Digital Transformation

Cloud-First

The Economic Advantages of Network & Security Transformation

Future-proof

Neil Thacker, EMEA CISO @ Netskope

netskope

Introduction

Ask the board of an organisation what their ultimate goal for digital transformation is and the response will be:

“to future-proof the organisation with digital services, improving top-line growth while applying operational cost efficiencies to maintain a healthy bottom line.”

Any change to traditional business revenue streams come with initial costs, but as digital transformation projects bed into an organisation, and processes and workflows adapt to the new opportunities (for both service innovation and cost reduction), so come the economic efficiencies. This same model applies to network and security transformation (as a subset of broader digital transformation), but with generally faster realisation of economic efficiencies.

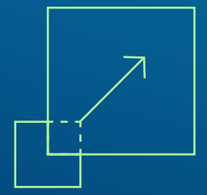
The year 2020 was a catalyst for organisations to rethink their network and security programmes for many reasons. For organisations in the midst of digital transformation, it was the obvious time to accelerate their network and security transformation to become cloud-first and move beyond the restrictive legacy hub-spoke network approach. For those that were delaying change, doing nothing stopped being an option as businesses were driven out of their comfort zone in a quest to ensure the organisation survived.

KPIs to track Digital Transformation

- Lifetime Value
- Hours Saved
- Business Sustainability
- Operational Improvement
- Workforce Productivity
- Rate of Innovation
- Operating Expenses and Contribution Margin
- Cloud Application Deployments

Economic motivations driving the move of network and security functions to the cloud:

Reduced costs through the use of shared cloud infrastructure and payment for only what is needed



Scalability on demand, without the need to re-architect

Adaptability of digital services enables innovation at scale

Best-in-class data analytics and opportunity for tighter integrations

Speed to deployment and the avoidance of physical supply issues (agility)

Breach risk reduction with security services on demand where needed

In this paper, we take a look at the economic advantages and implications of network and security transformation.

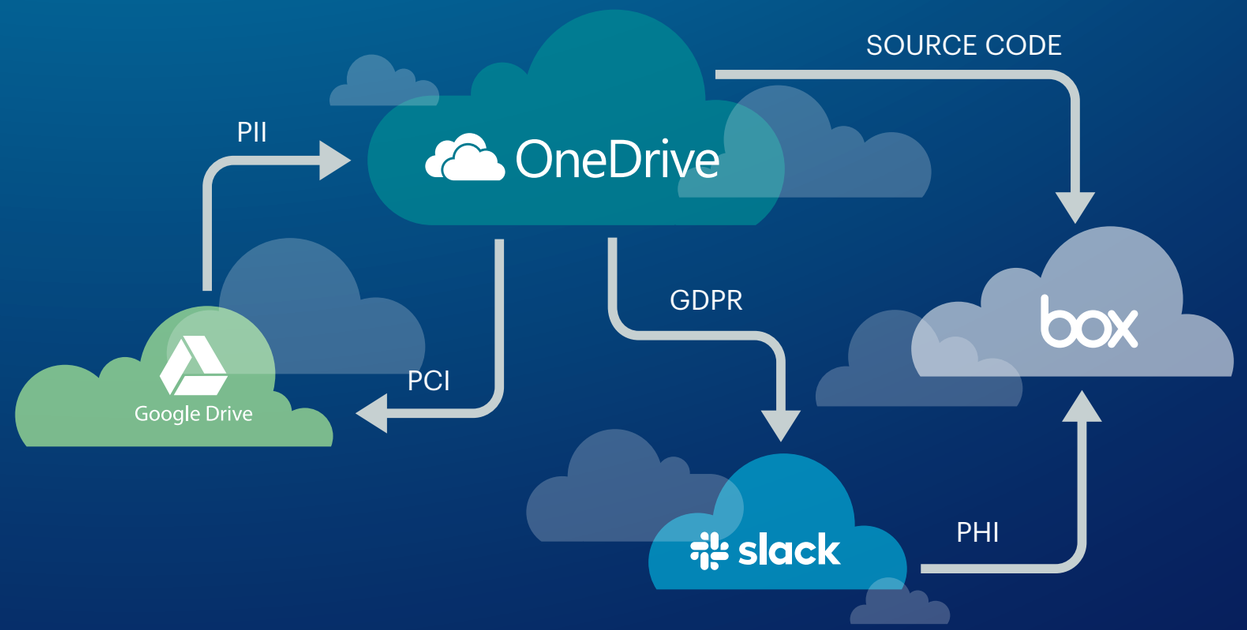
Using language that makes communication with finance and board-level teams easy, we identify the savings that transformation can enable, and look at the ways that organisations are reinvesting these newly-released funds to manage new demands upon the network and security teams.

Past: The problem with the legacy approach

As the majority of organisations 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[1], 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 sensitive

2,481
different apps and services involved

48%
of corporate data in the cloud

[1]Netskope Cloud and Threat Report, August 2020

Many organisations 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 2020 Ponemon Breach report reports the average breach cost to be $3.86M USD, encompassing costs from detection, escalation to notification, lost business, and post-breach response.

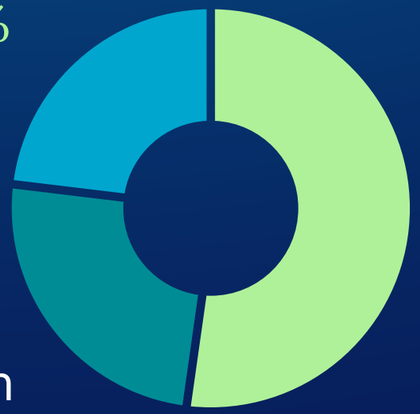
The associated breach causes were attributed to malicious cyber attacks (including phishing, cloud misconfigurations, third-party software vulnerabilities, compromised credentials, etc.) for over half, and the other half to human error and system glitches.

$3.86M

Average breach cost
IBM/Ponemon 2020

Data breach root cause breakdown

Human error
23%

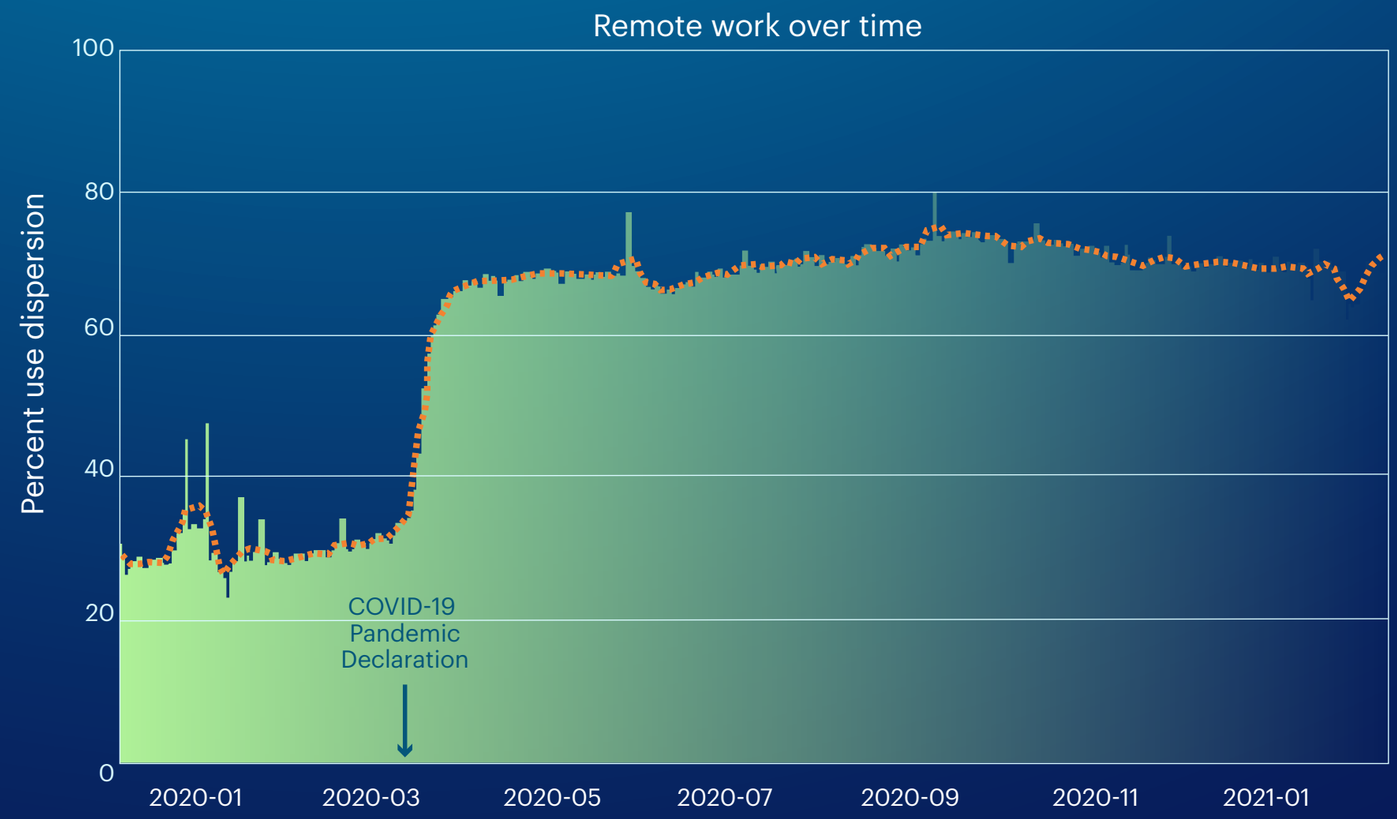


System glitch
25%

Malicious Attack
52%

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

What 2020 added to this established trend of cloud traffic 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.

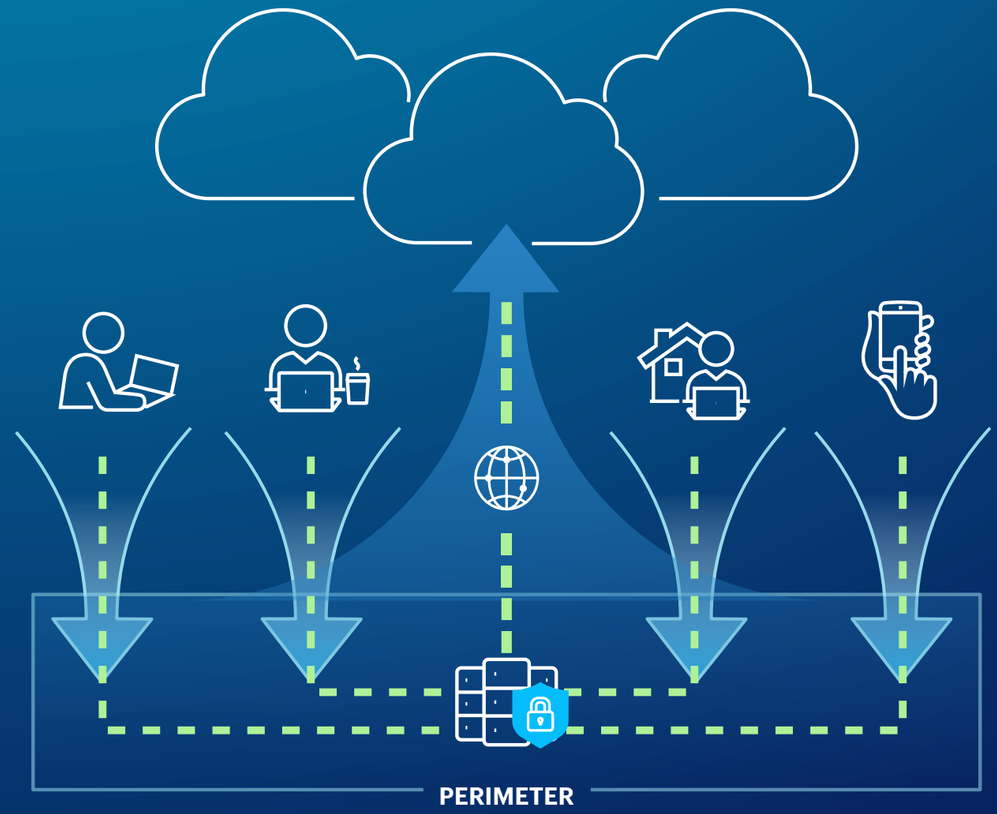


netskope

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

This was effective when the vast majority of applications resided in that data centre. 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 centre.

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 centre 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 centre.



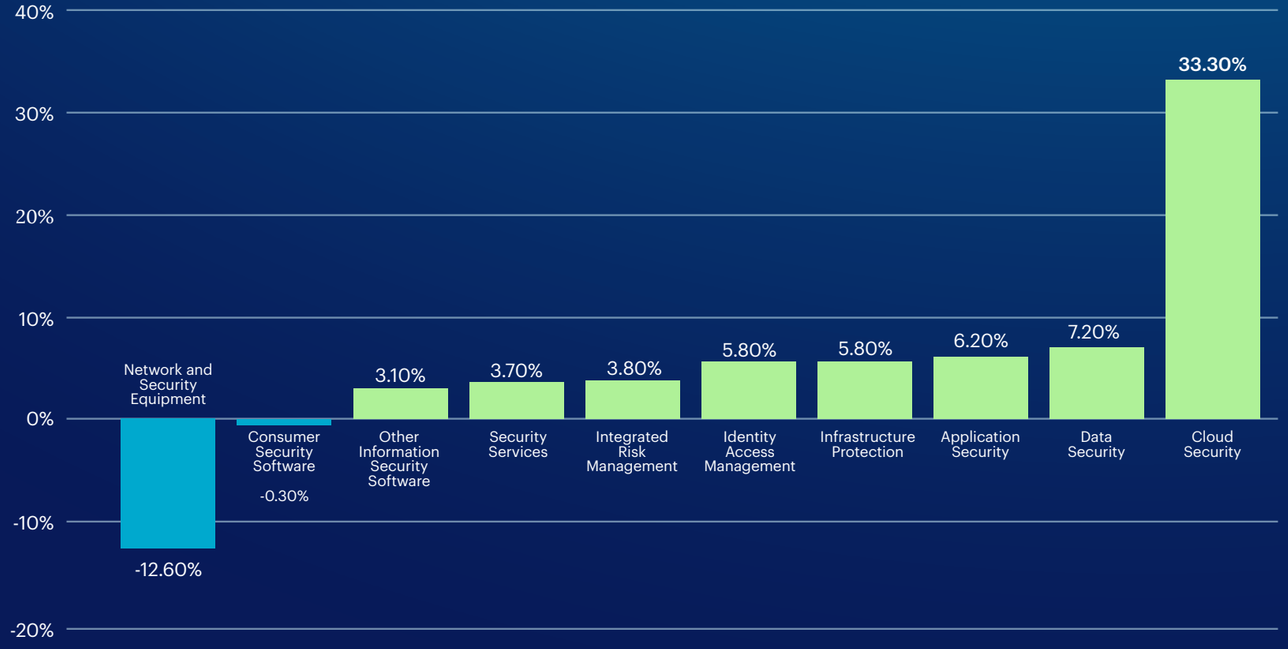
"You can continue to fund motorway expansions from three lanes to four, then five, and six, but it makes much more sense to reduce the requirement for every vehicle to travel on that stretch of road as part of every journey."

Present: Time to benefit

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 organisation has in the present. But we know that this future planning—attempting to guess functional needs and associated budgets—is rarely accurate in hindsight.

Worldwide Security Spending Growth by Segment, 2019-2020

Source: Gartner Forecasts Worldwide Security and Risk Managment Spending Growth to Slow but Remain Positive in 2020, June 17, 2020



According to Gartner, spending on Cloud Security, which is the fastest-growing cybersecurity market, was predicted to increase by 33% in 2020. Network security equipment on the other hand, including firewall and intrusion detection and prevention systems (IDPS), were impacted with a decrease in spend at -12.60%.

Sudden growth

At its most basic level, security budgets are often linked to employee numbers and securing an employee is an expense typically assessed for each budgetary year. Accuracy in predicting employee growth, organically and/or via mergers and acquisitions (M&A) is difficult and causes overprovisioning or tactical add-on expenses.

If an organisation has 20,000 employees, it's obvious that securing their IT is going to be more expensive and require more resources than securing 2,000 employees. However, we run into serious issues when attempting to accurately predict what employee count will be in 3-5 years. 2020 has shown us just how unexpected market conditions can be, but even in less tumultuous times events such as M&A can be a change agent that will shake up any IT and security strategy (and associated budgetary plans).

Predicting M&A IT onboarding costs usually involves new hardware or replacement hardware to scale to the organisation's new requirements. These capacity planning challenges often take months to plan, budget and apply, and will typically slow an organisation down at a critical time. Cloud infrastructure and services can be used to scale easily and quickly in these scenarios.

Adding another 5,000 employees to a NextGen Secure Web Gateway (NG-SWG) via the Netskope Security Cloud is as simple as updating the license. No new hardware, no shipping hardware to new locations, no racking and stacking, and procuring cabinet space and no complex capacity planning required. This flexibility and agility is an important cost advantage.

Of course in 2020 we saw sudden growth happen at a greater scale and speed than even the biggest M&A scenarios. With remote worker numbers expanding literally overnight, organisations found themselves desperately trying to acquire new appliances (from emergency budget pots as the expense could never have been foreseen). These efforts were thwarted due to supply chain issues—with appliance manufacturers literally unable to build and distribute the technology at any speed as the world locked down. And had supply chain issues not been an issue, basic market forces would have seen prices sky rocket, causing further cost pressures.

The economic advantages of OPEX, cloud approach is reduced costs from hardware overprovisioning, scalability on demand and deployment agility without supply chain constraints

Unexpected shrinkage

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.

As mentioned earlier, many organisations 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.

The key takeaway from this paper is to understand the changing economics of network and security programmes.

The following is a simple TCO example of traditional spend 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**
- **Labour Costs**

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

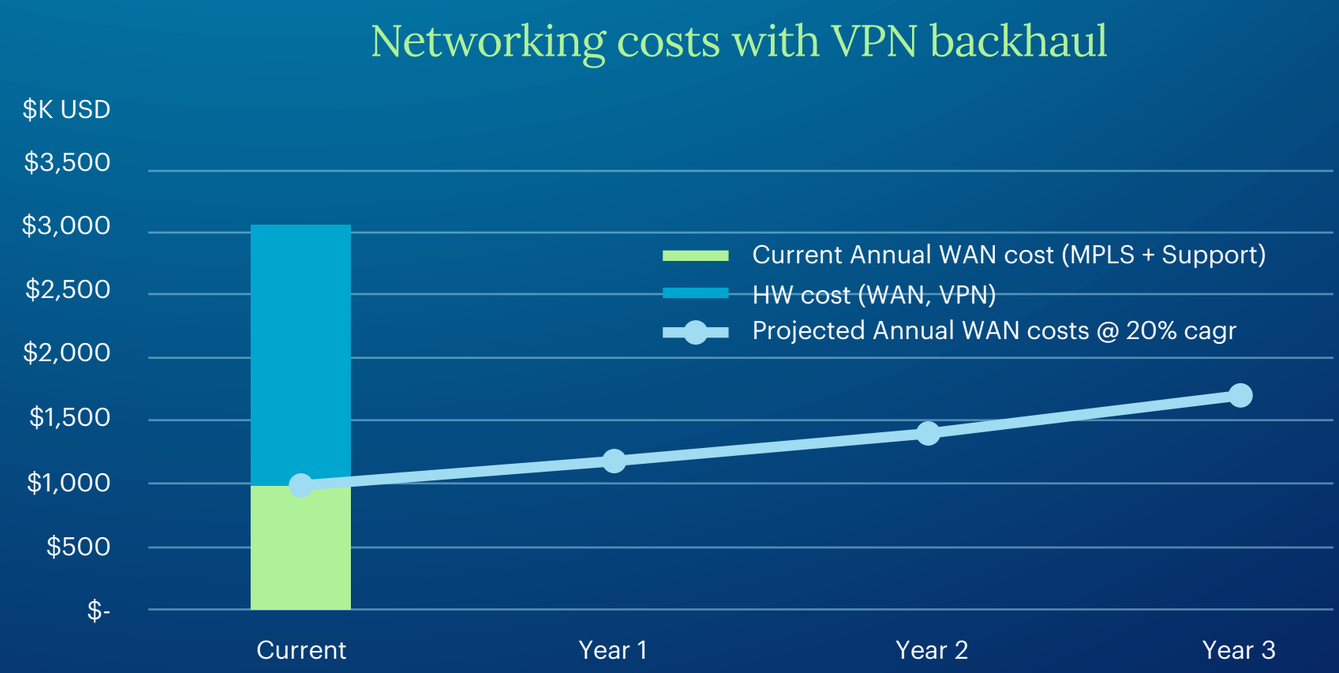
Category	Quantity	Cost per Appliance/License	Cost per Month	Branches	Year 1	Year 2 (+3%)	Year 3 (+3%)	Total Cost
Networking/Bandwidth Costs								
MPLS			$825	65	$643,500	$662,805	$682,689	$1,988.994
SDWAN Subscription	10	$5,000			$50,000	$51,500	$53,045	$154,545
ExpressRoute (1 Gbps - Metered)			$1,250	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**

These costs will only continue to increase as the traffic profile of the organisation 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 labour costs. The following two examples break out clear costs savings for network and security transformations.

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.



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)

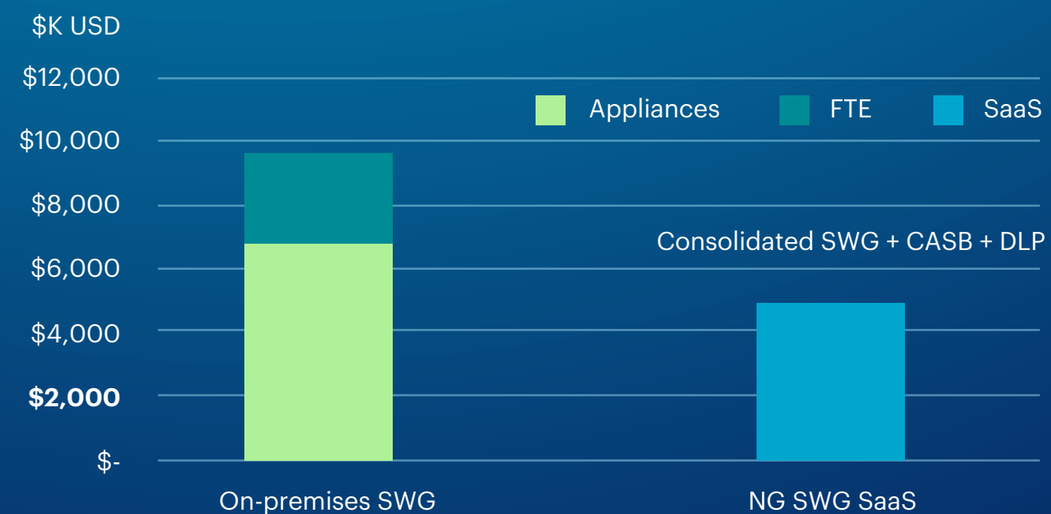
Example #2

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. This example shows more than $9M in cost savings over three years across the Secure Web Gateway appliance and resource expense. In this case over 100 SWG appliances were involved, and the cost advantages of consolidating SWG, CASB, and DLP to a single cloud service is clear.

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 organisations have.

3 Year Cost Advantage:

On-prem SWG vs NG SWG SaaS



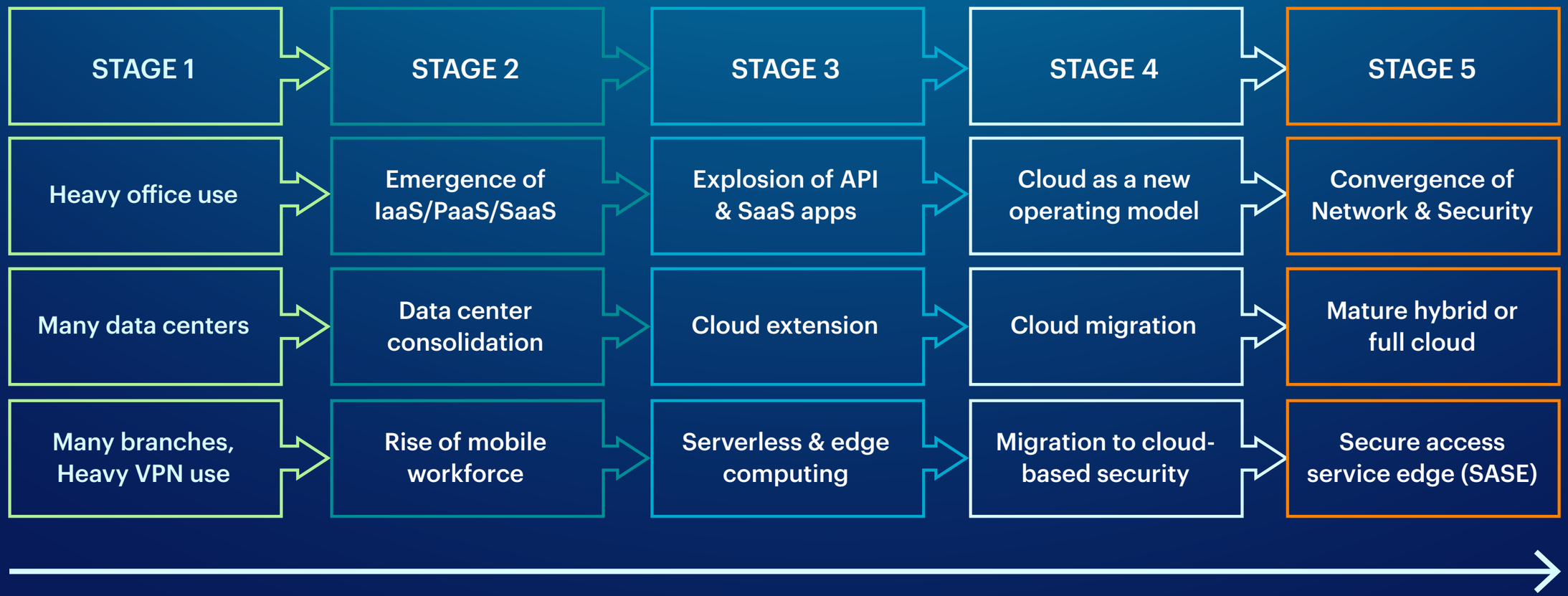
Not included: TLS/SSL decrypt appliances, DLP appliances

The security transformation may start with replacing branch location hardware and moving to the corporate data centre.

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.

Security and network consolidation

Organizations Maturity Level



The average organisation 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.

A staple for most organisations' future architecture is the focus on the following, ideally on as few platforms as possible, with API integrations and a fast and performant global network to provide access to business applications and infrastructure.

Identity & Zero Trust Network Access (IAM & ZTNA)

Web & Cloud Security Cloud/Gateway (SWG & CASB)

Data Protection (Data Classification & DLP)

Threat Protection (Anti-Malware, Sandboxing, Browser Isolation)

Endpoint Protection (NG-AV, EDR)

Automation & Orchestration (SIEM & SOAR)

As we assess cost reduction and this new model, we must continue to ensure we see value, benefit, and overall risk reduction to our organisations whilst providing the best connectivity and flexibility to our workforce. After all, a security budget should always be appropriate to the risk appetite of the organisation.

Many organisations are now realising the implications of not transforming their network to best serve their changing IT infrastructure.

For More Information

Netskope can help you achieve successful economic outcomes with your network and security transformations to the cloud. For more details, please contact your local Netskope sales representative or channel partner or refer to the following web pages:

Secure Access Service Edge:
https://resources.netskope.com/cloud-reports/adoption-guide-for-sase

Securing Remote Workers:
https://www.netskope.com/solutions/securing-remote-workers

Netskope NewEdge:
https://www.netskope.com/platform/newedge

Move Beyond VPNs:
https://www.netskope.com/solutions/virtual-private-networks

Netskope, a global cybersecurity leader, is redefining cloud, data, and network security to help organizations apply Zero Trust principles to protect data. The Netskope Intelligent Security Service Edge (SSE) platform is fast, easy to use, and secures people, devices, and data anywhere they go. Netskope helps customers reduce risk, accelerate performance, and get unrivaled visibility into any cloud, web, and private application activity. Thousands of customers, including more than 25 of the Fortune 100, trust Netskope to address evolving threats, new risks, technology shifts, organizational and network changes, and new regulatory requirements.

Learn how Netskope helps customers be ready for anything, visit netskope.com.