Reducing Costs With Next-generation Network Security

Investing in Innovation Pays Cost Savings Dividends

August 2013

Palo Alto Networks
3300 Olcott Street
Santa Clara, CA 95054
www.paloaltonetworks.com

Table of Contents

Executive Summary

For network security teams, the evolution of applications and threats, coupled with the stagnation of traditional network security technology has resulted in a loss of visibility and control. Despite efforts to regain visibility and control by adding more security appliances, most organizations remain stymied – unacceptably. In today's economic climate, however, any further increase in cost and complexity is similarly unacceptable. Some leading organizations, however, have found that investing in innovation, and bucking the trend of seemingly never-ending appliance sprawl in network security can result in the restoration of visibility and control, and substantial reduction in cost of ownership of security infrastructure.

This paper details real cases from three businesses, the legacy infrastructure they replaced, the Palo Alto Networks next-generation security platform they deployed, and the substantial savings they realized – cutting capital and operations costs by 50% on average.

Minimize Security Risks, and Regain Visibility and Control While Reducing Costs

Network security teams face a host of challenges - some of them are well understood (organizational issues, compliance), and others brand new (cloud and mobile computing, evolving applications, new cyberthreat landscape, APTs). More than ever, it is incumbent on the network security organization to address two seemingly conflicting mandates:

- Minimize cybersecurity risks and protect the organization from sophisticated threats and malware
- Manage and reduce costs

While these requirements seem to pull organizations in different directions; this paper will demonstrate how organizations can, by investing in innovation, meet these requirements with a common initiative.

Legacy Firewalls are Ineffective in Today's Application and Threat Landscape

In order to minimize cybersecurity risks and comply with regulations, organizations have to understand and control the applications, user behavior, and content on their network. Unfortunately, applications have evolved beyond the legacy set of network-based security infrastructure and can easily circumvent the capabilities of traditional security solutions and firewalls using encryption, proxies, port-hopping, tunneling or other evasive techniques. Today's reality is that most applications and cyberthreats easily knife through enterprise network security defenses. With the on-going escalation of cybersecurity concern, it has become clear to most security professionals that the old mapping of applications to ports is no longer relevant. Thus making the traditional security infrastructure based on legacy firewalls largely useless.

Security Add-ons Lead to Complex and Costly Appliance Sprawl

To the chagrin of many security professionals, the industry's traditional response to new threats and the evolution of technology towards cloud and mobile computing has been to add more appliances – each adding a network security function around a traditional firewall. This unsustainable approach has proven complex and costly, and now appears to be broken – since these security add-ons can't see all of the traffic, can't rely on a common classification of traffic, and no longer enable security professionals to act rapidly on suspicious traffic. Unfortunately, enterprises had little choice, most have adopted an array of security appliances – resulting in a network security infrastructure that is fragmented, expensive, difficult to manage, and increasingly ineffective at controlling application and minimizing cyberrisks.

Bleak Financial Climate Means That IT Must Reduce Costs

Given today's economical environment, many IT groups have a mandate to control costs. Budgetary and cost-saving pressures are extreme, and green IT initiatives continue. Given this climate, security teams must innovate or risk obsolescence – incremental changes to ineffective infrastructure can't solve these issues.

Band-Aids Aren't The Answer Band-Aids Aren't The Answer – It's Time to Fix Network Security

The firewall is the network security foundation for nearly every enterprise – with good reason: the firewall is in-line, sees all traffic, and thus is in a unique position to enforce control. It also demarcates the trust boundary. The problem, as stated above, is that legacy firewall implementations are not effective in today's application and threat environment, and "helpers" don't help. Next-generation firewalls from Palo Alto Networks fix the firewall, enabling enterprises to regain visibility and control over the applications, users, and content on their networks – and greatly reduce the number of security appliances that they have to maintain.

Invest in Innovations and Reduce Costs With Palo Alto Networks

Palo Alto Networks re-invented network security from the ground-up and integrated natively in its next-generation firewalls all key security functions. This has enabled organizations to regain the visibility and control that they had been lacking, and cut down on the expensive and complex security appliance sprawl they'd been forced into over the last decade. Cost savings come in two major areas: capital expenditures, and operational expenses.

Capital Expenditures: Palo Alto Networks Enables Simplification

Capital expenditures are relatively well understood – one device is typically cheaper than three. The challenge when modeling the cost of security devices is the timing of those purchases. Few enterprises decommission multiple types of devices across the enterprise at the same time. The scope and size of these costs, however, even being mindful of

phased purchases and depreciation schedules, merit serious consideration – since by eliminating some of security devices, utilizing the budget for one type of device might obviate the need for an additional purchase in the future.

Operational Expenses: Reduce Support and Subscriptions

Looking at "hard" operational expenses, there are 3 or 4 major categories: support and maintenance contracts, URL filtering subscriptions, threat prevention/IPS subscriptions (if not captured in IPS device maintenance/support), and power/HVAC. There are other "soft" operations costs that can be significant in a case for simplification – IT staff productivity, end user productivity, help desk calls, training, vendor management – but for maximum credibility, these costs are often better characterized rather than counted. Rack space is a potential exception, as some organizations have done enough analysis and can characterize all of their data center costs per unit of rack space (real estate, power, cooling, management, etc.).

Operational Expenses: Less Appliances Helps Green IT and Power Consumption

Regarding power and datacenter HVAC, many organizations have "green" efforts, attempting to reduce energy use and the amount of waste they generate. Given the amount of energy used by a typical datacenter, IT is often called upon to reduce the amount of power consumed by IT infrastructure and data center cooling. Effectively reducing the number of security devices can offer substantial energy savings – both directly (i.e., the power consumed by the security device) and indirectly (i.e., the power consumed by the data center cooling system to cool the device). A good rule of thumb is a watt of power consumed is a watt of power needed for cooling. Furthermore, fewer devices means less waste – combined with reduced energy use, makes a compelling "green" argument for Palo Alto Networks security platform.

Customer Examples Show Savings

Perhaps the best way to understand potential savings is by looking at a few examples. Here are three real-world examples – a very large organization, a medium-sized organization, and a smaller organization – their issues, expenses, and how – using Palo Alto Networks – they were able to regain visibility and control of their networks, while significantly reducing complexity and costs.

Customer Example #1: Large Financial Services Organization

Saving $331K/year with Palo Alto Networks: Using Palo Alto Networks, a large ($100 billion+ annual revenue), multinational financial services organization is undergoing an enterprise network security device consolidation project – and will save $331K/year in network security operations costs – at one location.

Legacy Deployment – Lots of Sprawl: Examining the legacy deployment at that location (mid-Atlantic, US, serving 5000 users), the IT organization maintained Cisco firewalls,

Sourcefire IPS appliances, Secure Computing appliances, and Blue Coat proxy appliances. The sheer number of security appliances dictates significant additional infrastructure just to accommodate their connectivity – including a dedicated switch and a pair of F5 Local Traffic Managers.

Palo Alto Networks – Greener and Faster: Given the state of the financial industry, operational cost reductions are welcome. Furthermore, "going green" has a significant value for many organizations (including this one), both internally and externally. In just one data center, this customer is showing a reduction in power and HVAC costs of nearly $40K annually – a savings of 90%. Palo Alto Networks could show substantial functional consolidation (firewall, URL filtering, threat prevention), and could also reduce the overall number of firewalls due to the Palo Alto Networks next generation firewall's superior performance and end-to-end security capabilities. Furthermore, the application visibility and control from Palo Alto Networks next-generation security platform gave the IT organization the tools they needed to better manage application use on their network – safely enabling core business applications, while preventing the use of undesirable applications.

Large Organization	Legacy	Palo Alto Networks	Savings
Capital Costs	$2,424,940	$480,000	**$1,944,940**
Annual Operations Costs			
Support Contracts	$424,785	$76,800	
URL Filtering	$40,000.00	$48,000	
Threat Prevention	n/a	$48,000	
Power/HVAC	$44,106	$4,403	
	---	---	
Total Annual Ops Costs	$508,891	$177,203	**$331,688**
Legacy equipment: Firewall: 12x Cisco ASA, IPS: 2x Sourcefire 3DS, URL filtering/proxy: 6x Secure Computing Webwasher + 5x Blue Coat ProxySG, Traffic management: 2x F5 Local Traffic Manager		**Palo Alto Networks equipment:** 10x PA-4000 Series	

Customer Example #2: Global Manufacturer

Saving $147K Per Location in Capital Costs With Palo Alto Networks: With Palo Alto Networks, this 30-site, $1B global manufacturer has reduced its annual remote site network security operations costs by 35%.

Legacy Security Infrastructure Was Expensive: This customer's standard security rack at each location included Cisco ASA firewalls, Tipping Point IPS, and a Microsoft ISA Server running on Dell hardware. The expenses surrounding the customization and upkeep of the ISA Server coupled with the limited capabilities of the Cisco firewalls prompted the IT group

to look to Palo Alto Networks to simplify their security infrastructure – and in doing so, give control of the network back to IT.

Palo Alto Networks is the New Standard: The visibility, control, and cost savings were significant enough that the organization quickly deployed Palo Alto Networks next-generation security platforms across 3 sites, and declared Palo Alto Networks as the standard deployment for all sites going forward. Looking at just the 3 deployed sites, the IT group was able to show a reduction in capital costs of over $117,000. Similarly, across the 3 deployed locations, the IT group was able to show annual savings of nearly $20,000. Once deployed across the remaining 27 sites, this will represent an enormous annual cost reduction.

Medium-sized Organization	Legacy	Palo Alto Networks	Savings
Capital Costs	$213,555	$96,000	**$117,555**
Annual Operations Costs			
Support Contracts	$34,168	$15,360	
URL Filtering	$15,000	$9,600	
Threat Prevention	n/a	$9,600	
Power/HVAC	$6,902	$1981	
	---	---	
Total Annual Ops Costs	$56,070	$36,541	**$19,529**
Legacy equipment – for each of 3 locations: Firewall: 2x Cisco ASA, IPS: 1x TippingPoint, URL filtering/proxy: 1x Dell Server and Microsoft ISA Server		**Palo Alto Networks equipment** – for each of 3 locations: 2x PA-2000 Series	

Customer Example #3: City Government and Schools

Cut Operational Expenses by 64%: The last example is a smaller organization, a city government and school system on the East Coast of the United States, who was able to show operations cost reduction of 64%.

Legacy Infrastructure Couldn't Perform: This organization was using Watchguard firewall/UTM devices and St. Bernard iPrism filtering appliances. Unfortunately, the city employees and school staff and students were able to use less than 10% of their Internet bandwidth due to the poor performance of their security infrastructure. Additionally, the fees associated with URL filtering and maintenance subscriptions were very high. Finally, students and staff easily bypassed these network security controls using proxies, encrypted applications (like Skype), and tunneling applications like UltraSurf and TOR.

Palo Alto Networks Restores Visibility, Control, and Performance: Replacing the end-of-life and poorly performing Watchguard and St. Bernard infrastructure saved the city thousands of dollars per year. The IT staff was able to present a compelling case for the Palo Alto Networks next-generation security platform – showing a capital cost savings of nearly $7,000 over replacing the $20,000 legacy infrastructure. Perhaps more importantly, by consolidating existing functions, and adding the application visibility and control that the

city needed, the security team was able to reduce network security operations costs from over $25,000 to just $9,200 per year – a savings of over $16,000 per year. Functionally, the city was able to see and control evasive applications, comply with regulations regarding school technology use, and safely enable a wide variety of Internet applications for staff.

Small Organization	Legacy	Palo Alto Networks	Savings
Capital Costs	$22,957	$16,000	**$6,957**
Annual Operations Costs			
Support Contracts	$3,673	$2,560	
URL Filtering	$20,000	$3,200	
Threat Prevention	n/a	$3,200	
Power/HVAC	$2,008	$330	
	---	---	
Total Annual Ops Costs	$25,682	$9,290	**$16,391**
Legacy equipment: Firewall/UTM: Watchguard Firebox, URL filtering – St. Bernard iPrism 50h (M11000)		**Palo Alto Networks equipment:** 1x PA-2000 Series	

Summary of Cost Savings With Palo Alto Networks

In all three cases, the savings in both capital costs and operations costs were substantial. On average, the three organizations examined in this paper reduced their capital budgets by more than 50%, and cut their annual operations costs by a similar number. Granted, there are big differences across these examples, but many Palo Alto Networks customers can easily demonstrate a rapid return on their investment – covering the upfront cost of the solution with the reduction in operations costs in the first year. Regaining control of the applications, users, and content on the network was of equal importance to the IT staffs in the enterprise customers examined in this paper, but demonstrating the cost advantages enabled these projects to move forward quickly – even in a tough economic climate. In brief summary:

- **Save 30%-80% in Capital Expenditures.** In all three examples, reducing the number of security appliances resulted in substantial reduction of capital expenditures – from 30% in our "small" example (we only replaced 2 boxes), to 80% in our "large" example.
- **Save 40%-65% in Operational Expenses.** In all three examples, hard operations costs went down significantly – what organizations spent on support/maintenance contracts, URL filtering subscriptions, and power was reduced: from 35% in our "medium" example to 65% in our "large" example.
- **Save on "Soft" Costs Too.** We didn't attempt to quantify "soft" costs, which, while significant, are difficult to quantify and often undermine the impact of a cost analysis. In our examples, the medium and small organizations reported substantial soft costs savings. For the manufacturer, deployment and integration efforts were greatly reduced, resulting

in demonstrable savings. Most important, customers cited a reduction in the time it took to find and resolve security problems – often before they resulted in a help desk call, for which they could easily demonstrate savings.

The bottom line for many organizations is that while they have security and compliance needs that must be met, few projects that don't demonstrate significant cost savings will be funded. For Palo Alto Networks customers, investing in innovation with a next-generation security platform has helped them regain visibility and control, and has enabled substantial cost savings – a rare combination of benefits that has resulted in increased stature within their organization.