

"We all know that becoming PCI compliant is a no-brainer. But between upgrading our systems, providing tracking and monitoring, and maintaining secure systems and applications, the whole process has become a real challenge, if not an out and our burden. There's got to be a better way."

– Senior Security Analyst

Sound familiar? It should. IT professionals the world over are facing these challenges on a daily basis. And sorting through the vast array of "solutions" can not only result in security holes, but open tickets waiting for resolution. Is there a better way? In this white paper, you will learn why it's not enough to have the best security application, but the best security platform as well; the Blue Coat Next Generation Security Platform.

The Changing World of PCI Compliance

Since the advent of PCI compliance standards, first with PCI DSS 1.1 and now with PCI DSS 2.0, the benefits from these standards to the education, financial services, healthcare, government, and retail sectors has been significant. In the wake of numerous high profile security breaches, these sectors now report a growing acceptance of these standards along with an accompanying sense of increased security. And yet, as all IT professionals know, the threats will not end. They will continue and morph to match the best security efforts currently available. Along with these threats will come more and better defined standards and new, more robust security applications.

But how is an IT professional to keep up with all of this? The traditional method is to keep adding layer upon layer of security appliances and applications to your existing network; eventually resulting in an

expensive tangle of what we call "Appliance Sprawl". (See Figure 1). This not only requires large amounts of capital and energy consumption, but also substantially increases the man hours necessary to maintain such a bloated network.

Or, they could take the Blue Coat approach. An approach that consolidates an entire network into a single box thereby eliminating the need for switches, routers, and fixed security applications. The result is a high performance "network-in-a box" or virtual infrastructure capable of running any security application from 5Gbps all the way to 150Gbps. Customers can choose the best-in-class security applications they want to run on the X-Series. The adaptable nature of the platform means that customers can easily provision new applications, change out old ones or scale performance without touching any part of the network architecture.

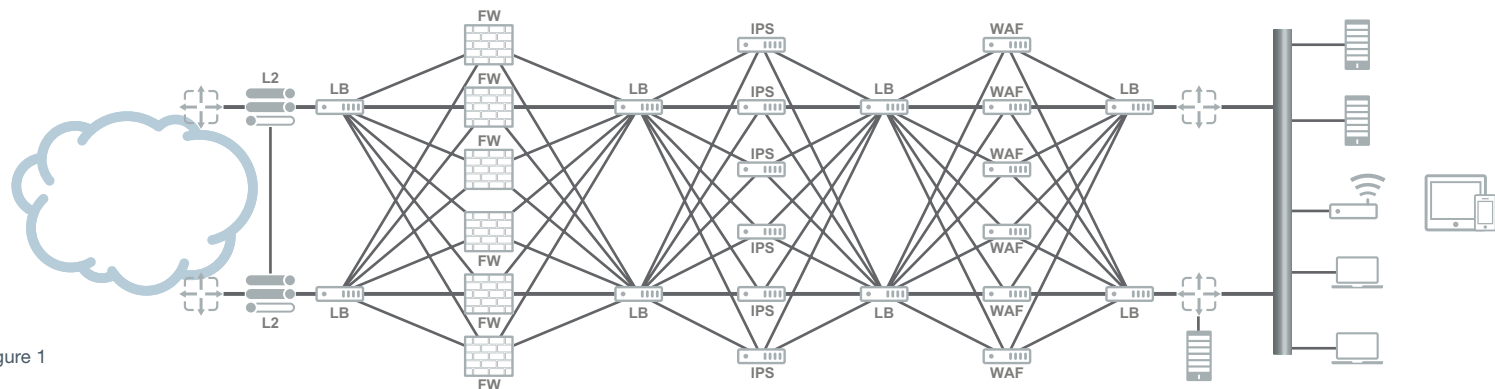


Figure 1

Be Adaptable to Change

In a world of changing threats and security responses, you need a system that can be integrated into your existing network, be easily scaled to meet your growing requirements, and be configured to meet your specific security needs. The Blue Coat X-Series platform provides this level of adaptability.

With its patented blade architecture, the X-Series platform provides a targeted approach to managing network traffic. Beginning with the Network Processing Module (NPM), incoming network traffic is directed, via customer specified policies, to security applications that reside on the Application Processing Module (APM). These security applications, in turn, can be deployed over multiple APMS (Virtual Application Groups or VAPs) to accommodate robust processing requirements. Together, the NPM and the APM work to control secure traffic flows according to custom policy requirements while maximizing performance. We call this “Secure Flow Processing”.

Given this flexible allocation of resources and security applications, it then becomes very simple to create a PCI compliant gateway solution with the correct functions applied in the desired order. The order can be changed, capacity reallocated, or functions added and removed at will. The flexible allocation of capacity is critical because database security may take up more processing horsepower than web application. Alternatively, for customers who see lower database query rates, a configuration with more APMs allocated for web application security may be more optimal.

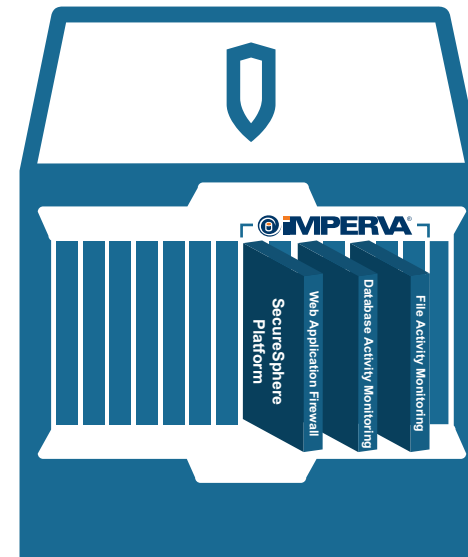
Enter Imperva

By partnering with Imperva, we have created the world’s most compliant security solution. With Imperva’s award winning Web Application Firewall and Database Security on Blue Coat, you get patented technologies that speed deployment, reduce operational costs, and enhance security including:

- **Universal User Tracking** – Empowers organizations to audit user access to data by tracking database transactions back to individual Web users.
- **Transparent Inspection** – Analyzes application logic and data usage with zero changes to applications, databases, and other network

infrastructure, while maintaining multi-gigabit transaction throughput and sub-millisecond latency.

- **Correlated Attack Validation** – Correlates multiple sources of information over time and across layers to accurately identify malicious activity.
- **Unified Management** – Enables businesses to configure, update, and monitor mixed Web and database deployments through a single, browser-based user interface.



Most importantly, Blue Coat’s PCI Compliance solution partnered with Imperva’s technology specifically addresses PCI DSS requirements 3, 6, and 10:

- **Requirement 3** – The SecureSphere Database Gateway on Blue Coat X-Series meets all of the requirements for compensating controls (section 3.4) by restricting data access by IP address, application, user name, or data type; restricting logical access to the database; blocking database attacks; and providing network segmentation.
- **Requirement 6** – The SecureSphere Web Application Firewall on Blue Coat X-Series meets all application security requirements in section 6.6 by automatically detecting application changes, thereby ensuring

that Web applications are always protected from the latest attacks, and by providing a much faster, easier, and less expensive alternative than an application source code review.

- **Requirement 10** – The SecureSphere Database Gateway on Blue Coat X-Series addresses all of the database monitoring and auditing requirements in Requirement 10 by monitoring all access to cardholder data, recording all database changes, auditing unauthorized access attempts, encrypting or digitally signing logs, and tracking end user activity with Universal User Tracking.

Thus, with Imperva on Blue Coat, administrators of large network security architectures can migrate to a total content security solution that:

- Handles both non-encrypted and encrypted traffic
- Provides complete web application protection, transparently without impacting application performance
- Delivers database attack protection by restricting logical access, and monitoring all database queries
- Delivers monitoring and auditing requirements for databases
- Optionally delivers traditional perimeter security such as firewall and intrusion protection

Summary – The Dramatic Benefits of the New Approach

The Blue Coat PCI compliance solution is unique because it completely breaks the old mold of rigid appliance farms built on the philosophy of “see a threat, buy a box.” Instead, as the very definition of a security gateway expands and changes each year, the architecture easily absorbs changes while continuing to deliver high performance and availability.

The Blue Coat solution helps customers consolidate anywhere from 20 to 50 existing separate appliances into one highly available, scalable system. When compared to competing solutions, customers can experience savings of \$500,000 to \$1 million in the first year alone simply by eliminating the capital and operational expenses associated with appliance sprawl. The performance gains of a system that can scale to throughput of 150Gbps also ensure a long product life with no fork-lift upgrades across multiple depreciation cycles.

Security teams who invest in the Blue Coat architecture report dramatic gains in productivity and security team effectiveness. Some customers have not added any network security staff in four years because of the simplicity and effectiveness of the solution. With best-of-breed security functionality from industry leaders as a foundational component of the Blue Coat PCI compliance solution, the defensive posture of the integrated offering is unequalled. The ultra-high performance and reliability of the Blue Coat platform ensure that network security teams deliver a safe end user experience without sacrificing security or availability, delivering new capabilities faster, with fewer devices, lower cost, and less staff.

© 2013 Blue Coat Systems, Inc. All rights reserved. Blue Coat, the Blue Coat logos, ProxySG, PacketShaper, CacheFlow, IntelligenceCenter, CacheEOS, CachePulse, Crossbeam, K9, the K9 logo, DRTR, Mach5, Packetwise, Policycenter, ProxyAV, ProxyClient, SGOS, WebPulse, Solera Networks, the Solera Networks logos, DeepSee, "See Everything. Know Everything.", "Security Empowers Business", and BlueTouch are registered trademarks or trademarks of Blue Coat Systems, Inc. or its affiliates in the U.S. and certain other countries. This list may not be complete, and the absence of a trademark from this list does not mean it is not a trademark of Blue Coat or that Blue Coat has stopped using the trademark. All other trademarks mentioned in this document owned by third parties are the property of their respective owners. This document is for informational purposes only. Blue Coat makes no warranties, express, implied, or statutory, as to the information in this document. Blue Coat products, technical services, and any other technical data referenced in this document are subject to U.S. export control and sanctions laws, regulations and requirements, and may be subject to export or import regulations in other countries. You agree to comply strictly with these laws, regulations and requirements, and acknowledge that you have the responsibility to obtain any licenses, permits or other approvals that may be required in order to export, re-export, transfer in country or import after delivery to you.

v.WP-SIMPLIFYING-PCI-COMPLIANCE-EN-v2a-0813

Blue Coat Systems Inc.
www.bluecoat.com

Corporate Headquarters
Sunnyvale, CA
+1.408.220.2200

EMEA Headquarters
Hampshire, UK
+44.1252.554600

APAC Headquarters
Singapore
+65.6826.7000