Deloitte.

netskope

Deloitte in association with Netskope presents:

Cybersecurity in the Cloud-First Era – The Economics of Secure Access Service Edge (SASE) and Zero Trust

January 21, 2025

Key takeaway for this paper: Understand how economic changes and technology transformations in the post-pandemic world affect enterprise network and security program opportunities

MAKING AN IMPACT THAT MATTERS since 1845

Executive summary

When COVID-19 forced a sudden and dramatic shift to an anytime, anywhere workforce, network and cybersecurity leaders reacted with unprecedented speed to maintain their organizations' productivity. Typically, that meant a rapid scaling-up of existing security systems, built on long-established network architectures.

Now that workforces have stabilized to a large degree into new hybrid or fully remote models, those systems and architectures are showing their age. Legacy network and cybersecurity approaches have been shown to cost more, are less secure, and result in lower levels of productivity compared to newer insights based on SASE network architecture and Zero Trust security principles.

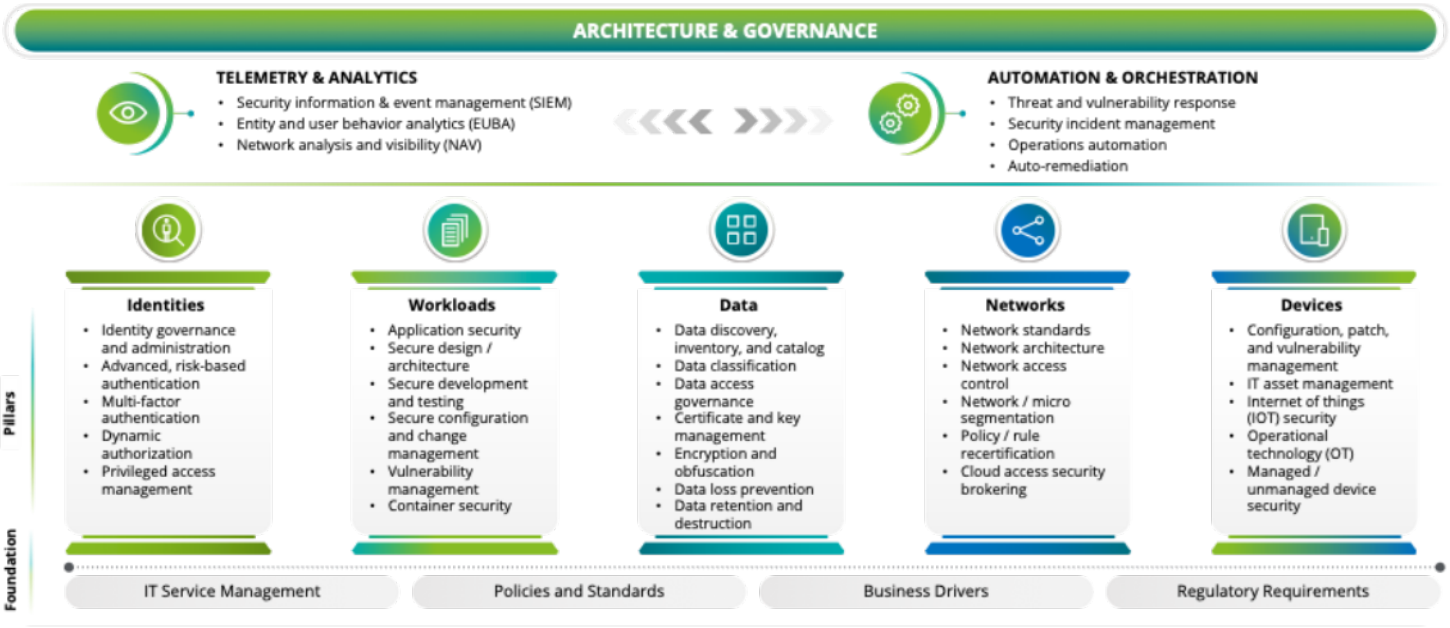
Specifically, legacy hub-and-spoke network architecture requires traffic to be routed from a user–wherever they may be–to the organization's headquarters or data center where security controls are implemented, rather than routing directly to cloud services or applications. The resulting poor user experience can affect productivity levels.

Meanwhile, traditional castle-and-moat cybersecurity designs, which focus on a secured network perimeter with implicit trust for anyone and anything on the inside, fail to properly protect users, data, and applications. This all-or-nothing approach has been superseded by dynamic security that continually evaluates the security level of users, actions, devices, applications and more, to determine which resources can be made available within the given context.

Ironically, Virtual Private Network (VPN) equipment–purpose-built to provide secure remote access–can now present a threat vector itself. For example, The Cybersecurity & Infrastructure Security Agency (CISA) Emergency Directive 24-01, called for the immediate disconnection of Ivanti VPN products because they had been compromised, underscoring the vulnerabilities of legacy VPN technology.

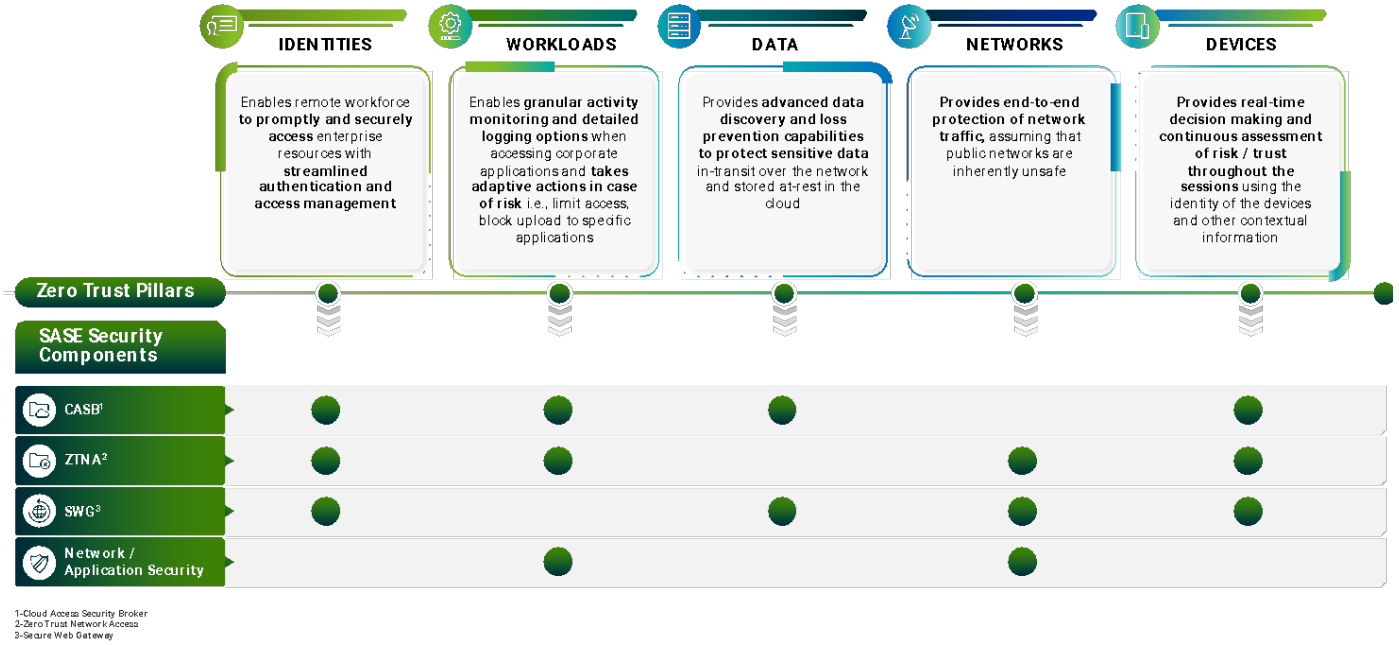
Organizations should consider newer technologies and methods to secure their cloud-first network environment and effectively serve a distributed workforce. A very effective way to achieve these objectives: adopt SASE built around core Zero Trust principles.

This new approach was captured by Sanjay Beri, CEO, and co-founder of Netskope, when he said; "In a world where data moves throughout cloud, SaaS, web, and private applications, and employees no longer spend all their time in corporate offices, SASE enables a Zero Trust approach to security. It provides access and security for data wherever it may reside or move, and however it may need to be accessed, all while optimizing network performance."



Many enterprises and vendors are now in the process of adopting Zero Trust principles as a framework for modern security. Zero Trust is a security strategy that rejects the concept of trust (of devices, identities, or networks) and requires contextual insights before granting access or activity rights to an organization's network or data. Deloitte's Zero Trust model is built upon strong foundational capabilities across five fundamental pillars: identities, workloads, data, networks, and devices.

Projects designed to support a Zero Trust approach are being pushed up the priority list. This is a positive trend. SASE is often seen as an enabler to Zero Trust, with several of its pillars enforced by various components of the SASE stack.



Since spend requires detailed justification, organizational enthusiasm is likely to waver when confronted by requests for the initial funding that any move from legacy technology requires. That funding covers various aspects of removing and replacing legacy systems, such as SASE license fees, and training and hiring to support the new system. Despite these costs, the significant potential cost savings to be gained from consolidating technology, as well as value obtained through more efficient operational processes as organizations move to a centralized SASE platform, make the move economically advisable.

Earlier rounds of digital transformation–mostly focused on moving from legacy hub-spoke to cloud-first networks–are now bearing fruit in the form of economic efficiencies and new service innovation and cost reduction opportunities. These later stage transformation projects are no different: new approaches to network structure and security are essential to save money and enable Zero Trust initiatives to self-fund and move forward.

Security has normally been part of the transformation to cloud-first networks. But organizations are now shining more of a spotlight on the way security solutions and processes are designed, applied, and managed. The threat landscape continues to change rapidly, putting organizations at risk of costly data breaches. Shifting to a new security approach should be well thought out, but also be done rapidly if organizations are to stay ahead of the curve and take a proactive approach to security.

It is important to set Key Performance Indicators (KPIs) and to measure and track results against anticipated benefits, expressed in terms of monetized value for increased productivity, reduced Full Time Equivalent (FTE) time, and reduced risk.

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*

Moving network and security functions to the cloud: economic drivers

In this paper, we look at the economic advantages and implications of network and security transformation–with a heavy emphasis on security.

Using language that makes communication with finance and board-level executives simpler, this paper identifies the savings that digital transformation can enable and examines the ways organizations are reinvesting these funds to manage new demands that are falling upon the network and security teams.

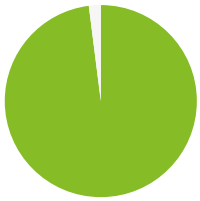
Drivers: network and security functions in the cloud

- ***Reduced costs*** *using 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 integration*
- ***Speed to deployment*** *and the avoidance of physical supply issues (agility)*
- ***Breach risk reduction*** *with security services on demand where needed*

Cloud-first security risks

Sustaining corporate-owned and managed infrastructure has been observed as inefficient, and today organizations worldwide take a cloud-centric approach for granted. Expensive dedicated Multi-Protocol Label Switching (MPLS) circuits and specialized routers are giving way to more flexible and affordable SD-WAN connectivity, and appliance-based VPNs that require periodic hardware replacement and ongoing maintenance are falling out of favor, replaced by SASE architectures. But the move to cloud apps, and the movement of private apps to public cloud specifically, leave on-premises security solutions behind.

Each month, the average employee interacts with 20 different cloud apps, and well over half (67%) upload data to those cloud apps.[1] In fact, 60% of corporate data is now stored in the cloud[2], yet many security solutions have minimal or no visibility and control over cloud apps and services. In practice, this means organizations cannot effectively enforce data protection policies - or manage threats - for cloud apps. This creates a strong potential for a data loss incident such as a compliance breach or the exfiltration of sensitive and competitive corporate data.



98% of corporations store at least some data in the cloud[3]

60% of corporate data is in cloud storage[4]

48% of cloud-stored data is sensitive[5]

Cyber professionals are on alert following a spate of high-profile data loss incidents. It is now abundantly clear: data migration to cloud environments creates vulnerabilities that can be expensive. But the benefits of cloud migration create a pull too strong to resist, even in the face of significant risk.

Security breaches have immediate and long-term consequences, affecting both the bottom line and brand reputation. Potential losses include the price of detection, escalation, notification, lost business, and post-breach response. According to IBM and the Ponemon Institute, in 2023 an average data breach cost the affected organization $4.45 million, up 15% from three years previously[6].

IBM and Ponemon Institute also reported in 2023 that 16% of data breaches trace back to phishing, making this the most prevalent attack vector[7]. It is also the most expensive, costing the organization on average $4.76 million[8].

Notably, IBM and Ponemon Institute emphasized that only a third of companies discover a data breach through their own security teams; 67% are reported by a benign third party or the attackers themselves.[9] And, when attackers disclose a breach, it costs nearly $1 million more for the affected company compared with internal detection[10]. Without the required visibility and control over cloud applications, it can be hard for an organization to identify when they have suffered a data loss incident. Hearing about an incident first from the threat actor's public claims is a worst-case–but unfortunately common–scenario.

Cloud-native SASE solutions built on Zero Trust principles are designed specifically to enable visibility and control across the modern IT infrastructure.

Impact of remote and hybrid work: network structure and security

Changes to the location of data are only one reason legacy security approaches now fail. Workers are also located differently: often they–and their devices–are outside the bounds of the corporate IT environment.

Ray Canzanese, Netskope Threat Labs Leaders says "Remote and hybrid work is now a permanent fixture of professional life for about 67% of the white-collar workforce and has held steady at that level for the past several years"[11]. Many 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.

The implications for security are profound.

Legacy systems using VPN technologies route remote user traffic first through the organization's data center, where threat and data protection policies are applied, and then out to the cloud–instead of connecting to the cloud directly. The resulting lag time impacts worker productivity significantly, which in turn often encourages users to seek alternative, less secure, ways to get their work done.

Budgetary considerations

An ambitious, long-term vision is part-and-parcel for digital transformation projects. Futureproofing is normally a key driver. Organizations' Request for Proposal (RFP) address future needs, as far as possible, rather than taking an overly myopic view of an organization's current requirements. This is common sense, but too much focus on the long-term can cause significant budgetary overspend.

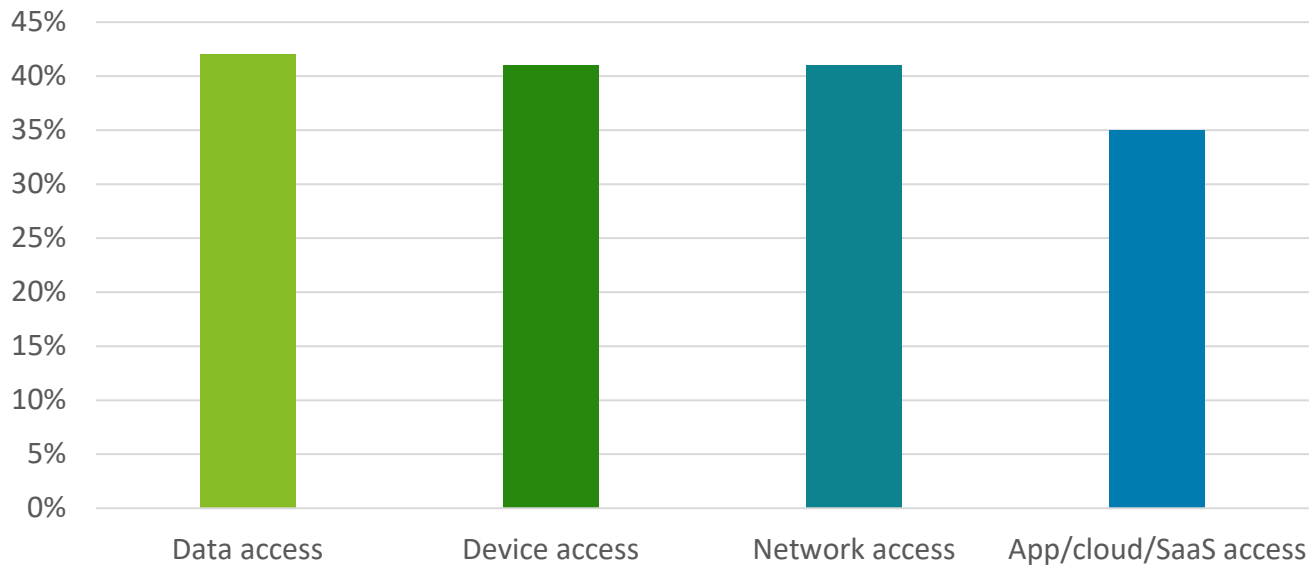
The danger comes from overinvesting in oversized appliances and excessive network bandwidth to prevent future shortages. Fortunately, the move toward cloud applications brings significant economic advantages that mitigate the risk of overspend to meet future-proofing goals: for example, adopting OpEx subscription models to replace CapEx purchases.

Similarly, security is now benefiting from its own cloud transformation and the associated economic advantages. These benefits sit alongside other positive trends: better user experience, reduced resource requirements, and more effective protection against modern threat actors.

Cloud-focused security adoption is gaining pace. Gartner predicts that, by 2027, more than 35% of new branch office firewall deployments will switch to firewall as-a-service, a significant increase from less than 10% in 2022[12].

The combined market for cloud access security brokers and cloud workload protection platforms will be worth $12.8 billion by 2027, up from $4.6 billion in 2022, Gartner further predicted[13]. Demand is also expected to increase for cloud-based detection and response solutions.

Netskope Survey: What Zero Trust projects are already underway in your organization?[14]



SASE deployment: Return on Investment (ROI) and time to benefit

Ideally, SASE should form a framework, supporting the delivery of advanced software-defined networks and security capabilities in conjunction with end-to-end orchestration.
The benefits of adopting SASE can be seen through a variety of lenses– including complexity, cost, and performance.

Complexity

A consolidated SASE approach to cybersecurity is inherently less complex. SASE enables organizations to consolidate legacy security tools such as web proxies, data loss prevention, cloud access security brokers, and even remote access VPNs into a single platform for visibility and policy enforcement. Through this consolidation, organizations minimize the need to support and manage multiple appliances, admin consoles, and client agents. They can also eliminate redundant workflows and processes and this approach helps strengthen the efficiency of the team by standardizing training on one platform rather than requiring specialization in several point solutions.

Direct cost

With simplicity, there is often efficiency to be gained in management, governance, and support processes. Process and workflow efficiencies can potentially result in a reduction of operational overhead and the total number of FTEs required to operate the infrastructure.

In addition, SASE platforms combine the functionality of multiple legacy appliances, reducing the costs of management and replacement.

Performance

An effective SASE deployment scales with business requirements and user demands, delivering a performance boost through cloud-based edge computing. It should also be designed, implemented, and managed in a way that accounts for low-latency apps, and speeds up inspection and decision-making. SASE performance benefits–from both computing and human experience perspectives–fundamentally depend on the system being able to monitor activity, detect risk, and take appropriate action based on enhanced telemetry and network traffic analytics.

SASE deployment considerations

SASE is now accepted as the future of managing and securing network services for distributed workforces in the cloud era. While some fundamental aspects of planning and deploying SASE are universal, the journey toward this new model will not be the same for every enterprise. How an organization defines, plans, and deploys SASE depends on several factors including size, business model and industry or vertical.

Let us test how these factors impact a SASE deployment.

Objectives and requirements

Organizations should consider beginning by identifying specific goals and outcomes they expect from this transformation. To do so, it is imperative to assess the current environment including both network and security infrastructure. Identifying areas for improvement and current gaps can assist in setting strategic objectives and requirements when choosing a SASE vendor. Starting with these strategic objectives–such as better network performance, improved security posture, or increased data visibility, --enables organizations to effectively prioritize use cases. It is also important at this point to determine how you measure the achievements of this transformation; clearly establishing which KPIs to track and how they will be interpreted is essential.

Broad view: network and security concerns

A SASE transformation is equally an organizational transformation, and a comprehensive approach determines many parts of an organization have ownership over the objectives and results. When you look at the core technologies that SASE encompasses, you can see the need for a number of different personas to be involved to be effective. Typically, it is easy to think of the network and security teams as the primary stakeholders for a SASE project, but ownership can include cloud infrastructure teams, application owners, operations, and support teams as well. Giving these personas a seat at the table helps your organization develop and design an architecture that not only addresses the issues of today but one that can scale and adapt to the business of tomorrow.

Zero Trust principles to simplify security architecture.

Traditional security architecture depended on the idea that everything inside the network is trusted by default. But the meaning of network blurs and evolves as organizations move to the cloud. Data security methodologies should consider evolve as well.

Essential Zero Trust principles

- Implicit trust is eliminated; the focus shifts from the network to the end user and the context in which they are acting.
- To reduce the risk of data leakage, every access attempt is authenticated and authorized.
- As the user's security risk changes, so do the requirements for access.
- Granular control policies allow organizations to dictate access based on contextual data available: user identity, device posture, location, time of day, etc.

With these Zero Trust principles in place, organizations can focus on simplifying their security architecture. Activities related to this might include replacing and/or consolidating solutions with overlapping features.

For example, in a typical enterprise network security stack, you may find a firewall, web proxy, and a cloud access security broker (CASB). Management, support, and maintenance of these appliances typically varies between network and security teams. By moving to a SASE architecture these three individual appliances are now replaced with a single cloud-based tenant with the ability to enforce granular policies based on various Zero Trust attributes such as user identity, device posture, location, source/destination, and data. Role-based Access Control for administrators enables co-ownership of this singular tenant, so both security and network teams can manage their appropriate functions. This reduces complexity in the overall architecture as well as the number of places policy changes need to occur.

Another consolidation example: simplifying and reducing the resources needed to ensure data is safely accessed and moved. Traditional VPNs are set up to control users' network access. By moving to ZTNA, organizations reduce and/or eliminate the need for VPNs in favor of contextually aware access control policies enforced on a per-user/device basis at the edge where apps are installed and used.

As noted earlier, how these benefits play out depends on the nature of the organization.

SASE built on Zero Trust: organizational considerations

A Financial Services organization is likely to be most challenged by regulatory compliance and integration with legacy applications.

Legacy applications such as core banking, trading, or other financial applications can be a challenge due to a lack of documentation or up-to-date inventory. Integrating these applications to a SASE architecture requires careful consideration as most applications have specific requirements when in a proxy-based architecture such as SASE. These organizations should start their SASE journey with a focus on an internal assessment of their application environment; understanding how users authenticate and interact with the application or in the case of B2B apps, how the app interacts with other assets on the internet. This information determines the approach to how and when it makes sense for an application to be onboarded to the SASE architecture as well what access control policies are built around them.

Life Sciences and Healthcare organizations, like Financial Services organizations, are likely to be challenged by regulatory compliance and legacy application integrations. However, patient privacy and quality care drive a very high standard for these organizations that implores a thoughtful approach to any transformation initiative. A SASE architecture that provides cost savings, through operational efficiencies and vendor consolidation, is compelling. A well-thought SASE approach that also provides strong data protection capabilities is paramount to protect patient data and privacy, as well as intellectual property in the case of many Life Sciences organizations. In addition, integration with IoT (Internet of Things) or more specifically IoMT (Internet of Medical Things) should be considered.

Managed services for SASE

Regardless of their exact path toward SASE deployment, many organizations are including a managed service package in their plans–and view this as a crucial aspect of achieving short-term and long-term ROI.

In a 2023 Deloitte survey[15], over half (59%) of cyber decision-makers said they are likely or extremely likely to purchase a managed SASE service within the next three years. On average, these buyers said they plan to spend about $1.1 million on external managed SASE services in the next three years, and about $1.9 million in the next five years. The complexity of managing security in a cloud environment and lack of in-house expertise are among the reasons for choosing this option.

When choosing a partner to outsource management of a SASE platform, organizations may add to their list of benefits things like assistance in meeting regulatory compliance and cost efficiencies achieved through lower Total Cost of Ownership (TCO). These are important enhancements on top of essential factors such as: resources to design, implement, and manage SASE; secure connectivity for a distributed workforce and hybrid assets; and verified features and processes to meet end-user experience expectations.

Regardless of whether an organization chooses to manage SASE in-house or to invest in a managed SASE service, pre-defined measures of achievements and ROI should include reducing complexity, cutting costs, and meeting the organization's specific business needs and objectives.

Immediate transformation savings

Today, appliances still take up the lion's share of most security budgets. They are a frequently recurring CapEx line-item and take a big bite out of OpEx with their requirement for ongoing maintenance.

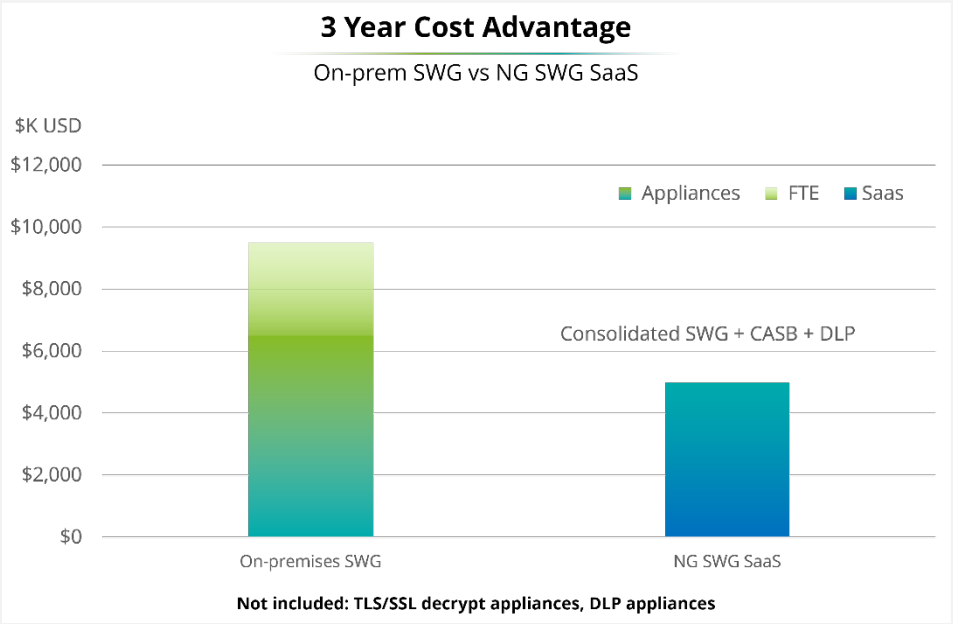
The economics of security appliances are analogous to buying a new car outright every three years and depreciating the full cost over that time with no residual value remaining.

For security appliances, however, the majority are securely destroyed and recycled after that period, no matter how well maintained they are. This is financially unsound and fails to support a happy and fulfilled security team since they lose evenings and weekends to this ongoing maintenance requirement. The constant production, shipping, and recycling of appliances is also not supportive of corporate social responsibility goals, which are increasingly important (and required) to do business.

An organization that shifts to consolidated security cloud services reaps an immediate benefit: eliminating the cost of appliances from their budget.

The security transformation may start with replacing branch location hardware first, and then moving on to the corporate data center.

In whatever order an organization chooses to migrate toward this new model, they stand to benefit from increased agility, a strong security posture, and effective risk-management controls for a multi-cloud infrastructure stack.



The example here 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, Cloud Access Security Broker (CASB), and Data Loss Prevention (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 organizations have.

The organization here stands to benefit from an operational perspective as well. SASE has long been looked at as the intersection of networking and security and this should be no different from an operational overhead perspective.

As shown below, by consolidating and moving to a SaaS based solution, FTE costs have reduced as employees no longer have to manage or update multiple tools. Time is used supporting individual tools; each with their own governance, support, and operational workflows. This simplification of processes and workflows can potentially lead to further efficiencies gained in managing, operating, and supporting the SASE environment.

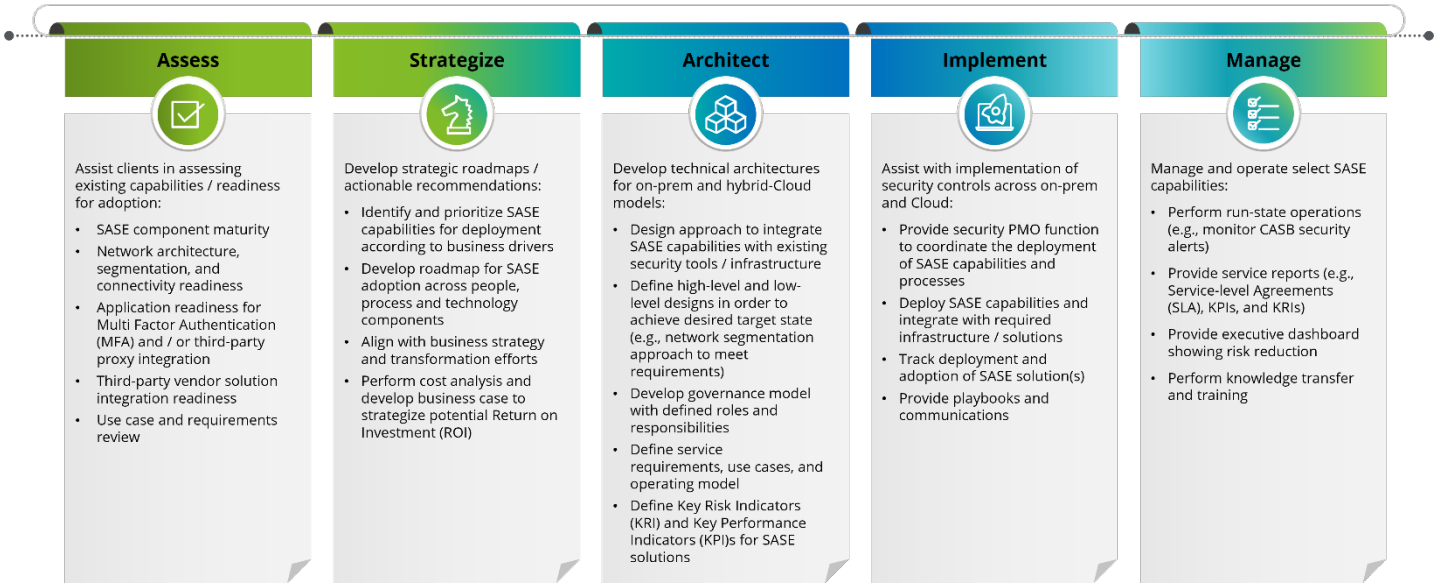
Embracing secure network transformation

Deloitte, a leading provider of cloud security professional services and Netskope, a leading SASE vendor focused on data and threat protection, have aligned to help enterprise, municipal, and federal organizations to better secure remote workers, protect critical workloads from internal and external threats, and enable the securing of Zero Trust-based architectures and initiatives.

Together, we help organizations safely embrace digital transformation initiatives, through the delivery of data protection and threat prevention technologies and services that combine Netskope's leading cloud-native Secure Access Service Edge platform with Deloitte's award-winning Cyber & Strategic Risk services. Through its experience and data-centric, systematic approach, Deloitte can help organizations efficiently manage the onboarding and transformation of cloud security programs to leverage Netskope's cloud-native security and networking technologies.

Deloitte's Managed SASE service includes leading cyber capabilities to capitalize on the outcome-focused, full potential of SASE, while reducing operational overhead and simplifying adoption. The service delivers tailored benefits to help meet organizations specific business needs and objectives.

A full range of Deloitte's SASE services can be seen below:



For more information

For more information, go to https://www2.deloitte.com/us/en/pages/consulting/solutions/netskope-alliance.html

---

Sources

1. Netskope Threat Labs, Cloud and Threat Report 2024, October 7th, 2024

2, 3, 4, 5. Thales, 2022 Thales Data Threat Report, February 28th, 2022

6, 7, 8, 9, 10. IBM Security (conducted by Ponemon Institute), Cost of a Data Breach Report 2023, June 21st, 2024

11. Ray Canzanese, How Has Remote Work Changed After 1 Year of the Covid-19 Pandemic, Mach 11th, 2021

12, 13. Gartner, Forecast Analysis: Information Security and Risk Management, Worldwide, February 29th, 2024

14. Netskope, CISOs Growing More Comfortable With Risk, But Better C-Suite Alignment Needed, June 2024

15. Deloitte, Deloitte Survey on Managed SASE, May 2023

16. Netskope, 3-year cost advantage: on-premises vs. SaaS, September 10th, 2024
