TECHNOLOGY SOLUTION BRIEF

ConSentry Networks' Robust Threat Control

Protecting the LAN from the Inside Out

NAC
Pre-Admission
Visibility
Post-Admission Control
User Access Control
Threat Control

CONSENTRY™
NETWORKS

Contents

Introduction

Companies have long had tools to protect themselves from attacks coming in over the WAN from the Internet. But given the open nature of LANs, the continual migration of laptops between unprotected Internet connections and the LAN, and the changing motivation of attackers, companies now need protection from the inside out. Malware is on the rise, and attacks are getting nastier – more targeted, more sophisticated, and driven by making money.

Viruses and worms are the most common types of attacks, according to research firms such as Gartner, and their danger is increasing as the time between an announced vulnerability and the availability of code to exploit that vulnerability shrinks. These days, just staying current with anti-virus software isn't sufficient protection. And in the case of OS patches intended to eliminate vulnerabilities, IT must test each release to ensure the changes don't break any existing applications, delaying when those security patches go into effect.

Enterprises remain fairly well protected from known attacks coming in from the WAN. Most of the devices architected for the periphery use signatures to detect attacks, so protect only against known attacks. The challenge now is to augment that defense with zero-hour protection deployed pervasively throughout the LAN.

The primary requirement is to combat the effect of worms, often more insidious than viruses because they can propagate without user intervention. As a secondary concern, IT needs to implement protections against non-host devices, such as printers and voice over IP (VoIP) phones, being used as a launch point for attacks. In addition, companies need protection against attacks that take advantage of company-specific configurations, such as a custom application designated to run over a specific L4 port that's opened through a firewall.

Threat control is only part of a total LAN security solution. A comprehensive LAN security solution needs to encompass these additional areas:

- **Network admission control (NAC)** – Controlling admission to the LAN entails controlling both who connects to the network and the machines they use – in other words, user authentication and host posture check. NAC is a good first-line defense, with many host posture check products assessing the status of OS patch levels and host anti-virus software, for example.
- **Visibility** – IT needs the ability to see all LAN traffic on a per-user, per-flow basis up to Layer 7, including details within Layer 7, such as the destination URL in an HTTP session or the file name involved in an FTP download. Comprehensive traffic visibility – into all flows, not just sampled data – is a prerequisite for access control and auditing as well as for granular threat control.
- **User access control** – NAC provides no control over where users go or what resources they access once they're admitted to the network, so IT also needs user-based, post-admission access controls. Specifically, IT needs role-based provisioning, the ability to define rights and permissions – as well as control and enforcement actions – based on a user's role in the organization. Role-based provisioning provides universal access control, ensuring that the correct rights and permissions are applied universally, regardless of a user's access medium or location.

Given the damage malware can wreak on an enterprise, this paper will detail the requirements for a comprehensive LAN-based threat control solution and ConSentry Networks' robust LAN security offering.

LAN-based Threat Control

Today, IT needs a way to control threats that originate on the LAN. Such a solution must detect malware – even malicious code never seen on the network before – and prevent it from propagating. It must alert IT to any unusual traffic and block it, whether it's a zero-hour attack, an attack launched from a printer or VoIP phone, or a rogue user connecting in via an open jack. A LAN security platform must also detect and block other sources of threats, such as invalid protocol headers which might indicate an attack.

Business Impact of Worms

	Today	With ConSentry Networks
Threat awareness	1 hrs	Real Time
Analyze traffic	30 hrs	Real Time
Determine infected users	50 hrs	Real Time
Problem isolation	30 hrs (Turn off ports)	Real Time (Quarantine Application)
Clean system	275 hrs (IT based cleanup)	10 hrs (User-based cleanup)
Total Hours	386 hrs	10 hrs

***Data source:** 6,000-node customer's experience with Nachi worm*

To be effective, a LAN-based threat control solution must meet the following requirements:

- **Operate inline for fast response time.** To ensure that malware is shut down as quickly as possible, a LAN security platform must operate inline. Solutions that operate off-line with mirrored traffic can detect but cannot directly block the malware. Instead, they must command enforcement devices to block the traffic. LAN security demands that the security platform be deployed inline so that detection and blocking can happen in real time.
- **Recognize zero-hour attacks.** Signature-based perimeter and host security solutions protect against known attacks but leave the network vulnerable to newly devised attacks. In addition to known malware, a robust threat control solution must be able to detect new worms for which no signatures yet exist.
- **Contain zero-hour attacks.** Worm propagation can quickly lead to network meltdown. Once a LAN security system has detected a new attack, it must quickly stop it from propagating.
- **Operate close to the host.** Limiting the spread of malware is key to minimizing system and network damage. A LAN security system must operate close to the host to contain an attack at the edges of the network and prevent it from spreading to the core.
- **Granularly block bad traffic.** A LAN security system must support the definition and enforcement of granular control policies. For instance, IT should have the flexibility to define a policy to block all traffic from an infected user or just the infected application. When a worm is detected on the network, the security platform must be able to automatically block it at whatever level of granularity IT has defined. Being able to block the application carrying the worm, for example, but not the entire host allows the user to continue to work and retain network access for remediation.
- **Minimize false positives and tuning.** Signature-based systems operate by looking for specific traffic characteristics, such as byte sequences in the payload or the packet size. However, signature-based systems, even those designed to catch variants of existing worms, cannot detect wholly new worms. In contrast, behavioral-based detection systems are more effective because they recognize the characteristics of malware propagation and can distinguish malicious traffic from normal traffic. As a result, behavioral-based systems can detect both known and unknown worms. Not all behavioral techniques are equal, however – to mitigate the curse of false positives, behavioral algorithms must use effective discriminating metrics and must be engineered to limit false positives.
- **Recognize and block attacks launched from non-user network devices.** Desktops and servers aren't the only vulnerable devices on the LAN. Any device on the network with an OS and IP address, including printers and VoIP phones, can be compromised and used to launch an attack. A LAN security system must be able to detect unusual traffic emanating from these devices and block that traffic.

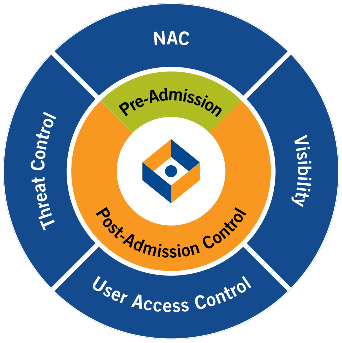
ConSentry Networks' Comprehensive Security Approach

ConSentry Networks delivers threat control as part of a comprehensive set of LAN security services supported by its LANShield product family, which includes the LANShield Switch and the LANShield Controller. This powerful combination of hardware and software operates at LAN speeds to control every user and secure every port on the LAN. At the heart of ConSentry's devices is the LANShield™ silicon architecture. Comprised of a 128-core processor and custom traffic-processing programmable ASICs, this flexible architecture provides stateful deep packet inspection and flow-based traffic tracking and control at gigabit speeds.

The LANShield operating system (OS) drives the silicon and provides traffic and malware controls. It also performs a three-way binding of IP address, MAC address, and user identity, learned during authentication, to support user-based visibility and role-based provisioning. Through the ConSentry InSight command center's graphical interface, IT can set global access policies, get at-a-glance views of network usage and security violations, perform incident response, and define malware policies – the actions the LANShield platform should take when a malware algorithm is triggered. InSight compiles information based on knowledge of user transactions, presenting IT with all activities and access violations tied to username.

The LANShield platforms provide:

- Authentication
- Host posture check



- Zero hour worm protection
- No tuning or maintenance

- Up to Layer 7
- All traffic tied to user

- Role-based provisioning
- Control access to resources

- **Network admission control (NAC)**
  ConSentry supports NAC by leveraging an organization's existing AAA servers and identity stores as well as its host integrity infrastructure. Where applicable, the LANShield device can actively participate in user authentication and host posture checks.

- **Visibility**
  A Layer 2-7 aware device, the LANShield platform provides in-depth packet inspection with full Layer 7 application decode, so it can distinguish between applications using the same L4 port or attempting to mask them using a port number not typically associated with that application. The platform can filter traffic based on packet contents, and by binding a user's name to IP and MAC addresses, the LANShield product family can track LAN traffic by individual users as well as user group, application, host or other resources, protocol, L4 port, transaction, or file access.

- **User access control**
  The LANShield products can apply access controls to everything they see. The platform gives IT the ability to define policies that limit users' access to networked resources based on their role in the organization. This role-based provisioning applies universally, regardless of where or how a user connects to the network.

- **Threat control**
  The LANShield devices protect against both known and unknown threats, providing more accurate detection with blocking at a finer level of granularity than security tools operating at lower layers. Incident reporting is based on knowledge of user transactions, and the LANShield platform can stop traffic on a per-user or per-application basis if malware is detected. Attempts to use printers or VoIP phones as a launch point for attacks are also prevented by limiting the protocols those devices can run and the network destinations they can reach.

ConSentry Controls Threats from the Inside Out

Recognizing the unique challenges local networks pose, ConSentry Networks engineered its LANShield architecture from the ground up to secure the LAN from the inside out. Combining LAN speed, deep-packet inspection and anomaly detection algorithms, the LANShield product family meets all the requirements for a LAN-based threat control solution:

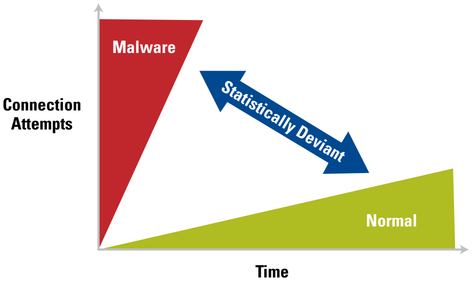
- **Operate inline for fast response time.** Both LANShield products operate inline: The LANShield Switch resides in the wiring closet, and the LANShield Controller sits inline between wiring closet switches and core switches/routers. The LANShield products operate at line-rate within the LAN infrastructure, monitoring, analyzing, and controlling traffic at Layer 7 and above. The LANShield device tracks all flows on the LAN, performing deep packet inspection at the initiation of each flow to ensure the traffic is not malicious and is in compliance with policy. Once a flow is determined to be safe, the LANShield platform forwards it without additional deep inspection. With 10 Gbps of throughput and latency averaging 30 microseconds, the ConSentry platform quickly identifies and automatically responds to attacks, blocking traffic as needed while maintaining LAN-speed throughput.

- **Recognize zero-hour attacks.** Given the prevalence of signature-based security products and their limitations against newly devised attacks, ConSentry focused on developing anomaly detection algorithms capable of recognizing both known and unknown threats. Leveraging the LANShield devices' stateful deep-packet inspection and other visibility capabilities, ConSentry developed application-specific algorithms that distinguish normal behavior from abnormal behavior for individual applications.

Worms designed to propagate quickly – so-called “fast” worms – initiate connection attempts at a high rate. The ConSentry platform tracks connection attempts, by application, and compares those rates, over time, to typical connection attempt rates. The ConSentry algorithm triggers when the connection attempt rate exceeds a threshold that varies based on the elapsed time. Having the threshold be time-dependent limits false positives.

Detecting Fast Worms

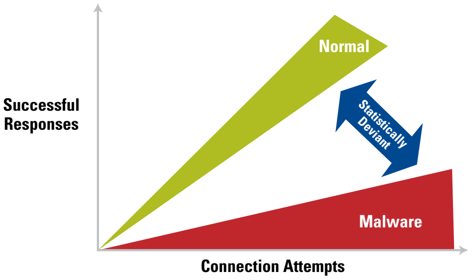
- » Track connection attempts by user and by app
- » Compare against typical rate for each app
- » High rate of attempts over short time = worm



Other worms propagate by attempting to spread to a large number of hosts. These “blind” worms generate random destination IP addresses; because a high percentage of those addresses don’t exist, the rate of failed connection attempts is high. One technique the ConSentry platform uses to detect malware is to compare the ratio of attempted to failed connections, over time and by application. A high failure ratio indicates an attack.

Detecting Blind Worms

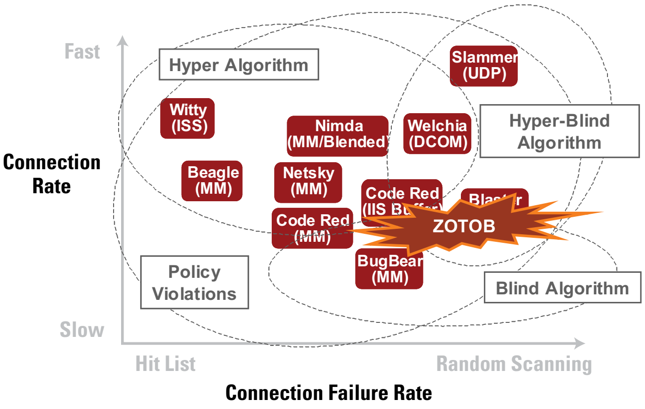
- » Track connection attempts and responses by user
- » Compare attempts to successful responses
- » High ratio of failed vs. attempted = worm



- » **Contain zero-hour attacks.** Once the LANShield platform detects a new worm, it quickly stops it from propagating. This quick action, along with the location close to user, makes the LANShield devices effective for stopping worm outbreaks and preventing network meltdown. In addition, if a company becomes the victim of a targeted attack, such as one taking advantage of a known opening through a firewall, the LANShield platform can be configured to block all but the accepted application associated with that L4 port.

Protection Against New Worms

- » Contain worms without signatures
- » Automatic response and blocking
- » No tuning, minimal false positives

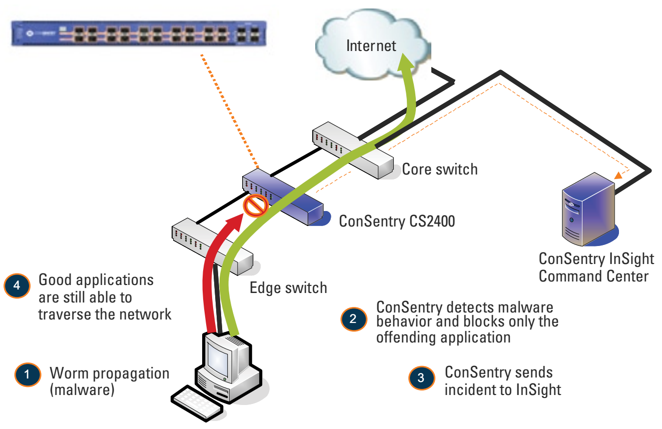


- » **Operate close to the host.** The LANShield devices’ location close to the user gives it visibility into and control over all user traffic. This location is critical to worm identification, because the device needs to see connection rates and connection attempts. This network location is also critical for quickly containing worm outbreaks. Firewalls and IDS/IPS devices at the perimeter, in contrast, cannot track individual application flows and have no visibility into LAN traffic.

- » **Granularly block bad traffic.** With its Layer 7+ visibility into all traffic flows, the LANShield platform can block worm traffic at a granular level. Using the InSight command center, IT can choose to receive alerts when abnormal traffic is detected or have policies for the LANShield device to take automatic action following worm detection.

  Specifically, IT can set the LANShield platform to block all traffic from an infected host or user or block just the malicious application. For example, if the LANShield device detects a worm in an HTTP flow, IT has the option to turn off HTTP for the infected host or turn off all traffic from the infected host.

  The ConSentry products can also look at data about multiple flows to enact malware policy. For example, if a series of applications on a host becomes infected – for example, FTP, then file sharing (CIFS), then SIP for VoIP calls – then the LANShield device will shut down all traffic from that host.



Worm Containment – Granular Block

Internet
Core switch
ConSentry CS2400
ConSentry InSight
Command Center
Edge switch
4 Good applications are still able to traverse the network
2 ConSentry detects malware behavior and blocks only the offending application
1 Worm propagation (malware)
3 ConSentry sends incident to InSight

- **Minimize false positives and tuning.** Because of their highly discriminating nature, taking elapsed time into account, the ConSentry anomaly detection algorithms minimize false positives. They also enable IT to avoid the tuning and maintenance required for signature-based systems.

- **Recognize and block attacks launched from non-user network devices.** IT can leverage theLANShield devices' visibility and control capabilities to protect non-host devices, such as printers and VoIP phones, from being used to launch an internal attack. For example, IT can implement policies that restrict the protocols those devices run or limit the destinations they are allowed to reach. That is, IT could configure printers to use only LPR (line printer remote) or HTTP protocols and set a policy within the LANShield platform to block any other protocol coming from a printer. Similarly, IT could configure the ConSentry platform to allow VoIP phones to use only SIP (Session Initiation Protocol) and to allow traffic from VoIP phones to reach only the call manager platform. Traffic to any other destination or running over any other protocol would be dropped.

The Evolving Threat Landscape

While viruses and worms are the primary threats that enterprises face today, the security landscape is always evolving. Unlike attacks by early hackers, who were motivated by a chance at notoriety, today's attacks are motivated by the potential to make money. The individuals and groups developing these attacks are more aggressive, using tools that allow them to quickly build bots and other malware that exploit security holes at an accelerating rate – making [zero-hour attacks more targeted and more dangerous. For example, software agents in the form of bots and key loggers can give hackers access to critical data or control over systems. So-called "botnets," a collection of bots installed and controlled by a hacker, can be used to launch a distributed denial of service attack, for example.

With its flexible, programmable LANShield architecture, ConSentry is well positioned to address evolving threats. ConSentry can quickly deploy new malware functionality via a simple software upgrade for the LANShield product family, enabling IT to combat emerging threats without having to overhaul the security infrastructure.

By operating from the inside out, the LANShield product family protects business information and therefore business operations, reducing risk exposure, improving business continuity, and helping organizations comply with governmental regulations. Leveraging existing infrastructure, ConSentry provides robust threat control in a cost-effective, high-performance, transparent fashion. Only ConSentry offers a comprehensive LAN security platform that brings together network admission control, full LAN visibility, user access control, and threat control in a single device, allowing organizations to secure the LAN as never before.

About ConSentry Networks

ConSentry Networks delivers comprehensive LAN security, enabling businesses to protect their corporate assets, ensure continuity of operations, and dramatically reduce the risk of security breaches. ConSentry enables this pervasive security while lowering IT's cost of operations through its flexible, high-performance platform powered by ground-breaking custom silicon and revolutionary LAN security software. Backed by blue-chip venture capital firms that include Accel Partners, INVESCO Private Capital, and Sequoia Capital, ConSentry is headquartered in Milpitas, California. For more information, visit the company's web site at www.consentry.com.

Corporate Headquarters

ConSentry Networks
1690 McCandless Drive
Milpitas CA 95035

Tel: 408-956-2100
Toll-Free: 866-841-9100
Fax: 408-956-2199
Email: sales@consentry.com

EMEA Office

ConSentry Networks
Lyoner Strasse 26 D-60528
Frankfurt Germany

Tel: +49 69 677 33 422
Fax: +49 69 677 33 200