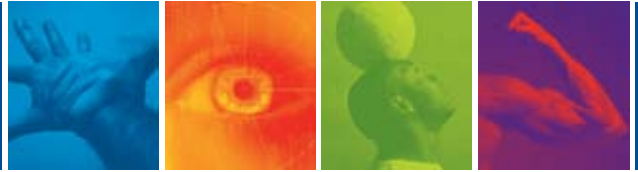


# ConSentry® LANShield™ Controller



## Cost-effective, Transparent Deployment



CS2400 LANShield Controller



CS1000 LANShield Controller

ConSentry Networks enables enterprises to secure their LANs. With ConSentry's purpose-built devices based on custom silicon, IT can control who is allowed onto the LAN, restrict what users can do on the LAN, and prevent threats from disrupting network services or compromising data.

ConSentry has developed the LANShield Controller to make it easy for IT to embed security directly into the LAN infrastructure. The Controller provides the full set of capabilities needed to protect enterprise assets:

- Network Admission Control (NAC) – authentication and posture check to control who can enter the LAN
- visibility – incident- and exception-based information at Layer 7, including attributes such as file name, tied back to the user
- identity-based control – role-based provisioning to control user activities on the LAN
- threat control – detect and block propagation of worms and other malware to prevent network meltdown

The LANShield Controller works with existing LAN infrastructure and authentication databases to provide these control capabilities.

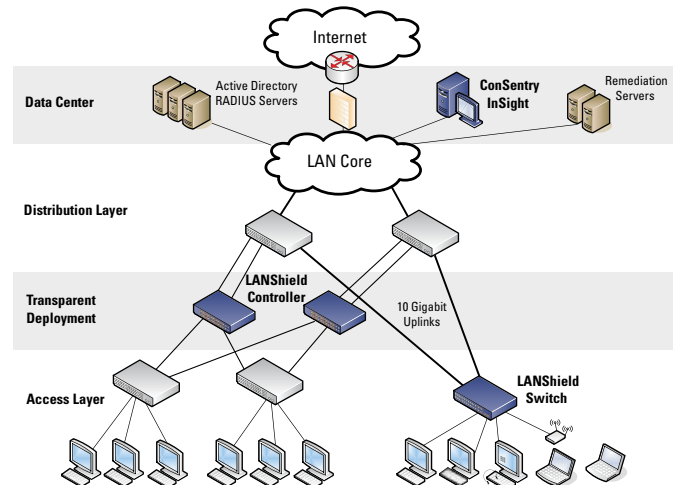
The ConSentry LANShield silicon architecture provides the foundation for the LANShield Controller capabilities. This custom hardware includes a 128-core processor and two programmable ASICs that work together to perform deep packet inspection at 10 Gbps. The programmability of the hardware enables ConSentry to keep pace with changes in applications and security requirements.

### Deployment – Transparency, High Availability, Key IT Projects

The LANShield Controller sits between access switches and the distribution or core layer, aggregating uplinks from the wiring closets and enforcing access policies on all traffic. A transparent device, the LANShield Controller requires no changes to network design or user behavior, simplifying deployment and IT's cost of operations.

The Controller supports high availability and resiliency modes. Enterprises that have dual-homed their wiring closet switches can deploy two ConSentry LANShield Controllers as peers – the two platforms share authentication state and will preserve user

authentications in case of failover. In addition, the Controller itself supports two failure modes. IT can set the device to fail to passthrough, where all LAN traffic will traverse the Controller untouched, or fail to block, where all traffic is stopped. The Controller also includes redundant power supplies and fans.



IT can leverage the LANShield Controller to meet a variety of key IT initiatives, such as:

- NAC, without requiring 802.1X
- guest/contractor access
- securing wireless or open Ethernet jacks
- LAN segmentation for role-based provisioning
- protecting VoIP devices and services
- securing remote access users
- regulatory compliance with HIPAA, PCI, or S-Ox
- malware control or internal IPS

### Product Family

The LANShield Controller is available in two models. The CS1000 supports up to 800 authenticated users across four gigabit uplinks, with deep packet inspection at 4 Gbps. The CS2400 supports up to 2000 authenticated users across 10 gigabit uplinks, with 10 Gbps of deep packet inspection.

## ConSentry LANShield Controller Product Specifications

### Security Features – Leveraging LANShield OS

#### User / Machine Authentication

- Authentication via captive portal or MAC address
- Passive Active Directory authentication snooping
- Passive RADIUS authentication snooping
- Trusted DHCP server

#### Role Derivation

- RADIUS attributes
- Active Directory attributes
- Physical location
- Combination of above

#### Role-Based Policy

Control access by:

- user group
- application
- select application attributes
- destination port
- resource (e.g., servers)

#### Host Posture Check

- Dissolvable agent
- Scans for known threats, anti-virus definition, servicepacks, and custom registry keys and files

#### Threat Detection / Mitigation

- Zero-hour threat detection
- No signature updates necessary
- Drops malformed packets
- Block by: physical port, SRC MAC, offending application

#### Enforcement Actions

- Allow
- Deny
- TCP reset
- Mirroring, logging

#### Visualization

- Ties usernames to applications and security violations
- Identifies applications and application content
- Reports application details to centralized policy center

#### Centralized Visualization

- Ties into ConSentry InSight Command Center
- User and application usage repository
- Real-time alert dashboard
- Fully drillable forensics capability
- Reporting with scheduler
- Full policy and role-derivation configuration GUI

#### Logging and Reporting

- Direct syslog reporting
- Detailed security log messages
- Formatted for SIEM integration

#### Management and Control

- Industry-standard Command Line Interface (CLI)
- Managed by ConSentry InSight Command Center
- SNMP v1/v2c
- Formatted syslog to multiple destinations
- Telnet
- SSH
- TFTP
- Standard and privileged access modes

#### Administrator Authentication

- RADIUS authentication

### Physical Features – Optimized for High-Density Resilient Installation

#### Standards and Protocols

- 802.1D Bridging
- 802.3 10Base-T
- 802.3u 100Base-TX
- 802.3z 1000Base-SX/T

#### Layer 2 Features

- 4,096 VLANs

#### Data Interface Ports

- CS1000: 4 secure SFP port pairs
- CS2400: 10 secure SFP port pairs

#### SFPs available

- Single-mode or multimode 1 Gbps fiber, 10/100/1000 copper

#### Non-data interface ports

- CS1000: Two extensibility ports for packet mirroring or HA and one rear management port
- CS2400: Four extensibility ports for packet mirroring or HA and one rear management port

#### Secured processing throughput

- CS1000: 4 Gbps
- CS2400: 10 Gbps

#### Authenticated users

- CS1000: 400 users base model, 800 users via upgrade license
- CS2400: 1000 users base model, 2000 users via upgrade license

#### Resiliency

- Dual active-active high-availability mode
- Fail pass-through (open)
- Fail block (closed)

#### Latency

- Average 30 microseconds

#### Applications Classified

- 300+ at Layer 4
- 30+ at Layer 7

#### Dimensions

- 17.5 in. x 17 in. x 1.7in - 1U (44.5 x 43.2 x 3.8 cm)

#### Weight

- 15 lbs. (6.9 kg)

#### Operating requirements

- Temperature: 0° – 40°
- Humidity: 5% to 90%, non-condensing

#### Certifications

##### Emissions

- FCC Part 15, sub part B (USA)
- Class A, ICES-003 (Canada)
- EN55022 (CE Mark)
- Class A, EN55024 (CE Mark)
- VCCI Class A (Japan)

##### Safety

- UL 60950-1 (USA)
- CSA C2.22 No. 60950-1 (Canada)
- EN 60950-1 (CE Mark)
- IEC 60950-1 (International)
- NOM (Mexico)
- C-TICK (Australia)

##### Power

- Dual redundant 180W 90-264VAC full range, 47-63Hz

##### Cooling

- Front-to-back air flow



**Corporate Headquarters**  
ConSentry Networks  
1690 McCandless Drive  
Milpitas CA 95035  
**Phone** 408.956.2100 **Fax** 408.956.2199  
**Toll-Free** 866.841.9100  
**Email** info@consentry.com  
www.consentry.com

**Germany**  
ConSentry Networks  
Lyoner Strasse 6 D-605 8  
Frankfurt Germany  
**Phone** +49 69 677 33 4  
**Fax** +49 69 677 33 00

**United Kingdom**  
ConSentry Networks  
Lakeside House 1, Furzeground Way  
Stockley Park, Heathrow, UB11 1BD  
**Phone** +44 (0) 2086 22 3020  
**Fax** +44 (0) 2086 22 3200

**Japan**  
ConSentry Networks  
Hibiya Central Bldg. 14F  
1-2-9, Nishi Shinbashi, Minato-ku  
Tokyo 105-0003 Japan  
**Phone** +813-5532-7630  
**Fax** +813-5532-7373