Enterprise Application Delivery: No User Left Behind

A Whitepaper on Blue Coat ProxyClient Architecture
**Executive Summary**

Enterprises are increasing their dependence on public infrastructure, in a variety of ways both predictable and unforeseen. Applications continue to be consolidated, but not necessarily within the enterprise datacenter – many applications have been outsourced. On the other side of the IT equation, users are moving outside the four walls of the organization at a rapid pace – driven by a variety of business needs, including travel, higher productivity, and customer intimacy – and therefore not able to use the infrastructure IT has traditionally depended on to deliver critical business applications. To make matters worse, the public (and sometimes personal) infrastructure and devices these users connect to in order to do their jobs is rife with performance issues and security threats – and IT has no control over any of it.

Consequently, poor WAN application performance for users, unnecessary risks to the organization, and obstacles to productivity are the unwanted results of these trends. None are acceptable, but all are hard to solve when the network, and even the endpoint machine itself, are outside of IT’s control.

While there are a variety of potential solutions, most lack the ability to “deliver” applications – they can accelerate or compress packets, or provide network or OS security features, or even address branch offices or headquarters locations only. Yet they never do all at once, leading to an ever-growing number of clients cluttering the desktop. Furthermore, none have any answer for unmanaged devices connecting over the Internet.

Enterprises need the ability to deliver applications, with the appropriate levels of performance and security to all users, using any device, across any network. Any proposed solution short of these requirements misses the mark.

Blue Coat ProxyClient is a client-based platform that extends application delivery infrastructure from HQ and branch office locations all the way out to the end-user’s device. With the ability to accelerate and secure user to application interaction, ProxyClient enlarges IT’s sphere of influence beyond the traditional physical boundaries of the enterprise. Blue Coat ProxyClient is part of an overall enterprise solution for application delivery that interconnects with Blue Coat’s ProxySG appliances to provide application acceleration and security for all users whether at headquarters, regional and branch offices, on the road, or at home.
The “Enterprise Network” is Shrinking…and yet Growing

The number of users and applications physically housed in the traditional enterprise private network is shrinking, yet an ever-growing population of “enterprise” users are connecting from just about anywhere to enterprise applications all over the world.

Application consolidation is part of the equation. Servers are being consolidated for a variety of compliance and cost reasons, but not always back to enterprise headquarters. In many cases, applications are being outsourced. Sometimes this is a strategic decision to hand-off customized, dedicated applications for management purposes. Even more common is outsourcing in the form of “software-as-a-service,” or ASPs, which offer organizations a cost-effective way to meet common business needs with commodity services. Regardless, in many cases, IT no longer controls the servers that host the organization’s critical applications.

At the same time, and driven by similar pressures, branch office issues have vaulted to the forefront of IT infrastructure planners’ thinking. Branch office solutions are a hot topic: how to address consolidated, poorly performing, high-latency, chatty applications and at the same time overcome the significant control issues associated with being outside of headquarters. While branch office issues will remain critical for most organizations, many have overflowed the branch, and are spawning remote users at a frenetic pace. Driven by the need for closer customer relationships, global supply chains and sales operations, outsourcing and talent scarcity, the number of remote users that IT is responsible for delivering applications to is booming. In some cases, without a server, managed LAN or other IT resources, the branch office concept itself becomes anachronistic. When every employee has broadband, a printer and a coffee pot at home, why maintain a remote office at all?

Important to remember, however, is that not all remote users are created equal. Different classes of users use different devices, and connect to different types of application over different networks. Not surprisingly, different users also have different problems across the application delivery spectrum. Some examples are shown in Figure 1 below.
There are two interesting facts in the above chart particularly worth noting.
First, users almost always connect over the Internet. Second, in some cases, users connect using an unmanaged device. The best examples of unmanaged devices include occasional teleworkers using personal PCs to access enterprise applications, traveling executives using public Internet kiosks, and external business partners and consultants using their own equipment. The other scenario IT faces for unmanaged devices is maintaining business continuity in the face of a disaster, where users may need to utilize their personal PCs to keep the business process moving.

When IT doesn’t own the device, IT cannot trust the device – it has no policy, no control over configuration, nor any protection – meaning that it could be (and likely is) infected with viruses, malware, keyloggers, framegrabbers, or other types of spyware. To make matters worse, nearly all remote users connect to applications over the Internet, exposing them directly to Internet risks while providing an inferior [albeit very inexpensive] connection back to internal applications.

**IT Has Lost Control**

Without owning the LAN infrastructure the user is connecting to, IT’s usual mechanisms to exert control over performance and security are absent.

Typically, IT has depended on owning the user’s machine, the application server, and the intervening infrastructure, so they could implement whatever...
controls necessary to ensure application performance. In many cases today, IT owns few (in some cases, none) of the above, making it difficult to exert any influence over the performance of user-application interaction. Furthermore, since users can literally be anywhere, long distances, lossy networks and chatty protocols can slow applications significantly, while non-critical applications running on the desktop (e.g., P2P, streaming, spyware, and unproductive surfing) can crowd out critical business traffic.

Traditionally, IT has held an "inside vs. outside" view of security – protecting enterprise user/application/information is possible because it is bound inside a finite logical and physical space. With users spread all over the globe, applications consolidated in a variety of inside and outside locations, and increasing dependence on public infrastructure, IT can no longer manage risk with the usual mechanisms. Firewalls, IDS, AV, and other types of network and OS security remain necessary but are not longer sufficient. While those measures are still useful, even required, they’re inadequate to provide security in a world where everything looks the same from a packet perspective – i.e., most applications look like web applications [be they encrypted or in the clear].

**Regaining Control is Difficult**

To deliver applications, it isn’t enough to understand just the network aspects. The network port has long since ceased to be a reliable indicator of the application. Even protocols, by themselves, are not a strong marker when nearly everything tunnels over HTTP or SSL. Effective application delivery requires an understanding of the application, the user, and the nature of the interaction between the two. Delivering applications for the full range of remote users means IT has to address performance and security from where the user sits. Given that an overwhelming percentage of remote users connect via the Internet, companies not only have to address the performance aspects of application delivery, but the security aspects as well. This includes some elements that can impinge upon performance (what applications are active, and how much of the network/resources they can consume), as well as elements that affect overall end-user productivity and risk to the organization. Moreover, with unmanaged devices, IT must concede that anything (spyware, keyloggers, malware, etc.) can be running on that device and still protect the application and the information contained within the application appropriately.
Any solution must incorporate managed and unmanaged endpoints/devices. As noted previously, IT doesn’t always own the device the user depends on to access the application. In those cases, IT must be able to deliver applications in a high-performance and secured manner to an untrusted platform. This typically means a dynamically downloaded client-based tool that provides application delivery services, and leaves no trace when finished.

To be effective in a large organization, a solution must address all users across the extended enterprise with a single policy. Whether users sit in main office locations, branch offices, customer sites, or work from home – or all of the above throughout the course of the work week – an application delivery infrastructure must be able to manage their experience with a single policy and management capability.

**Existing Technology Has Limits**

Most technologies claiming to alleviate this problem set have serious limitations that will require years of effort to overcome. There are three key characteristics where existing technologies fall short – architectural, functional, and geographical:

Architectural limits: Unfortunately, many of the existing technologies focus on low-level infrastructure. While appropriate for their core function, technology that focuses only on packet security (personal firewalls), packet access (VPNs), performance (WAN Optimization clients and web accelerators), or OS security (anti-virus and anti-spyware) lacks the wherewithal to understand and manage users, applications, and transactions.

Functional limits: Most technology addresses either security, or performance – but not both – leading to client proliferation on the desktop. That in turn leads to greater system instability, vendors blaming each other for bugs and ultimately a higher cost of servicing laptop and remote PCs.

Geographical limits: There are technologies available that address performance issues, at the right level, but only for certain locations within the enterprise – e.g., security for HQ, performance for the branch, or compression at the endpoint. Tying all of these locations together with a
common policy and management interface will remain a challenge for most technology vendors for the foreseeable future.

**Blue Coat: Application Delivery for the Whole Enterprise**

Blue Coat ProxySG appliances made history by being the first offering in the application delivery market to offer a solution that gives IT control of both application security and performance. Blue Coat’s market-leading application security controls all aspects of user-application interaction, subjecting who, what, where, when, and how to enterprise policy, even encrypted traffic. Blue Coat’s 5-part Multiprotocol Accelerated Caching Hierarchy (MACH5), accelerates the widest array of applications of any WAN application solution (including internally and externally-hosted encrypted applications).

Blue Coat ProxyClient is a proxy-based client platform that extends the same control and policy, security and acceleration, with common management and reporting for the whole enterprise – regardless of where the endpoint happens to be.

![ProxyClient Architecture](image)

**Figure 2: ProxyClient Architecture**
Security
For managed devices, IT can continue to maintain an “inside” view with Blue Coat ProxyClient – where owning the device means maintaining the configuration to a certain standard. This means keeping users from downloading certain types of applications and executable content, either deliberately or inadvertently. Moreover, most organizations have acceptable use policies governing use of the Internet for productivity and risk management but lack the ability to enforce these policies outside of a LAN. Blue Coat ProxyClient extends the enforcement of the enterprise policy and enables a single policy to cover all users, regardless of where they connect to the Internet. Additionally, the ProxyClient connects the user to the Blue Coat WebFilter ecosystem that continually tracks, evaluates and dynamically rates millions of websites every day. Thus, once the user leaves the sphere of control created by the corporate secure gateway, they remain protected from Internet threats such as spyware and phishing. Blue Coat ProxyClient can also ensure that while traveling remote laptops don’t have your corporate logo on one side of the machine, and inappropriate content on the other.

Performance
Blue Coat ProxyClient incorporates all of the appropriate MACH5 optimization and acceleration techniques, including:

- Protocol optimization – both TCP and application protocols
- Object caching – appropriately storing application objects locally
- Byte caching – drastically reducing the amount of data sent over the WAN
- Compression – further reduction of bytes sent over the network

For managed devices, IT’s ownership of the device enables the organization to offer a much wider range of applications such as office applications, file server access, web-based applications. Accordingly, ProxyClient’s MACH5 acceleration module will improve the performance of internal applications even over low-quality public networks.

Blue Coat ProxyClient, because of its position in the network, has a unique advantage in understanding the end user’s application experience. Blue Coat is incorporating monitoring into the ProxyClient architecture, giving enterprises the ability to understand the quality of end-user application experience. By being able to monitor applications all the way to the endpoint,
IT can finally make promises over perhaps the most important quality metric: the time from “click” to “satisfaction”.

**Part of an Enterprise Solution**

Blue Coat’s application delivery solution covers all enterprise locations to ensure that no user is left behind. From Blue Coat ProxyClient for endpoint machines to a wide range of Blue Coat ProxySG appliances that scale from the small branch to the largest datacenter, Blue Coat brings together applications that can be anywhere, with users that go everywhere. Large deployments of Blue Coat solutions exist all over the world – accelerating applications and securing organizations at the same time. Blue Coat’s reporting and centralized management infrastructure - provided by Blue Coat Reporter and Director, respectively – has proven itself in large deployments in some of the largest organizations in the world.

**Conclusion**

Users and applications are spilling out of IT’s sphere of control, costing the organization productivity, momentum, and exposing it to additional risk. IT must reassert control over application delivery by extending application security and acceleration beyond the headquarters and the branch, to include all remote users regardless of whether they use managed or unmanaged clients. Unfortunately, the existing mechanisms IT depends on today either lack the required application intelligence, address only a point solution, or are too large to fit in a laptop bag. To deliver applications to users who are everywhere, connecting over any network and potentially from any computer they find, organizations need new solutions that provide speed, security and flexibility to their applications. Blue Coat ProxyClient extends Blue Coat’s visionary application delivery infrastructure to include all of these use cases – from any network, any device, and any application – keeping users productive wherever the business takes them.