

Service Management Made Simple For Mid-Sized Organizations

A White Paper Prepared for Raritan, Inc.
April 2006



ENTERPRISE MANAGEMENT
ASSOCIATES®

Table of Contents

- Executive Summary 1
- Introduction to Service Management Best Practices 1
- Raritan’s CommandCenter Service Management Architecture 3
 - CommandCenter NOC 3
 - CommandCenter Secure Gateway..... 4
- Customer Case Study..... 5
- EMA’s Perspective 5
- About Raritan 6

Service Management Made Simple For Mid-Sized Organizations

Executive Summary

There is no question that companies who harness the power of IT most effectively stand to gain a competitive edge, while also reducing costs. Whether it's pursuing the latest advances in applications, infrastructure management, business intelligence, or the seemingly infinite number of promising Web-based initiatives, deploying the right IT solutions and processes, at the right time, in the right manner, has become a critical strategic business objective.

As if bracing for each new technological development isn't challenging enough, the IT function is further expected to manage and implement these changes in an orderly "best practices" manner to help ensure continuity of IT deployment in all appropriate business processes. This approach has ushered in the era of service management, where applications are viewed by end-users as utility-grade services available to authorized users throughout the networked company, rather than as siloed, discrete applications unique to individual users and departments.

Due to their substantial financial resources and depth of technical expertise, Fortune 1000-sized companies traditionally have led the way in the implementation of IT best practices. By comparison, mid-tier businesses, generally defined as firms with \$50 million to \$500 million in revenue, and typically with 100 to 1,000 employees, have felt overmatched and outflanked by the cost and complexity of IT service management adoption.

As a result, Mid-Sized Businesses (MSBs) are highly conservative in their approach to IT, avoiding large projects and demanding quick paybacks from investments. But this approach may lead to complacency, milking "cash cows" and failing to invest enough in the future. These companies face the ever-present risk of not innovating enough, and barriers of cost and complexity are generally the cause.

This is evident in the reluctance of mid-tier companies to implement such structured methodologies as Cobit (Control Objectives for Information and Related Technology) and ITIL (IT Infrastructure Library), the industry's most widely accepted approach to IT service management best practices. But precisely because process focus is less evolved in MSBs than in larger enterprises, mid-tier IT adopters need to invest in the core

principles and best practices of service management that support and simplify process initiatives like ITIL.

However, the challenge for MSBs remains how to make it simple. In reality, implementing service management for mid-sized businesses does not have to be a huge, expensive undertaking. The key is to start with core principles and then deploy the right tools to support them.

In this white paper, Enterprise Management Associates (EMA) discusses an approach to service management offered by Raritan Inc. that appeals specifically to mid-tier companies. Raritan, with a long history in out-of-band, remote access KVM and serial console management, has recently introduced the CommandCenter® management product family, starting with CommandCenter NOC (CC-NOC) and CommandCenter Secure Gateway (CC-Secure Gateway). Other CommandCenter solutions will follow, all geared to simplifying IT processes and operations particularly for MSBs and medium-sized business units or divisions of larger organizations.

The remainder of this document reviews the market drivers for service management best practices for mid-tier companies, covers the primary capabilities and customer benefits of the CommandCenter NOC and CommandCenter Secure Gateway products, and provides a customer example of the product in action. The report concludes with EMA's assessment of Raritan's success factors in this vital area of service management for mid-tier companies.

Introduction to Service Management Best Practices

When it comes to marshaling IT resources, mid-tier companies are essentially just scaled-down versions of larger firms. MSBs have the same multi-tier architectures and multi-vendor environments as the multi-billion dollar multi-nationals, but in more limited deployments and with far fewer users.

Similarly, they also lack the budget and depth of technical and business expertise compared with Fortune 1000 companies. This means they must "do more with less" in terms of IT in order to compete effectively with companies of all sizes and establish a solid strategy for sustainable, profitable business growth.

Mastering service management need not be an overly complex matter, and is one way mid-tier companies can

Service Management Made Simple For Mid-Sized Organizations

indeed “get more IT” without going on a spending spree or disproportionately growing their IT staffs.

The core principles of service management are focused on the assertion that the whole should be greater than the sum of its parts. Service management best practices provide a holistic view of the health of the complete IT landscape, rather than managing discrete enterprise elements or “silos.”

The IT environment of any organization is defined by, and often optimized for use by, individual business units, specific applications, prioritized resource considerations, and a host of other isolated processes and resources that all tend to fight each other for control. Via an integrated view of the interdependencies that make these various silos work, the service management approach maximizes availability and performance of all IT resources. In other words, a rising tide lifts all boats.

An effective mid-tier service management solution deployment strategy contains such attributes as the following:

- **Integration** – support a breadth of functionality (e.g., security, network management, application performance) from a single management view rather than requiring multiple monitoring tools and interfaces. A baseline management platform is established that supports multiple technologies and vendor solutions to maximize interoperability and use of best-of-breed tools.
 - Effective alerts – efficient, lightweight data collection capabilities plus intelligent event gathering that recognizes redundant alarms and supports rapid root cause analysis.
 - Minimal MTTR (Mean Time To Repair) and MTBF (Mean Time Between Failures) – for MTTR, this includes applying baseline diagnostics to fix simple, common problems with easy navigation. It also requires a clear escalation procedure to address more complex problems as quickly as possible. MTBF can be minimized by maintaining up-to-date hardware and software support contracts and managing configuration guidelines that promote consistent desired state levels.

- Proactive monitoring to reduce outages – maintain proper due diligence to set operational and performance thresholds and monitor compliance before problems such as security threats, network outages, and bandwidth allocation issues develop that can affect normal operations.
- Quick remediation of problems when they do happen (related to proactive monitoring and reduced MTBF) – have effective fault management and root cause analysis along with clear escalation procedures to address more complex issues as they arise. However, it’s also contingent on solutions that enable the active repair of critical IT infrastructure resources that are not vulnerable to connectivity issues and/or hung devices. Achieving this level of service management availability usually requires an integrated out-of-band and in-band approach.
- Integrating in-band and out-of-band monitoring and management relies on the primary IT network to monitor and manage activity and behavior of enterprise resources, but takes advantage of out-of-band connectivity, such as KVM (Keyboard, Video and Mouse) and serial port direct connections, as well as specialized VPN (Virtual Private Network), dial-up or other non-production network links to provide high-value, secure, remote management and resolution capabilities.

While in-band management and monitoring remains the primary point of control, out-of-band capabilities allow console and BIOS-level control of IT resources to reboot stalled servers and network devices remotely, without using precious in-band capacity. This allows IT personnel to access, control and manage the company’s servers even if the corporate network itself is down. For mid-tier businesses, this can be an ideal solution to maintaining peak operation of equipment located at distant branch offices, where personnel at those locations is not prepared to perform troubleshooting, diagnostic and restorative procedures.

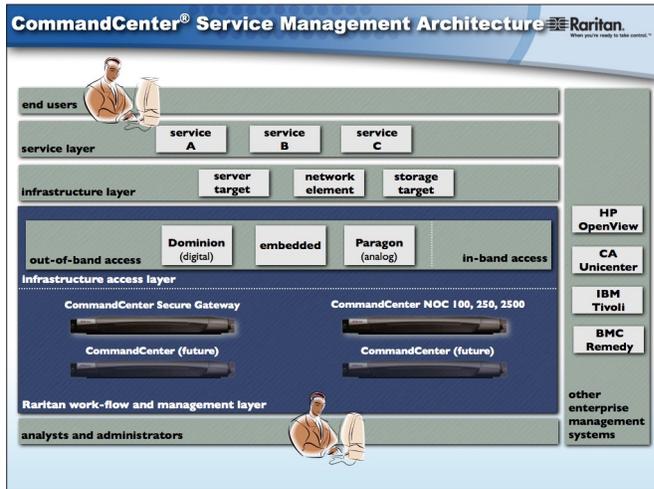
Service Management Made Simple For Mid-Sized Organizations

- **Management of changing environments and conditions** – Service management processes detect changes in configurations, new devices, applications and networks, sudden shifts in traffic flow or routing, denial of service attacks and other random or unexpected threats that can create havoc within any IT infrastructure.
- **Modular deployment** – A modular approach provides the best of both worlds – enabling an integrated, holistic management strategy that can conform to best practices, while enabling flexibility and choice in making management investments. Well-designed modular solutions should also be easy to deploy.
- **Resilience and reliability** – The design objective of service management best practices is to be adaptive to change, and since they are based on defined standards of performance, functionality and management, they are also highly reliable.

No process improvement can succeed without the right technology to support it. This clearly applies to service management best practices. The next section examines how Raritan's new CommandCenter® product family addresses the core principles of service management.

Raritan's CommandCenter Service Management Architecture

Designed specifically to simplify IT operations for MSBs, Raritan's CommandCenter portfolio is a new addition to the company's family of service management solutions. It currently comprises the CommandCenter NOC (CC-NOC) and CommandCenter Secure Gateway (CC-Secure Gateway) products, which collectively extend the company's expertise in secure, remote KVM and serial console access products. The CommandCenter NOC family builds on the Oculan brand of products acquired by Raritan in mid-2005. These products are easy to buy, simple to deploy, and simple to use, yet deliver price-performance value that is easily cost-justified by mid-tier businesses. EMA believes that Raritan has preserved the Oculan product benefits and, based on customer comments and product/architecture briefings, will increase the value and modularity of the products over time.



CommandCenter NOC

CommandCenter NOC integrates systems, network and proactive security management in a family of easy-to-use, multi-function IT infrastructure management appliances. It also offers asset discovery, monitoring and alerting of fault and performance of system, networks, applications, intrusion detection and vulnerability scanning. By combining proactive management and integrated workflow with secure, remote in-band and out-of-band access via CommandCenter Secure Gateway, CC-NOC promotes improved service and application availability and network resource utilization. This combination of features helps IT departments identify problems before they affect service levels and, thanks to out-of-band controls, fix them without leaving their chairs.

Principal features:

- *Reporting and asset management to document network performance against IT security regulations and mandated performance standards.* Reporting is based on XML for ease of customization, and supports audit requirements such as those for Sarbanes-Oxley, HIPAA, BASEL II and the Gramm-Leach-Bliley Act (GLBA). Hardware and software configurations are maintained to simplify audit and asset management tasks.
- *Fault and Performance monitoring, trending and analysis support proactive monitoring of the IT network to spot problems before end-users notice a degradation in service.* Performance data is collected on all monitored IT resources (typically key systems and network devices, including their services and applications) to

Service Management Made Simple For Mid-Sized Organizations

identify under-utilized assets and simplify upgrade and new purchase decisions. When threshold violations occur, notifications are routed to the appropriate party, based on roles and responsibilities, to expedite prompt problem resolution. In addition, network performance statistics are reported to provide documentation to meet SLA requirements. Autonomics allows restarting of hung services without user intervention.

- *Network and system security includes vulnerability scanning and intrusion detection to guard against hackers, worms, viruses and other security threats.* Intrusion detection and management recommends solutions to such events, while log file consolidation tracks risk management steps taken by firewalls, antivirus software and Windows® servers. Unlimited vulnerability scans and one-click reporting uncover weaknesses and unpatched systems, and suggest possible solutions. These solutions extend to support desktops and remote devices.

The system comes in three models: the CommandCenter NOC 2500, NOC 250, and NOC 100. They differ primarily in the number of servers and devices they support, but otherwise offer essentially the same features and capabilities. The high-end NOC 2500 series can support up to 2500 client PCs, 250 servers and 250 network devices. The NOC 250 supports up to 250 PCs, 25 servers and 25 network devices, while the CC NOC 100 manages IT infrastructures of up to 100 client PCs, 10 servers and 10 network devices.

Collectively, the CommandCenter NOC features deliver the essential core principles that simplify the task of implementing service management best practices for MSBs. The product family provides effective network and system management and traffic analysis along with vulnerability scanning and intrusion detection. In addition, the CC-NOC family is field upgradable to scale economically as the infrastructure grows.

CommandCenter Secure Gateway

CommandCenter Secure Gateway is a management appliance designed to secure access and control of IT devices. It enables integrated out-of-band and in-band access to complement the CommandCenter NOC in-band monitoring and management functionality. CC-Secure Gateway works as a gateway for aggregat-

ing access, providing centralized management of serial, KVM, IPMI, iLO/RiLOE and power control devices in multiple data centers, branch offices and remote locations via single, secure browser-based access. It consolidates management of Raritan devices and all servers and network devices connected to Raritan equipment. It allows customizable user access and control through policy management tools, and eases management of IT assets through device discovery and advanced configuration management.

The CommandCenter Secure Gateway product provides secure, remote out-of-band access to all target devices and a single Web interface over VPN, intranet or Internet sessions. It is able to centralize the management of more than 10,000 devices with only one IP address. It offers robust security, high availability and strong performance while also providing ease of use and ease of management with low Total Cost of Ownership (TCO).

All network devices and targets can be seen via customizable logical and physical views that further ease service management tasks. Rather than studying rows of tedious IP address tables, IT staff have simplified views that show all servers, network equipment, and other IT resources by device type, geographic location, business unit or department, or service or application – even by individual users or groups of users. IT staff also can view all devices from a single vendor, such as all Cisco equipment, wherever it is installed throughout the enterprise.

CommandCenter Secure Gateway supports a broad range of authentication protocols e.g., LDAP, Active directory®, TACACS+ and RADIUS, and supports primary as well as backup authentication servers. User access can be controlled by IP address as well as by policy management and log-in attempts. Full 128-bit SSL encryption is provided for all KVM traffic, and proxy mode enables secure access through VPNs and firewalls. CC-Secure Gateway employs a closed, Linux-based appliance architecture, which guards against backdoor passwords.

The CommandCenter Secure Gateway offers ease of use and management features for multi-site, multi-platform data center equipment, consolidated access, and administration of server assets and power devices from a single dashboard. It supports SNMP traps and events,

Service Management Made Simple For Mid-Sized Organizations

OS updates, and other change management capabilities, customizable user access and control, reporting tools, and built-in diagnostic capabilities.

Security management is a critical requirement of all corporate and IT governance mandates. The CommandCenter Secure-Gateway enables simplified single sign-on access to gain secure, centralized management of multiple data centers, branch offices and remote locations. With comprehensive, Web-based monitoring, diagnostics and reporting, CC-Secure Gateway simplifies secure service management for MSBs leveraging both in-band and out-of-band capabilities.

Customer Case Study

EMA conducted an in-depth interview with the technical director of testing labs for a global non-profit IT industry trade association. This organization is responsible for authoring standards in its area of expertise for subsequent ISO certification, which is followed by uniform adoption by vendors around the world.

The association's primary lab environment is in the U.S. and contains approximately \$40 million worth of equipment donated by 60 association member companies for use in testing broad compliance with ongoing standards. Affiliated labs in China, Japan, Singapore and Australia are connected with the U.S. lab via VPN links to enable members in those regions to connect and download the association's specifications from the U.S. lab and conduct further testing on their own locally.

The lab had a growing need to perform 24/7 tests, which drove a parallel growth in its need to combine their existing KVM with a "smarter package" that included a portfolio including Command Center NOC and out-of-band Raritan solutions.

The association deployed CommandCenter NOC at its U.S. facility and at labs in China, Japan and Singapore for tech support and fault management on a follow-the-sun basis to drill down into what was going on in those network links back to the U.S. In the past, the association was faced with primarily "unstructured and non-specific complaints," in an ineffective flurry of e-mails. But with CommandCenter NOC it could assign a permanent IP address to each vendor. If there were problems, CommandCenter NOC would find and diagnose the problems quickly, eliminating the need for core IT personnel to provide first level of support.

The association had a rather memorable "baptism by fire" with CommandCenter NOC. Barely an hour after the device was installed, a hacker broke into a member's network and began to launch a denial-of-service attack. CC-NOC detected the threat right away and posted log entries indicating the level of activity and affected hosts. It immediately traced the source of the problem to a member's network, which enabled the problem to be contained and resolved quickly. In the past, such a problem would have taken many hours or even days to isolate before remediation could take effect. "This experience convinced everyone to trust the VPN with the new Raritan system," said the association's technical director.

Initially the association didn't think the product could work in such a diverse multi-vendor environment, but that skepticism was proven wrong. A single director with a few university interns can now do the job estimated to require seven to ten IT professionals.

This example demonstrates the ability of the CommandCenter NOC platform to simplify the complex task of monitoring service levels in centralized as well as distributed IT environments. Automated fault and security management capabilities led to prompt discovery and notification of service management issues, enabling a return to proper operational levels as quickly as possible with little or no human intervention required.

EMA's Perspective

Service management for mid-tier businesses has been underserved by the IT management industry. Most solutions are either too costly or hard to deploy, underpowered, or are point solutions and lose the benefit of integration.

Raritan's CommandCenter Service Management Architecture, combining service management capabilities with both in-band and out-of-band monitoring and remediation, is unique and valuable. Raritan's portfolio promises to deliver to IT shops with limited resources easy and sophisticated ways to step up to best practices for service management without getting buried in complexity and non-relevant detail.

The CommandCenter family is a timely and strategic addition to Raritan's KVM-oriented portfolio. The company lacked a strong in-band service management solution, and has filled that gap effectively with CC-NOC's

Service Management Made Simple For Mid-Sized Organizations

powerful and well-integrated monitoring, remediation and reporting capabilities. Meanwhile, CC-Secure Gateway expands Raritan's out-of-band secure management capabilities considerably, with intuitive logical and physical views of IT resources and simplified user interface. Together, the two products, plus other members of the CommandCenter management product family expected in the foreseeable future, promise to allow MSBs to simplify the task of service management best practices considerably.

At the same time, Raritan is underscoring its leadership position in the KVM market. While this segment is approaching maturity and industry revenue growth has slowed, it is still a sizable and important market, estimated at approximately \$600 million by EMA. Raritan's "KVM on a chip" technology, gained through its acquisition of Peppercon Technologies, places all intelligence on a single chip, reducing footprint and costs for customers. The company continues to invest in remote KVM, serial, and power control, and has a number of next-generation products planned.

There are plenty of other solutions in the market that combine a mix of security, asset and monitoring capabilities. However, to EMA's knowledge, virtually none of them can compete at Raritan's price point, and none are as well designed for out-of-the-box deployment and ease of administration. Moreover, Raritan's versatile operations portfolio, workflow and nascent help desk capabilities, combined with out-of-band remote control, is a distinctive, and in EMA's opinion, winning mixture to support service management for mid-tier businesses.

About Raritan

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.



About Enterprise Management Associates, Inc.

Enterprise Management Associates, Inc. is the fastest-growing analyst firm focused on the management software and services market. EMA brings strategic insights to both vendors and IT professionals seeking to leverage areas of growth across e-business, network, systems, and application management. Enterprise Management Associates' vision and insights draw from its ongoing research and the perspectives of an experienced team with diverse, real-world backgrounds in the IT, service provider, ISV, and publishing communities, and is frequently requested to share their observations at management forums worldwide.

Corporate Headquarters:
Enterprise Management Associates
2585 Central Avenue, Suite 100
Boulder, CO 80301, U.S.A.

This report in whole or in part may not be duplicated, reproduced, stored in a retrieval system, or retransmitted without prior written permission of Enterprise Management Associates, Inc. All opinions and estimates herein constitute our judgement as of this date and are subject to change without notice. Product names mentioned herein may be trademarks and/or registered trademarks of their respective companies. ©2006 Enterprise Management Associates, Inc. All Rights Reserved.



**ENTERPRISE MANAGEMENT
ASSOCIATES®**

Phone: 303.543.9500

Fax: 303.543.7687

info@enterprisemanagement.com

www.enterprisemanagement.com

1095.041806