

White Paper

The Benefits of a Hybrid Security Architecture

By Jon Oltsik, Senior Principal Analyst

November, 2011

This ESG White Paper was commissioned by Blue Coat Systems, Inc, and is distributed under license from ESG.

Contents

Executive Summary	3
The Increasingly Dangerous Web Threat Landscape.....	3
Large Organizations Are Investing In Web Threat Management	4
Which Web Threat Management Model Is Best?	5
Web Threat Management Gateways Are Great for Large Collocated Organizations	5
Cloud-based Web Threat Management Makes Sense for Distributed Enterprises.....	6
Large Global Enterprises Need a Hybrid Security Architecture.....	7
Hybrid Web Threat Management Provides Flexibility and Immediate Security Benefits	8
The Bigger Truth	9

All trademark names are property of their respective companies. Information contained in this publication has been obtained by sources The Enterprise Strategy Group (ESG) considers to be reliable but is not warranted by ESG. This publication may contain opinions of ESG, which are subject to change from time to time. This publication is copyrighted by The Enterprise Strategy Group, Inc. Any reproduction or redistribution of this publication, in whole or in part, whether in hard-copy format, electronically, or otherwise to persons not authorized to receive it, without the express consent of the Enterprise Strategy Group, Inc., is in violation of U.S. copyright law and will be subject to an action for civil damages and, if applicable, criminal prosecution. Should you have any questions, please contact ESG Client Relations at (508) 482-0188.

Executive Summary

Cloud computing has become a viable model for a multitude of IT requirements. In some cases, large organizations purchase cloud-based CPU cycles on an as-needed basis for test, development, and batch processing using Infrastructure-as-aService (IaaS) offerings from vendors like Amazon, Rackspace, and Terremark. Other times they simply outsource an entire application, handing email to Google, CRM to Salesforce.com, or payroll to ADP.

In spite of its value however, IT professionals remain engaged in a philosophical debate on the value of cloud computing. They ask if cloud computing and SaaS designed for the masses are really suitable alternatives to on-site IT equipment residing in corporate data centers. After all, premise-based IT equipment offers line-speed performance and can be tuned for the specific requirements of an individual organization.

Recently, CISOs have had similar deliberations with regard to information security requirements, especially as they relate to web threat management. Security professionals ponder a similar question: Should large organizations opt for on-premise security gateways or simply offload web threat management to the cloud? This paper concludes:

- **Regardless of the solution choice, web threat management needs to be addressed as soon as possible.** While theoretical pondering about on-premise versus cloud services persists, web threat management is an increasingly insidious risk. As a result, ESG Research indicates that large organizations are actively investing in web threat management solutions.
- **On-premise and cloud deployments have strengths and weaknesses.** Web threat management gateways work well in large centralized facilities while SaaS is a good fit for remote offices and mobile workers. Unfortunately, large global organizations need coverage in all of these areas so neither security gateways nor SaaS are adequate on their own. CISOs wonder if they should settle on one choice or implement multiple solutions from multiple vendors.
- **Large global organizations need tightly-integrated hybrid solutions.** Typical multi-national enterprises have a combination of large populations of centralized and distributed employees. These firms need consistent policy management, enforcement, and oversight in order to provide strong security for all employees regardless of the location of the networks they connect to. In fact, this is the most compelling reason for a unified hybrid web security solution combining the on-premise control of appliances with the flexibility of cloud. Using a hybrid architecture, large global organizations get central management, distributed enforcement, and capitalize on the crowd sourcing aspects of a cloud computing community for mobile, remote, and centralized employees alike. This best-of-both-worlds architecture will become a standard enterprise deployment moving forward.

The Increasingly Dangerous Web Threat Landscape

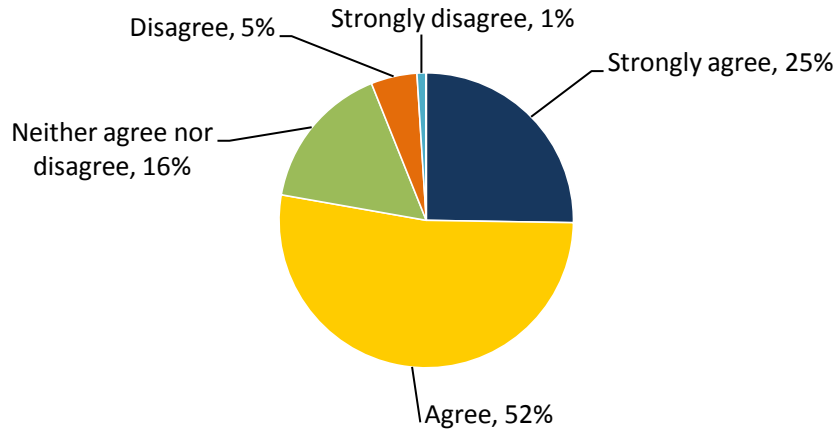
Defending against viruses, worms, and Trojans has always been difficult but many CISOs admit that threat management is getting precipitously more difficult each day. This is due to the fact that large organizations face traditional attack vectors as well as increasingly dangerous web threats. Things will only get worse because of:

- **Unprecedented malicious code volume.** According to the latest Blue Coat web threat report, the volume of web threats grew more than 500% over the past year alone. Additionally, the volume of malicious code variants grew by over 300% while phishing attacks were up more than 600%.
- **Dangerous web content.** Nearly half of malicious code threats now target Internet browsers because many web applications are vulnerable, making them easy targets to infect. Users also tend to trust websites from high-traffic sites like Google, Yahoo, and Bing which have been compromised in the past and used for malware proliferation. Web 2.0 is driven by dynamic content, a new and perpetually changing threat vector. Finally, web threats can be targeted at a specific organization or individual making detection and prevention extremely difficult.
- **Social networking vectors.** Social networking sites have quickly become criminal enclaves. For example, the Zeus botnet sent over 1.5 million phishing messages on Facebook over the past few years. Little

wonder then that more than three-quarters (77%) of security professionals working at enterprise organizations (i.e., more than 1,000 employees) believe that employee access to social networking sites increases the likelihood of a sophisticated attack (see Figure 1)¹.

Figure 1. Belief that Social Networking Sites Increase Likelihood of APT Attacks

Please respond to the following statement: “I believe that employee access to social networking sites (e.g., Facebook, Twitter, etc.) increases the likelihood of an APT or other type of sophisticated attack.” (Percent of respondents, N=244)



Source: Enterprise Strategy Group, 2011.

- Increased mobility.** Employees regularly access a combination of corporate and consumer web applications using laptops, smart phones and tablet PCs. While this mobility can help bolster productivity, it makes it more difficult to manage device configuration, update security signatures, or monitor activity for suspicious and/or anomalous behavior.

Large Organizations Are Investing In Web Threat Management

Wikipedia defines the term “web threat” as follows:

“A web threat is any threat that uses the internet to facilitate cybercrime. Web threats use multiple types of malware and fraud, all of which utilize HTTP or HTTPS protocols, but may also employ other protocols and components, such as links in email or IM, or malware attachments or on servers that access the Web. They benefit cybercriminals by stealing information for subsequent sale and help absorb infected PCs into botnets.

Web threats pose a broad range of risks, including financial damages, identity theft, loss of confidential information/data, theft of network resources, damaged brand/personal reputation, and erosion of consumer confidence in e-commerce and online banking.”

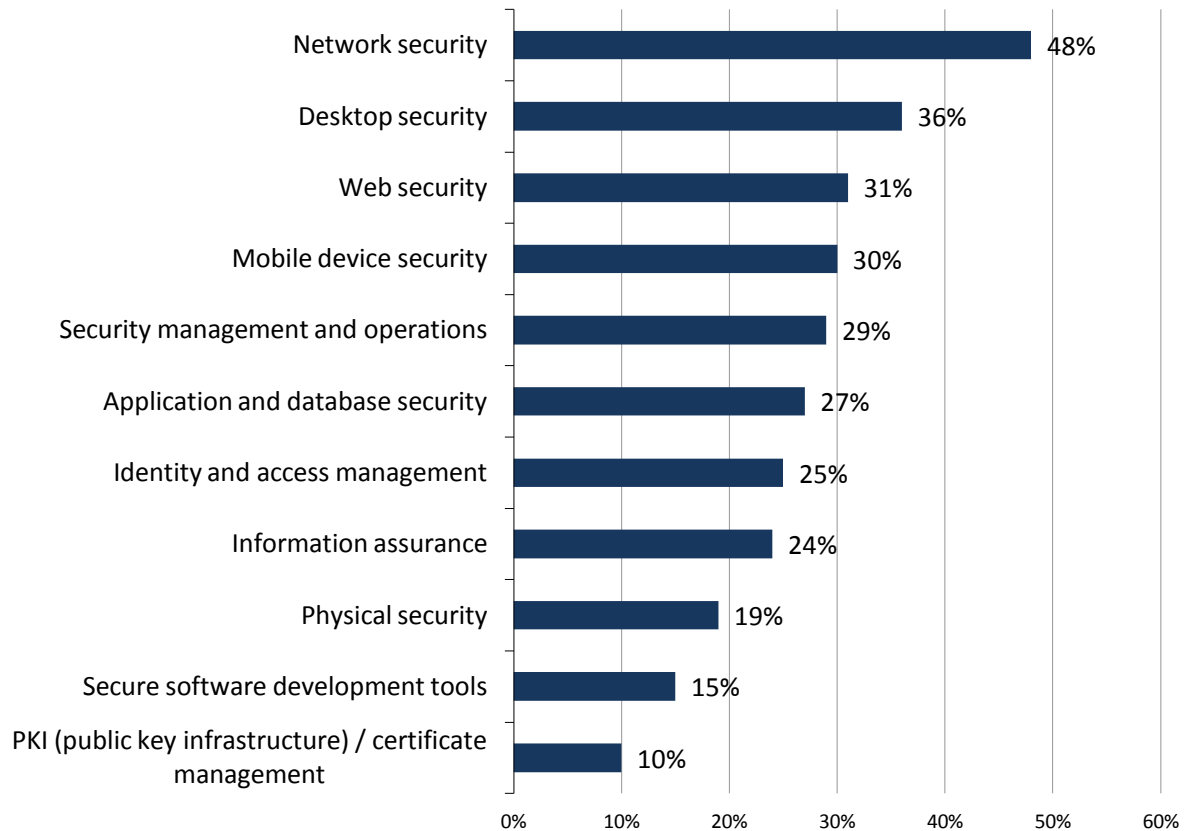
Given the ubiquity, volume, and growth of web threats, CISOs are investing in specific web threat safeguards. This is demonstrated in recent ESG Research. Nearly one-third of organizations said that they will invest in web security in 2011 (see Figure 2)².

¹ Source: ESG Research Report, [U.S. Advanced Persistent Threat Analysis](#), November 2011.

² Source: ESG Research Report, [2011 IT Spending Intentions Survey](#), January 2011.

Figure 2. Large Organizations Will Invest in Web Security

With regards to specific spending plans for security, in which of the following areas will your organization make the most significant investments over the next 12-18 months? (Percent of respondents, N=286, five responses accepted)



Source: Enterprise Strategy Group, 2011.

Which Web Threat Management Model Is Best?

When CISOs look for web threat management technology safeguards, they face a daunting and often confusing number of choices. While hyperbolic vendor claims are to be expected, many security executives confront a new decision criterion: Should they purchase and implement traditional gateway security solutions or bypass on-site options in favor of SaaS-based cloud services?

Web Threat Management Gateways Are Great for Large Collocated Organizations

Web threat management gateways reside at network ingress/egress points in order to filter and block malicious web content like phishing exploits, viruses, worms, Trojans, and botnets. To maintain protection over time, security vendors regularly update on-site web threat management gateways with new rules and signatures as new malware threats are discovered.

In the past, large organizations usually opted for on-premise web threat management gateways. These traditional “bastion servers” offer a number of benefits such as:

- High performance.** Gateway appliances are designed to operate at “wire speed,” with minimal latency or impact on network performance. Large organizations with enterprise-class IT, networking, and security skills can easily implement and tune a gateway security appliance so it delivers strong security protection for thousands of network-based employees without any adverse impact on performance requirements.

- **Customizable policy management and enforcement.** Enterprise companies have varied security needs based upon regulations, industry-specific threats, and internal governance. To meet these disparate requirements, many gateway web threat management appliances provide granular controls for policy management and security enforcement. In this way, web threat management gateways can be customized to enforce security policy rules based on a particular user, group, location, or time of day.
- **Central command-and-control.** Large organizations that span multiple facilities or campuses with multiple network ingress/egress points may need several web threat management gateways. To meet this requirement, leading web threat management gateways provide central command-and-control for multiple appliances. In this way, CISOs can have common policies across multiple web threat management gateway appliances, or customize individual appliances for specific needs.
- **Integration with other security functionality.** In many cases, web threat management may be combined with other security applications, like DLP, anti-virus, or URL filtering, residing on high-performance security gateways. Large organizations can then standardize on a single security appliance in order to lower capital costs, streamline ongoing operations, and centralize maintenance and support. Integrated security appliances may also help improve overall security by correlating events and consolidating reporting.

Cloud-based Web Threat Management Makes Sense for Distributed Enterprises

Web threat management gateways are most beneficial for large centralized organizations where hundreds or thousands of employees are tethered to the network across multiple collocated facilities. In today's global business environment however, many organizations depend upon a highly distributed and often mobile workforce residing in branch offices, remote locations, or simply on the road.

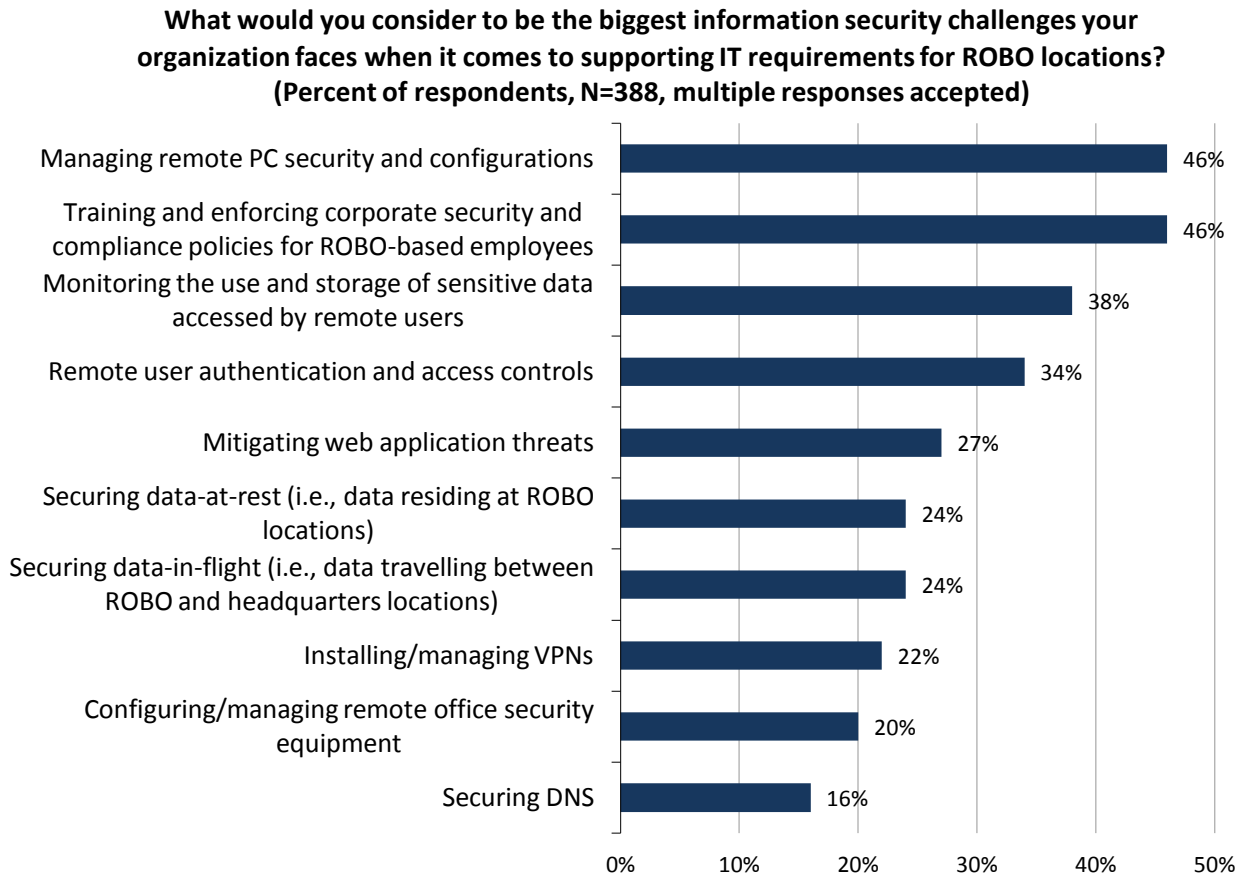
Over the past few years, a growing number of security vendors have embraced a SaaS or cloud delivery model as an alternative to traditional gateway appliances. Distributed enterprises could certainly benefit from web threat management via the cloud as this type of delivery model offers:

- **Easy deployment and operations.** SaaS provides a "turnkey" solution in that there is no need to purchase, test, deploy, or manage new equipment. With web threat management services, it is as simple as routing all web ingress/egress traffic to a cloud-based IP address and, voila, web threat management policies are enforced remotely.
- **Efficient and effective protection.** Since cloud vendors design their solutions for the masses, SaaS solutions tend to provide ample protection against the most common types of attacks. With regard to web threat management, this means that cloud services are likely to block malicious URLs and content, phishing sites, and known malware distribution servers. Think of cloud web threat management services as enforcing the 80%/20% rule. They may not offer the customization or security integration of on-premise gateways but they can deliver efficient and effective protection against likely web threats.
- **Support for remote offices and mobile workers.** Based upon recent research, ESG believes that employees working at remote and branch offices present a bigger security challenge than those in central locations, especially with regard to PC configuration management, end-user training, and monitoring of remote employee use of sensitive data (see Figure 3)³. These remote offices with dozens of employees need web threat management but since it may not make economic or technical sense to deploy a gateway appliance at each remote facility, cloud services are especially attractive. Mobile workers are rarely "behind the firewall." Because of that, gateway appliances offer no protection whatsoever, so SaaS is the best fit.

Cloud-based security services also have a potential security advantage due to the "network effect" and "crowd sourcing." In this model, all cloud clients act as intelligence agents and report back to the cloud when they discover new attack vectors like a previously unseen malicious code executable or compromised URL. Once a new attack is identified, everyone else in the cloud security community is safeguarded from the threat.

³ Source: ESG Research Report, [Remote Office/Branch Office Technology Trends](#), July 2011.

Figure 3. Security Challenges for Supporting Remote Office/Branch Office Requirements



Source: Enterprise Strategy Group, 2011.

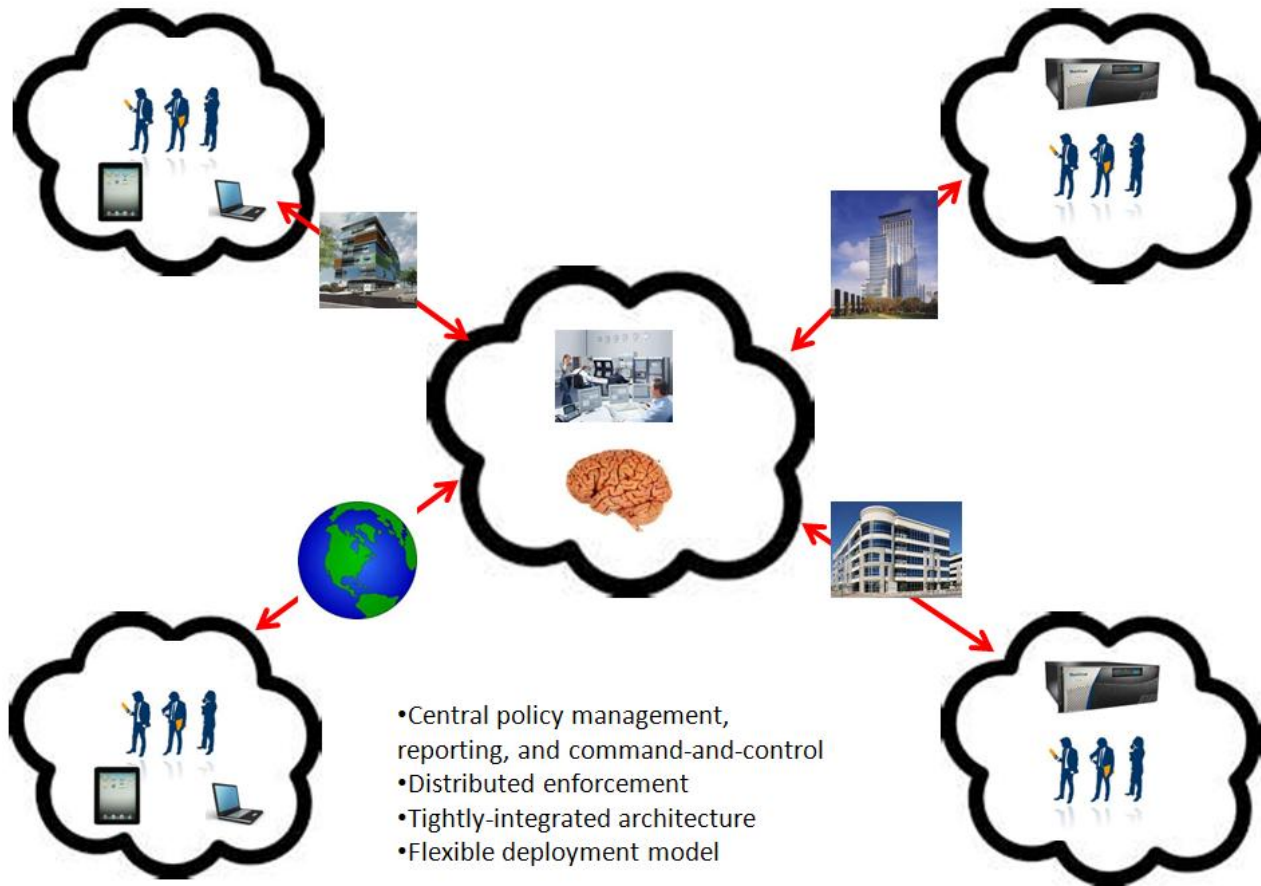
Large Global Enterprises Need a Hybrid Security Architecture

Some companies will naturally gravitate toward on-premise web threat management gateways or SaaS solutions based upon a single decision point—whether their organization is centralized or distributed. That said, many global organizations are made up of pockets of central campuses combined with a multitude of remote offices and mobile workers. Should these firms go with on-premise equipment, cloud services, or both types of solutions?

It's easy to see that large global enterprises need web threat management solutions capable of protecting all employees and IT assets whether they reside in the data center or remote offices, or access applications over public networks. Unfortunately, this could mean implementing multiple solutions from multiple vendors, an on-premise solution for the corporate network and a cloud service for remote offices and mobile employees. Yes, multiple solutions may provide coverage and protection but they will also carry high costs and redundant operations.

What's needed here is a new hybrid architecture that combines on-site performance and management benefits with cloud-based flexibility and coverage (see Figure 4).

Figure 4. Hybrid Security Architecture



Source: Enterprise Strategy Group, 2011.

To meet the large global enterprise requirements, hybrid web threat management architectures must contain:

- **Centralized management and distributed enforcement.** A hybrid web threat management architecture provides for consistent policy management and security enforcement regardless of whether these activities execute within an on-premise appliance or in the cloud. Appliances and cloud services are managed through a consistent GUI while reports can be customized for views across the enterprise (i.e. aggregate view of on-premise appliances and cloud services) or any subset of locations regardless of form factor.
- **Cloud-centric intelligence.** Threat intelligence is based firmly in the cloud while users and on-premise appliances contribute to intelligence gathering through crowd sourcing as described above. New threats are shared immediately through real-time updates of on-premise appliances.
- **Tight integration.** On-premise and cloud management and enforcement can be applied in a flexible way to cover any use case. In addition, a hybrid threat management architecture can be extended for further kinds of security requirements. For example, web threat management can be enhanced with DLP capabilities to address malicious code attacks at network ingress and data exfiltration at network egress.

Hybrid Web Threat Management Provides Flexibility and Immediate Security Benefits

ESG believes that a hybrid architecture can deliver both short- and long-term benefits that begin almost immediately. A hybrid web security architecture offers these advantages because it:

- **Improves security for remote workers.** According to ESG Research, IT support of remote offices creates numerous security challenges including web threat management (see Figure 3). And these same security

challenges holds true for mobile workers as well. A hybrid web threat management architecture provides an elegant and effective solution as it alleviates the need to deploy new equipment or one-off SaaS security services. Rather, CISOs can leverage central IT security skills and best-of-breed web security tools to apply blanket coverage for employees regardless of their geographic or network location. The result? Instant security improvement that directly addresses some of the challenges identified in the ESG Research.

- **Offers global visibility and control for rapid problem detection and remediation.** With today's sophisticated cyber attacks like APTs, all it takes is one compromised device to cascade into a major data breach. Addressing this risk means monitoring all devices and activities. Since hybrid web threat management architectures provide central command-and-control, policy management, and reporting, CISOs can have visibility and oversight over all devices and enforcement activities across the entire network. This visibility and control can accelerate problem detection and remediation.
- **Creates a cloud migration path.** Hybrid web threat management architecture combines the strengths of on-premise equipment and cloud ubiquity. Yes, this provides comprehensive coverage, but some organizations may want to offload web and other threat management activities to the cloud over time, especially as cloud security services mature. A hybrid web threat management architecture provides a flexible path for future security migration. CISOs can simply adjust network settings, replace network-based appliances with cloud services, and take advantage of cloud-based economics and security skills as they become enterprise-class options in the future.

The Bigger Truth

Cloud computing and SaaS are too often represented as binary alternatives to traditional IT efforts—either you do something yourself or wash your hands of the entire matter. This is an unfortunate portrayal that totally ignores the whole notion of “hybrid clouds.” Yes, few companies actually burst application workload capacity to public clouds today but this may become a standard method for capacity planning, business continuity, and disaster recovery in the future.

This same thought process should also be applied to more granular IT requirements like web threat management. On-premise and cloud solutions offer many benefits but neither of these options provides end-to-end coverage. Rather than choose one of these incomplete options however, smart CISOs will look for hybrid options offering the best of both. The best hybrid options will be designed for central management and distributed security enforcement woven together as a tightly integrated architecture. This is what Blue Coat offers with a web threat management architecture spanning ProxySG/WebFilter appliances and web security cloud security—both powered by the WebPulse Collaborative Defense.



Enterprise Strategy Group | **Getting to the bigger truth.**