Raritan.
When you're ready to take control®

Features and Benefits

CommandCenter® NOC

Features	Benefits
Out of Band access to target systems *(via CommandCenter Secure Gateway)*	Provides one click access and sign on to distressed remote target servers, greatly improving mean time to repair. Users are able to move between management systems easily to gain the information needed to resolve incidents quickly.
Network management	Proactively monitors and maintains all devices and services on a network and alert on changes within the environment. For example, SNMP trap support helps users find events that occur and then take appropriate actions.
Windows system management	Provides network administrators the ability to manage servers and workstations by providing a single repository for performance, inventory, and event data.
Vulnerability scanning and assessment	Scans the network for vulnerabilities and assist network administrators in resolving security concerns.
Intrusion detection	Allows administrators to monitor and analyze system events for unauthorized attempts to access system resources.
Network traffic analysis	Provides the ability to analyze traffic flow and create reports that show the presence, absence, amount, direction, and frequency of network traffic.
Asset inventory and tracking	Provides administrators the ability to deliver on-demand reports of hardware and software inventories.
Third-party authentication including AD, LDAP, RADIUS and TACACS *(via CommandCenter Secure Gateway)*	Simplifies installation and database modifications.
Reporting, asset management and IT compliance	Provides reports on network performance, and conformance with IT security regulations. Performance reports include, Delta Inventory Reporting which notes hardware and software additions, removals and changes. It aids administrators by providing the ITIL feature for tracking "Configuration Item Changes."

Features	Benefits
Infrastructure reliability and performance trending and analysis	Allows administrators to proactively monitor and maintain the network and spot problems, often before anyone notices degradations in service. CommandCenter NOC allows the IT infrastructure and employees to work at full strength.
Network and system security	Hackers, worms and other security threats may be entering the network undetected. CommandCenter NOC's vulnerability scanning and intrusion detection discover security problems before they cause harm.
SNMP Trap management of Raritan devices	Allows proactive monitoring of out-of-band network devices.
Performance thresholds	Alerts potential problems before an outage occurs.

CommandCenter® NOC 2500

Network, Security and Systems Management

CommandCenter NOC

Manage and secure your IT infrastructure

NOC 2500N

– 250 SNMP-enabled devices
– Supports up to five NOC 2500Ms
– Supports up to five NOC 2500Ss
– Supports up to five event forwarders (NOC 100, NOC 250, NOC 2500N)

Optional components:

NOC 2500M

– 50 Windows servers
– 500 Windows PCs

NOC 2500S

– Intrusion detection
– Network traffic analysis

The CommandCenter NOC 2500 series of multifunction IT infrastructure management appliances enables businesses to solve a wide range of IT problems before they occur. The NOC 2500 is intended for medium-size IT operations with up to 250 Windows® servers, 250 SNMP-enabled devices including Linux/UNIX servers, routers and switches and 2500 Windows PCs, in a distributed network.

CommandCenter NOC 2500 integrates world-class network and systems management, traffic analysis, vulnerability scanning, intrusion detection, asset management and reporting functionality into easily deployed appliances. Designed to guard your network against outages, performance slowdowns, security weaknesses and incoming attacks, the CommandCenter NOC 2500 helps ensure application availability and network resource optimization.

The CommandCenter NOC 2500 is part of Raritan's CommandCenter family of Service Management solutions, the first to integrate the power of systems, network, application and proactive security management with secure, remote in-band and out-of-band server and network device access. This extremely powerful combination delivers alerts together with detailed diagnostic information, and direct connection to the device in distress from a single interface.

Reporting, asset management and IT compliance:

The CommandCenter NOC 2500 produces a set of standard reports on your network's performance. XML-formatted data can be exported so you can create unlimited custom reports. This allows you to make informed decisions and satisfy regulatory audit requirements.

- IT infrastructure reports can support compliance audit requirements for regulations like Sarbanes-Oxley, HIPAA, the Gramm-Leach-Bliley Act (GLBA) and Basel II.
- Comprehensive hardware and software configuration inventories and installed application license counts simplify audits and asset management.
- Delta Inventory Reporting notes hardware and software additions, removals and changes. This can help implement ITIL best practices.

Infrastructure reliability and performance trending and analysis:

- Performance data collection lets you make informed decisions on new upgrades and purchases, or eliminate costs of underutilized infrastructure.
- Notifications are sent to the appropriate party, based on roles and responsibilities, when critical performance thresholds are violated so you can take action quickly.
- Network traffic reports let you understand your network usage and trends.

Raritan®
When you're ready to take control®

Manage and Secure Your IT Infrastructure...

Network management and system security:

Hyper-Access™ is the revolutionary way CommandCenter management products combine proactive monitoring with secure, remote access to get you right to the heart of problems. When trouble occurs anywhere in your network, CommandCenter NOC can send an e-mail alert notification with a Hyper-Access link. The Hyper-Access link connects to diagnostic information about the device that triggered the alarm plus instant, click-and-fix in-band and out-of-band access to the distressed device through CommandCenter Secure Gateway. This can all be accomplished within a single screen and without anyone leaving their chair.

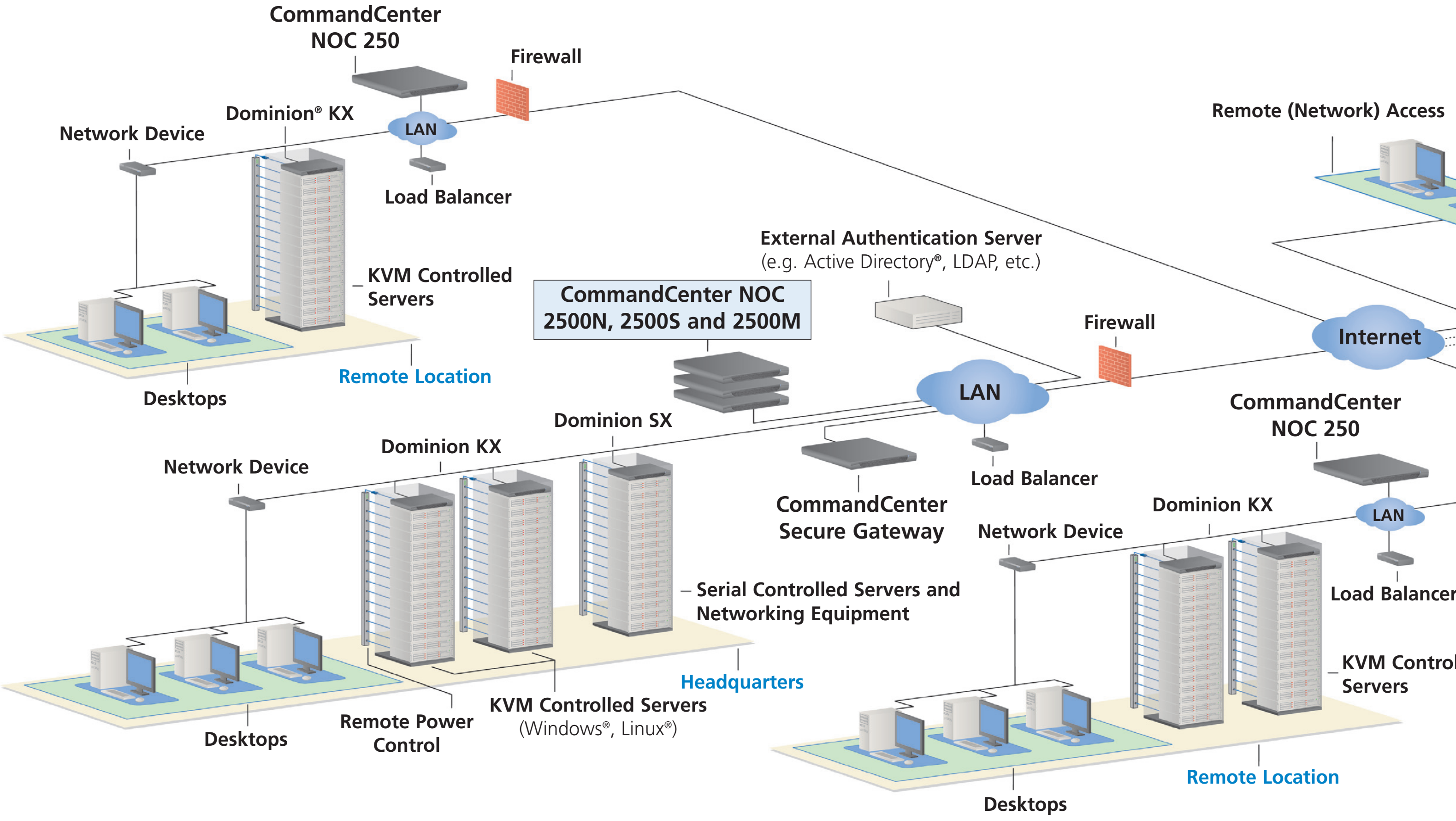
Hackers, worms and other security threats may be entering your network without your knowledge. The CommandCenter NOC 2500 provides vulnerability scanning and intrusion detection to discover security problems before they cause harm.

- Intrusion detection and management discovers security threats and recommends solutions.
- Log file consolidation supports numerous IT assets including firewalls, antivirus software and Windows servers.
- Unlimited vulnerability scans and one-click reporting uncover weaknesses, unpatched systems and provide recommended solutions.

A distributed platform:

The CommandCenter NOC 2500 series consists of three components: the NOC 2500N base unit, the NOC 2500M enhanced systems management unit and the NOC 2500S enhanced security unit. The distributed architecture, which requires at least one NOC 2500N, allows you to configure a system based on your architecture and topology now, and scale it cost effectively as your company grows.

The CommandCenter NOC 2500N supports systems management, vulnerability scanning, asset management and reporting for up to 250 network devices.



At a Fraction of the Cost and Complexity of Alternatives

The CommandCenter NOC 2500M adds enhanced Windows® system management for up to 50 Windows servers and 500 Windows client PCs. Up to five NOC 2500M units can be added to a NOC 2500N, bringing the capability up to a total of 250 Windows servers and 2,500 Windows client PCs.

The CommandCenter NOC 2500S adds enhanced security management and network traffic analysis to the capabilities of the NOC 2500N. It provides network intrusion detection and traffic analysis that is limited only by where it is placed in the network architecture.

NOC 2500N functionality:

➤ Storage of up to one year of performance metrics and outage information in perpetuity (80GB hard drive)

➤ Network notifications to any email, pager or phone when critical performance thresholds are violated

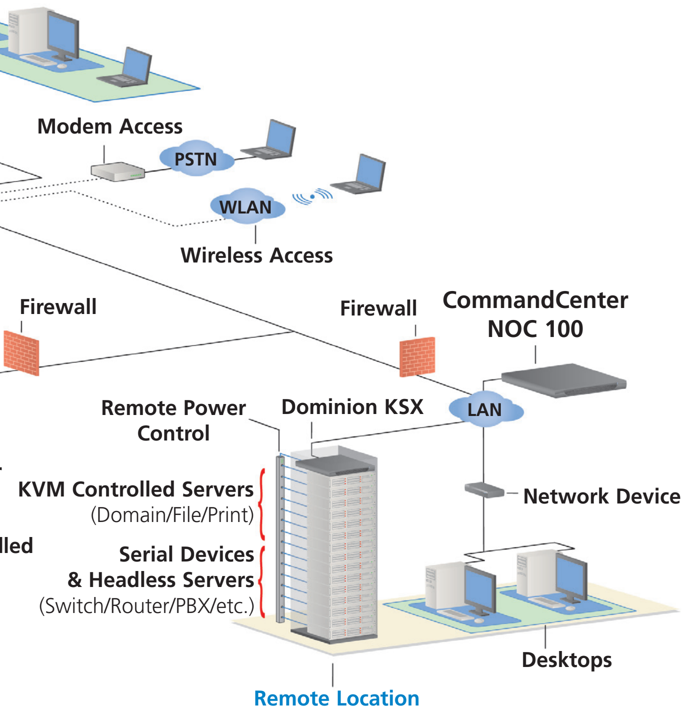
➤ Network management subsystem
- Ad-hoc and daily scheduled reports
- Immediate and automatic initiation of discovery (re-discovery occurs every 24 hours thereafter)
- Discovery and polling of services and protocols using synthetic transactions
- Custom category and user views based on TCP/IP address or service
- Performance data collection from managed devices via either SNMPv1, SNMPv2c or Windows Management Instrumentation (WMI)
- Support for over 2700 standard and vendor SNMP traps and notifications, including Raritan's CommandCenter Secure Gateway and Dominion® products
- Multisite management capability, which allows all events to be filtered and forwarded to any SNMP-based management system
- Support for Syslog messages from Linux and UNIX systems, firewalls, etc.

➤ Vulnerability scanning
- Individually defined network scans of an unlimited number of hosts with ability to schedule scans for one-time or recurring scans
- Four discrete levels: port scanning, profiling, intrusion attempts and malicious intrusions
- Vulnerability descriptions include background and solution information

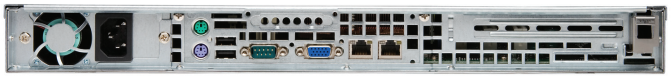
➤ Asset tracking, reporting and management
- Parallel database allows tracking of critical location, vendor and support information
- Import/export facility allows population with existing data or export for use in spreadsheets

➤ Notification subsystem
- Group-based configuration paradigm with automatic in-group and super-group escalation
- Configurable event notifications deliverable to any email-addressable device or telephone or pager

➤ Reports
- Reports can be viewed in a browser in PDF or HTML, downloaded as a ZIP file, sent via e-mail, or exported in XML format for customization
- Standard reports: Network Report Card, Availability Report, Outage Report, Intrusion Detection Reports, Vulnerability Report, SNMP Performance Reports, Windows Management Performance Reports, Inventory Report and Delta Inventory Report

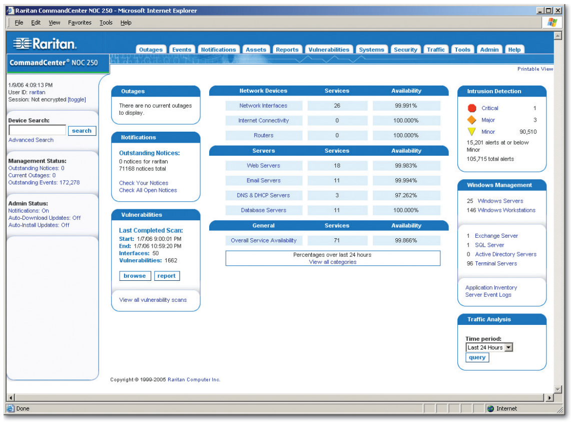


Specifications



Specifications for all CommandCenter NOC Models	
Form Factor	1U full width, rack mountable
Dimensions (DxWxH)	24.21"x 19.09"x 1.75"; 615 x 485 x 44mm
Weight	23.80lb; 10.80kg
Power	Single supply (1 x 300 watt)
Maximum Heating Value	856 BTU
Cooling	Redundant fans
Operating Temperature	50°-95°F; 10°-35°C
Humidity	8% - 90% RH
Mean Time Between Failure (MTBF)	36,354 hours
Hardware Processor Hard Disc and Controller CD/ROM Drive	 AMD Opteron 146 Two 80-GB SATA @7200 rpm, RAID 1 DVD-ROM
Local Access Port KVM Admin Port Serial Admin Port	 DB15 + PS2 or USB keyboard/mouse DB9
Remote Connection Network Protocols	 Two 10/100/1000 Ethernet (RJ-45) TCP/IP, HTTP, HTTPS, UDP, SNTP, RADIUS, LDAP, TCACS+, SNMP, SNTP
Discovery and Polling Services and Protocols	 Citrix®/ICA®, DHCP, DNS, FTP, HTTP, HTTP:8000, HTTP:8080, HTTPS, ICMP, IMAP, Informix®, LDAP, Lotus® Domino®/IIOP, MySQL®, Oracle®, POP3, PostgreSQL, SMTP, SNMP, SQL Server®, SSH, Sybase® and user-customizable pollers
Warranty	One year hardware warranty. Extended warranty also available. Software support agreement required. Agreement provides: remote technical support, software updates and software releases as available.

When you're ready to take control, do it with CommandCenter NOC.



1/9/06 4:09:13 PM
User ID: raritan
Session: Not encrypted [toggle]

Device Search:
Advanced Search

Management Status:
Outstanding Notices: 0
Current Outages: 0
Outstanding Events: 172,278

Admin Status:
Notifications: On
Auto-Download Updates: Off
Auto-Install Updates: Off

Outages
There are no current outages to display.

Notifications
Outstanding Notices:
0 notices for raritan
71168 notices total

Check Your Notices
Check All Open Notices

Vulnerabilities
Last Completed Scan:
Start: 1/7/06 9:00:01 PM
End: 1/7/06 10:59:20 PM
Interfaces: 50
Vulnerabilities: 1662

View all vulnerability scans

Network Devices	Services	Availability
Network Interfaces	26	99.991%
Internet Connectivity	0	100.000%
Routers	0	100.000%
Servers	**Services**	**Availability**
Web Servers	18	99.983%
Email Servers	11	99.994%
DNS & DHCP Servers	3	97.262%
Database Servers	11	100.000%
General	**Services**	**Availability**
Overall Service Availability	71	99.866%

Percentages over last 24 hours
View all categories

Intrusion Detection

Critical	1
Major	3
Minor	90,510

15,201 alerts at or below Minor
105,715 total alerts

Windows Management
25 Windows Servers
146 Windows Workstations

1 Exchange Server
1 SQL Server
0 Active Directory Servers
96 Terminal Servers

Application Inventory
Server Event Logs

Traffic Analysis
Time period: Last 24 Hours

Copyright © 1999-2005 Raritan Computer Inc.

NOC 2500M functionality:

➤ Windows management subsystem
- Discovers all devices, by domain, via WMI
- Automatic categorization of server vs. desktop based on operating system
- Collects performance metrics from servers and selected desktops including proccesor, network, memory and logical disk.
- Consolidates all system, security and application event log entries (error and failure)
- Sends notification if service fails to restart
- Hardware, software and configuration inventories and optional performance data collection available for desktop-class systems

NOC 2500S functionality:

➤ Intrusion detection subsystem
- Dedicated secure interface for traffic capture
- Signature-based NIDS
- Event descriptions contain hyperlinks to Raritan's Web library of intrusion information
- Over 20Mbits/sec data rates
- Raritan's Signature Profiler allows for rule-based auto-configuration of signatures

➤ Network utilization and bandwidth analysis
- Leverages promiscuous listening to analyze traffic
- Delivers "Top 10" reports: Top Talkers, Top Sessions, Most Visited Web Sites and Top DNS Requests

Raritan is a leading supplier of solutions for managing IT infrastructure equipment and the mission-critical applications and services that run on it. Raritan was founded in 1985, and since then has been making products that are used to manage IT infrastructures at more than 50,000 network data centers, computer test labs and multi-workstation environments around the world. From the small business to the enterprise, Raritan's complete line of compatible and scalable IT management solutions offers IT professionals the most reliable, flexible and secure in-band and out-of-band solutions to simplify the management of data center equipment, applications and services, while improving operational productivity. More information on the company is available at Raritan.com.