flood, Port sweep, TCP Flood (Syn, Syn-Ack, Ack, Fin, Xmas, Rst), and distributed DoS
- Protection against viruses and worms such as Welchia, Slammer, Blaster and MyDoom
- Protection against Multi-Vector worms, Polymorphic viruses, blended attacks and Day-Zero threats

The Sentriant security appliance is aimed at securing the network interior against rapidly propagating threats, such as virus or worm storms. Designed to protect the network from old and new virus or worm attacks, Sentriant can reduce threat mitigation time down to seconds. This appliance is designed to complement existing perimeter and end-point security solutions. When used in conjunction with Extreme Networks® switches, Sentriant offers unparalleled multi-gigabit security across all enterprise end-points. Sentriant provides effective threat detection and mitigation on interior LANs. Unlike other internal LAN security systems, Sentriant is not an inline device, creates no performance impact to networks, and cannot jeopardize network availability which is especially critical while under attack. The Sentriant security appliance uses behavior-based threat detection methods (no signatures or heuristics) to detect threats—including new threats for which no signatures exist at the time of attack. It also includes a sophisticated early warning system that employs unused IP space to identify threats. Further, Sentriant incorporates a unique patent-pending threat termination technology called Cloaking. Cloaking is an aggressive, protocol-independent, automated threat termination capability that does not use software desktop agents, TCP resets, or switch-dependent VLAN shunting to compartmentalize an infected end-point.

Passive Operation

Sentriant is commonly deployed on a mirror port on a switch, much like a network sniffer. However, unlike sniffers, Sentriant can actively engage, deter and terminate malicious behavior. This deployment model gives system administrators strong security control over the internal network without the latency or single point of failure risks associated with inline devices.

www.howard.com

888.912.3151 general 888.323.3151 tech support 601.399.5060 fax

extreme networks™

Active Deception

Sentriant deceives fingerprinting malware designed to provide precise data about operating systems and application versions present on a network by giving false data about the network topology, making it difficult for it to attack effectively.

Sentriant can also actively engage an attacker during the network reconnaissance phase that generally precedes a threat, dramatically slowing the scanning process and giving administrators time to understand and thwart the attack. During this time, Sentriant will continue to provide false data to the scan itself, slowing or even stopping the attack and providing misleading information to the attacker.

Hyper Detection

On a typical network that uses private IP address space, as much as 80% of IP address space is unassigned. Sentriant uses this asset to identify threats. Sentriant creates a network of "virtual decoys" that populates all or part of the unused IP address space in a broadcast domain.

Since most worms must conduct reconnaissance to spread, there is a high probability that worm activity will hit the virtual decoys in the unused IP address space. Therefore, administrators have a much better chance of being alerted to malicious activity quickly, giving them more time to respond.

Surgical Defense

Sentriant can logically insert itself in between one or more attackers and one or more target devices by redirecting communication streams from attackers to itself. Sentriant can then selectively pass or silently drop packets based on the threat potential, thereby isolating infected computers while permitting all other communication to flow normally on a network. This process occurs at both Layer 2 and Layer 3 of the OSI reference model.

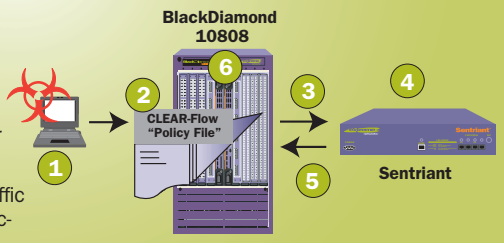
Surgical defense can be invoked either manually by an administrator or automatically by Sentriant when a threat is detected. This represents a departure from previous network security systems by combining the best characteristics of an inline protection technology with the performance and reliability benefits of a passive device.

Deployment Modes

Sentriant is designed to operate seamlessly with perimeter and end-point security products in a stand-alone deployment mode; however, Sentriant offers the greatest benefits operating in an integrated deployment mode (see Figure 1). Sentriant provides a unique and differentiated set of features in the stand-alone and integrated deployment modes (see Figure 2).

At Automated Attack Mitigation in Integrated Deployment Mode

1. An infected source enters the network.
2. BlackDiamond® 10808 static ACLs and CLEAR-Flow rules filter out DoS attacks, determine traffic class as 'suspicious'.
3. Selectively port-mirror traffic to Sentriant for further analysis.
4. Sentriant continues to watch suspicious traffic and uses its internal rules to escalate traffic-class from suspicious to high level alert.



5. Sentriant initiates a dynamic ACL on the BlackDiamond 10808. BlackDiamond 10808 applies the dynamic ACL in real-time and continues to port-mirror suspicious traffic. Sentriant also sends the mitigation action to Extreme Networks EPICenter® network management software.
6. EPICenter works with core and edge switches to enforce the security policy (mitigation action).

Figure 1

Integrated Deployment	Stand-alone Deployment
Sentriant works with Extreme Networks switches running ExtemeWare® XOS™, CLEAR-Flow, and the XML-API for dynamic switch assisted mitigation.	Sentriant works with all vendor switches in broadcast only and fully mirrored deployments.
More effective use of Sentriant resources acting on a reduced load filtered by the CLEAR-Flow security rules engine. Scales a single Sentriant across the whole network.	Without CLEAR-Flow, Sentriant continues to provide effective detection and mitigation of the source of attacks.
Sentriant can dynamically refine filtering criteria using dynamic ACLs to the core switch.	Sentriant filtering criteria are not coupled with the switch ACLs.
Detection and mitigation across a single mirrored port at multi-gigabit line rates with CLEAR-Flow, including 25 Gbps and beyond.	Detection and mitigation across a single mirrored port at 1 Gbps.
Unified Management Structure and CLEAR-Flow enable rich policy features (example: Role, Port, VLAN, QoS—finer granularity for each detection or mitigation action).	Distinct device-level manager (Sentriant Console Manager) and basic Cloaking mitigation.

Figure 2

www.extremenetworks.com email: info@extremenetworks.com

Corporate Headquarters
North America, Canada and Mexico
Extreme Networks, Inc.
3585 Monroe Street,
Santa Clara, CA 95051 USA
Phone +1 408 579 2800

Europe, Middle East, Africa and South America
Phone +31 30 800 5100

Asia Pacific
Phone +852 2517 1123

Japan
Phone +81 3 5842 4011