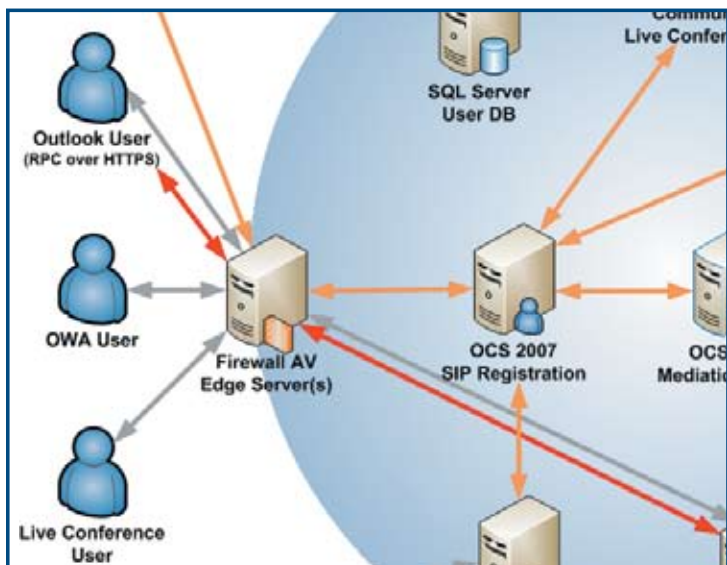


# Bandwidth

The Leading IT Security & Data Center Solutions Publication – Vol. 09, Issue 1

## IN THIS ISSUE...



### Realizing the Value of Unified Communications

Unified Communications is changing the way business is done. Learn what exactly is Unified Communications and how it can help your business become more agile, respond quicker to change, and increase collaboration. Discover some of the key components to UC; where the value proposition lies; and how you can begin to implement a UC strategy throughout your organization.

[Read more from Akibia on page 4](#)

### Actionable Intelligence RSA enVision

Read how RSA enVision has helped businesses to be proactive with security monitoring and comply with PCI standards - [page 6](#)

### DNS Security: Old Vulnerabilities and New Realities

Learn why DNS security is both important and challenging, and the importance of managing DNS and other core network services including DHCP and IPAM - [page 8](#)

### How to Ensure Your Virtual Environment is Secure - Check Point VPN-1 Virtual Edition

Check Point's latest release of enterprise firewall software VPN-1 Virtual Edition protects your virtual systems with the same best of class security that you rely on for your physical network - [page 10](#)

### Akibia Introduces 24x7 Support for Blue Coat Systems - page 2

### Leveraging the Benefits of Migrating to Exchange 2007 - page 14

### Reduce Data Center Support Costs up to 40% while Ensuring the Highest Level of Service and Support - page 14



# TABLE OF CONTENTS

3 Case Study: The Show Must Go On with Akibia and the Boston Red Sox

4 Realizing the Value of Unified Communications by Akibia

6 Actionable Intelligence RSA enVision

8 DNS Security: Old Vulnerabilities and New Realities by Infoblox

10 How to Ensure Your Virtual Environment is Secure by Check Point

12 WAN Optimization In Practice at Akibia with Blue Coat

13 Akibia News

Bandwidth is a publication of



Please send comments, questions or suggestions for future issues to [bandwidth@akibia.com](mailto:bandwidth@akibia.com)

## Akibia Partner News

### Akibia Named RSA Secure World East Partner of the Year

**RSA, the Security Division of EMC, recently recognized Akibia as the RSA SecurWorld East Partner of the Year.** RSA highlighted Akibia's "continuous ability to perform" supporting the entire suite of RSA security products and bringing compelling security solutions to its expanding customer base. Over the course of the ten year channel partnership Akibia and RSA have developed working processes that help ensure evolving customer demands are met quickly and effectively. Akibia's team of RSA certified engineers leverage best practices developed over hundreds of engagements to ensure a seamless implementation that improves the customer's security posture while achieving compliance with industry regulations, and limiting risk.

"With a focus on addressing the unique challenges of each customer, Akibia works to deliver best-in-class solutions that will solve real world challenges related to data loss prevention, security information and event management, and identity management," said Anthony D'Angelo, director, Channel Sales, RSA, The Security Division of EMC. "RSA's solutions are engineered to successfully solve these challenges, resulting in significant success, for the customer as well as Akibia and RSA. We are excited to recognize Akibia's accomplishments with the RSA East Partner of the Year Award."

### Akibia Offers New Support Service for Blue Coat Systems

Akibia is committed to continuously introducing new services that help customers realize the maximum value from their data center, network and security infrastructure. **Akibia has introduced 24x7 support for Blue Coat Systems WAN optimization and web security solutions.** The new offering will allow Akibia's customers to benefit from a single point of contact for design, implementation and support.

Akibia is known for its support of high-end systems from Sun, HP, IBM and Dell and the Check Point and Nokia product lines, having supported these environments for some of the largest organizations in the world for the past 20 years. Already a trusted integration partner of Blue Coat Systems, Akibia is adding support capabilities for these products so that customers can benefit from a single point of contact throughout the design, implementation and support process.

The Akibia technical support center is available 24x7 and is staffed by certified engineers, who are experts in the devices they are supporting. Akibia's flexible and innovative approach to providing technical support allows significant customization to suit each client's specific requirements. Akibia's Network and Security Infrastructure Support provides the following benefits to its customers:

- **Faster Problem Resolution** – Industry-trained and certified engineers answer calls quickly. Akibia's average call answer time is less than 25 seconds, and the company does not use voicemail.
- **Customized and Knowledgeable Support** – Akibia support representatives can seamlessly collaborate with the security engineer responsible for the original implementation to identify other issues unique to the customer.
- **Single Point of Contact** – With multiple security devices in the IT infrastructure, it can be difficult for organizations to maintain multiple support contracts with every vendor. As a multivendor security infrastructure partner Akibia can support high-performance Blue Coat, Check Point and Nokia solutions, eliminating the need for customers to make multiple calls when an issue arises.

# The Show Must Go On!

## Akibia's Customer-First Approach Helps the Red Sox Avert Internet Issues During the Neil Diamond Concert at Fenway Park



When the Red Sox open up Fenway Park, one of Major League Baseball's most cherished ballparks, for performances by famed musicians fans come to the event expecting a great experience. The fans are not thinking about the technology and the IT support services that go into making such an appearance possible. However, behind the scenes, in the Red Sox IT organization, a lot of effort goes into ensuring the technology infrastructure is running smoothly and able to support the production needs of the band. When Neil Diamond played Fenway Park in the summer of 2008 quick thinking by the Red Sox IT department and Akibia's agility and flexibility in providing unique solutions for its customers helped to ensure a successful performance and positive fan experience.

### Challenge

As the Red Sox organization was preparing Fenway Park for Diamond's performance, the IT department noticed its firewall was continuously rebooting, often taking 15-20 minutes to come back up, resulting in lost Internet access and crippling the organization's ability to monitor their own infrastructure. A combination of issues was causing the failure, including an over-heating service room that caused the hardware to shut down, and a faulty processor. Without

monitoring capabilities, the IT team had no way of knowing if or when the Internet was down.

"We were preparing for the Neil Diamond concert and knew that we did not have the staff to be onsite during the weekend," said Randy George, senior systems analyst at the Red Sox Organization. "But without monitoring capabilities we would only know if it went down if the band's production team called to say they had no Internet access—and that would be too late."

The Red Sox called their firewall support provider and trusted security advisor, Akibia.

### Solution

Akibia's Premium Support provides clients with 24x7 access to our technical support center and incorporates guaranteed response times, ensuring efficient and effective problem resolution. Akibia also provides Managed and Monitored Firewall services as part of our total network and security solutions, but the Red Sox organization is not currently a customer of this service.

However, the Red Sox know Akibia is an agile and customer-focused service provider, so when an issue arose that was outside of the companies' existing agreement, the Red Sox didn't hesitate to call Akibia anyway.

Akibia leveraged its monitoring service to set up a remote monitoring solution for the Red Sox firewall. The Akibia support team had the solution up and running within hours, effectively averting a crisis for the Red Sox organization.

### Result

"Ultimately the firewall did not fail once monitoring had been set up, but if it had, Akibia's quick solution would have been able to alert us of a failure before anyone in the Park, or any member of the band's

production team had even realized a problem," said George.

While the stop-gap measure helped the Red Sox organization get through the weekend without an incident, Akibia was also able to quickly fix the firewall problem, going onsite the next business day to repair the hardware and install a second firewall device at a remote location for failover.

According to George, Akibia's commitment to customer service is unmatched. "Their quick response with a unique agent-less way to monitor the firewall offsite is just one example of Akibia's customer service. I wouldn't have received that level of service from anyone but Akibia."

#### INDUSTRY

Sports & Entertainment

#### CHALLENGE

Keep a Firewall from crashing during the Neil Diamond concert at Fenway Park. A crash would have caused problems for the band.

#### SOLUTION

Akibia's Security Infrastructure Support

#### BUSINESS BENEFITS

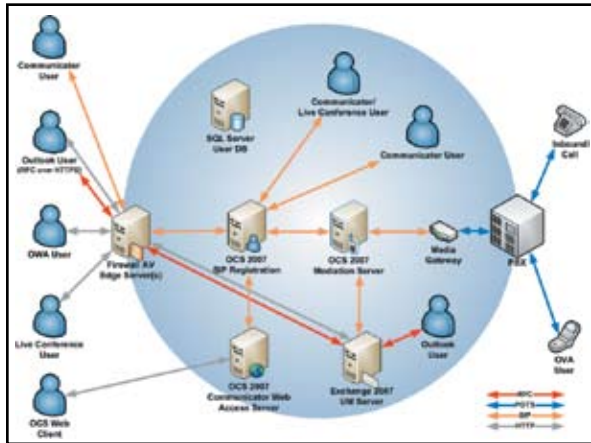
Potential issues were diverted before the end-users noticed any issues with the firewall and Internet connection.



[www.akibia.com](http://www.akibia.com)

# Realizing the Value of Unified Communications

By Mark Bushey, SENIOR CONSULTANT, AKIBIA, INC.



The following diagram illustrates how UC is accomplished with Microsoft Office Communications Server 2007 and Exchange 2007 Unified Messaging.

## What is UC?

The reason the great companies of the world have become successful is because they understand the need for the technology that drives that success and the fact that you are reading this article means that you understand that concept. In addition, tough economic times call for ways to cut costs while improving productivity. That's what UC is all about; driving success by streamlining communications while cutting costs by leveraging existing infrastructure; tying all the people, devices, and information together into a more intuitive and controlled platform.

Along with the confusion about the different UC solutions in the vast UC ecosystem, when you ask people what UC actually is you may get a range of different definitions depending on what they are selling. So what exactly is Unified Communications and how can it affect your business? To put it simply, UC integrates all the systems that a user might already be using and helps those

systems work together in real time, increasing both the quantity and quality of collaboration. There is also a bigger picture here; UC changes the way business is done by allowing organizations to become much more agile. It allows businesses to respond to change quicker, meet that competitive challenge more efficiently, increase collaboration, and simply enable people to do their jobs better. The results are shortened sales cycles, decreased workflow process time, increased

customer satisfaction, more secure transactions, reduced travel expenses, and increased employee productivity. UC is going to simplify the way business is done forever and now is the time to begin thinking about where you want to position your business within the UC landscape.

## Components

There are many differing components to UC and they may not all apply to your specific business objectives. Here are some key ingredients to Unified Communications:

- **Unified Messaging** - UM delivers all messages into one inbox; fully integrating e-mail, fax and voice mail to the end user. The result is that all messages are available in whatever tool is most convenient.
- **Instant Messaging** - a main component of almost all UC solutions; IM will allow most companies to benefit greatly from having a more

secure instant messaging solution that has a further reach into the enterprise.

- **Presence/Identity** - A UC solution with presence allows for more choice, further reach, and a true collaboration experience. By replacing people's numerous phone numbers, e-mail addresses, and IM addresses with a single Identity you can view other people's presence, or availability status, and taken action on it with whichever tools are most appropriate for any given situation.
- **Existing Infrastructure** - Many companies are also looking to cut costs by leveraging existing infrastructure. Having the choice to integrate your UC solution into your existing PBX and Active Directory infrastructure may be a critical component of your chosen solution.
- **Video Conferencing** - This is another component to UC that has the potential to save companies a lot of money in travel expenses by allowing for ad-hoc meetings, webcasts, training events, meetings, and presentations.
- **CEBP** - A UC solution built on a future-proof software foundation opens the door to Communications Enabled Business Processes where you can integrate your UC solution into information stores such as CRM, ERP, databases, SharePoint, and Supply chain management applications.

## So Where is the Value?

It's important to target your specific objectives as you begin to plan your UC strategy because the amount of value that may exist depends on matching these

objectives with the right technology for your specific business. Some companies will realize the value of UC by replacing the use of an insecure application like Skype with a more controlled and integrated business solution such as Microsoft Office Communications Server (OCS 2007). Within the credit card industry, value might be achieved by being able to link UC to Communication Enabled Business Processes (CEBP). Thereby improving customer satisfaction and reducing workflow process time by automating the validation of credit card transactions that are outside the normal area of usage. Another enterprise might see value in deploying a virtual meeting telepresence solution such as Microsoft RoundTable which allows businesses to communicate quicker, reduce travel costs, offer flexibility, and draw on collective knowledge and talent that may exist elsewhere within your own company. Overall, most companies will see the value of UC in a solution that has presence and identity at the core. For example, in Microsoft's Office Communicator client, presence uses a single identity that captures user availability status and communication information, enabling someone who needs to get in touch with someone else to track that individual down using the most effective medium for the situation.

## How Do I Get There?

So where do you go from here? How do you begin your UC strategy? Some concepts that should be thought of while planning any UC project include strategies like:

- **Don't rip and replace** – A common misconception is that you need to upgrade much more of your infrastructure for UC. By choosing an application layer software solution you stand to benefit from keeping much of your existing investments and keeping costs to a minimum.
- **Target business objectives** – Again, there are many different facets to Unified Communications and they may not all apply to your specific business. Determining your specific business goals, pain points, and objectives will allow

you to get the most out of UC without wasting time and money on pieces that you may not need.

- **Phased modular approach** – UC is in rapid development and you want to make sure your solution matures and evolves with it. Match your business objectives to the technology and start with an assessment, UM, IM, or evaluating a media gateway that will allow you to scale into a larger UC solution later. Make educated business decisions and phase into your UC solution.
- **Network, security, and storage considerations** – Assessing your network is the first step you should take before implementing your chosen UC solution. You are transitioning much of the traffic that was once running on the PSTN and PBX into your data network and this creates many new challenges. Failure to assess your network to ensure that it is sufficient for UC is a recipe for disaster. You want to ensure call quality and avoid user resistance at all costs. Securing your solution is also equally important. New requirements are brought to the surface when deploying UC; things such as Securing IM and SIP traffic need to be addressed. Storage is another consideration; with Exchange 2007 Unified Messaging you are taking voicemails off of your PBX and putting them in your information store which raises questions that need to be answered with the proper storage architecture.
- **Proving ROI** – This becomes a difficult task with UC because of the fact that the technology has the ability to affect the entire enterprise. Having a trusted advisor to help you with this process of determining ROI is essential to justifying your UC project budget.
- **Partner up** – UC deployments are "IT all hands on deck" projects with a lot of moving parts and may require software expertise or project management skills instead of just a product certification alone. Organizations that successfully deploy UC often turn to a partner for help with everything from evaluating how UC

can impact the business to selection and deployment of technology. As you begin developing a UC strategy, it is important to determine who can help you with the process. We believe the best approach is to select an objective, vendor-agnostic business partner who can help determine how and where UC can impact your business, and how to best integrate UC into your existing infrastructure – all with an eye on reducing risk and maximizing ROI. You need a partner that can help you Optimize, Secure, Manage, and Support your critical IT infrastructure to meet your business needs. These elements are critical to the success of any UC project. Make sure you are in good hands and you will enjoy all the wonderful benefits that UC has to offer your business.

## Akibia Whitepaper Unified Communications: Unleashing the Power of Collaboration

A well-designed and deployed UC architecture can provide organization's with strong competitive advantage; increased efficiencies and significant return on investment. Read Akibia's whitepaper to better understand the benefits and pitfalls of Unified Communications.

Download the whitepaper at: [www.akibia.com](http://www.akibia.com) in the newsletters and whitepapers section.



[www.akibia.com](http://www.akibia.com)

# Actionable Intelligence RSA enVision™

## **RSA enVision® in a leadership position in the 2008 Gartner Magic Quadrant for Security Information and Event Management.**

Have you had a chance to read the 2008 Magic Quadrant Report for Security Information and Event Management, which shows RSA enVision™ in a leadership position? This report notes that RSA has the largest installed base with well over 1,400 customers. RSA not only has extensive market knowledge but also is committed to their customers to provide future product enhancements. This report details best in breed vendors and steps the decision makers need to choose a log management and Security information and Event Management solution.

## **News – The Wall Street Journal:**

Williams-Sonoma Inc. selected enVision software from the RSA security division of EMC Corp. to help it comply with PCI and other security requirements and to reduce the amount of time its staff spends on compliance audits. As a result, Williams-Sonoma has been able to cut in half the time it takes to perform a security audit and to trim by 75% the security team's response time to problems. Go to [www.rsa.com](http://www.rsa.com) under the news and events section to read the October 27, 2008 article titled "Looking for Trouble" from The Wall Street Journal.

## **Awards:**

RSA enVision Wins Info Security Products Guide 2008 Global Product Excellence Award for Customer Trust in Event Management Solution Category.

RSA enVision Named 8 of the Channel's Hottest Security Offerings from Computer Reseller News.

## **RSA enVision® PLATFORM EMPOWERS DTCC THE DEPOSITORY TRUST & CLEARING CORPORATION TO BE PROACTIVE WITH SECURITY MONITORING**

*"RSA enVision enables us to find a needle in a haystack. The product points us to the area to look for the needle and sometimes it puts the needle right on top of the haystack."*

**PARTHIV SHAH, Director of Vulnerability Management in DTCC Security Operations Group**

## **BUSINESS CHALLENGE**

Continual security audits and SEC evaluations require up-to-date security monitoring on privileged users, multiple logins and many more security issues.

DTCC recognized a passive approach to security was not an option for their company in order to meet the internal and external policies.

## **SOLUTION**

RSA enVision provided the multi-platform support, pulling logs from disparate systems - legacy and new.

Aggregation and correlation of security data was key to DTCC to understand behaviors and trends which could trigger security alerts.

## **RESULTS**

DTCC now has a better sense of privileged users and user authentication behavior, giving them data to solve problems around login issues or unusual access behavior.

DTCC currently captures 85 million events per day through logs and therefore feels confident they truly have a picture of all the data to make better security decisions.

## NOVA INFORMATION SYSTEMS ACHIEVES GLOBAL PCI DSS COMPLIANCE WITH THE RSA enVision® PLATFORM.

*“The RSA enVision platform has changed how we work. Before, with over 1,400 device logs to analyze, it was virtually impossible to research and investigate system and network events thoroughly. Now with RSA enVision technology, we can quickly and efficiently troubleshoot incidents and find the root cause of an event.”*

**ADRIAN SANABRIA, Security Architect, NOVA Information Systems, Inc.**

### BUSINESS CHALLENGE

As a payment processor, NOVA is required to comply with the PCI standard.

With worldwide heterogeneous data centers, they needed local data capture that can be managed centrally and be scalable to grow with the business.

### SOLUTION

The RSA enVision IPBD LogSmart database allowed fast access to All the Data™ for both its real-time trouble shooting and incident analysis.

The RSA enVision platform allows NOVA to readily add all its diverse systems, network devices, applications and databases, efficiently collecting and protecting All the Data™.

### RESULTS

Audit trails are easy to collect, complete and secure from a compliance standpoint.

The RSA enVision platform enables Nova to meet its security and compliance requirements.

## RSA enVision® PLATFORM HELPS GIANT EAGLE TO COMPLY WITH THE PCI STANDARD

*“We selected RSA enVision because it offered a superior proof of concept when we tested it in our lab and because it includes packaged compliance reports that allow us to easily implement compliance with industry standards.”*

**RYAN VOLOCH, Data Security Analyst**

### BUSINESS CHALLENGE

Complying with multiple industry standards for safeguarding information.

Efficiently consolidate vast amounts of disparate log information from over 2,500 devices and applications from over 300 locations.

### SOLUTION

The RSA enVision solution delivers 100 percent visibility into all compliance and security threats across the entire information infrastructure.

With the use of RSA enVision's baseline learning system Giant Eagle could see exactly what usual-or-unusual-patterns formed on the network.

### RESULTS

IT can respond faster to external threats and uncover internal ones by gaining unified and comprehensive visibility over the network.

Be compliant and provide enterprise wide logo management within weeks to hit the PCI DSS deadlines.

Please contact your Akibia sales representative for a copy of the 2008 Gartner Magic Quadrant for SIEM, Proactive Security Monitoring with RSA enVision® Platform report, developed by IANS Working Knowledge Series™ or for a copies of the Nova Information Systems or Giant Eagle case studies.



The Security Division of EMC

[www.rsa.com](http://www.rsa.com)

# DNS Security: Old Vulnerabilities and

By **Greg Ness**, SENIOR DIRECTOR, INFOBLOX

Infoblox VP Cricket Liu was on a webinar with Dan Kaminsky the week before Dan's DNS cache poisoning exploit discovery was accidentally leaked by security experts. News of the leak managed to bring even more attention to an issue impacting close to 12 million recursive name servers; and it also helped to sustain a massive global collaboration effort that resulted in close to 70% of those vulnerable servers being patched.

long term demands on DNS that have emerged since Kaminsky's Black Hat presentation.

According to Liu, DNS was already strained by developments in its incredible 25 year history. DNS was already doing things far beyond the vision of its creators. The DNS exploit discovery simply exposed a broader audience to one of many new security implications inherent with this ubiquitous core network service.

## Cricket: We've entered a new age of DNS

Cricket advises enterprise IT professionals that they are going to have to be faster and more proactive in coming years as the security implications play themselves out between the security industry and malicious hackers. According to a recent CSI Survey Report, within months of the DNS exploit discovery targeted attacks started appearing:

*"Enterprises are beginning to feel the heat from two emerging classes of exploits that have emerged over the past year: targeted attacks and DNS vulnerabilities, according to a new study scheduled to be released next week." Tim Wilson, Dark Reading October 3, 2008*

And it is unlikely that these attacks will stop, as many security experts are acknowledging that there will be more patches and more exploits as more attention is focused on DNS. Clearly, these increasing pressures will drive more IT pros to deploy core network service automation solutions from vendors like Infoblox.

Infoblox has launched a new twenty minute deep dive bloxTalk™ on the exploit itself and why it is such a significant threat to the integrity of the Internet. Infoblox has also released the aforementioned series of bloxTV Cricket interviews about DNSSEC.

DNSSEC (for Domain Name System Security Extensions) is a set of extensions to DNS that address data origin and integrity, and denial of existence. One of the key challenges it faces is a kind of "chicken and egg" problem; that is, it won't be truly effective until it enjoys widespread adoption. As of fall 2008 adoption has been very limited. Perhaps



*Cricket Liu is the author of O'Reilly's DNS and BIND and one of the world's leading authorities on DNS*

The popularity of the webinar inspired Infoblox to create a new streaming media series dedicated to topics like DNS security and others related to core network services, including DHCP and IPAM (IP address management). It was no accident that the first five episodes are related to DNS security. These episodes and more are now available at [www.infoblox.com](http://www.infoblox.com).

In the first episodes of bloxTV Cricket talks about the initial impact of the DNS exploit on DNS security as well as new

When you combine the widespread existence of the vulnerability with its ability to be exploited in seconds via a cache poisoning attack you have the making of what Cricket calls the "biggest" vulnerability ever. Kaminsky didn't discover the vulnerability; he actually discovered a new and powerful exploit. His discover is having a significant impact on the management and security of DNS.

# New Realities

its biggest boost came when the federal government mandated adoption by federal agencies by December 2009.

## Why DNSSEC is both Important and Challenging

If DNSSEC is adopted it could be very effective remediation for the Kaminsky-discovered DNS exploit, as it would verify the authenticity and integrity of the session being initiated on a DNS server. Spoofing a server with random guesses in an effort to poison its cache would become much more difficult.

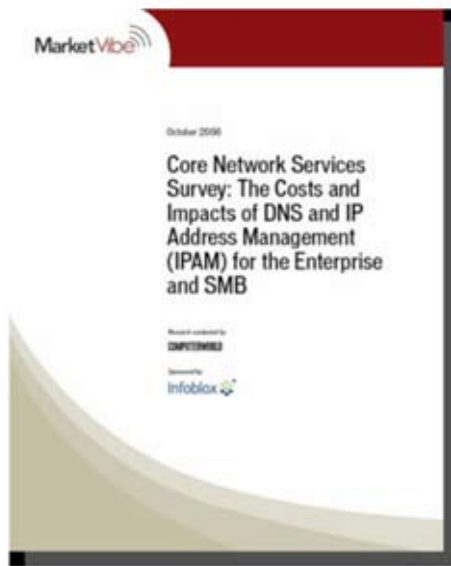
DNSSEC won't be easy to deploy, however, as administration is complex and available tools require specialized expertise. Yet the alternative - of patching repeatedly as patches are updated to protect against new vectors- will also be difficult without the automation of core network services.

## Manual Labor versus Tight Budgets

A newer strain on DNS security is no doubt the emerging cautious enterprise IT spending climate. Some enterprises may be forced to accept higher exposure to DNS vulnerability attacks because they haven't invested in automation; every new patch will take longer and tie up more network management resources. Even today, studies show that more than 20% of recursive name servers are still not patched. As enterprises tighten their budgets, we could see "unpatched" levels go even higher.

Larger networks could be particularly vulnerable as they are already bearing the brunt of rising IP Address Management (IPAM) costs, as discovered recently by Computerworld research. As networks grow, management costs increase. It is likely that the costs of managing DNS and

other core network services will increase with these new demands.



*Recent Computerworld Survey Report shows larger Enterprises Paying Greater per IP Management Costs*

2009 promises to be a year of many new challenges when it comes to DNS and the management of core network services. With proper planning and the right tools, our customers should come through in even better shape than they were in 2008.

## The Beginning of the End of Static Infrastructure

The growing realization that enterprises are deploying more dynamic systems within IT while still depending upon manual processes around DNS, DHCP, and IP Address Management has led to online conversations about Dynamic Infrastructure, or Infrastructure 2.0.

By automating core network services, networks can be made more dynamic and can keep up with changes without the costs and availability risks inherent with manual configuration. You can read more at the new Infrastructure 2.0 blog, including links to third party discussion about the network implications of virtualization and cloud computing at [www.infra20.com](http://www.infra20.com).

Infoblox 

[www.infoblox.com](http://www.infoblox.com)

# How to Ensure Your Virtual Environment is Secure – Check Point VPN-1 Virtual Edition

Total Security for Virtual Systems



Server Virtualization is a technology that has provided tremendous benefits to the IT world. It has lowered operational costs and increased operational efficiency through optimized performance, lower hardware costs and shorter provisioning times among other things.

What has been lost in this migration to a virtual environment is that a virtual server is still very much a server. While traditional best practices still apply, there are a “host” of other factors that need to be considered in virtual deployments. Some of which are a direct result of having many eggs in a single basket from a hardware and operational perspective.

To understand why security is so critical in virtual environments, let’s briefly cover the basics. At its most simplified description, an ESX Host (in the VMWare world) is a single physical machine that concurrently runs multiple instances of servers known as guests or VM’s. The ESX host does this by tricking each guest into thinking that it has direct and unique access to all physical system resources (memory, CPU, I/O calls, etc.). The piece of technology used to do the tricking is called the hypervisor. The hypervisor intercepts calls to physical resources and allocates them to individual VM’s as policy or configuration dictates. This lies at the root of why security is so critical in a VM’ed environment.

There are 2 primary categories of security risks in a virtualized environment: Intra-host threats and hyper-jacking. Intra-host threats are those where a single guest VM becomes compromised via an application or OS vulnerability. Because there are no security solutions that sit between each guest host, upon being

Because VPN-1 VE keeps traffic within the virtual appliance server, it eliminates the complication of adding security appliances and switches to secure your virtual environment.

compromised, that individual guest could then impact or bring down every other VM on that physical server. The second attack risk, hyper-jacking, is when the physical server is compromised through a

vulnerability or access to the hypervisor. Due to the fact that the hypervisor can typically only be accessed from either the console or remote access to the console, Industry pundits have acknowledged that Intra-host threats comprise the more vulnerable and concerning infrastructure risk. That being said, both should be considered.

So let’s do just that. To adequately secure intra-host communication, there needs to exist a (virtualized) network device, preferably a firewall, that sits between them. The sensitive nature of virtualized environments also dictates that any solution deployed has been time tested and Enterprise ready. One such technology is Check Point’s VPN-1 Virtual Edition. VPN-1 Virtual Edition is the latest release of Check Point’s enterprise firewall software that has been certified and tested to fully integrate with VMWare ESX Servers. VPN-1 VE is a product that is based on the very mature and stable SecurePlatform hardened operating system. Because VPN-1 VE keeps traffic within the virtual appliance server, it eliminates the complication of adding security appliances and switches to secure your virtual environment. The VPN-1 VE installs with such options as memory allocation and core allocation pre-set, enabling you to get the system secure as quick as possible. You may also customize all settings – including network interfaces and others – to protect your particular environment. By installing Virtual Edition in your ESX environments, you can take advantage of the security offered by Check Point’s VPN-1. Providing robust security between your guest hosts you will quickly and transparently protect against intra-host vulnerabilities.

Now, let's go back and discuss how to protect the hypervisor from outside attack. Just like any other network host, the hypervisor's vulnerabilities are based on its relationship with the physical server. Protect the physical server and the hypervisor is protected as well. Check Point's VPN-1 gateways provide that functionality.

What has been lost in this migration to a virtual environment is that a virtual server is still very much a server.

While enterprise security has always been Check Point's hallmark, management continues to be a distinct differentiator. This is the case with VPN-1 VE as well. Check Point's existing management tools are all that is necessary to deploy the solution. Via SmartCenter or Provider-1 you can manage a VPN-1 Virtual Edition gateway as though it were like any other, taking advantage of SmartDefense, SSL or IPSEC VPN functionality or any other traditional VPN-1 feature. Only Check Point's management solutions can secure both your virtual and physical hosts all from the same console.

Ultimately, the security of your virtualized environment will be based on 3 criteria: the implementation of your VMWare deployment, the integration with certified

VMSafe security technologies, and the ability for your in-house IT staff to monitor and maintain that infrastructure.

Selecting a solution that is enterprise ready, that is based on technologies that your staff already has expertise in, will significantly shorten deployment times and increase operational efficiencies. Check Point's mature and robust security solutions continue to evolve in supporting the latest threats to your environment. VPN-1 Virtual Edition is the latest demonstration of that.

Here are some of the deployment scenarios that customers have been able to take advantage of with VPN-1 Virtual Edition:

#### *Flexible Deployment Scenarios*

VPN-1 VE is designed to protect virtual environments from attack. With the flexibility of the Check Point solutions, you gain options beyond that.

- **Disaster Recovery:** When a site is unavailable, you can provision security services as well as other applications at another location to get information available quickly.
- **Office in a Box:** You can place all necessary applications for a small office - such as email or Web servers - in a virtual environment alongside your VPN-1 gateway to provide a single, secure server that provides all functionality needed by the remote office.
- **Virtualized Management:** The VPN-1 VE also allows you to place the SmartCenter management server within an ESX virtual environment to consolidate applications.

To find out how you can take advantage of Check Point's best of breed technology to fully secure your virtual environment please go to [www.checkpoint.com](http://www.checkpoint.com), or contact your Akibia sales representative.



**Check Point**<sup>™</sup>  
SOFTWARE TECHNOLOGIES LTD.

[www.checkpoint.com](http://www.checkpoint.com)



# WAN Optimization In Practice at Akibia

## Akibia Deploys Blue Coat Appliances for WAN Optimization and Branch Office Web Security



Akibia needed to speed access to centralized files and reduce bandwidth consumption. To achieve this Akibia turned to its trusted WAN Optimization and Secure Web Gateway partner Blue Coat Systems, Inc. Akibia deployed Blue Coat® ProxySG® appliances at its headquarters in Westborough, Mass. and at six branch offices around the U.S. The appliances have reduced the company's bandwidth consumption by 84 percent, resulting in significant operational savings.

### The Challenge

Before adding the Blue Coat appliances for WAN optimization, file access time was subpar, according to Akibia's IT department, and impacted employee productivity. In particular, important Excel files used by Akibia to quote projects took an excessively long time to exchange between a branch office employee and the centralized file server at the company's data center. Akibia's use of ProxySG appliances have made file access nearly instantaneous. In addition, Akibia had been transitioning to a Microsoft SharePoint file system that was slow to access in branch offices over its existing WAN.

"We wanted to accelerate only business-critical applications, while stopping or managing anything malicious or unimportant," said Rick Onorato,

IT director, Akibia. "At the same time, ProxySG appliances give us the ability to secure and accelerate direct Internet connections at each branch office."

### The Solution

To give each branch office direct Internet access, Akibia adopted a "direct-to-the-net" model, which reduced bandwidth by eliminating the need to backhaul Internet traffic to the centralized Internet gateway in the company's data center. With the Blue Coat solution, the same ProxySG appliance in each branch office serves both to protect the office from malicious threats resulting from a direct Internet connection and to provide acceleration for acceptable Web content and applications.

Like many of its own customers, Akibia realized it could improve productivity and overall business processes by accelerating file access in its branch offices, and recognized that the Blue Coat ProxySG appliance could provide faster access while also reducing strain on the network from non-critical applications.

"Akibia's "Think Like a Customer" philosophy is predicated on us leveraging the services and solutions we provide our clients and ensuring they meet successful standards in real-world application," said Robert Klotz, vice president of

Technology at Akibia. "As users of these technologies from Blue Coat Systems and other partners we are able to provide our customers with first-hand knowledge and proven best practices."

"ProxySG appliances enable enterprises and organizations to regain control of their networks by accelerating business-critical content and applications while stopping, managing or mitigating the unimportant," said Steve Rowland, vice president of sales, North America, Blue Coat Systems. "Akibia uses Blue Coat appliances to develop a state-of-the-art network to increase efficiency and productivity, reduce costs and minimize threats."



# Akibia News

## Akibia Introduces Robert Klotz as Vice President of Technology Recognized Technology Visionary Will Lead Akibia's Customer-Focused Solution Development

Akibia announced that Robert Klotz, a leading technology visionary with proven experience in the industry, has joined the company as vice president of Technology.

Mr. Klotz will lead Akibia's team in delivering service offerings that meet the evolving requirements of today's enterprise organizations. As Akibia's technical evangelist, Mr. Klotz will articulate Akibia's strategic vision to customers, partners, prospects and the industry as a whole. He will partner with Akibia's customers, serving as a high-level resource for advice and best practices while also ensuring the company is delivering services that align with customer priorities.

"Robert brings a deep technical background, with specific expertise in systems monitoring,

network management and managed services delivery to Akibia," said Tom Tucker, president of Akibia. "His keen understanding of the evolving technology industry and his talent to quickly identify emerging solutions and opportunities will benefit our customers as he helps them ensure their IT infrastructure investments achieve business objectives in the short and long term. Similarly, his ability to collaborate with customers to develop new solutions will ensure Akibia delivers the IT services enterprise organizations require."

Mr. Klotz has more than 15 years experience creating and delivering leading-edge technology solutions. Prior to Akibia, Mr. Klotz was general manager at Eirteic Consulting where he was instrumental in

launching a new enterprise management focused business partnering with companies such as IBM. Before working at Eirteic he was the founder and vice president of Technical Services at SilverBack Technologies, which was acquired by Dell. In 2001 he was named one of Computer World Magazine's "Premier 100 IT Leaders."

"Akibia is truly dedicated to its customer-focused philosophy. This manifests in an unwavering commitment to superior customer service, but also enables Akibia to react quickly and nimbly to deliver new services that address customer pains," said Klotz. "I am excited about the opportunity to exceed customer requirements with compelling solutions that address evolving business and IT challenges."

---

## Introducing Akibia's Blog: The Practical Guide to Enterprise Technology <http://blog.akibia.com>

Many organizations struggle to navigate through the clutter and noise generated by the technology marketplace. Which technologies will have the greatest impact on achieving IT goals, and which are overhyped marketing speak? Akibia "Thinks Like a Customer" - we review and assess technologies and determine their effectiveness in real world environments and from a practical use perspective. Our new blog, found at <http://blog.akibia.com>, will deconstruct the critical technologies on the market today - such as cloud computing, virtualization, compliance solutions, and security and networking tools - and provide insight into technology's ability to increase efficiencies, reduce costs and improve performance.

Take, for example, virtualization. Gartner states that less than 20% of the industry has virtualized their environment, proving broad

adoption has yet to take place. Yet Gartner has already moved past virtualization and on to hyping the latest and greatest technologies around cloud computing. Gartner's role is to stay ahead of the curve and identify the next big technology. Other organizations, such as The Tolly Group take these newer technologies and validate that they do what the vendor says they do - also needed in the ever changing world of technology. Still, a large information gap exists between the introduction of the product and practically deploying it.

What resources can we leverage to find the information we need in the crucial deployment stage? Most typically, we mine this information from trade rags, peers, proofs of concept, consultants, and ultimately trial and error. This approach is costly, time consuming and confusing. It adds significant overhead to every new deployment. There

needs to be a better way to leverage the experience of your peers across vertical markets and gain easy access to the right processes, procedures, and pitfalls to avoid when deploying these technologies. Solution-based approaches are the first step to solving this issue, but there is a requirement for more. This next generation approach - Practical Use - incorporates evaluation, optimized deployment, disaster recovery and business continuity considerations, process, support, and maintenance, while taking into account the evolution of the environment and technology to maximize cost savings and increase efficiency in your real-world environment.

Please visit our blog at <http://blog.akibia.com> for further dissection and analysis of technology trends and solutions, and to learn their benefits and advantages when put to "Practical Use."

## Akibia News cont.

# Akibia's Multivendor Systems Maintenance Helps Organizations Save Up to 40% in Support Costs

Economic uncertainty has led to tighter budgets, and IT departments, CFOs and others are looking for ways to creatively reduce costs. There is a way to reduce overall IT budgets without sacrificing IT innovation and critical technology deployments - multivendor systems maintenance from Akibia. Akibia's customers are experiencing significant savings. For example, a global telecommunications provider/xSP, was able to realize approximately \$1.5 million in annual savings on their mission-critical Sun Microsystems and Hewlett-Packard data center support services with Akibia's "Service Partner" Akibia's innovative approach to self maintenance.

"Service Partner" can save your team up to 40%. Akibia's Service Partner is a cost-effective alternative to traditional on-site support service, enabling customers to leverage their own internal IT staff to perform the actual systems

maintenance while taking advantage of Akibia's economies of scale, best-in-class logistics operations, and multivendor hardware and software technical expertise as part of an efficient self-maintenance support solution. In general, Akibia's Service Partner customers have experienced up to 40% in savings over standard on-site maintenance plans while ensuring high availability and uptime. This is largely due to the fact that Service Partner is an inherently lower cost, and more responsive, business model than traditional on-site maintenance plans.

According to Gartner Analyst Eric Rocco, roughly 40% of all outsourcing costs can be attributed to dispatched labor. Akibia simply removes labor from the equation, enabling you to consolidate vendors across multiple hardware types and operating systems. Specifically, Akibia's Service Partner solution provides 24x7 problem diagnosis for hardware

and software issues, logistics including replacement parts, and technical education for your staff.

## Customized Solutions Enhance ROI

For many customers, Akibia creates a customized solution combining on-site service and "Service Partner," with a variety of response times and coverage options, depending how critical the systems are and the level of service required. Our tailored solutions also offer customer-specific call flows and escalation paths, remote diagnostic tools, consigned parts and dedicated on-site engineers.

# Microsoft Exchange 2003 to 2007 Migration Planning Leverage the Benefits of Exchange 2007: Increased Operational Efficiencies and Cost Savings

**With Microsoft discontinuing mainstream Exchange 2003 support on April 14th, 2009,** Akibia can help you to plan a low risk, smooth migration from your current Exchange 2003 platform to Exchange 2007. Upgrading to Microsoft Exchange 2007 is not simply loading new software onto your current Exchange 2003 server and storage platform. Migrating to Exchange 2007 requires that customers enhance their server platform and create a new messaging architecture in order to take advantage of the Microsoft Exchange 2007 capabilities which include: **improved**

**operational efficiency; enhanced security and encryption; compliance; improved anywhere access; and unified communications.**

As a Microsoft Gold Certified Partner and Exchange Deployment Planning Services (EDPS) Provider, Akibia can help you to understand how to successfully implement a migration from Exchange 2003 to Exchange 2007 without disruption to your current messaging environment; create plans that reduce business risk; identify what resources are required for a successful

migration; and to lower the total cost of operating your Exchange environment.

For a limited time, Akibia is providing you with an opportunity to speak with one of our Senior Microsoft Consultants at your location absolutely free. **Call now to schedule your FREE 90-minute Exchange 2007 whiteboard session with one of our Senior Microsoft Consultants.** For more information contact your Akibia Sales Representative or call **1-866-4-AKIBIA.**

# Domain Name System: Is it Working? Has Anyone Complained? There Is Much More to a DNS Audit.

## Organizations Should Conduct a DNS Audit Now to Ensure Critical Needs are Met

Many companies are taking the same short-sighted approach to managing and auditing their existing DNS infrastructure: If it's working, and no users are complaining about network access, then DNS must be fine. As a result, often a DNS audit goes something like this: Is it working? Check.

With this simplistic approach to a DNS audit, critical aspects of the DNS infrastructure are overlooked, opening up potential mis-configuration, disaster recovery, security, and compliance challenges.

- **Disaster recovery** - is it backed up? Will you be able to restore it? Most organizations lack a process for moving their existing DNS infrastructure into Disaster Recovery mode, which can prove costly should a failure occur. Are there mechanisms in place to provide services seamlessly during hardware and software failures? Can you still manage your environment during a disaster?
- **Security** - Is your system secure and patched? The security of the DNS architecture depends on the strength of the operating system and server it runs on. It's important to leverage a dedicated server, and ensure the server and OS receive timely patches and updates. It's important to leverage dedicated, hardened servers. Management of your DNS systems and its data should be reviewed on a regular basis to ensure it meets company security requirements. Security controls like firewall rules and access control lists should be applied to your DNS systems and periodically reviewed.
- **Compliance & Reporting** - Do you know who's making changes to your

system? Reporting via log management is required for most audits to ensure regulatory and industry compliance. When leveraging Excel spreadsheets organizations rely on manually updated information. As a result, they are unable to easily determine which systems were assigned which IP address, and when, calling into question the accuracy of data when audited. Beyond compliance and auditing, without a strong DNS solution, companies lose out on significant benefits related to monitoring capacity and performance statistics.

- **Mis-configuration** - Who is making changes to your DNS and have they been properly trained? The amount of people making changes opens up possibilities for mistakes in configuration. Legacy settings, lack of error checking, stale data, and typos can cause slow applications, including email response.

## The Increasing Demands on DNS Means It Needs Your Attention

The increasing adoption of VOIP and wireless networking is resulting in greater need for advanced DNS, DHCP and overall IP address management. More IP addresses are required and distributed within the company and more users are accessing the network, making it harder and harder to manage IP addresses and naming with an excel spreadsheet shared amongst the IT staff. As DNS has taken on more responsibility and sophistication, a more extensive and appropriate DNS audit becomes necessary.

It's increasingly likely that that an organization's current DNS infrastructure, while functioning, is no longer meeting the requirements of the company.

According to Gartner Group, in a research note titled "Active Directory and DNS Integration," February 11, 2008, choices exist in managing DNS. "Third-party DNS solutions are gaining momentum, will remain viable for the near term, and offer the best choice for enterprises that want the highest level of control over and management of their DNS environments." The DNS choices available to enterprises today, including Microsoft, Infoblox and others means it's time to conduct a true DNS audit, ascertain whether it is meeting the requirements of the organization, and then make changes and modifications based on the results.

## Sidebar: Still Don't Think You Need a DNS Audit?

Every organization that uses DNS just suffered through the greatest security gut check. This summer's major DNS threat (documented here: <http://www.kb.cert.org/vuls/id/800113>) found millions of open recursive servers on the Internet. This is a major security violation, and the majority of organizations were impacted.

Standard best practices employed in Akibia's DNS audit, such as patching software and controlling DNS queries to your servers would have identified the mis-configuration issues found in this DNS vulnerability. If every company had regularly conducted a DNS audit, the vulnerability would have been a non-issue.

While this is just the most recent example of the importance of a DNS audit, there are other reasons to conduct one as well. Hackers have paid more attention to DNS recently than at any time in history, and the attention is not going to go away. Industry security experts stress that DNS is incredibly simple to hack if mis-configured.

# Akibia Can Help You Save 25-40% Off Your Server & Storage Maintenance Costs

Akibia would like the opportunity to show you how to **save 25-40% on the maintenance of your IBM, Sun, HP, Dell and EMC server and storage systems** - with a free analysis of your current maintenance programs.

Akibia's economies of scale, best practices and customized approach to delivering service enable us to reduce maintenance costs for our clients, while providing a higher level of service and satisfaction than the OEM. We have helped clients reduce their data center support costs through:

- **Increased Data Center Efficiencies** - Akibia offers a single point of contact for all your server and storage support needs by consolidating vendors under one contract.
- **Improved TCO on Current Infrastructure Investments** - Akibia supports all systems including out-of-warranty systems the OEM may no longer support.
- **Customized Service Level Agreements (SLAs)** - Unlike the OEM, Akibia will customize each SLA per server, ensuring you only pay for the service levels you need.

Akibia has been providing mission-critical data center support to Fortune 1000 companies since 1988. **Akibia delivers its high-value service at 25-40% less than the OEM's costs.**

**To learn how your company can significantly reduce its maintenance costs while increasing service levels, contact your Akibia Sales Representative or call 1-866-4-AKIBIA.**

For an electronic copy of the current or past issues of Bandwidth, please visit [www.akibia.com/knowledge](http://www.akibia.com/knowledge)

Akibia, Inc.  
4 Technology Drive  
Westborough, MA 01581

USA: 1-866-4-AKIBIA  
EMEA: +31 (0) 318 581950  
[www.akibia.com](http://www.akibia.com)

PRESORTED  
FIRST CLASS MAIL  
U.S. POSTAGE  
PAID  
N. READING, MA  
PERMIT NO. 254