Sentriant® NG300

Sentriant NG300 protects your network from rapidly propagating Day-Zero threats.

Features

- Defends against threats without interfering with network traffic or lowering network availability
- Delivers fast detection with a network of virtual decoys creating an early warning system that fires an alert when a virtual target is contacted
- Protects IP Telephony devices from targeted attacks
- 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 viruses and worms such as Welchia, Slammer, Blaster and MyDoom
- Protection against Multi-Vector worms, Polymorphic viruses, blended attacks and Day-Zero threats
- Protection against Denial of Service (DoS) 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 for IP Telephony devices from targeted attacks

Sentriant NG300 is a security appliance that secures 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 NG300 can reduce threat mitigation time down to seconds. Sentriant NG300 uses behavior-based threat detection methods (no signatures, no traffic sampling as in sFlow) 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. This appliance is designed to complement existing perimeter and endpoint security solutions. Sentriant NG300 incorporates a unique 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 endpoint. When used in conjunction with Extreme Networks® switches, Sentriant NG300 offers unparalleled multi-gigabit security across all enterprise endpoints. Unlike other internal LAN security systems, Sentriant NG300 is not an inline device, which means that it creates no performance impact to networks, and cannot jeopardize network availability.

Detect Threats Early

On a typical network that uses private IP address space, as much as 80% of IP address space is unassigned. Sentriant NG300 uses this asset to identify threats by creating 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 of malicious activity quickly, giving them more time to respond.

Slow Down Attacks

Sentriant NG300 actively engages an attacker during the network reconnaissance phase that generally precedes a threat and dramatically slows the scanning process. This gives network administrators time to understand and thwart the attack. During this time, Sentriant NG300 will continue to provide false data to the scanning device, slowing or even stopping the attack.

Sentriant NG300 also 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.

Mitigate Threats Precisely

Sentriant NG300 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 NG300 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. 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.

Protect Your Network

Sentriant NG300 continuously monitors all endpoints on your network and protects the network from the following types of threats:

- Viruses/Worms: Zotob, Sasser, Welchia, SQL Slammer, Blaster MyDoom and others
- DoS: IP spoofing, MAC spoofing, smurf, ping of death, ping sweep, ping flood, port sweep, SYN flood, TCP Xmas, Syn/Fin, Null, All Flags
- Day-Zero, Multi-Vector, blended attacks, polymorphic viruses
- Targeted attacks on IP Telephony devices

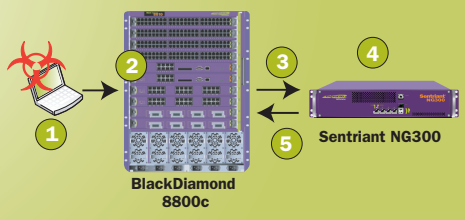
Voice Class Availability

Sentriant NG300 is commonly deployed on a mirror port on a switch, much like a network sniffer. However, unlike sniffers, Sentriant NG300 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.

Deployment Modes

Sentriant NG300 is designed to operate seamlessly with perimeter and endpoint security products in a standalone deployment mode; however, Sentriant NG300 offers the greatest benefits operating in an integrated deployment mode (see Figure 1). Sentriant NG300 provides a unique and differentiated set of features in the standalone and integrated deployment modes (see Figure 2).

1, An infected source enters the network.
2. ExtremeXOS® static ACLs and CLEAR-Flow rules filter out DoS attacks, determine traffic class as 'suspicious'.
3. Selectively port-mirror suspicious traffic to Sentriant NG300 for further analysis.
4. Sentriant NG300 continues to watch suspicious traffic and uses its internal rules to escalate traffic-class from suspicious to high level alert.
5. Sentriant NG300 initiates a dynamic ACL on the ExtremeXOS switch*. The switch applies the dynamic ACL in real-time and continues to port-mirror suspicious traffic.



* Summit® X450a series, BlackDiamond® 8800c series, BlackDiamond 10808, and BlackDiamond 12800 series switches.

5187-01

Figure 1: Automated Attack Mitigation in Integrated Deployment Mode

Integrated Deployment	Standalone Deployment
Sentriant NG300 works with Extreme Networks switches* running ExtremeXOS, CLEAR-Flow and the XML-API for dynamic switch assisted mitigation.	Sentriant NG300 works with all switches from all vendors in broadcast only and fully mirrored modes.
Sentriant NG300 can dynamically refine filtering criteria using dynamic ACLs to the core switch.	Sentriant NG300 filtering criteria are not coupled with the switch ACLs.
Detection and mitigation across a single mirrored port at multi-gigabit line rates using CLEAR-Flow Security Rules Engine.	Detection and mitigation across a single mirrored port at 1 Gbps.

* Summit X450a series, BlackDiamond 8800c series, BlackDiamond 10808, and BlackDiamond 12800 series switches.

Figure 2: Comparison of Integrated and Standalone Deployment Modes

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

Corporate and North America
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