netskope

White Paper

Unlock Savings and Simplify Operations Through Network & Security Transformation

Legacy network and security approaches were not built for the cloud. As the majority of organizations have adopted a cloud-first strategy the legacy model of running and supporting a corporate network starts to show diminishing returns.

The steadily increasing consumption of cloud apps and movement of private apps to public cloud has left on- premises security solutions behind. The average enterprise uses over 2400 cloud applications, and has increased the volume of corporate data in the cloud. This digital transformation trend has created risks of data loss from cloud apps and services.

20%

of users move data between cloud apps

35%

of cross-app data movement is considered sensitive

2,480+

different apps and services are involved

48%

of corporate data is in the cloud

Many organizations take short-term, tactical steps towards securing cloud apps, resulting in greater complexity and costs and minimally affecting risk of breach or data loss. The most recent Ponemon Breach report holds that data breaches with a lifecycle of more than 200 days had an average cost of $4.87 million, compared to $3.61 million when under 200 days.

The associated breach causes were attributed to malicious cyber attacks (including phishing, cloud misconfigurations, third-party software vulnerabilities, compromised credentials, etc.) for over half, and the other half to human error and system glitches.

Average breach cost*

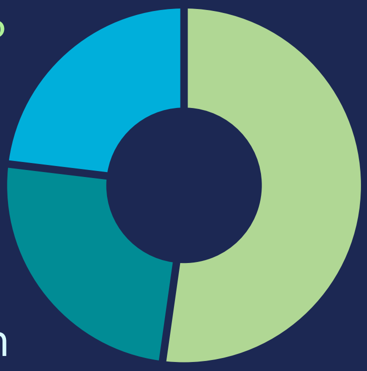
$4.87M

lifecycle of more than 200 days

$3.61M

lifecycle under 200 days

Data breach root cause breakdown*



Human error
23%

System glitch
25%

Malicious Attack
52%

- Compromised credentials
- Cloud misconfigurations
- Third-party software vulerability
- Phishing

*IBM/Ponemon 2021

WHAT WE OFTEN GET WRONG IN SECURITY AND NETWORKING BUDGETS

What the COVID-19 pandemic added to this established trend of cloud overtaking web traffic was an enormous global surge in remote workers. IT leaders across all business verticals are acknowledging that those workers will not be returning to work within traditional office settings even once the pandemic has passed. Cloud usage irreversibly accelerated, and we have entered a permanent model of a dispersed workforce.

A significant amount of budgetary overspend also comes from an attempt at future proofing with oversized appliances. Even accounting for the length of time that a procurement process can take, any RFP must be designed to address future needs, as far as possible, rather than those that an organization has in the present. But we know that this future planning—attempting to guess functional needs and associated budgets—is rarely accurate in hindsight.

In the legacy security set up using SWG and VPN, everything a remote user does is routed back through the organization's data center, where threat and data protection policies can be applied.

This was effective when the vast majority of applications resided in that data center. However, the majority of applications and services are now provisioned from the cloud and consumed by employees on mobile devices (laptops, tablets, smartphones, etc.) outside of the corporate network. Security has become the only reason for remote worker traffic to go back to the corporate data center.

From an economic perspective this means a continual investment in network bandwidth, appliance capacity, and specialist support hours for the sake of security alone and often at the expense of good user experience. The corporate data center and network has become a bottleneck, and bottlenecks require further investment to expand their capacity and avoid slowing down productivity. It is a significant cost that can be avoided when security services can take place within the cloud, away from the corporate data center.

Our budgetary guesswork is often wrong in the other direction too. While some shrinkage can be foreseen and planned for through hardware lifecycle planning, not everything is predictable. Many organizations buy more capacity than they need today, in readiness for a future capacity need which may not occur.

Whether due to macro economic forces, or individual company circumstances, one of the most obvious drawbacks of any CapEx IT investment is that you have to make a big outlay at the start and trust that you see the value and efficiencies further down the line based on a projection, which is hardly a reliable indicator.

Moving to a predictable OpEx subscription-based model supports operational cost efficiencies, is simpler to forecast, and, as security becomes a full services-based industry, supports cost avoidance while allowing for additional consolidation opportunities.

IMMEDIATE TRANSFORMATION SAVINGS

The big-ticket items for most security budgets are the appliance spend and the ongoing maintenance of these appliances over their short lifetime. Monthly updates with new features, patching newly-found vulnerabilities, and the racking and stacking of appliances as the traffic throughput increases are all costly, especially when change maintenance windows may only be possible overnight or on weekends.

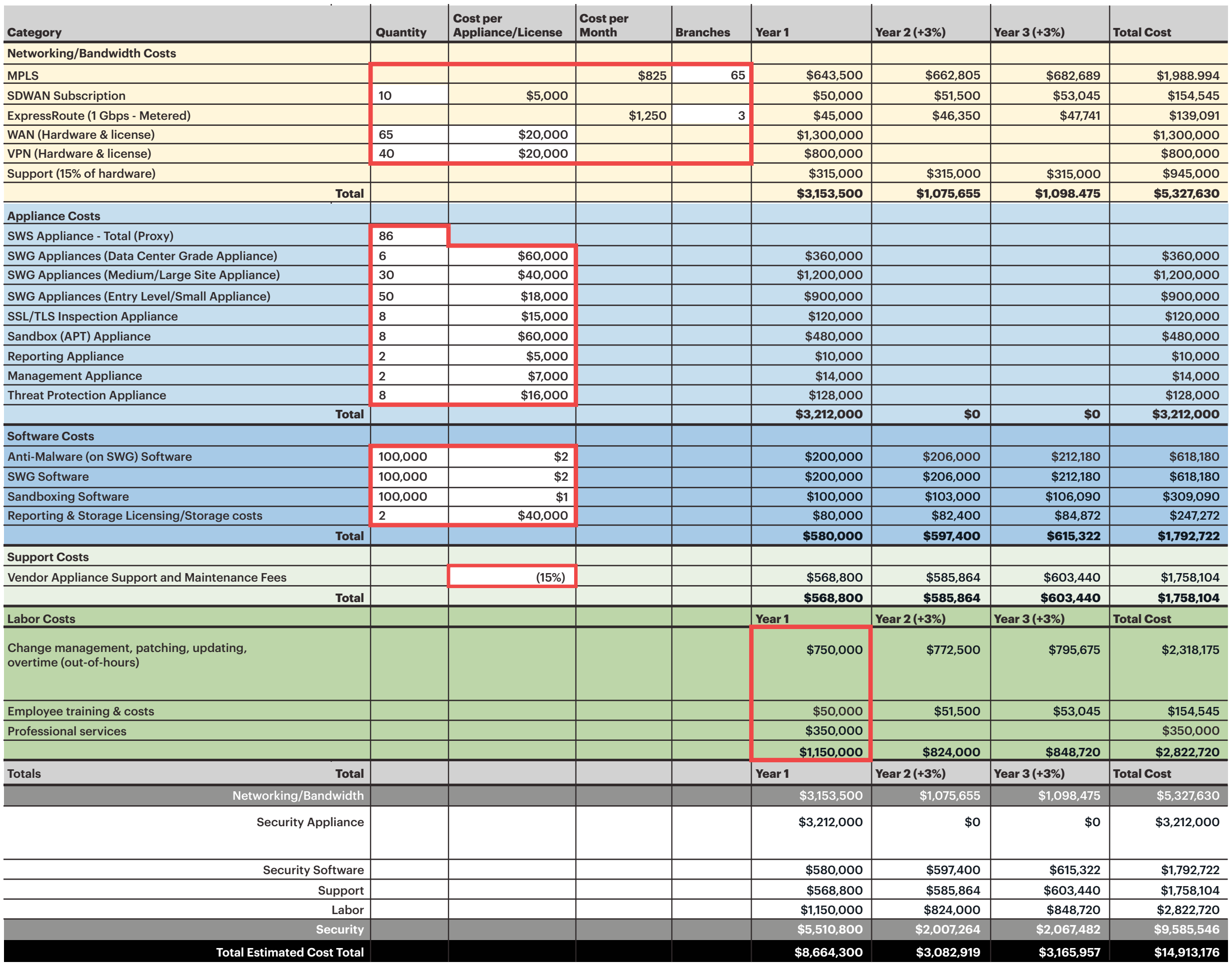
The economics of security appliances are analogous to buying a new car outright every three years and depreciating the full cost over that time with no residual value remaining. At least when buying a car we get a trade-in price for 30-50% of the value after the three years. For appliances, however, the majority are securely destroyed and recycled after that period, no matter how well maintained they are. Not only does this not make financial sense, but it's also not the best approach to support a happy and fulfilled security team with evenings and weekends lost to this ongoing maintenance requirement. Plus, the constant production, shipping, and recycling of appliances is not supportive of corporate social responsibility goals, which are increasingly important (and required) to do business.

On the following page is a simple TCO example of traditional network and security technology spend by an organization with 65 branch offices across the globe focused on web and cloud security. The total spend is $15M USD for fundamental network and security costs over three years. These costs have been broken into:

- Networking & Bandwidth Costs (excluding dedicated internet/ telecom lines)
- Security Appliance Costs
- Security Software Costs
- Support Costs
- Labor Costs

These costs will only continue to increase as the traffic profile of the organization increases with the use of more web and cloud services. The goal of any network and security transformation programme is to replace many of these CapEx spend items such as appliances, and support and labor costs.

Total Cost of Ownership Model: Network and Security Spend for Web and Cloud Security



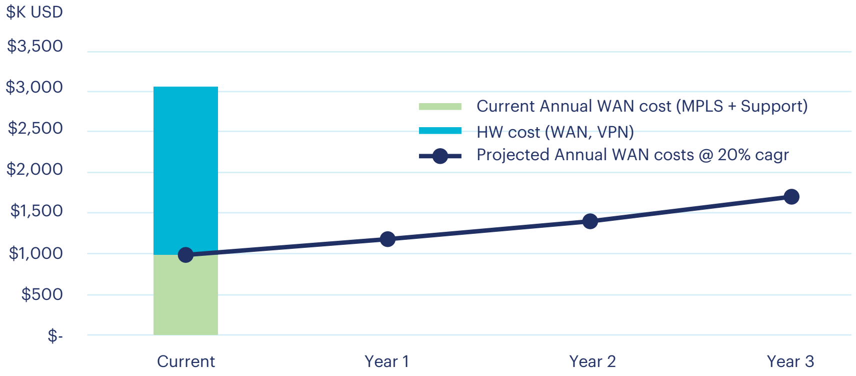
Category	Quantity	Cost per Appliance/License	Cost per Month	Branches	Year 1	Year 2 (+3%)	Year 3 (+3%)	Total Cost
Networking/Bandwidth Costs								
MPLS			$825	65	$643,500	$662,805	$682,689	$1,988.994
SDWAN Subscription	10	$5,000			$50,000	$51,500	$53,045	$154,545
ExpressRoute (1 Gbps - Metered)			$1,250	3	$45,000	$46,350	$47,741	$139,091
WAN (Hardware & license)	65	$20,000			$1,300,000			$1,300,000
VPN (Hardware & license)	40	$20,000			$800,000			$800,000
Support (15% of hardware)					$315,000	$315,000	$315,000	$945,000
Total					**$3,153,500**	**$1,075,655**	**$1,098.475**	**$5,327,630**
Appliance Costs								
SWS Appliance - Total (Proxy)	86							
SWG Appliances (Data Center Grade Appliance)	6	$60,000			$360,000			$360,000
SWG Appliances (Medium/Large Site Appliance)	30	$40,000			$1,200,000			$1,200,000
SWG Appliances (Entry Level/Small Appliance)	50	$18,000			$900,000			$900,000
SSL/TLS Inspection Appliance	8	$15,000			$120,000			$120,000
Sandbox (APT) Appliance	8	$60,000			$480,000			$480,000
Reporting Appliance	2	$5,000			$10,000			$10,000
Management Appliance	2	$7,000			$14,000			$14,000
Threat Protection Appliance	8	$16,000			$128,000			$128,000
Total					**$3,212,000**	**$0**	**$0**	**$3,212,000**
Software Costs								
Anti-Malware (on SWG) Software	100,000	$2			$200,000	$206,000	$212,180	$618,180
SWG Software	100,000	$2			$200,000	$206,000	$212,180	$618,180
Sandboxing Software	100,000	$1			$100,000	$103,000	$106,090	$309,090
Reporting & Storage Licensing/Storage costs	2	$40,000			$80,000	$82,400	$84,872	$247,272
Total					**$580,000**	**$597,400**	**$615,322**	**$1,792,722**
Support Costs								
Vendor Appliance Support and Maintenance Fees		(15%)			$568,800	$585,864	$603,440	$1,758,104
Total					**$568,800**	**$585,864**	**$603,440**	**$1,758,104**
Labor Costs					**Year 1**	**Year 2 (+3%)**	**Year 3 (+3%)**	**Total Cost**
Change management, patching, updating, overtime (out-of-hours)					$750,000	$772,500	$795,675	$2,318,175
Employee training & costs					$50,000	$51,500	$53,045	$154,545
Professional services					$350,000			$350,000
					$1,150,000	**$824,000**	**$848,720**	**$2,822,720**
Totals **Total**					**Year 1**	**Year 2 (+3%)**	**Year 3 (+3%)**	**Total Cost**
Networking/Bandwidth					$3,153,500	$1,075,655	$1,098,475	$5,327,630
Security Appliance					$3,212,000	$0	$0	$3,212,000
Security Software					$580,000	$597,400	$615,322	$1,792,722
Support					$568,800	$585,864	$603,440	$1,758,104
Labor					$1,150,000	$824,000	$848,720	$2,822,720
Security					$5,510,800	$2,007,264	$2,067,482	$9,585,546
Total Estimated Cost Total					**$8,664,300**	**$3,082,919**	**$3,165,957**	**$14,913,176**

PRACTICAL EXAMPLES OF SECURITY AND NETWORKING TCO SAVINGS

Example 1

Network costs of backhauling or hairpinning traffic back across costly MPLS networks to the data center security stack are immediate targets for elimination, particularly for traffic going to Cloud applications. The savings of sending remote users traffic directly to the internet, or leveraging SD WAN at branch locations to increase bandwidth for direct to internet connections are through elimination of VPN and WAN router, optimisation hardware, and expensive MPLS links.

Networking costs with VPN backhaul

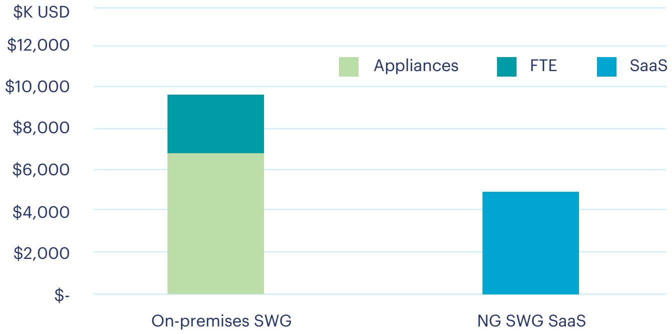


Network cost avoidance of $6.3M over three years, 65 branch locations
$2.1M in HW CAPEX, $4.2M in annual WAN costs (MPLS, service)

Example 2

Once completed, the question of the utilization and the need for the on-premises security appliances arises. The shift to consolidated security cloud services offers the immediate benefit of replacing complex appliances that require operational and engineering resources to maintain. More than $9M in cost savings over three years can be achieved across the Secure Web Gateway appliance and resource expense. The case becomes even more valuable with the added cost of TLS/SSL decrypt appliances and DLP appliances factored into the on-premises deployment that many organizations have.

3 Year Cost Advantage:
On-prem SWG vs NG SWG SaaS



Not included: TLS/SSL decrypt appliances, DLP appliances

The security transformation may start with replacing branch location hardware and moving to the corporate data center. Whatever the order, the strategic economic opportunity for security and networking teams is to achieve both the agility and the security posture needed in your business. Considering the risk management controls needed in a multi-cloud architecture is also part of the economics of transformation. Real-time information on third-party risk, user behavior, data and threat anomalies are essential to faster detection, and more effective resolution.

The average organization has acquired many technologies and solutions over the years that are ready for replacement in a cloud-first world. The phrase most often heard from a CIO/CISO is "I need to consolidate." Consolidation of technologies is not a simple task but it can be made easier by using concepts such as Gartner's Secure Access Service Edge (SASE) to identify what key capabilities are required to support the organisation's future ecosystem.