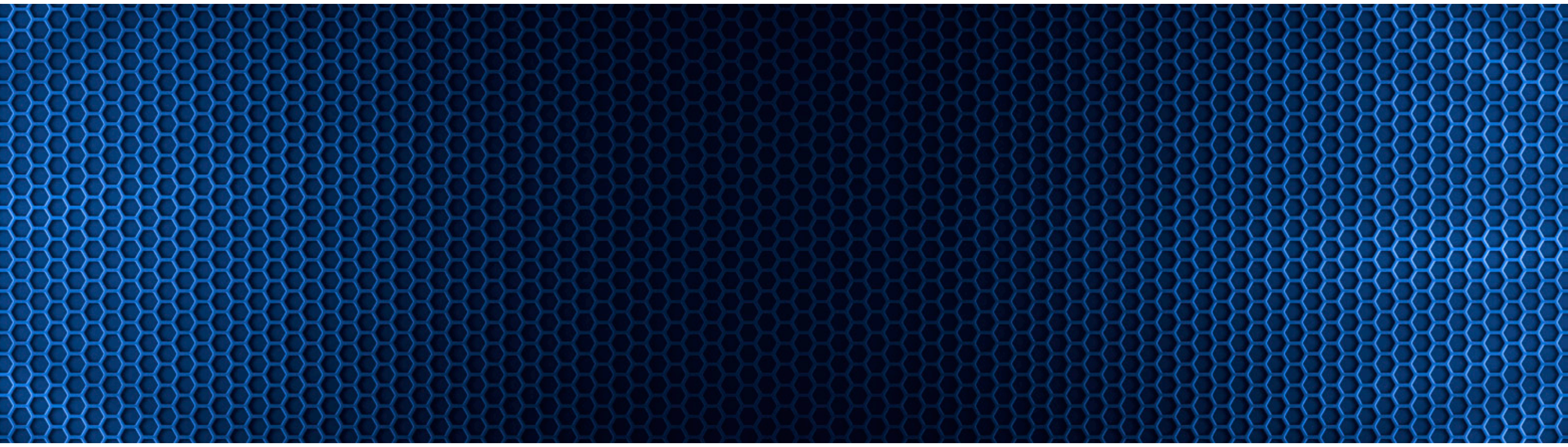
Blue Coat

White Paper



Unified Web Security Solutions >

Deliver No-Boundaries Protection To Users That Are Always On

Unified Web Security Solutions

It's a new world. Organizations are dealing with a workforce that is increasingly mobile, connected and demanding – they are using their own devices and want access to corporate data at all times, from any location. Organizations must be able to extend the boundaries of their corporate network to provide consistent web security protection, policies and reporting for all users on any device or network. By taking a unified approach to security that incorporates dynamic cloud services into traditional appliance-based web security deployments, savvy organizations can protect vital corporate assets and provide comprehensive, consistent protection to users wherever they are on whatever devices they are using. Here's how.

Corporations and their workers have never been more connected than they are today: Connected to one another, to customers, to suppliers, to the outside world. In fact, one of the imperatives of IT organizations worldwide is to ensure that these connections are always available, no matter where employees and customers are located, no matter what devices they are using. Businesses have entered an era of *always on* connectivity and there is no going back.

In this new era, organizations need a new approach to web security that can extend their security perimeters to consistently protect all users in any location and on any device. Why?

1. **Companies must reduce the growing risk of data loss by remote and mobile users/devices that are not adequately protected.** Data loss can be devastating, resulting in financial losses, fines and damage to the corporate brand. Cybercriminals are increasingly targeting remote and mobile workers because they are increasingly vulnerable: A report by IBM predicted there would be twice as many attacks on mobile devices in 2011 versus 2010, abetted by the adoption of smartphones and tablets in the enterprise – including the "bring your own device" approach that allows personal devices to access the corporate network. In addition to the threat of malicious attack, companies face significant risk of data loss through theft and user negligence. In a recent survey on mobile security by Check Point, more than 70 percent of IT professionals said careless employees are a greater security threat than hackers.
2. **IT and security professionals must be able to manage and enforce consistent policies throughout the entire work force.** Consistent policy enforcement across all users is vital for safely enabling user mobility and flexibility. The growing use of social media, for example, adds significant risk to a business: More than 50 percent of organizations have experienced an increase in malware attacks as a result of employees' use of social media, according to a survey by the Ponemon Institute. Organizations must be able to establish and enforce policies around social media to mitigate the risk of lost data, reduced employee productivity and malware threats, no matter the user's device or location.
3. **Organizations have to be more agile and vigilant in identifying and reacting to threats.** Companies have to be able to identify and quickly respond to threats wherever they are. In its 2012 Web Security Report, Blue Coat reported a 240 percent increase in malicious sites with the average business facing 5,000 unique threats per month. Mobility is increasing the risk: "For years, observers have been wondering when malware would become a real problem for the latest generation of mobile devices," notes IBM. "It appears that the wait is over." This means having a security infrastructure that enables agility through the use of both cloud-based and premises-based solutions, combined with an industry-leading threat-detection solution.

Organizations of all sizes have no choice but to support and encourage this *always on* way of doing business. If the organization doesn't provide support and security for the devices that users want to use, it opens itself up to even bigger risks: Users will not be denied and if their activities are not properly managed and monitored, the damage could be severe.

Rethinking Security Approaches

The far more strategic and forward-looking approach that businesses must take is to enable and connect their users – wherever they are – by extending the boundaries of the corporate network. To do this, savvy IT leaders must adopt a new security approach that can protect *always on* users.

The first step in addressing the security needs of this mobile workforce is to understand the ways in which workers are now working and the additional threats inherent in this new environment. The reality is that many workers these days are always on – they take their work with them from the office to the home to the local coffee shop to wherever they need or want to be. These days, more and more workers aren't even in a corporate office at all. That means they are connecting into the corporate network through networks over which IT has no control.

From these different locations, users often access the network on more than one device, whether it is a laptop, smartphone, tablet or all-of-the-above. What's more, the same devices these workers are using for corporate activities are also used for personal activities, exposing the users – as well as the corporate network – to greater risk.

There was a time when it was relatively simple for an organization's IT department to define the perimeter of their network, but that paradigm has disappeared. The world has shifted from a static, centralized model in which security is a fortress around the network to a highly dynamic user-driven model. Today's reality is that the perimeter of the network is much more fluid, extending to whatever device is in the hands of the users, wherever the users happen to be.

Security With No Boundaries

While the activities and locations of users have changed, the need to protect them and the corporate network has not. So, the challenge becomes how to extend security in this new environment without creating a restrictive atmosphere. Security must be able to address every single use case: From stationary users in corporate headquarters to remote workers in branch offices to mobile workers who take their devices wherever they go.

The best way to address this growing challenge of securing a more fluid and mobile perimeter is with a solution that allows your security policy to follow users across networks and devices. Since users are always on, businesses need to have *always on* security.

This type of *always on* security can be achieved through a unified web security solution that extends existing appliance-based solutions with the flexibility and scalability of cloud-based web security. In this type of unified architecture, appliances and a cloud-based service can be optimized according to business and location-specific requirements, affording organizations the best of both worlds in managing ROI, delivering top performance and speed, and ensuring agility and scalability.

Cloud-based services are particularly effective for extending protection and policies to remote or branch offices and mobile workers. A research report from Enterprise Strategy Group notes that employees working at remote and branch offices present a bigger security challenge than those in central locations. "These remote offices with dozens of employees need web threat management," ESG notes, "but since it may not make economic or technical sense to deploy a gateway appliance at each remote facility, cloud services are especially attractive."

In an integrated, unified web security environment, cloud-based solutions can extend security to users and offices that aren't traditionally protected by appliances. The biggest advantage of cloud-based solutions for these locations is that they can be easily deployed and scaled.

Taking A Unified Approach To Security

For some organizations, particularly mid-sized and small businesses, a cloud-based approach may be sufficient to address the needs of the enterprise – provided the solution offers state-of-the-art functionality, such as global threat detection, flexible policies and unified reporting.

For many other businesses, particularly larger enterprises, deploying a web security cloud solution is most effective when it is part of a unified approach to security where the cloud service can be deployed with web security appliances. This enables the organization to provide security solutions that follow the user from corporate locations, with on-premises appliances, to branch office, to remote location and to mobile devices, providing the same levels of policy and protection from one location to the next.

There are significant advantages to taking this type of unified approach, including:

-> **Reduce Risk of Data Loss:** The unfortunate reality is that many remote and mobile workers – and their devices – are largely unprotected today. In a recent survey by Check Point, nearly 90 percent of IT professionals said mobile devices such as smartphones or tablets are connecting to their corporate network and nearly 50 percent said customer data is stored on these devices. With a unified approach, organizations can close the security gap by offering consistent policy enforcement and protection to all users – even on personal devices.

-> **Protect ROI:** There are many organizations that have invested in web security appliances and require them to comply with various regulations. At the same time, they still need to protect remote and mobile users. With a unified security approach, they can now extend web security cloud services to those users while protecting their appliance investment. Unified policy and reporting make this a seamless security deployment across all users while protecting the investment in appliances.

-> **Reduce Complexity:** By using a unified approach, organizations can dramatically simplify policy enforcement and reporting, so that policy can be created centrally and pushed to all users. Complexity is also reduced because the IT department is dealing with a smaller number of vendors, so there are less risks of incompatibilities or finger pointing among providers.

- **Increase Scalability:** It's clear that the use of mobile devices will grow, driven by employee adoption as well as corporate iPad and other tablet initiatives. Only now are businesses discovering how they can use tablets to make their workers more efficient and portable. A unified web security solution enables businesses to scale seamlessly and extend consistent policy and protection to new users, devices and office locations.
- **Enhance Agility:** One of the major advantages of using a cloud-based service as part of a unified approach to security is that it provides the IT organization with much more agility in managing capital budgets. With a cloud solution, organizations don't have to make a significant up-front investment in technology and can stage users in groups to enhance flexibility.

Choosing the Right Solution

In order to achieve all of these benefits and provide all workers with comprehensive protection wherever they are, it is important not just to choose a unified approach, but to choose a unified approach that offers the benefits, performance and features that will actually deliver on the promise of increased ROI, reduced complexity, increased scalability and enhanced agility.

It is also important to choose a solution that delivers global threat protection, consistent policies and unified reporting. With these functions unified, the organization can centrally manage all users, regardless of their device and location.

Deploying a single-vendor solution for a complete unified defense enhances an organization's ability to maximize performance, scalability, agility and simplicity. In helping organizations build a successful unified web security solution, Blue Coat offers significant benefits to customers and significant advantages versus competitors. Blue Coat Unified Web Security Solutions deliver universal web security to users on any network, at any time, on any device through:

- **Global Threat Protection:** Consistent enterprise-grade protection that doesn't compromise performance, backed by the best malware defense in the industry
- **One Identity Policies:** Identity-based policies follow users across any network or device, built on the industry's most flexible policy engine
- **Unified Reporting:** Actionable intelligence across all users and devices with real-time data and granular drill-down for incident resolution

Conclusion

Given the new threats inherent in an increasingly mobile workforce and the blurring of lines between business and personal use of devices, it is clear that conventional methods of securing the perimeter in this new environment are not up to the task. For a workforce that is increasingly mobile, organizations can most effectively maximize their security efforts by incorporating a cloud-based solution as part of a unified approach. This way they can deliver *always on* security to their *always on* users, protecting their organizations from threats that are always on the web.

Blue Coat Systems, Inc. • 1.866.30.BCOAT • +1.408.220.2200 Direct
+1.408.220.2250 Fax • www.bluecoat.com