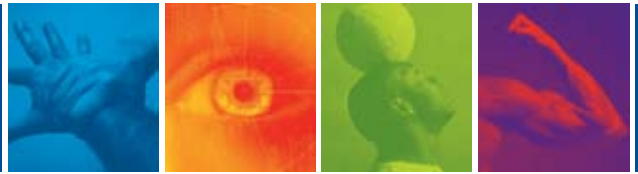


ConSentry® LANShield™ OS



Intelligent LAN Security Software

ConSentry Networks enables enterprises to secure their LANs. The ConSentry LANShield OS drives the company's LANShield architecture, the custom programmable silicon at the heart of the LANShield product family.

With ConSentry's purpose-built security devices, 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.

The LANShield silicon and OS are common to both the LANShield Controller and the LANShield Switch. These products enable IT to embed security directly into the LAN – either behind existing wiring closet switches with the Controller or as the switching fabric with the LANShield Switch. The LANShield OS and LANShield devices provide 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 – block propagation of worms and other malware to prevent network meltdown

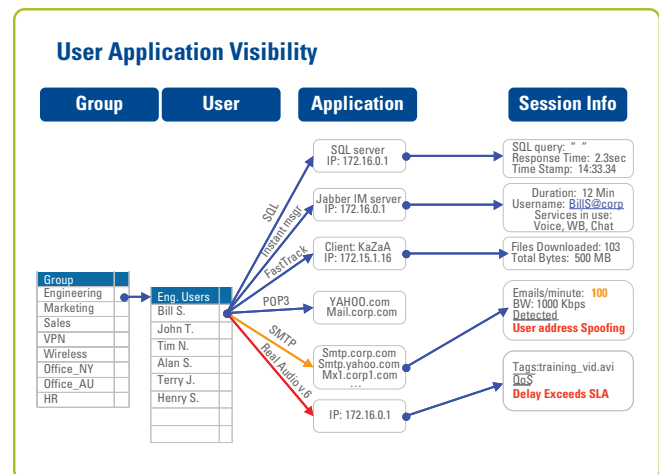
LANShield Architecture

The ConSentry LANShield OS drives the massive parallel processing capabilities of the LANShield silicon. The 128-core LANShield CPU processes 128 threads simultaneously, enabling deep packet inspection and policy enforcement. The accompanying programmable ASICs provide wire-speed forwarding on already inspected flows and session tracking for reporting and auditing. Together, the LANShield CPU and ASICs deliver full LAN security at 10 Gbps rates, enabling ConSentry to secure the LAN while maintaining wire-speed performance.

The LANShield OS is critical to ConSentry's user- and application-based visibility and control. The OS performs the three-way binding among a username, addresses, and applications, so all reporting and control ties back to the user or user role. The OS enables active or passive authentication, supports posture checks on desktops via a dissolvable agent, and learns the user's role for applying policy.

The OS also enables the ConSentry LANShield devices to recognize and classify applications. The system names more than 300 applications at Layer 4, and it inspects more than 30 at Layer 7. The LANShield devices then use that application knowledge to apply policies that control what users can access.

This application knowledge, tied to user behavior, is a cornerstone of the LANShield threat control capabilities as well. The OS tracks both connection attempts and the ratio of connection failures vs. attempts, by application and over time, to detect anomalous behavior characteristic of worms. The OS can then block just the infected application or the entire user, depending on the policy IT has in place.



Integration with ConSentry InSight

The LANShield OS coordinates the processing onboard a LANShield device and also interfaces with the ConSentry InSight Command Center software. That software sends policies to LANShield Controllers and LANShield Switches via the LANShield OS, and the OS sends back to InSight extensive data about incidents, session information, user status, and other LAN security data collected by the LANShield silicon.

The OS also provides an industry-standard command line interface (CLI) for access to LANShield devices. The CLI allows IT to configure the ConSentry platform, apply user control policies, learn user and incident information, and set malware policies.

ConSentry LANShield OS 3.0 Specifications

Authentication, Posture Check, Role Derivation	Visibility
Authentication Passive <ul style="list-style-type: none">Kerberos snooping<ul style="list-style-type: none">Windows Active DirectoryLinuxMacintoshRADIUS snoopingTrusted DHCP server Active <ul style="list-style-type: none">Customizable captive portalMAC-based via RADIUS Whitelists of approved devices <ul style="list-style-type: none">by MAC/IP address (including wildcards), port, or VLAN Host Posture Check Dissolvable agent <ul style="list-style-type: none">Scans for known threats, anti-virus definition, service-packs, and custom registry keys and files Role-based policy <ul style="list-style-type: none">Designate which users to check Role Derivation <ul style="list-style-type: none">RADIUSMicrosoft Active Directory attributesPhysical locationDHCP attributesTime of dayCombination of above	Identity Awareness <ul style="list-style-type: none">Bind username to IP/MAC address and applications Application Classification <ul style="list-style-type: none">Identifies 300+ applications at Layer 4Identifies the following applications at Layer 7Business Applications<ul style="list-style-type: none">Oracle TNSSAP R/3VoIP<ul style="list-style-type: none">SIPH.323Cisco SCCP (Skinny)Web/Mail<ul style="list-style-type: none">HTTPSMTPPOP3IMAPFile Transfer<ul style="list-style-type: none">FTP, FTP-Data, TFTPCIFS/SMB/NetBIOS <ul style="list-style-type: none">Network Services<ul style="list-style-type: none">DNSDHCP/BOOTPKerberosSUNRPC PortmapperMS-RPCRADIUSConnectivity<ul style="list-style-type: none">SSHTelnetVNCRTSPMS-MediaIM<ul style="list-style-type: none">MSNYahooAOLP2P<ul style="list-style-type: none">BitTorrenteDonkey 2000GnutellaWinNYeMuleKazaaAppleJuiceDirectConnect

Identity-based Control – Policy Enforcement	Threat Control
Policy Features <ul style="list-style-type: none">LANShield platforms integrate policy decision and policy enforcementPolicies stored on each LANShield deviceCentralized configuration and policy distribution with ConSentry InSight Command CenterGranular policies<ul style="list-style-type: none">including Layer 4, Layer 7, and Layer 7 attributes (such as file name) Enforcement Actions <ul style="list-style-type: none">AllowDenyTCP resetMirroring Logging and Reporting <ul style="list-style-type: none">Detailed security syslog messagesFormatted for SIEM integrationIntegrates with ConSentry InSight Command Center	Worm Containment <ul style="list-style-type: none">Prevents network meltdown by detecting and blocking worm spreadCustom malware detection algorithms for zero-hour and known wormsIT can block only infected application vs. entire userNear-zero tuning – pre-tuned per application categoryAllows user to maintain network connectivity during clean-up Threat Detection <ul style="list-style-type: none">Detects network reconnaissance scans<ul style="list-style-type: none">NMAP scanNessus scanDetects DoS attacks against servers Packet Validity Checks <ul style="list-style-type: none">LAND AttackEmpty FragmentMicro FragmentICMP Ping Of DeathUDP Port LoopbackBad IP Header LenBad IP FlagsBad IP TTL <ul style="list-style-type: none">Bad IP Payload LenBad IP Fragment OfsOversize IP PayloadBad IP ChecksumBad TCP Urgent OfsTCP Short HeaderTCP Null ScanTCP Fragmented HdrUDP Short HeaderBad UDP LengthTCP XMAS Scan Management and Control <ul style="list-style-type: none">Managed by ConSentry InSight Command CenterSNMP v1/v2cIndustry-standard Command Line Interface (CLI)Formatted syslog to multiple destinationsTelnetSSHTFTPDual administrator access levelsRADIUS administrator authentication



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, Furzegrund 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