

Proactive Network, Security and Systems Management in One Affordable Appliance

The CommandCenter NOC 250 and NOC 100 are multi-function IT infrastructure management appliances that enable mid-sized businesses to solve a wide range of IT problems before they occur. The NOC 250 is intended for mid-sized businesses or business units of larger enterprises with up to 250 client PCs, 25 servers and 25 network devices. The NOC 100 manages IT infrastructures of up to 100 client PCs, 10 servers and 10 network devices.



Both products integrate world-class network and systems management, traffic analysis, vulnerability scanning, intrusion detection, asset management and reporting functionality into one easily deployed platform. Designed to guard your network against outages, degradation, performance slowdowns, security weaknesses and incoming attacks, the CommandCenter NOC 250 and NOC 100 keep your IT infrastructure under constant scrutiny. They help ensure application availability and network resource optimization including the ability to have an outside party such as an MSP or consultant monitor your environment. They help implement your company's IT compliance tactics and strategies. Their integrated management dashboard and reporting give your IT decision makers actionable intelligence.

Reporting, asset management and IT compliance:

The CommandCenter NOC 250 and NOC 100 provide reports so you know how your network is performing, and whether or not it meets IT security regulations. CommandCenter NOC delivers performance reports so you can make informed decisions.

- Customizable XML-based reports provide the information you need presented the way you want.
- IT infrastructure reports can support compliance audit requirements for regulations like Sarbanes-Oxley, HIPAA and the Gramm-Leach-Bliley Act (GLBA).
- Comprehensive hardware and software configuration inventories and installed application license counts, simplify audits and asset management.

Infrastructure reliability and performance trending and analysis:

With CommandCenter NOC 250 and NOC 100 you can proactively monitor and maintain your network and spot problems, often before anyone notices degradations in service. CommandCenter NOC allows your IT infrastructure and employees to work at full strength.

- 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.
- Statistical network traffic reports let you document performance against service level agreements (SLAs).

Manage and Secure Your IT Infrastructure...

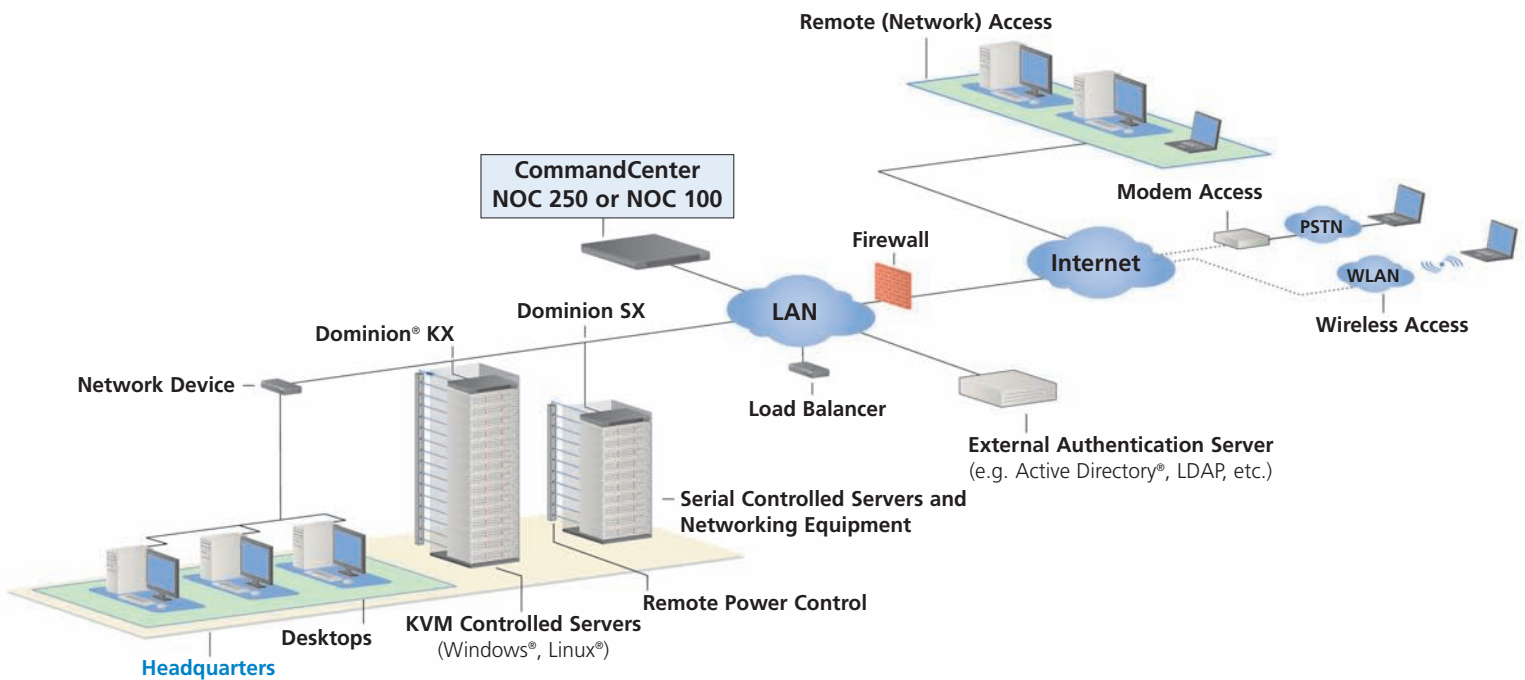
Network and system security:

Hackers, worms and other security threats may be entering your network without your knowledge. The CommandCenter NOC 250 and NOC 100 provide 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.

NOC 250 and NOC 100 functionality:

- Storage of up to one year of performance metrics and outage information in perpetuity (80GB hard drive)
- Network notifications to any email/pager/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 or SNMPv2c



At a Fraction of the Cost and Complexity of Alternatives

- Support for over 2700 unique standard and vendor SNMP traps and notifications
- Multi-site management capability 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.
- Scheduled outages accommodate service windows and other planned downtime
- User-configurable browser view and reports
- Vulnerability scanning
 - Individually defined network scans of an unlimited number of hosts with ability to schedule scans for one-time or recurring scan
 - 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 by event that generates the notification, destination, time of delivery and escalation
 - Deliverable to any email-addressable device or telephone or pager
- Reports
 - Reports can be scheduled to automatically be produced and delivered via e-mail
 - 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 report types: Network report card, availability, outage, intrusion detection, vulnerability, SNMP performance, inventory and performance trending
- Windows management subsystem
 - Discovers all devices, by domain, via Windows Management Instrumentation (WMI)
 - Automatic categorization of server vs. desktop based on operating system
 - Collects performance metrics from servers and selected desktops including:
 - **processor** (queue length, interrupts per second, % interrupt time, % privileged time, % processor time, % user time)
 - **network** (total bytes per second, bytes transmitted and received per second, current bandwidth, output queue length)
 - **memory** (available bytes, page faults per second, commit limit, committed bytes)
 - **logical disk** (% free space), physical disk (average disk queue length, current disk queue length) and paging file (% usage, % usage at peak)
 - 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
- Intrusion detection subsystem
 - Dedicated secure interface (promiscuous mode) for traffic capture
 - Signature-based NIDS
 - Event descriptions contain hyperlinks to Raritan's Web library of intrusion information
 - Over 20Mbits/sec data rates with no packet loss
 - Raritan's Signature Profiler allows for rule-based auto-configuration of signatures
- Network utilization and bandwidth analysis
 - Leverages promiscuous listening to analyze traffic
 - Graphically illustrates bandwidth utilization by Ethernet, IP and application protocols
 - Delivers "Top 10" reports: Top Talkers, Top Sessions, Most Visited Web Sites and Top DNS Requests

Specifications



Specifications for all CommandCenter NOC Models	
Form Factor	1U full width, rack mountable
Dimensions - (DxWxH)	14.1" x 16.8" x 1.7"; 358 x 426 x 43mm
Weight	15.5 lbs; 7.0 kg
Power	100V/240V 50/60Hz 5A
Operating Temperature	5°-40°C; 41°-104°F
Humidity	20% - 90% RH
Processors	Intel® Pentium® 4-based industrial server components
Remote Connection	
Network	Two 10/100/1000 Ethernet (RJ-45) LAN 1: Network connection LAN 2: Traffic and intrusion detection
Protocols	TCP/IP, HTTP, HTTPS, UDP, SNMP, DHCP
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
Local Access Port	
Serial	RS-232(M)
Video	HD15(F) VGA
Keyboard	Mini-DIN6(F) or USB A(F)
Screen Resolution	
PC text mode	720 x 400 (local access/configuration)
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.**

Call 1.800.724.8090 or visit Raritan.com/ccnoc

© 2005 Raritan, Inc. All rights reserved. Raritan, Dominion and CommandCenter are registered trademarks of Raritan, Inc. in the United States and/or other countries. All others are trademarks of their respective owners.

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 control millions of servers 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 KVM and remote connectivity products offers IT professionals the most reliable, flexible and secure in-band and out-of-band solutions to manage data center equipment applications and services, while improving operational productivity. More information on the company is available at Raritan.com.