CROSSBEAM® SYSTEMS

Virtualization.
Consolidation.
Simplification.
Choice.

WHITE PAPER

An Inconvenient Balance?

Can the Data Center go Green Without Stifling Corporate Growth?

Table Of Contents

Introduction

The 21st Century CIO is becoming one of the most critical leaders in modern business and is under massive pressures to optimize and grow the business, stem the global energy crisis in the data center, and reduce the carbon footprint – all with the same resources. Can a balance be struck that has a win/win outcome? **YES.**

This white paper explains the growing importance of the CIO, the new technologies that can positively impact the data center's energy consumption without sacrificing performance or the need to be change-ready, and exactly how to calculate the energy and cost savings.

Situation Room

Enterprise IT organizations are mercilessly put in the spotlight to save the day and provide the business with both bottom line cost improvements and top line company competitiveness, all with the same budget and head count. Enter the global energy crisis and the overwhelming pressure to take action on reducing the corporate carbon footprint, and you end up with a melting pot of problems for the twenty first century CIO.

Not surprisingly, the data center is at the heart of most discussions when it comes to balancing corporate needs, energy demand, and the environment. Electricity intensity in a typical data center (in watts/ft2) is twenty times that of a standard office building. Hence, investors, shareholders, and governments want to see a "Green IT" action plan rolled out for all industries. This is no more apparent than in Europe, and specifically the U.K., where the government is introducing legal binding limits on CO_2 emissions, aiming for a 60%[1] cut by 2050. Carbon caps across Europe and parts of North America will follow suit shortly thereafter.

The fundamental predicament is rooted in the necessity for the enterprise to keep pace with IT innovation to remain competitive and efficient. This translates into adding more servers, larger data storage, increased security, faster connectivity, and mobility improvements that all have a direct impact on the data center and, more importantly, the energy it consumes. IT services are simply outstripping energy supply and, consequently, placing an added burden on the environment. Gartner forecasts that in 2008, 50%[2] of data centers will have insufficient power and cooling to meet the business demands. This was confirmed in a recent study indicating that 63%[3] of enterprises have already run out of space, power, and cooling capacity without warning.

Aside from the socially responsible behavior of reducing energy consumption inside the data center, the IT organization is primarily concerned with:

- The capital cost to build additional data centers due to current power/cooling shortfalls
- Restricted growth due to the fact no more power is available at the current data center
- Ever rising electricity costs hitting the bottom line

This paper will explain how the data center can be transformed to meet business needs, alleviate energy demands, and provide real substance for a company's Green IT plan.

Enter the Green CIO

The CIO is fast becoming the CEO (Chief Energy Officer), due to the rapid growth of IT in the business and the fact that the CIO is responsible for a progressively larger share of enterprise energy costs. With overall power density in data centers increasing by 15%[4] per year compounded with the cost of cooling (which can amount to 125% more in electricity), costs for IT are ballooning out of control and now account for 10-30% of the entire IT budget.

As Green IT becomes a hot topic in the eyes of the shareholders, the CIO is in the perfect position to create a showcase environment and raise the green consciousness of the company, enhancing the image and, consequently, brand reputation. The question becomes: What are the best technologies to lower consumption without compromising functionality or incurring additional capital and operational costs?

The Impact of Security Sprawl

What is the Problem?

The mandates on businesses to provide continuous IT operation, protect the corporate brand from web hackers, and comply with governmental compliance regulations are just some of the reasons why data centers have seen an explosion of security equipment and appliance sprawl. The net effect does not help the energy crisis and, in fact, increases operational spending on electricity for the following three reasons:

1) **Power Conversion:** A significant portion of the power and energy that goes into every box is either wasted in the power supply conversion or diverted to non-computing loads such as internal fans for rejecting heat; the more appliances, the more waste.
2) **Processing Inefficiency:** Traditional, dedicated one-box appliances inevitably lead to over provisioning and under utilization of processing assets, but the larger problem is that the same traffic that flows through one appliance invariably needs to be routed to other appliances to check for different security threats. Additional energy is used to take the same information and perform almost the same compute functions over and over again.
3) **Network Connectivity:** Every appliance has its own set of connectivity ports that, in the past, drew very little power. However, the power/performance ratio has not kept pace and 1Gbps verses 10/100 Fast Ethernet takes six times the power per port, while 10Gbps Ethernet takes a staggering 6-10W per port. The bottom line is that appliances have gained weight over the past 10 years, growing from 100W to an amazing 400W today.

Impacting Technologies

The two most impactful rules a CIO should follow when maximizing the efficiency of the data center are:

- Enhance the processor resource utilization everywhere:

  Think **Virtualization**

- Minimize additional box sprawl and additional connectivity:

  Think **Consolidation**

Crossbeam and Green IT

Crossbeam fundamentally transforms the way enterprises, service providers, and government agencies architect and deliver security services. The Crossbeam Next Generation Security Platform facilitates the consolidation, virtualization, and simplification of security services delivery while preserving the choice of best-of-breed security applications. This powerful combination strikes back at the wasteful appliance model of the 1990s and provides a new choice for a greener data center.

Motivated by the alarming growth of energy consumption and the need for CIOs to maximize energy efficiency, Crossbeam is participating in a global consortium dedicated to the advancement of energy efficiency in data centers and business computing ecosystems. Crossbeam is a member of the Green Grid[5], a non-profit trade organization of IT professionals with a charter to address power and cooling throughout the data center. The Green Grid does not endorse any vendor-specific products or solutions, but it provides industry-wide recommendations on best practices, metrics, and technologies that will improve overall data center efficiencies.

Crossbeam is dedicated to the reduction of energy in data centers. The company has spent more than 500 engineering man years developing a platform that facilitates a truly green approach to enabling "best-in-class" security services via the consolidation and virtualization of both network infrastructure and application processing resources.

Since so much energy is wasted in the power conversion stage from AC to DC, Crossbeam has purposely chosen the use of military grade power supplies, providing conversion efficiencies of approximately 90%. This means that only 10% of the energy is wasted as heat as the power is converted from AC to DC for use by the main processor boards.

The result is a unique architecture that vastly reduces the numbers of network switches, load balancers, and special purpose appliances, at the same time maximizing processor efficiency and power conversion – amounting to a 53% reduction in power over an appliance-based architecture.

The simplified approach translates into the following positive benefits for the IT organization:

- Enable the rapid move to a greener data center, showing clear accountability for the environment to the board of directors.
- Reduce energy consumption for all security related equipment by up to 53%, alleviating the data center crisis.
- Provide the business with a change-ready platform that can adapt to future green initiatives and security threats.
- Implement security services with no performance compromises, as well as linear scalability for future business expansion.

Security Virtualization and Consolidation

Virtualization is at the core of technology for optimizing the data center for energy consumption. However, unlike server and storage virtualization, security virtualization has a unique set of attributes driven from the following demands:

- It must be able to dynamically adapt to capacity fluctuations in the event of an attack or sudden surges in traffic.
- It must provide intelligence at the network level to apply the right combination of security services, depending on the type of traffic being routed.
- It must be able to accomplish all these things without sacrificing performance.

Additionally, security virtualization needs to take into account how each company defines and enforces its security and compliance policies. Not all assets and communications present the same level of risk. Thus, security virtualization needs to be flexible and change-ready in order to meet the company's policies.

Mainstream virtualization solutions cannot support the network performance and uptime requirements of these environments, which is one of the biggest concerns with security virtualization. A virtualization solution has to effectively combine software and specialized hardware to consolidate entire infrastructure segments onto a single platform, as well as provide intelligent hardware that can route traffic between applications at switch-like latencies.

A side effect of security virtualization is the enormous energy savings via the consolidation of devices such as appliances, LAN switches, power supplies, fan trays, transceivers, and load balancers. For companies that have ventured down this road, the benefits of security virtualization have been significant. One financial services company utilizing Crossbeam's solution reduced the number of devices used for its firewall defense and intrusion detection system (IDS) from 70 to seven. Moreover, in this

new virtualized environment, the company was able to dynamically and intelligently manage capacity and apply the right combination of security applications in the event of an attack or change in the environment. With less hardware and software, and fewer accompanying licenses to procure and manage, the organization was able to achieve significant annual operational savings, attaining two times ROI within three years.

Appliance Sprawl

In the traditional, non-virtualized environment, companies address their security issues by deploying special-purpose appliances built to run a host of security applications, from firewalls and content gateways to IDS devices and URL filters. Connecting this array of appliances is an excess of additional switching equipment, patch cabling, and load balancers. In this environment, network security has been in favor of the security vendors, with their response to each new threat being, "Have I got a box for you, and by the way, you are going to need a lot of them."

The good news is there are numerous innovative companies focusing on a particular security threat area. That focus is a big plus for customers. The downside is that these focused companies typically require that another box be added in order to deploy their solution. The requirement for redundancy and ever-increasing traffic demands accelerate growth in the number of appliances deployed. This phenomenon is known as "appliance sprawl" (see Figure 1).

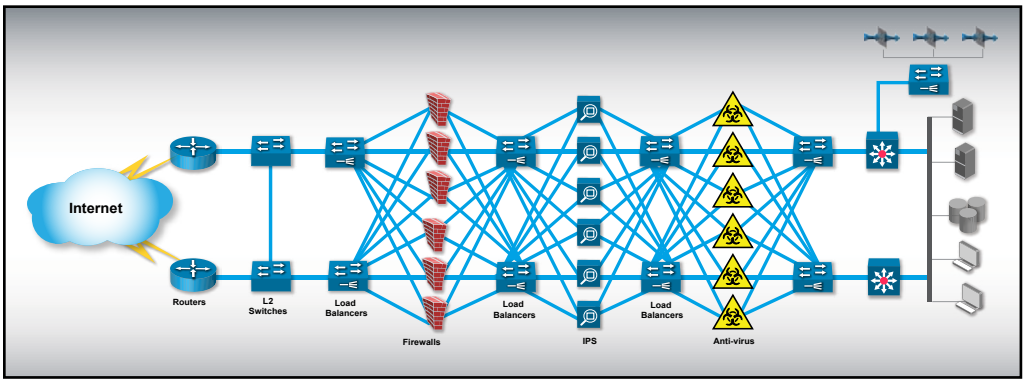

Figure 1 – Before security virtualization: complex appliance sprawl in traditional networks.

Appliance sprawl yields extraordinarily complex data center architectures, leading to wasted space, growing energy usage, and difficulty in fault diagnosis. Moreover, because these devices require connections to Layer 2 and 3 network switches plus load balancers, and have limited networking and application processing power, they essentially become embedded, single-purpose elements in the network. This means that when the security services need to be expanded or upgraded, so does the network – an expensive and inefficient use of IT and security resources.

Application Virtualization

In many ways, virtualizing security is like virtualizing any application. Vendors of security appliances need to virtualize an application instance (e.g., a firewall) and apply it on-demand to an application processor. This is the first step in any virtualization process because it treats a set of processing modules as a pool of resources that can be profiled at will, according to capacity needs.

However, a major obstacle for security appliance vendors exists: How do they ensure that multiple applications running on a single device correctly sequence communications consistent with the company security policy, with applications running on other virtual machines or other physical devices in the network? Furthermore, how do they prevent communications bottlenecks that could result from network-intensive applications like security? That is where the next element of security services virtualization comes in.

Network Virtualization

Most IT organizations today use network architecture to enforce security policies by deploying different security devices in different network segment or zones. Yet trying to create zones based on geographic or wiring closet locations is very expensive and the zones become difficult to troubleshoot and manage. Thus, in order to virtualize security services, a key element is the ability to virtualize the network switching fabric in a way that facilitates zoning and simplifies deployment, all without compromising performance, architecture preferences, or company security policies.

Control Virtualization and Policy Implementation

The final critical element to enabling security virtualization is the creation of a virtual representation of the appliance or chassis that controls which services will run on which blades and how policy selection is governed and implemented. Additionally, the virtual chassis and its components must govern failover policies, service priority, and service preemption rights.

The benefits of security virtualization and its reduced energy and carbon footprint are enormous, as can be seen in Figure 2.

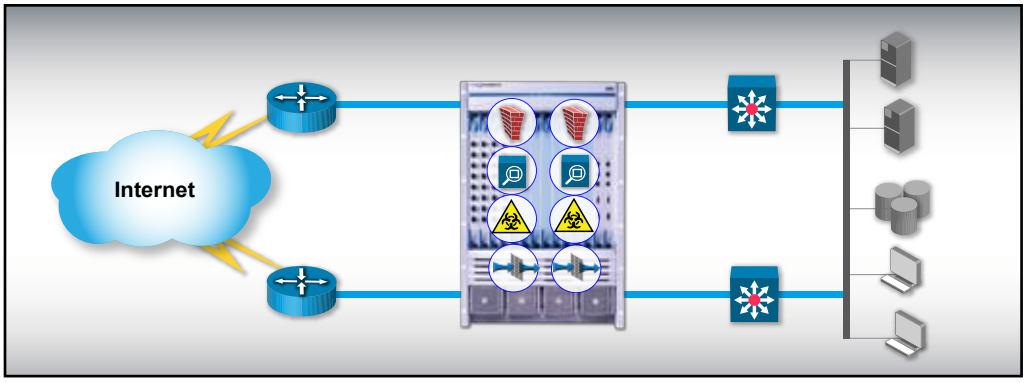

Figure 2 – After virtualization: massive consolidation and ease of management through security virtualization of both network infrastructure and applications saves up to 70% in energy cost.

Energy TCO Overview

Security virtualization and consolidation can have a compelling and dramatic effect of the total cost of ownership (TCO), lowering both long term capital expense and ongoing operational expense. Although the power and cooling expenses are a smaller part of the overall TCO calculation, the effect of alleviating the power burden on data centers and preventing delaying or reversing the need for new data centers is huge – not to mention the lower output of greenhouse-emitting gases.

An online calculator, available at www.crossbeam.com/green, can automate the task and provide cost and Green IT savings for the number of appliances to be consolidated.

Energy Cost Savings Calculation

The power consumed by security appliances and associated equipment can be calculated by adding the power ratings of each device in the data center. Because this number represents the maximum power used, it should be de-rated to achieve steady-state power consumption. To de-rate simply means to lower the rated capability of an electric apparatus. The steady-state constant is determined empirically. According to the American Power Conversion Corporation, the maximum power rating of most IT devices is well in excess of the actual running load by a factor of 33%.

To calculate the annual savings, use the following equation:

Savings = $TP_{\$}[(ß\lambda\phi\delta)-(B\lambda\phi\delta)]$

Input	Description	Default Value	Source
ß	Maximum power of appliances/ devices to be consolidated	Before	Available from manufactures website/data sheets
B	Maximum power of the Crossbeam solution	After	See Table 3
δ	British Thermal Unit (BTU) to kWh	0.000293	The Carbon Trust[6]
λ	Steady-state constant	0.67	American Power Conversion[7]
ϕ	kW to BTU	3.412	
$P_{\$}$	Price per hour of 1kW of electricity	$0.0946c	Energy Information Administration[8]
T	Hours per year of operation	8760	(24-hour operation, 365 days per year)

Table 1

Cooling Cost Savings Calculation

All data center electrical equipment produces heat and, in fact, heat dissipation is more expensive than power. Thus, the layout of data centers is critical. Best practices suggest a hot aisle/cold aisle layout, which mitigates the unacceptable temperature gradients associated with front-to-back layouts.

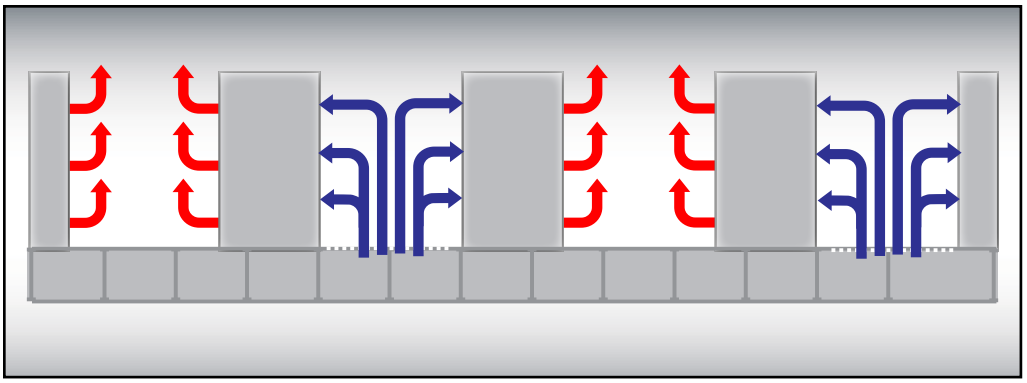

Figure 3 – Proper airflow in a hot aisle/cold aisle layout.

For simplicity, the equation to calculate cooling cost savings will focus solely on the security appliances and associated devices.
Three variables need to be taken into account:

1) **Energy Conversion Ratio:** According to HP laboratories, 0.8W of power is consumed by the cooling equipment for every 1W of heat dissipation in the data center.
2) **Airflow Redundancy:** Even with an optimized layout, as much as 25% airflow redundancy is required.
3) **De-rating:** Generally 80% of the cooling capacity can be used for cooling. The rest goes to humidification and normal losses in inefficiency. Humidification is required to reduce the potential damage of static discharge. Most AC units, however, induce humidity loss that is caused by the air-cooling function. To maintain an acceptable humidity level, supplemental humidification is required – which creates additional load on computer room AC units.

To calculate the annual cooling savings, use the following equation:

Savings = ω(TP$[(ßλφδL)-(Bλφδ∧)])

Input	Description	Default Value	Source
ß	Maximum power of appliances/ devices to be consolidated	Before	Available from manufactures website/data sheets
B	Maximum power of the Crossbeam solution	After	See Table 3
L	Energy conversion ratio	0.8	HP Laboratories[9]
p	Airflow redundancy factor	1.25	Search Data Center[10]
ω	Inefficiency/de-rating	1.25 (reciprocal of 80%)	Search Data Center[10]
λ	Steady-state constant	0.67	American Power Conversion
Φ	kW to BTU	3.412	
P$	Price per hour of 1kW of electricity	$0.0946c	Energy Information Administration
T	Hours per year of operation	8760	(24 hour operation, 365 days per year)

Table 2

Crossbeam	Watts (Peak)
Application Processor Module 8600 (APM)	260W
Network Processor Module 8600 (NPM)	110W
Control Processor Module (CPM)	260W
X-Series Chassis	106W

Table 3

The Power of Security Virtualization

To demonstrate the effectiveness, three examples are shown in Table 4 that provide details of annual energy and cooling operational savings together with Green IT metrics. To demonstrate how much CO_2 can be saved from moving to security virtualization architecture, three green metrics are shown below: cars, plants, and flights. The amount of CO2 saved is the final metric.

The calculations directly compare an appliance model to a security virtualization Crossbeam model:

- One appliance (each 380W) = One Crossbeam APM
- For every two appliances, a pair of load balances is required to provide fully redundant upstream and downstream flow balancing (each 10G load balancer 460W)
- A pair of load balancers = One Crossbeam NPM
- For every eight Crossbeam APMs include one X-Series chassis and two Crossbeam CPMs

	Consolidation of 16 Appliances	Consolidation of 50 Appliances	Consolidation of 100 Appliances
Power Saving (%)	53	52	53
Annual kWh Saving (U.S.$)	41,941	128,311	260,296
Annual Energy Saving (U.S.$)	3,967	12,138	24,624
Annual Cooling Saving (U.S.$)	4,690	15,173	30,780
Three-year Total Cost Savings (U.S.$)	26,782	81,933	166,212
Annual CO2 Emission Savings (kg)[11]	21,935	67,107	136,135
Annual CO2 Emission Savings (lbs)	48,358	147,944	300,122
Cars Off the Highway[12]	5	17	34
Number of Trees Planted[13]	26	79	160
Number of Trans-Atlantic Flights[14]	18	56	114

Table 4

Conclusions and Next Steps

Technologies that not only meet the business demands for performance, continuity, and compliance, but concurrently help the data center reduce energy consumption and have a low TCO, should be added to the IT roadmap for investigation. These are the technologies that will help bring balance to the data center and provide a business with the tools it needs to continue to grow and operate.

Naturally, while the data center is a critical component, CIOs must consider the energy and carbon footprint of the whole organization and make recommendations on where technology can enable the most impactful savings. Technologies such as security virtualization that create data center consolidation can significant impact energy usage (as demonstrated in this white paper), but further simple changes in behavior can have staggering benefits.

For Crossbeam, being part of the Green IT solution is about being able to help transform the security ecosystem of the data center and, in doing so, empower businesses with a platform to become change-ready for whatever lies ahead.

About Crossbeam Systems®

Crossbeam Systems, Inc. transforms the way enterprises, service providers and government agencies architect and deliver security services. The basis of Crossbeam's solution is its Next Generation Security Platform, a highly scalable hardware platform that facilitates the consolidation, virtualization, and simplification of security services delivery, while preserving the customers' choice of best-of-breed security applications. Crossbeam offers the only security platform that delivers unparalleled network performance, scalability, adaptability, and resiliency. Customers choose Crossbeam to intelligently manage risk, accelerate and maintain compliance, and protect their businesses from evolving threats. Crossbeam is headquartered in Boxborough, Mass., and has offices in Europe and Asia Pacific. More information is available at: www.crossbeam.com.

References and Resources

1 http://en.wikipedia.org/wiki/Energy_policy_of_the_United_Kingdom

2 http://www.gartner.com/it/page.jsp?id=499090

3 http://www.onstor.com/pdfs/GoGreen_survey_UK.pdf

4 http://www.thegreengrid.org

5 http://www.thecarbontrust.co.uk/energy/

6 Sawyer, Richard "Calculating Total Power Requirements for Data Centers" American Power Conversion, 2004

7 http://www.eia.doe.gov/cneaf/electricity/epa/epat7p4.html

8 Patel, Chandrakant D, Shah, Amip J "Cost Model for Planning, Development, and Operation of a Data Center"

9 http://searchdatacenter.techtarget.com/news/column/0,294698,sid80_gci1148906,00.html

10 http://searchdatacenter.techtarget.com/news/column/0,294698,sid80_gci1148906,00.html

11 http://www.aea-energy-and-environment.com/ 0.5230 Conversion factor for mains electricity (kWh to kg CO2)

12 http://www.aea-energy-and-environment.com/0.3372 Conversion factor for standard petrol car 12,000 miles per year (mile/kg CO2)

13 http://www.aea-energy-and-environment.com/ Average tree removed 850kg CO2 over life

14 http://www.aea-energy-and-environment.com/ Return flight from Boston to London Heathrow equates to 1,200 kg CO2

Corporate Headquarters
Crossbeam Systems, Inc.
80 Central Street
Boxborough, MA 01719
Tel: +1 (978) 318 7500
Fax: +1 (978) 287 4210
www.crossbeam.com

WP_GREEN_IT_050908