

Real Help for Migrating to a Virtual Infrastructure

New Ecora whitepaper shares five keys for consolidating physical servers into a virtual environment

by Bryan Cote, Senior Product Manager

Since the late 1990s, exponential increases in CPU power combined with plummeting hardware prices have led to an explosion of servers in the modern IT organization. This “one application to one server” philosophy made tremendous sense when it came to managing the deployment of new solutions across the enterprise.

Over time, however, this approach has led to a proliferation of under-utilized assets (both software and hardware); the sheer quantity of physical servers has contributed to a vast increase in management, complexity, maintenance, and utility costs. In the continuing effort to reduce costs and increase efficiency, the “virtual machine”—a concept dating back to mainframe days—has been quickly gaining popularity.



A Yankee Group Report from January 2007, *SMB Infrastructure Goes Virtual*, asserts, “the initial and obvious benefits of virtualization were server consolidation and higher server utilization. As the products matured, other benefits such as disaster recovery, high availability, easier management and backup, and improved security started to be realized.”

Yankee Group also found that sixty-two percent of survey respondents already had a virtualization

solution in place, or are in the process of migration. Of those having existing virtualized servers, VMware is the clear leader, with 55% of the market.

In spite of the advantages that virtualization provides, challenges remain. The ease and flexibility in creating virtualized servers have helped consolidate where servers are located—greatly reducing the number of physical machines—but has, simultaneously, resulted in an enormous increase in the number

continued page 3

Spring Breakfast Seminar Series Draws Hundreds

Across the country, leading IT executives bear advice for driving down the cost of compliance

Ecora recently concluded a six week, eighteen-city breakfast seminar series focused on “Driving Down the Cost of Compliance.” Over the course of the series, more than 200 IT executives turned out to hear leading IT security, audit, and operations experts share how they successfully avoided some of the costs associated with documenting security controls and meeting multiple compliance requirements using automated software solutions.

Industry experts presenting included Michael Hoelsing, IS Audit Manager at First Bank Nebraska, Inc.; Nick Garbidakis, CIO/CTO at American Bible Society; Rick Hayes, IT Security Manager at Carter’s, Inc.; Dick Stark, President of

RightStar Systems; Jeff Dalton, Western Region CTO for Stewart Information Systems; Pete Keenan, IT Manager at Central Garden & Pets; and Brian Young, Senior Server Analyst with TriHealth. Alex Bakman, Chairman and Founder; James Sayles, Chief Compliance Advisor; Bryan Cote, Senior Product Manager; and John Walsh, Vice President of Engineering, served as hosts and co-presenters for Ecora throughout the series.

Those in attendance were able to learn how to:

- Address PCI DSS, SOX, HIPAA, and other compliance requirements
- Avoid common compliance challenges and shortfalls

- Understand the scope auditors will use for their assessment
- Anticipate the control validation auditors will expect to see
- Reduce audit preparation and compliance validation time by 95%
- Use automation to proactively identify authorized and unauthorized system changes
- Prepare for future IT compliance and governance demands

If you were unable to attend any of the live presentations, we offer a recorded webinar version, recorded live at the Phoenix event. This presentation features Michael Hoelsing and Ecora’s James Sayles. [Click here](#) to download the presentation.

“Securing Cardholder Data So You Don’t Make Headlines” **2**

New Ecora webinar and whitepaper help you leverage compliance requirements to improve information security...

New PCI Gap Analysis Service

Identify control and process gaps; ensure compliance with the Payment Card Industry Data Security Standard...

Take Advantage of Ecora’s Self-Service Support Portal **3**

Search Ecora knowledgebase, submit or review cases—quickly and easily...

Patch Manager 5.0 SP1 Now Available

The release of Patch Manager 5.0 SP1 is just one of the benefits you receive from your investment in ongoing maintenance and support.

Neos Banca **4**

Automating Business Processes to Ensure Security, Compliance, and Disaster Preparedness...

Alliance Update

New Partnerships Extend Ecora’s Reach...

New PCI Gap Analysis Service

Identify control and process gaps; ensure compliance with the Payment Card Industry Data Security Standard

With this new Ecora service, merchants and service providers can quickly identify the existing process and control gaps associated with areas within nine of the twelve requirements that form the PCI Data Security Standard.

You'll discover the vulnerabilities and risks that threaten your current IT operation, and benefit from a gap analysis report that you can use to correct these vulnerabilities. You'll also learn how you can implement automated processes for reporting on PCI DSS assessment requirements.

During the Gap Analysis, Ecora professionals will identify the PCI-significant systems that Ecora Auditor Professional will collect and analyze any PCI-significant systems, determine any existing security processes, document security gaps within your information systems environment that stores cardholder information, and prepare a comprehensive gap analysis report.

Ecora's PCI Gap Analysis Service can enable you to lower the overall cost of maintaining and validating compliance, and reduce the cost of the assessment process itself. Additionally, Ecora's software solutions provide an ongoing process and framework for establishing a state of continuous compliance.

To learn more, [click here](#) to download the PCI Gap Analysis Service data sheet.

"Securing Cardholder Data So You Don't Make Headlines" *New Ecora webinar and whitepaper help you leverage compliance requirements to improve information security*

by James Sayles, Chief Compliance Advisor

Breaches in network security—particularly those that threaten customer credit card data—have impacted organizations of all sizes and types, from some of the world's most recognized brands to small, regional businesses, and these security breaches have made national, and international, headlines.

An escalation in the number of security breaches did not come about because the companies affected didn't have solid network security controls in place; most of them did. The fact is that security, and what needs to be secured, is more complex than ever before. It is no longer effective to secure just the enterprise perimeter. Today's organizations must secure the entire infrastructure, and they must control the people and processes that interact with the infrastructure as well. Neglecting security efforts in any one of these areas can leave an organization vulnerable to a security breach.

In fact, in today's business environment, focusing on IT security alone isn't enough. Organizations must broaden their thinking to encompass overall information risk. Information risk management is a business function and encompasses regulatory compliance as well as issues of intellectual property protection, insider abuse, and privacy.

Security and Compliance through PCI-DSS

The Payment Card Industry Data Security Standard or PCI-DSS ensures that cardholder data is protected in the event of a security breach by requiring merchants and service providers that store, process, or transmit cardholder data to meet specific security requirements. When organizations work toward and achieve PCI compliance, they will have also implemented a number of key initiatives that improve overall information security.

According to Forrester Research, an audit for compliance with the PCI standard focuses on three primary areas reflecting the "processes," "technology infrastructure," and "people" that are critical to both compliance and security.

1. Identification of sensitive data within your environment
2. Identification of areas where data may be transmitted or stored
3. Identification of all consumers of sensitive data

Developing an Automated PCI Compliance Process

The most common challenges to PCI compliance center on protecting and managing data, controlling change, and auditing and enforcing policies. These challenges also link directly to the most commonly cited PCI violations.

The five most common PCI DSS violations include:

- Storage of prohibited data (e.g., full track, CVV2, PIN)
- Systems on which patches are not kept up to date
- Use of vendor default settings and passwords, such as with unsecured wireless
- SQL injection from poorly coded web-facing applications
- Unnecessary and vulnerable services on servers

With the sheer volume of information processed, transmitted, and/or stored on virtually any infrastructure, collecting data manually is time consuming, expensive, and often not repeatable. In addition, because manual collection efforts may be conducted by different teams and at different intervals, auditors may not view the information as reliable, auditable evidence. Automated, systemic data collection is preferred to substantiate IT controls.



Forrester's Seven Steps to Developing an Effective Compliance Process

1. Document the policy and control environment
2. Assign appropriate oversight of compliance management
3. Require personnel screening and access control
4. Ensure compliance through training and communication
5. Implement regular control monitoring and auditing
6. Consistently enforce the control environment
7. Prevent and respond to incidents and gaps in controls

The Evolution of IT Compliance and Best Practices

In the face of increasing requirements and expectation for continuous compliance, it is essential that compliance initiatives are strategic, integrated business processes and not one-time "projects." It is no longer acceptable to be in compliance for "audits only," and it is important to evaluate the effectiveness of IT controls and compliance initiatives regularly to ensure that goals are being met.

When compliance initiatives are treated as strategic, integrated processes, maintaining continuous compliance simply becomes a part of the way an organization does business. A centralized CMDB provides a single repository for data connection, configuration and change management becomes

continued page 3

Patch Manager 5.0 SP1 Now Available

The release of Patch Manager 5.0 SP1 is just one of the benefits you receive from your investment in ongoing maintenance and support.

Key improvements you'll find in this latest release include:

- Patch support added for Microsoft Core XML Services
- Database support extended to include SQL Server 2005 and SQL Server 2005 Express
- Concurrent user limits removed for Reporting Center 1.7
- Significant usability improvements based on customer feedback in both Patch Manager and Reporting Center

The release of Patch Manager 5.0 SP1 reflects Ecora's ongoing commitment to support Patch Manager and the customers who rely on us to help keep their IT infrastructure secure.

To read the complete release notes for Patch Manager Release 5.0 SP1, [click here](#). If you have questions or would like additional information about Patch Manager, [click here](#).

Take Advantage of Ecora's Self-Service Support Portal

Search Ecora knowledgebase, submit or review cases—quickly and easily

by Ed Bell, Director of Technical Services



Ecora's Self-Service Support Portal continues to grow. Since its launch, we've added more than 350 knowledgebase solutions—and nearly 300 users have joined.

The Ecora Self-Service Support Portal provides you with an easy-to-use online tool to search the solutions knowledgebase, log support calls, and interface with Ecora support personnel to resolve your

issue. Using the Portal also gives you a history of your support tickets and solutions.

Take a look at the [Top-Ten Portal Solutions](#):

- Patch Manager and Windows 2003 SP2
- Auditor Command Line Migration Instructions
- Installation Halted— The VMware VCOM Scripting API is required
- Patch Manager and SQL 2005
- An error [-5006 : 0x80004005] has occurred while running setup
- How to license Auditor manually
- Patch Manager different from Windows Update

- How to download Ecora software products
- Dashboard stuck at recalculating
- How to set the MSI path for multiple systems

The Ecora Self-Service Support Portal is available to customers with valid maintenance and support contracts. To access the portal, [click here](#), and then click on the Support Portal link. To request access to the portal, [click here](#), or contact your Ecora sales representative for more information. Customers using Auditor Lite or under a trial are not permitted access to the Portal and should continue to submit questions using the online [submit form](#).

Real Help for Migrating to a Virtual Infrastructure

continued from page 1

of logical servers. And, as the number of servers has grown exponentially, so has the configuration complexity facing IT departments.

Successfully consolidating physical servers into a virtual environment requires careful planning, accurate documentation, intelligent decision-making, and ongoing oversight and management of the changes to your physical and virtual infrastructure.

Enterprise organizations looking to capitalize on the virtualization trend should invest in an automated solution that collects enterprise-wide configuration data and generates the detailed reports required for effective capacity planning. They should make this investment prior to beginning the complex migration process. Any such solution should also provide easily accessible, enterprise-wide visibili-

ty into the ongoing configuration changes required in both the physical and virtual environment.

This whitepaper shares five keys to ensure your efforts to consolidate physical servers into a virtual environment are a success. [Click here](#) to download the whitepaper.

“Securing Cardholder Data So You Don’t Make Headlines”

continued from page 2

more effective, and policies are consistently enforced. In addition, because testing and reporting can be streamlined across the entire infrastructure, the workload and expense of manual identification can be eliminated, and organizations can reallocate scarce IT resources to focus on key, revenue-generating initiatives.

Building a Sustainable, Automated IT Compliance Program
Ecora provides software and services that allow organizations to implement sustainable, automated IT compliance programs. Organizations can realize both compliance and security, as well as greater operational efficiency. They will also benefit from the ability to validate compliance over time

with a systematic approach to ensuring compliance throughout the IT infrastructure.

To view the webinar “Securing Cardholder Data So You Don’t Make Headlines” on demand, [click here](#). To download the whitepaper, [click here](#).

Alliance Update New Partnerships Extend Ecora's Reach

by Mike Booth, Vice President of Business Development

Ecora actively pursues partnerships with other world-class technology companies to ensure organizations are able to gain the level of enterprise configuration visibility necessary to ensure their IT infrastructure is secure, compliant, and operationally effective.

We're pleased to announce three new partnerships that will provide expanded opportunities for users worldwide to benefit from Ecora's automated compliance and configuration change reporting solutions.

- **Ecora Teams with BMC in Marketzone Reseller Relationship.** BMC will now offer Ecora's Auditor Professional as a compliance capability to customers worldwide. As part of the BMC Marketzone Alliance program, Ecora extends its reach with the support of BMC's 1,800 sales professionals and authorized reseller partners around the globe.
- **Ecora and Dell Agree to Reseller Relationship.** Ecora's Auditor Professional will now be available to all Dell customers through Dell's Third-Party Supplier Catalog.
- **MTM Technologies and Ecora Join Forces to Provide IT Configuration Reporting at Exco Oil.** MTM Technologies, Inc., a leading national provider of information technology solutions and services, and Ecora recently partnered to support an IT configuration reporting initiative at Exco Oil. MTM consultants are using Ecora's Auditor Professional in their consulting engagements to capture network configuration settings quickly and accurately. Auditor Professional provides MTM a real competitive advantage through the more effective use of their consulting resources.

Neos Banca

Automating Business Processes to Ensure Security, Compliance, and Disaster Preparedness

A subsidiary of leading Italian financial services provider Gruppo Intesa Sanpaolo, Neos Banca provides consumer financing options to more than four million customers across Italy. The company has more than 1,200 employees who serve its customers through 300 branches, retail locations, and independent agencies.

Neos Banca deploys a multivendor IT infrastructure, which runs a combination of approximately 50 servers running varied platforms like Linux, Solaris, AIX, and Windows across multiple locations. In addition to its headquarters in Bologna, Neos Banca operates a disaster recovery location in the Torino headquarters of parent company Gruppo Intesa Sanpaolo.

Ensuring Up-to-Date Documentation, Change and Configuration Management, and Control

It is essential for financial services organizations to have a strong focus on security and an effective plan for disaster recovery. Neos Banca is no exception. According to Giovanni Aiello, C.S.O. for Neos Banca, the first step to securing the IT infrastructure and ensuring access to critical data even in the face of a natural or man-made disaster is having complete documentation of IT systems. "Ensuring

security and disaster recovery has become a priority for Neos Banca over the past several years," Aiello explained, "and documenting our IT systems manually to establish a recovery guide was inefficient at best. It was also nearly impossible to track and control configuration changes."

Compounding the problem, Neos Banca was moving its headquarters from Bologna to Torino, causing the organization's IT infrastructure to become even more de-centralized. "With the relocation of our headquarters, ensuring overall control of all our systems became even more important," Aiello said. "I began my search for a tool that would automate our documentation, as well as our change management processes, giving us greater control overall."

Proven Technology in a Comprehensive, Easy-to-Use Solution

After evaluating many of the solutions on the market, Neos Banca chose Ecora Auditor Professional.

"Ecora impressed us right from the start," Aiello said. "Auditor Professional was surprisingly straightforward and easy to install and use. It enabled us to produce exactly the kind of system documentation we needed right away."

"Ecora impressed us right from the start. Auditor Professional was surprisingly straightforward and easy to install and use. It enabled us to produce exactly the kind of system documentation we needed right away. We had considered a number of other solutions, but we discovered that they were far more monolithic and complex to install and operate. In the end, they couldn't really provide what they said they could. Ecora Auditor delivers exactly what it promises."

— Giovanni Aiello Chief Security Officer Neos Banca



We had considered a number of other solutions, but we discovered that they were far more monolithic and complex to install and operate. In the end, they couldn't really provide what they said they could. Ecora Auditor delivers exactly what it promises."

Prior to choosing Ecora, Neos Banca had also looked to consultants to provide documentation support. "The cost for a consultant to document our IT infrastructure would have been hundreds of thousands of Euros," Aiello said. "We would have also needed to contend with the cost of updating documentation after changes had been made and whether the documentation would meet our standards, regardless of who compiled it. When we discovered Auditor Professional's automated capabilities, we realized that our documentation would always be up to date and would always meet our internal standards, regardless of who initiated the documentation process."

[Click here](#) to see full Case Study.