



Application Delivery Networks:  
The New Imperative for IT Visibility, Acceleration and Security >



## Application Delivery Networks: The New Imperative for IT Visibility, Acceleration and Security

Your business depends on one thing: getting the right information to the right people at the right time. To gain a competitive advantage, improve customer service and access more business intelligence, you have to ensure fast and responsive application delivery to users wherever they are. At the same time, you have to protect users, systems and applications from malicious threats so workers, customers and partners can confidently transact business whether they're using Oracle, Salesforce.com or VoIP.

The key trends driving business today – centralization, mobilization and globalization – often make it difficult, if not downright impossible, to support on-demand application delivery. IT initiatives such as server consolidation and voice, video and data convergence can disrupt network service. Your mobile applications and devices can be compromised by security breaches and data theft. And global IT infrastructures often harbor data silos that are difficult to penetrate and manage, obscuring the view of your IT resources.

If you're not supporting the information delivery your business demands, you need to look at the technologies you're using to monitor application performance, optimize your WAN and secure your Web gateway. Together, these capabilities are absolutely vital to meeting business needs today, and preparing for future requirements down the road.

### Managing new business drivers demands a new approach

Businesses that drive toward greater IT centralization, mobilization and globalization need to:

- > See their IT and business processes more clearly.
- > Accelerate information and business results across the enterprise.
- > Secure data and users wherever they are.

To achieve these goals you first need to understand how these business drivers impact your infrastructure.

### Centralization: The challenge of achieving greater control and flexibility

Enterprises like yours are always looking for new ways to centralize resources to gain greater IT control and reduce management costs. The more your infrastructure expands, the more you need to consolidate so you can:



- > Enable branch office server consolidation.
- > Ensure business continuity in the event of a major IT failure.
- > Accelerate backup and recovery operations.
- > Regain control of WAN and Internet gateway connections.
- > Increase flexibility for innovative Web technologies.

But tightening the reins on your information resources can have a downside, too. Centralization can degrade application performance for branch office employees, making it harder to move quickly in a changing business climate. Strict policy controls can occasionally prevent users from accessing Web 2.0 applications and mash-ups that are used for legitimate business purposes. So the challenge for IT is to achieve and maintain centralized control, while still providing flexible application delivery across the enterprise.

#### **Mobilization: Accelerate applications and data any time, anywhere**

Any business that really wants to compete in today's economy has to prepare for a business future driven by ubiquitous connectivity and seamless access to information. It's not enough to drive people to Web sites. Your business has to use technology in smart and effective ways that enable connectivity from almost anywhere. And it's up to IT to help business leaders understand how new mobile technologies can directly support business goals, such as increasing revenue and customer satisfaction.

Ultimately, the goal of mobilization is to improve business productivity and:

- > Accelerate business processes and communication.
- > Enable key corporate initiatives, such as video for training, VoIP and new application rollouts.
- > Provide the security and performance of a headquarters work experience anywhere.

Of course, accelerating information to all parts of the world carries significant security risks. To successfully manage on-demand information delivery, you need the intelligence to distinguish business-critical from harmful traffic, prevent data breaches and ensure your business stays compliant with government regulations. You also have to manage the increased strain on your network from Web 2.0 applications, video sites and mash-ups.

Unfortunately, the answer isn't as simple as blocking traffic to questionable sites and content. You need effective ways to regulate the demands on



bandwidth generated by personal Internet use without completely denying access. The job of IT is to know how to leverage mobile technologies and Web applications to drive key corporate initiatives while maintaining the security and integrity of sensitive business data.

### **Globalization: Securely scale your business to leverage new growth opportunities**

Globalization is one of the most important business drivers today. Any company that wants to succeed globally needs the right mix of tactical and visionary IT leadership to handle everyday management issues while strategically preparing for future growth opportunities. The more your business expands across the world, the more your IT organization needs to:

- > Mitigate risk and ensure compliance through integrated network security controls based on visibility, intelligence and policy.
- > Change policies on demand to instantly respond to evolving technology, organizational and market conditions.
- > Prevent data leaks with centralized policy controls over network use and access.
- > Proactively respond to application performance demands across a growing distributed enterprise.

Today, for instance, global transactions increasingly depend on software-as-a-service (SaaS) applications such as Salesforce.com, and unified communications such as video conferencing and instant messaging. In addition, service-oriented architectures (SOA) combine applications and data from multiple sources, so your infrastructure must understand what is business-critical and what isn't. You have to accelerate essential applications, stop unwanted or dangerous traffic and manage or mitigate everything in between.

In addition to optimizing daily network performance, many companies are already preparing to deliver the next wave of anytime, anywhere business applications by converging their voice, video and data networks. The business benefits of network convergence are clear: fast, dependable, real-time communication, unprecedented information mobility and worker flexibility, and the ability to instantly deliver a variety of data types to almost any device, anywhere in the world. But how can you ensure these new models of application delivery enforce your corporate security policies, mitigate security risks and help you achieve compliance?



And, more importantly, what will information delivery look like in the next few years, and how should you prepare for it now? These are questions IT leaders need to address to help the business maintain a competitive edge in the global marketplace.

### **The Future of Application Delivery**

While the challenges of consolidating and mobilizing global IT resources are far from simple, you can start to tackle them by learning how to achieve greater application visibility, acceleration and security within your infrastructure.

One of the biggest obstacles to delivering fast, secure and reliable application performance lies in the connectivity layer. While networks route traffic and deliver packets very efficiently, the connectivity layer can't tell you whether the content is helpful, harmful or even potentially catastrophic. To adequately assess the quality of network transactions, application performance and user experiences across your network, you need a new layer of IT control that helps you confidently deliver applications, not just packets.

### **The Application Delivery Network: A new layer of intelligent control**

While many companies can manage the individual issues that compromise application performance, every enterprise still needs a critical layer that can go beyond just keeping applications up and running. You need the ability to stop malicious activities and deliver applications precisely when and where they're needed most. Now and in the future.

The Application Delivery Network does just that. It answers the demand for greater application mobility and security in a changing global business environment. By combining three core capabilities – Application Performance Monitoring, WAN Optimization and Secure Web Gateway technologies – the Application Delivery Network helps you:

- > See applications and users and how they behave on the network, and troubleshoot performance issues.
- > Accelerate mission-critical applications, streaming video, SSL and other enterprise applications.
- > Secure against malware, data leaks and performance degradation.
- > Enable a highly efficient and productive end-to-end user experience anytime, anywhere.



## Building the Application Delivery Network

To help you get started, this white paper describes the components and processes you need to establish an Application Delivery Network in your infrastructure.

### Application performance monitoring:

#### Identify and resolve the critical factors that impact performance.

Monitoring application performance is one of the toughest and most essential jobs in any IT organization. To do it well, you have to:

#### See all the traffic on your network.

This kind of intelligence work requires tools that can automatically identify hundreds of applications on your network every day. To separate the good from the bad, you have to distinguish between business-critical content and malware and recreational traffic such as iTunes, YouTube and peer-to-peer (P2P) applications. You have to be able to sub-classify complex environments, including Web-delivered suites such as Oracle and SAP, so the most important operations and users within these applications have the highest priority.

#### Monitor the end-user experience.

When your IT organization is successful, users rarely know how hard you work to keep applications up and running, maintain data integrity and prevent hardware crashes. But preventative measures are only as effective as the tools in your arsenal. You also need the ability to measure and alert IT about specific factors that impact the user experience, such as P2P applications that steal bandwidth from your critical business applications.

#### Determine the source of network problems.

Application performance problems can come from almost anywhere, so you need to execute a range of tasks to quickly isolate the main issues, whether it's a delay between the server and network, or problematic hosts, servers or applications that cause the most performance degradation. Next you have to analyze the causes, whether it's a spike in application usage or a protocol problem, and use this detailed analysis to fine-tune the environment and get your applications back up to speed.

#### Get end-to-end visibility.

Many IT organizations have traditionally performed these tasks with a diverse set of connectivity layer tools from different vendors, which can lead to



compatibility problems. However, a complete, integrated solution is more scalable and cost-effective in the long run, and can help you achieve ROI faster than a disparate group of tools that require integration. Application acceleration and control technologies also integrate service-level metrics and statistics into comprehensive reports that help you manage the user experience by identifying and resolving problems quickly.

### **WAN Optimization:**

**Outstanding business performance depends on fast application performance.**

**Manage the user experience throughout your distributed enterprise.**

Most corporate environments today have hundreds of applications running on the network at any given time, in any location. They can all have different management issues, depending on the application type:

#### **Internal bulk applications**

This type of application uses CIFS, MAPI, FTP or TCP and includes file access, storage consolidation, email, Internet, backup and applications used to distribute updates, patches and new firmware images around your company.

#### **External applications**

These applications cross the spectrum from business-critical to downright malicious. Therefore, external applications can be the most challenging – and the most important – to manage. They can include everything from corporate training videos and Salesforce.com to the hundreds of recreational applications your users access from your corporate network.

Managing access to recreational sites can be tricky, because many of these sites, such as YouTube or instant messaging, are sometimes used for business purposes as well as personal entertainment. So the key is to distinguish between business and recreational use, maintain control of your network resources and stop the malicious traffic that can piggyback across your network.

#### **Real-time applications**

Applications such as VoIP, video conferencing, credit card transactions, financial trades and order processing are often the most sensitive to delay and the most critical to the business. How can you keep them available 24/7?

**Centralized management and control from data center to device.**

To help ensure consistent performance across all these application types, you have to manage and protect business data all the way to the device level. And that requires the ability to enforce corporate policies and protect information from theft, loss and malware outbreaks. As a result, you can accelerate the performance of all your client/server applications and enable transparent access among VPN users who occasionally work in the office.

**Secure Web Gateway:**

**Anticipate and block threats to your business at the point of entry.**

**You have to be ready for anything.**

You never know which new form of malware will try to breach your gateway to steal or alter financial data, personnel information, customer histories and more. That's why your technology strategy must constantly evolve in response to potential threats, both physical and digital. The challenge for large enterprises is to ensure global security without compromising global agility. To secure your entire enterprise, you have to protect every point of access to your business – the devices and workers themselves.

Any IT strategy should include these four key security requirements:

**Protect against malware.** Technology from leading anti-malware vendors such as Kaspersky, Sophos, Panda and McAfee can help prevent malware outbreaks by filtering both incoming and outgoing Web traffic in real time, and reduce your exposure to malicious Web content.

**Guard employee productivity.** Not all recreational applications are counterproductive to your business. You just need the right tools to know when recreational use is depleting bandwidth and employee productivity, so you can control it according to your corporate policy and business needs.

**Prevent information leaks.** Ensure your data leakage protection capabilities offer the ability to watch, alert and prevent the theft of information from databases and other vulnerable resources throughout your company. Consider tools that integrate with Symantec/Vontu, RSA/Tablus, Code Green Networks and other leading vendors.

**Validate trust.** The bottom line is, you simply have to secure your enterprise from the inside out, because business loss comes in many forms: information



theft, downtime, decreased productivity, accidental or intentional data corruption and more. With all these threats, it's easy to wonder if you'll ever have enough security to protect your business. But by integrating extensive capabilities for URL filtering, data leakage prevention, malware protection, policy management and identity authentication into your network management arsenal, you can dramatically improve your overall security approach.

### **Blue Coat provides the intelligent control you need**

You face a converging set of business drivers – centralization, mobilization and globalization. While many companies provide the tools to manage aspects of these business challenges, only Blue Coat helps you tackle them head-on with Application Delivery Network solutions. Our core technologies – application performance monitoring, WAN optimization and Secure Web Gateway – deliver the visibility and control you need to see, secure and accelerate applications like never before.

### **Visibility**

Blue Coat Application Delivery Network solutions provide the ability to identify and classify applications and users across the network. Our capabilities allow you to discover all application traffic, monitor the user experience, troubleshoot performance issues and resolve problems before they impact the user experience. More specifically, we help you to:

- > Automatically discover 600+ applications
- > Identify P2P, recreational or streaming applications over any port
- > Sub-classify complex applications such as SAP, Oracle, Citrix, Web, CIFS, MAPI and DCOM
- > Discover URL and external sites within HTTP
- > Identify problem hosts, servers and applications

### **Acceleration**

Blue Coat helps you accelerate business-critical applications, including internal, external and real-time applications to any user, anywhere. And we do it while ensuring a headquarters work experience, wherever your users are located. Our acceleration technologies include:

- > Object and byte caching
- > Compression and basic quality-of-service (QoS) capabilities



- > External Web/SSL acceleration
- > Protocol acceleration for TCP, CIFS/NFS, MAPI, HTTP and more
- > Advanced Web policy and bandwidth management
- > Advanced application ID technology

### **Security**

Blue Coat secures your Internet gateway to help protect users from malicious content and applications. Our security capabilities include:

- > Anti-virus and malware scanning
- > URL and Web content filtering
- > Centrally managed distributed gateway
- > Granular policy management across over 500 variables, including user, group, application, source, content types and transaction
- > Logging, statistics and SNMP support

Blue Coat Application Delivery Network solutions deliver the intelligent control you need centralize, mobilize and globalize your entire IT infrastructure.

With Blue Coat, you can optimize application and network performance for any user, anywhere across a distributed enterprise. Let your IT organization become the engine that drives greater business efficiency, effectiveness and competitiveness. Learn how implementing an Application Delivery Network can help your organization prepare for the next wave of converging IT and business challenges. Find out more at [www.bluecoat.com](http://www.bluecoat.com).



Blue Coat Systems, Inc. • 1.866.30.BCOAT • +1.408.220.2200 Direct  
+1.408.220.2250 Fax • [www.bluecoat.com](http://www.bluecoat.com)



Copyright© 2008 Blue Coat Systems, Inc. All rights reserved worldwide. No part of this document may be reproduced by any means nor translated to any electronic medium without the written consent of Blue Coat Systems, Inc. Specifications are subject to change without notice. Information contained in this document is believed to be accurate and reliable, however, Blue Coat Systems, Inc. assumes no responsibility for its use. Blue Coat is a registered trademark of Blue Coat Systems, Inc. in the U.S. and worldwide. All other trademarks mentioned in this document are the property of their respective owners.