netskope

WHITE PAPER

SASE and the Seven Forces Shaping Security Transformation

JAMES CHRISTIANSEN
CSO VP, Cloud Security Transformation

NEIL THACKER
CISSP, CIPP/E, CEH, & CISO EMEA

EXECUTIVE SUMMARY

The CISO position is more difficult than ever during these times of rapid change in our society, technology, and business objectives. The need to quickly adjust your security program requires a system that is agile and able to change at the speed of the business. Successful CISO's have learned how to stay in tune with the business and continuously show value.

At Netskope we have had the opportunity to talk with CISO's worldwide and found there is a commonality in the challenges they face. We see many organizations shifting their security program to support the rapidly changing business requirements. As a security practitioner for more than 25 years, I've seen major shifts but never at the pace we see today. There couldn't be a better, more exciting time to be working in security.

> **As a security practitioner for more than 25 years, I've seen major shifts but never at the pace we see today. There couldn't be a better, more exciting time to be working in security.**

This paper discusses the critical aspects of how to create a security program strategy that is risk-based, aligned with the business, and agile to enable the security program to adjust to the changing business environment. There are seven key forces that impact the security program strategy: Business Strategy, Information Technology Operations, Risk Management and Risk Reporting, Organizational Culture, Adversaries and Threats, Government and Industry Regulations, and Global Social and Economic Forces. For each of these forces, we will explore how the changing environment drives a change in your security program, with the goal of helping CISOs better monitor these forces and adapt quickly to meet business and risk management demands.

In summation, with this paper, we want to make it clear to practitioners that:

- Security is going through a significant transformation and now is the time to review your strategy
- Given the changes driven by digital transformation and remote workers, SASE represents the new architecture that every security officer should have a roadmap for deployment
- Changes in any of these seven forces have the potential to impact your security strategy, so it is key to understand them in-depth

INTRODUCTION

At the monumental intersection of digital transformation, a sweeping industry-wide focus on SASE, and the continuing effects of COVID-19 on the way workforces function, we have never experienced such a seismic shift in all facets of business over such a short period of time. Today we see the outgrowths of this transformation driving corporate culture, business processes, and technology changes at such a rapid pace, our current security strategy cannot keep up. Now is the time to reevaluate your security strategy.

Unlike past evolutions that were driven entirely by advances in technology, this change is driven by the digital transformation of businesses and the way workforces operate. The introduction of cloud has given organizations a low-cost option for implementing significant processing power. Plus, workforces now demand the ability to work from anywhere, whether it's their office, their home, the coffee shop, and even while on vacation. Today more than 90%[1] of devices sold are mobile (e.g. laptops, cell phones, tablets) and they are accessing business systems off-premises more than 50%[2] of the time.

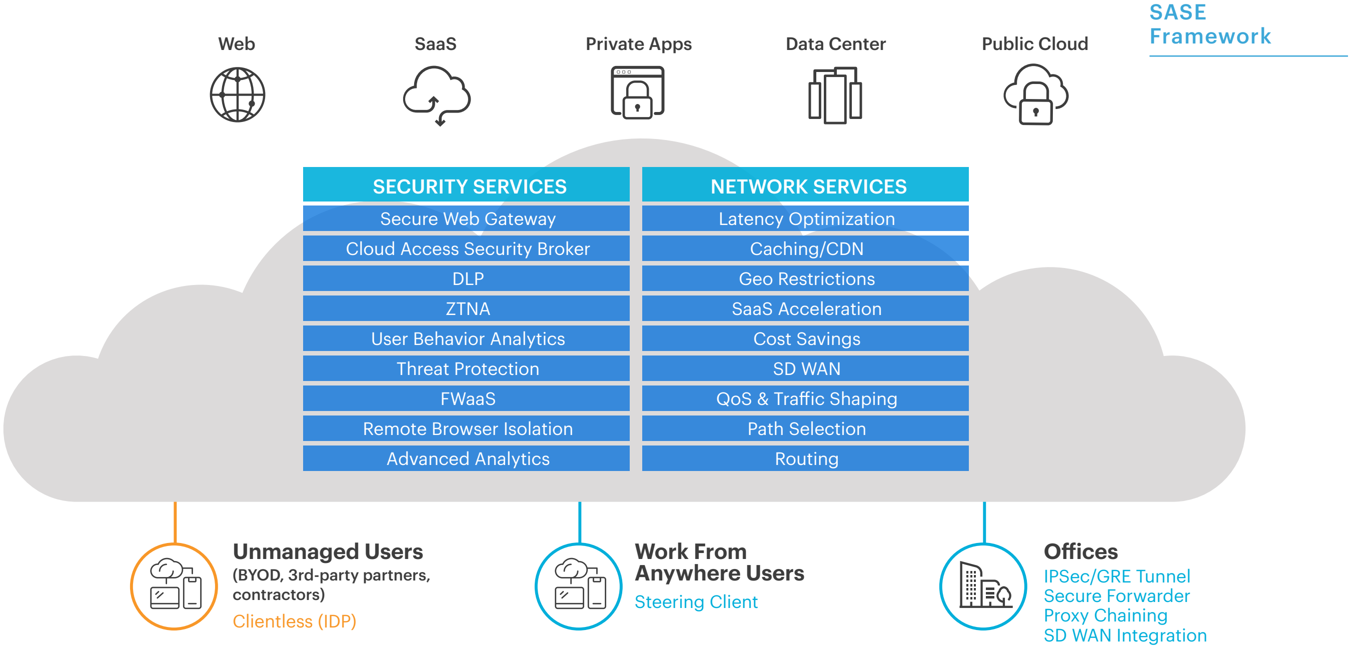
Digital transformation requires a security program tranformation.

The digitalization of business processes has also driven the use of thousands of outsourced business applications. For example, the typical enterprise has, on average, more than 1,200 SaaS applications in use, far exceeding the number of on-premises applications. This explosion in the amount of data and the number of locations it exists in has significantly increased the attack surface. Digital transformation requires a security program transformation.

The use of SaaS business applications has also drastically changed the volume and nature of network traffic. In the past, most internet traffic was accessing static information sites, but now more than 50%[3] of internet traffic related to SaaS and cloud apps contains business essential information. This shift in network traffic has resulted in a network inversion, diverting traffic away from on-premises security appliances in the data center, and direct to the cloud.

The SASE architecture provides the framework to completely rethink your network security strategy and cloud data protection.

In October of 2019, Gartner coined the term Secure Access Service Edge, or SASE, to describe this emerging security and network framework. The Gartner SASE model addresses the changing security landscape due to digital transformation, whereby users, data, and applications are increasingly outside of the traditional data center in the cloud and must be managed and secured accordingly. Necessary security services like secure web gateways (SWG), cloud access security brokers (CASB), data loss prevention (DLP), advanced threat protection (ATP) are converged in this cloud-native model and utilize a global, high-capacity, low-latency edge network for high performance. The SASE architecture provides the framework to completely rethink your network security strategy and cloud data protection.



SASE Framework

SECURITY SERVICES	NETWORK SERVICES
Secure Web Gateway	Latency Optimization
Cloud Access Security Broker	Caching/CDN
DLP	Geo Restrictions
ZTNA	SaaS Acceleration
User Behavior Analytics	Cost Savings
Threat Protection	SD WAN
FWaaS	QoS & Traffic Shaping
Remote Browser Isolation	Path Selection
Advanced Analytics	Routing

Unmanaged Users
(BYOD, 3rd-party partners, contractors)
Clientless (IDP)

Work From Anywhere Users
Steering Client

Offices
IPSec/GRE Tunnel
Secure Forwarder
Proxy Chaining
SD WAN Integration

[1, 2, 3] Source: Netskope Research

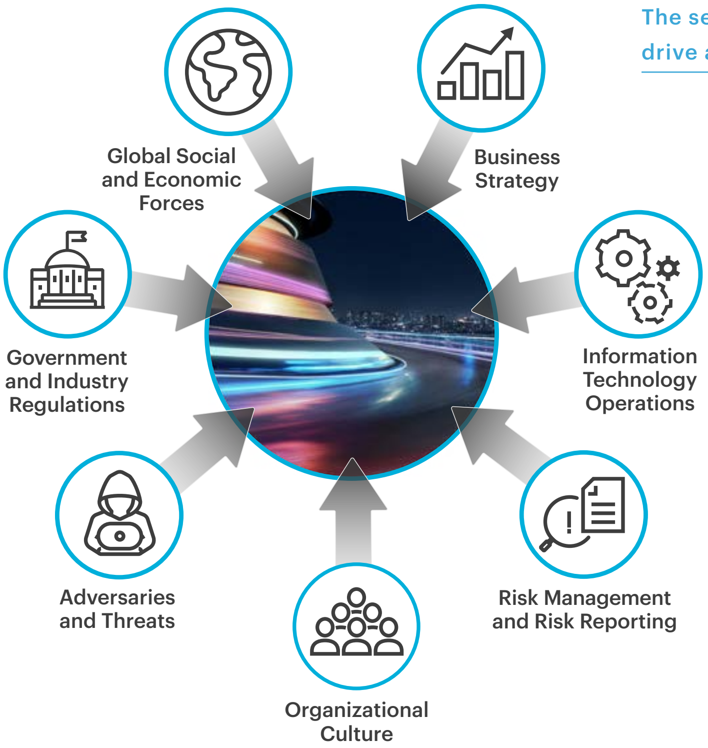
> **As a security officer, the most important reality we have to face is that data is no longer on devices you own, and it traverses across a network that you do not control, and resides on an application that you did not write.**

The worldwide response to COVID-19 also forced organizations to shift their workforces from office environments to home offices, resulting in a need to rapidly change the security strategy for remote workers. As a security officer, the most important reality we have to face is that data is no longer on devices you own, and it traverses across a network that you do not control, and resides on an application that you did not write.

All of these changes are huge, and happening at an accelerated pace. It's clear that your security strategy needs to evolve to keep up with these changes, but it may be difficult to figure out where to start. With this in mind, we will examine the following seven primary forces that drive a security strategy:

1. Business Strategy
2. Information Technology Operations
3. Risk Management and Risk Reporting
4. Organizational Culture
5. Adversaries and Threats
6. Government and Industry Regulations
7. Global Social and Economic Forces

CISOs should have a solid understanding of the seven strategic forces that impact the organization, and having an agile security strategy requires that you consider changes in each of these forces and adjust your strategy accordingly. When you look closely, you will see that the impact of your strategy transcends many of these strategic forces.


Global Social and Economic Forces
Business Strategy
Government and Industry Regulations
Information Technology Operations
Adversaries and Threats
Risk Management and Risk Reporting
Organizational Culture

The seven primary forces that drive a security strategy

Force 1: Business Strategy

Changes in business strategy are driving a major shift in how you need to think about your security strategy. As part of digital transformation, a significant amount of business processes are moving from internally developed on-premise applications to SaaS-based applications running in the cloud. This business-driven movement is having a greater impact on security strategy than ever seen before.

> ***"Is digital transformation changing the way my organization functions?"***

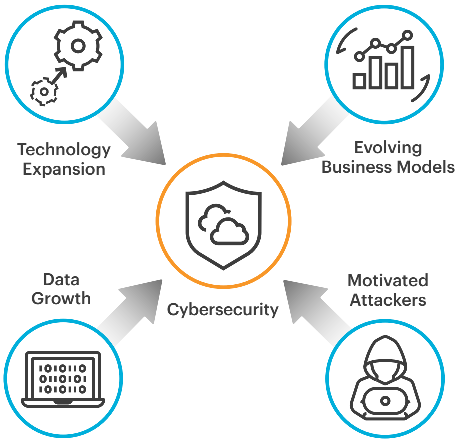
First, ask yourself, *"Is digital transformation changing the way my organization functions?"* The movement of the data from internal data centers to cloud-based applications will ultimately mean a shift in your controls and processes. With many businesses becoming digital service providers, their business now covers multiple revenue channels that require managing and securing. However, as new revenue channels are created, there is a logical increase in volumes of data the organization must store, process, and secure.

Most successful business organizations have concluded that access to timely operations information results in higher-performing companies. Data analytics have become the lifeblood of the company and access to the data needs to be available from anywhere at all times. As a result, successful CISOs need to enable the business to access the data and perform their jobs without the impediment of the individual user or application's location. Each company differs, but all successful companies are maximizing their potential by using new SaaS-based applications.

Given these major shifts in business strategy are driving changes in the way we manage and think about data, we have long held onto the principle of least privilege. It's time to re-evaluate the principle considering the changing business needs to perform analytics at a rapid pace without impediment. This is not to suggest that all data be open to the entire organization, but more that non-sensitive operational data be made available to the data scientists in the organization to allow for business operations innovation. Moving away from need-to-know, but allowing the discovery of what is useful for operational analytics.

The Perfect Storm

Along with the need for pervasive data access the volume of data has grown exponentially. In the past two years, 90% of the world data has been created[4]. This explosion of the amount of data, movement to cloud SaaS applications, and the mobilization of the workforce has created the perfect storm.



The forces driving growth and efficiency may create a broad attack surface

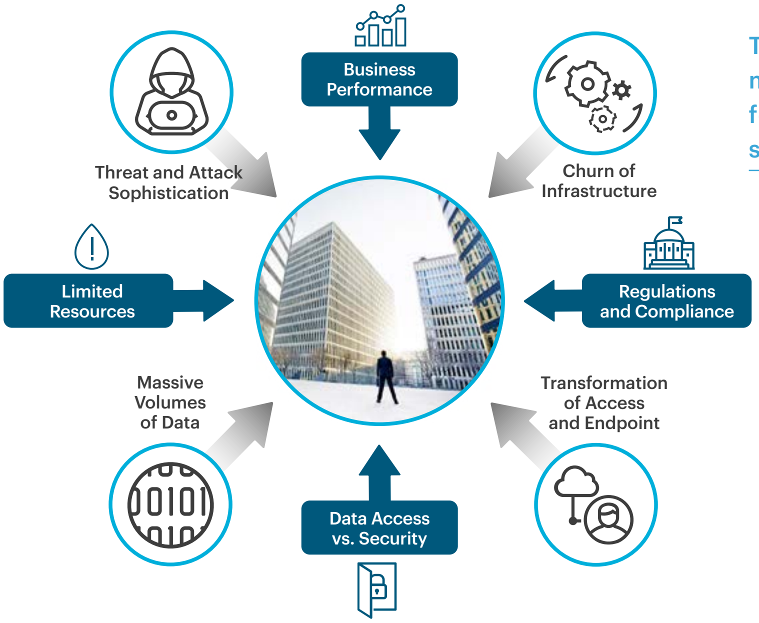
[4] Source: Forbes, *How Much Data Do We Create Every Day? The Mind-Blowing Stats Everyone Should Read,* May 28, 2018

The Challenge

There are four fundamental macro issues security teams are being forced to face:

- Threats and attacks are becoming highly sophisticated and targeted toward specific organizations
- Exponential growth of data to be classified and protected
- Fundamental churn and change of infrastructure is underway due to cloud and virtualization
- Endpoints are transforming from static corporate-owned and controlled assets to personally owned and operated devices to allow for the fast and convenient access of business information

At the same time, security teams face the pressures of business performance. More than ever the information security team is a critical component of business success. Security staff resources are limited and are costly. The balancing of data access versus keeping the data secure is more difficult than ever, and the regulatory environment continues to establish strict rules on how data can be used alongside the required security controls.



The four fundamental macro issues and four pressures facing security teams

Remote Workforce

As a real-world example of these challenges in practice, global health concerns resulting from the COVID-19 pandemic have caused a major shift in remote working strategy. In the past, most organizations had only a small percentage of staff working from home, but that has all changed now and for the foreseeable future. This massive increase in remote workers also expands the attack surface and, because of the specific threats posed by the recent proliferation of remote staff, security leaders should assess both short-term and long-term needs.

Remote working strategy should start with the endpoint. Many workers will use corporate provided devices that are equipped with the typical endpoint security capabilities. However, many remote workers are also using personal devices to perform their daily work duties. Organizations should implement an inspection process at connection time to check that the device attaching to the network has adequate security controls.

Zero Trust Network Access (ZTNA) should be implemented with robust multi-factor authentication to ensure the user is who they claim to be before connecting to the corporate network or vital applications. Services that can enable both secure access to SaaS applications and private applications hosted in the data center or IaaS provides the advantage of enabling direct-to-internet connection rather than routing all the remote worker network traffic through the data center, to the application, back to the data center and then to the end-user.

Utilization of security as a service capabilities can accelerate deployment and save the expensive cost of routing all the traffic to the data center. Instead, this involves routing user traffic through inspection prior to connecting to the application by using a cloud security platform. Cloud security platforms can inspect the traffic for data leakage concerns, threats to the user or application, and filter destination sites. Better organizations are moving away from VPNs that are often not used by end-users and provide full network access when used. Next generation VPN services have the advantage of being able to inspect the destination and then, if authorized, connect users to the specific application. This provides the user with a transparent route directly to the cloud application or to the private application hosted in the data center without providing broad network access.

Security as a Business Accelerator

Like the brakes on a car, which give a driver the ability to go at higher speeds with less risk, the best security measures allow a business to move faster, not slower. Security in today's digital reality should only introduce constraints that remove barriers to delivering data into the hands of the business decision-makers who need it most.

As data explodes, user behaviors evolve, and business models change rapidly, security can be an accelerator that allows the enterprise to fully harness data's potential. The most successful CISOs have transitioned from a "No, you can't," to a "Yes we can, and here's how" mindset. Safely allowing users access to all relevant data, all the time, empowers the enterprise to secure its most competitive asset—its data—and thus gain an edge in the race to answer the most pressing business questions.

Force 2: Information Technology Operations

Complexity is the enemy of security and we have made our security architecture too complex. Over the years we have seen a compounding effect of adding layers of security, especially at the endpoint. Unless you have done a recent cleanup you will find the endpoint has numerous client security applications, all performing similar and/or overlapping controls. It is time to take a fresh look at what is running in the environment and consolidate and simplify the architecture. Moving toward best of breed platforms that provide integrated/seamless functionality will simplify and lower operational costs.

As organizations go through this transformation they need a clear understanding of the maturity of the current IT and security operations program. Most IT teams are undertaking a major shift in their strategy moving to a "Cloud First" approach, replacing core enterprise applications with those offered as SaaS applications in the cloud. At the same time, there is also a further shift in this strategy to "Cloud Only," in which companies are moving to completely eliminate their data centers. This is driving reinvestment in people, processes, and technologies to meet the new requirements while managing both threat and data protection. While almost every area of security is impacted, some of the key areas to review include:

Authentication | **Adaptive Trust** | **Network Security** | **Visibility**

Authentication

Remote workers require a more robust authentication system. You cannot only rely on physical location or device. Multi-factor systems that are almost transparent to the end-user need to find a balance between good security and ease of use. Workers today require the ability to work from multiple devices such as their laptop, tablet, phone, and even personal computers. The digital world is built around the user and modern technology gives them lots of choices. In the past, we considered the user as the weakest link, but now the user has the most power.

For a long time, we have implemented the concepts of "least-privilege" or "need-to-know," wherein we granted users minimal access with strong protections. Similar to how we shifted our network strategy from "allow-only" to "Zero Trust networks," we need to shift the way we approach user access. The new normal will be allowed access, "user decides," and applying restrictions to data by exception, shifting the focus to enabling data use. If you do make the shift to lower restrictions on data access, it will require implementing more sophisticated behavior analytics to detect data misuse.

Adaptive Trust

More than 90% of new computers purchased are now mobile devices. Today's power users demand the ability to log in from anywhere, on any device, and access everything. To meet this new demand, companies need to adjust their authentication and authorization processes and technology.

One way to approach the problem is via an adaptive trust scheme. An adaptive trust scheme matches the level of confidence in the authentication to the level of risk of the asset being accessed or changed. An adaptive trust model looks at five core elements to determine if access is granted:

1. Authentication Level
2. Access Level
3. Application Trust
4. Device Trust
5. Asset Classification

Implementing Adaptive Trust

Using these five core elements of adaptive trust, a dynamic decision can be made in real-time as to whether access should be granted. Higher value information and access level requires more trust in the user, device, and application. Higher levels of trust are more costly and intrusive, so a better security program will find the balance between the trust level required and the action being requested. Keep in mind that Zero Trust goes beyond the user and includes the devices, applications, etc. In today's dynamic world there is not any implicit trust anywhere in the transaction.

Network Security

Secure access service edge (SASE) is the convergence of network-as-a-service and security-as-a-service and an emerging security and network framework that guides the approach in which data and applications are deployed and consumed. SASE further evolves security infrastructure to protect an increasingly perimeterless environment. The goal of the SASE model is to shift operations from managing security appliances for both cloud and web to delivering a central, policy-based service via a cloud-native microservice platform. This is where we see the emergence of a Next Generation Secure Web Gateway (NG SWG) that is cloud-native and understands the new protocol languages of both the internet and cloud.

The shift to information-rich cloud applications has moved the majority of traffic from inside the data centers to cloud-based applications, so it no longer makes sense to backhaul all the information. Without proper controls, this eliminates the security, visibility, and threat protection of a traditional data center. Zero Trust Network Access (ZTNA) is a methodology for addressing and supporting the mobile workforce. ZTNA is not a single technology or process, but a number of principles that when brought together provide the ability to match the level of authentication and device attributes (managed versus unmanaged) with the associated level of risk. The level of risk is related to the employee, the sensitivity of the information, the type of access, and the trust level of the application.

When using a SaaS application there is a higher need to understand who is using the application and for what purpose. SaaS applications typically have a great deal of functionality and the best way to handle the changes is through a cloud access security broker (CASB) with advanced threat protection and DLP. Using a CASB provides the ability to identify and protect against malware, provide visibility into the SaaS applications being used, and control how they are being used. The approach must also include blocking or allowing types of data through data loss prevention (DLP) policies and identify the risk level of an application to protect against the use of high-risk cloud applications.

Visibility

Visibility is one of the most important controls to prevent massive security breaches. If you can detect and respond immediately when an endpoint is compromised then there is no material financial impact. If the breach takes months or years to detect there are significant financial and business operations costs, possibly in the millions.

The lack of visibility is a very real problem for many organizations. Businesses are finding solutions to their most pressing needs in new SaaS-based applications. But, it's possible that the security organization doesn't even know the business is using a given SaaS app, and you can't manage the risk of something you can't see. This is especially true when SaaS solution providers rarely give you access to application logs, traditionally used to build SIEM. Unless you have forced hairpinning of all the network traffic from the managed devices through your data center, it's going directly to the cloud-based applications. If your users are going directly to O365, G Suite, or Salesforce then you are completely blind to the transaction, unless you implement a monitoring proxy. Further exacerbating the problem is that most users have more than one machine and are accessing the applications from their personal machines, tablets, or phones. Without implementing the right technologies there is another big hole in your visibility.

Given this shift in network traffic, your strategy needs to include a forward and reverse proxy capability to enable inspection of the network traffic. This is because most cloud applications have implemented SSL encryption, which leaves traditional decryption methods blind as well. The solution must look beyond just the destination URL deep into the JSON and be able to decode the cloud traffic to be context- and content-aware. Your solution also needs to be inline to be able to react in real-time and answer these sorts of questions: *Is the user accessing a corporate or personal instance of the application? Are they trying to read, write, or share the data? Is the data sensitive and does our corporate policy allow this transaction?*

SaaS solution providers are going to need pressure from the industry to provide the logs to their customers to keep the system in check and to provide the necessary oversight to meet our risk management and regulatory demands.

Force 3: Risk Management and Risk Reporting

A fundamental requirement of any business is to manage risk. Risk is pervasive across an enterprise with employees making multiple decisions a day that will impact the risk posture of the organization. These decisions require a level of diligence to be applied to identify any new risks that may be introduced or changes to existing risks that have previously been measured. These changes can include taking on a new vendor, processing a new category of data, or launching a new digital service. These factors are further subject to disruption and require an informed analysis of the additional areas of risk. Business digitalization is changing the risk management discipline as rapidly as the changes in technology.

The changing business models are forcing a change in the way organizations handle their risk management. Business digitization processes are too dynamic and evolve too quickly for traditional risk management. The ability for business units to independently subscribe to a new cloud service presents a significant risk to the overall organization. Processes to discover, monitor, and control new business cloud services need to be implemented to understand and mitigate acceptable risk. In addition, risk must be reported across the business in a decentralized manner, ensuring that risk and data owners are aware of the effectiveness of the controls and countermeasures that have been applied.

Data security and regulatory risk are further complicated by business digitalization. Understanding data flows, as required under many of the privacy regulations such as GDPR requires constant discovery of cloud services and the ability to "geofence" data so it doesn't cross international borders. A strong data protection program is required to be able to inspect the traffic, determine if it is regulated data, and then enforce restrictions to stay compliant with the laws.

In traditional corporations, you set expectations for application security through corporate policies. In the cloud service world, the expectations are set by contracts.

Cloud Service Provider Contracts

When reviewing your risk management processes you need to review the contracts with the SaaS services. Often for SaaS services, there are click through EULAs that the business unit will accept while signing up for the service without any legal or security review. Establish a policy and process requiring any cloud service that will process or store sensitive information, or where a disruption of service would have a material impact on the business, and have a legal and security review performed prior to committing to the service. There are seven key risk management elements to review in a contract: Security Safeguards, Security Service Level Agreements, Restrictions on Outsourcing, Breach Notification, Right to Audit, Cyber Insurance, and Exit Strategy.

Security Safeguards

Security Service Level Agreements

Restrictions on Outsourcing

Breach Notification

Right to Audit

Cyber Insurance

Exit Strategy

Third-party Risk

Third-party risk has been a major threat to companies for a long time but as we shift to more cloud applications hosting sensitive information and business systems the impacts could be larger. Further complicating the problem is the use of fourth-parties. Doesn't it make sense if you are outsourcing that a successful third-party would also be outsourcing parts of their operations? How do you currently understand the impact of all parties in the services supply chain?

Historically the approach of evaluating third-party risk involved understanding the data type and regulatory information, as well as the dollar amount of business impact and the maturity of a vendor's security controls. Taken together, this would determine the likelihood of a failure in their security program that would cause a financial loss, brand damage, or even damage to your organization's regulatory good standing.

While today's third-party risk management processes have seen some innovation and scale with scoring, automation, monitoring, and exchanges, it is still behind other parts of security programs. However, as you look forward, things are about to change.

Moving from Third-party Risk to Application Risk

The current process of evaluating a vendor's infrastructure security and development practices will soon be obsolete. Most companies already have more applications running on SaaS and IasS solutions than they do on-premise. And in cases where applications are still on-premise, organizations are using middleware, APIs, and other technology to connect cloud services to access the data and information.

This means we need to make a fundamental shift in how we think about third-party risk, from vendor risk to application risk. This means moving away from vendor IT risk that focuses on the core infrastructure questions, (e.g. *"Do you have written policies?"*) to asking the questions that really matter to determine the security level in the cloud application world, such as:

"Show examples of your policy being applied to application development and support"

"What are the authentication methods implemented?"

"How often has the application been penetration tested?"

"Do you have a bug-bounty program?"

Calculating Application Risk

Think about the fundamentals: the inherent risk and offsetting controls. To understand the business profile risk of the vendor, assess their financial stability and the country risk remains the same. The focus then needs to turn to the application. First understand how much risk you have associated with an application, given the sensitivity of data and criticality of the application to your business operations. The combination of the business profile risk and the sensitivity/criticality is commonly referred to as "inherent risk."

The current best-practice is to do a validated assessment of the vendor's security practices based on ISO27001/2, NIST 800-53/CSF, CSA CSM, or other similar security frameworks. Today we rely upon representations made by the third-party on their security practices and information that can be gathered from the internet about their infrastructure vulnerabilities.

In the future, when your security team shows up to perform an onsite audit, they're likely going to find the vendor is using cloud applications to develop and deploy their solutions with no infrastructure at all, and possibly not writing any application code either! That is the future of third-party risk. Moving from vendor risk to application risk and having the ability to understand how resilient the application is for availability, and how vulnerable it is to a possible disclosure. Shift your assessments to focus on the security and availability of the application, and choose a system that can provide application risk scoring. Some good standards for secure application development are Open Web Application Security Project (OWASP) or Building Security in Maturity Model (BSIMM).

Fourth-party Risk

Fourth-party risk has always been difficult to identify and, with the power of APIs, an application may be communicating with other applications to process or even store your sensitive information. Consider an application that you are using for analytics of confidential data. You contract an analytics provider that has seemingly a good system. You do your due diligence on the vendor's financial standing and country risk, given the level of the sensitivity of the data, and you fully understand your inherent risk. Next is assessing the application risk of the system you will be using, as the vendor may have many applications in their portfolio.

Once all of this is complete you feel that you understand the level of controls in place for the application and all is good. Except, unknowingly, the vendor stores all your data at a partner's location. This is fourth-party risk. This can be in the form of transferring data, doing API calls for application functionality, etc. All of this exposure to your information has gone unchecked. Hence the need to understand all applications that the system uses and the data flows outside of the system.

Continuous Monitoring

A vital part of the third-party risk program is to consistently monitor the health of the provider and the security of the applications. We are closer than ever to being able to continuously monitor controls in real-time. This is where the elusive continuous risk monitoring comes into play. There are a number of controls that can be continuously monitored for critical health as it relates to security. Establish a regular cadence of evaluating the applications based on the level of inherent risk. Consider the application security testing tools as part of your program to validate the claims of the vendor. Implement automatic alerts during times of change such as financial status, new releases, and acquisitions.

We are closer than ever to being able to continuously monitor controls in real time.

We need to think differently about how we approach third-party risk and retool our strategies and systems to better understand application risk. Of course, being a realist, nothing is 100% and there will be hybrid environments just like we see in the cloud today. But the trends are moving more to applications being built on cloud platforms and away from internally developed solutions. The time to rethink your strategy and investments is now.

Force 4: Organizational Culture

Organizational culture can have a significant impact on the security program. A shift in executive leadership or board often changes the organization's risk appetite and priority of the security program. Most boards are now requiring a minimum report to the full board and a quarterly report to the audit subcommittee of the board.

Impact of Pandemic

The most significant change we have seen in changing organizational cultures is the rise of the remote worker amid the COVID-19 pandemic. Whilst traditional organizations prefer to see people in the office and collaborate face-to-face, the goal for most employees is to be flexible in their working environment. Pandemic planning aside, most workers will choose their employer and ask questions at the interview stage on this flexibility to ensure they have the best work-life balance. In addition, the next-generation workforce will demand this level of flexibility. With concerns over health, rising house prices, the increasing cost of affordable housing near workplaces, and the costs of travel assessed against salary, most workers will need this flexibility. As organizations reimagine their strategies, understanding their mobilization of the workforce will be critical. The mentality of work from anywhere, at any time, from any device, access any application, and share any information, is supportive of this cultural change. This shift away from the traditional office is evident in most industry sectors today.

As organizations reimagine their strategies, understanding their mobilization of the workforce will be critical.

Organization’s Risk Appetite

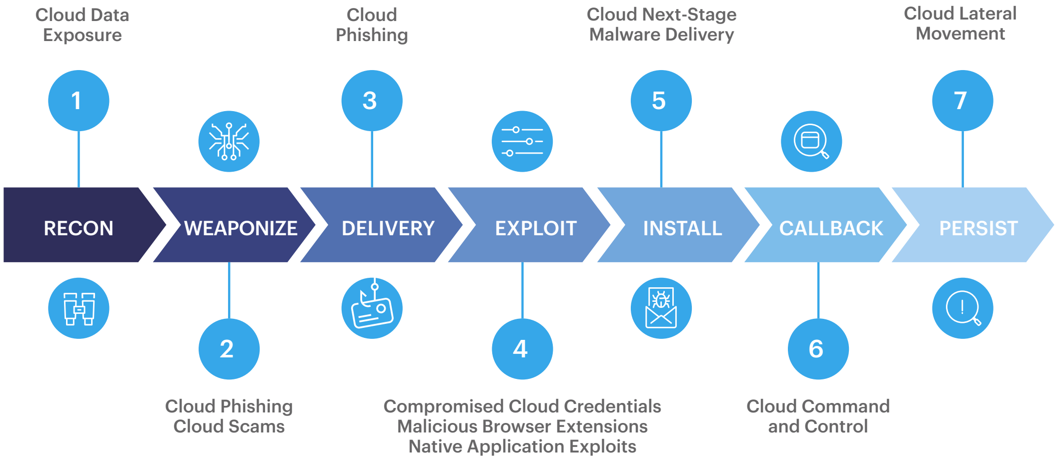
With a flexible and innovative workforce, there also comes a shift in an organization’s risk appetite. So, how is that changing? Risk management was traditionally used to block high-risk activities and maintain alignment with company and security policy. It was a simple binary approach that most employees understood. However, as organizations become more complex in the offering of their goods and services through digital transformation that involves complex supply chains, these simple approaches no longer scale. New risks need to be identified based on behavior specifically on the most critical asset an organization has: its data. As more risk management programs become data-centric, so must their measurements on the likelihood and impact of these risks. Organizations today have become more open and willing to take new risks that, when managed appropriately, can increase their revenues.

Changes in Financial Policy

Chief Financial Officers are looking closely at the savings they can realize moving away from capital investments and moving to subscription-based contracts. Investment in technology is no longer a barrier with cloud services on a pay-as-you-innovate model. However, some industries such as critical national infrastructure (CNI) may still have a risk-averse culture and a more restrictive security strategy that is appropriate. Generally, this is where today’s CISO must be able to adjust to new technologies, new controls, more open policies that allow for a more open and collaborative culture to excel.

Today’s CISO must be able to adjust to new technologies, new controls, more open policies that allow for a more open and collaborative culture to excel.

Force 5: Adversaries and Threats


Cloud Data Exposure
1
RECON
2
WEAPONIZE
Cloud Phishing Cloud Scams
Cloud Phishing
3
DELIVERY
4
EXPLOIT
Compromised Cloud Credentials
Malicious Browser Extensions
Native Application Exploits
Cloud Next-Stage Malware Delivery
5
INSTALL
6
CALLBACK
Cloud Command and Control
Cloud Lateral Movement
7
PERSIST

The threat landscape is a baseline measurement of the current threats observed by most organizations. However, the threat landscape is only accurate if we identify and measure against all threats. One example is that phishing is still talked about in every organization as one of their primary concerns. This is obvious as phishing produces a visual identifier in the form of a phishing email that can be traced to the start of an incident.

Now, let's talk about other common threats that are not always visible. Both cloud and web-based attacks, which continue to grow in numbers and according to ENISA (the European Agency for Cybersecurity), are a top-three threat, yet many organizations may not have true visibility of this threat. For many, encrypted traffic to and from the organization is not always analyzed for threats. Even worse, traffic to and from cloud applications is often overlooked. More than 50%[5] of internet traffic related to SaaS and cloud apps contains business essential information, therefore we should assume that this traffic should be analyzed for threats from not only an external threat actor perspective but also from an insider or accidental threat perspective.

As we broaden our visibility into this traffic we also must ensure we understand that data is no longer on a computer we own or control. The movement from on-premise applications to third-party developed applications provides a new threat kill chain to be considered. New models and updates to existing threat kill chains should also be acknowledged and considered for remote workers when the attack surface is multiplied. Similarly, they should also address how CISOs are required to manage and apply security controls to both remote staff and third-parties that threat actors may use to gain trusted access to the real target.

From an adversarial and threat perspective, an important strategy, control, and measurement should always be to reduce attack surface and dwell time. Dwell time can be measured as the duration a threat actor has undetected access to a network, system, application, device, etc. until access is identified and removed. Measurements for dwell time MUST extend to cloud applications and web services to further protect these environments from a confidentiality and data integrity perspective. Not identifying a threat actor with access to an organization's IaaS platform or data lake will cause a significant impact to the organization.

Insider Threat

The "insider threat" has been one of the greatest threats since the beginning of IT and over the years, the insider threat still remains dominant. Some of the biggest security breaches are due to an insider being focused on a business process and did not result in a public disclosure of regulated data. These types of breaches go vastly unreported due to the brand damage they bring to the company and, without a requirement, executive teams will often decide to not prosecute the case. Breach notification statistics recognize the number is only a small portion of the actual breaches that occur.

[5] Source: Netskope Research

Complex business systems and access requirements have enabled a different insider. One that is looking to do their job just not the way you intended. These insiders, power users, and untrained users shoot the gaps in our systems and processes to be more efficient. They do so in the name of the customer and the business, many times in the heat of the moment. Often doing all the wrong things for all the right reasons. This insider, while well-defined, is evolving. As users move to cloud, SaaS, and web applications they have more access to more and more data and systems. The trends suggest that targets for common attacks, such as phishing, whaling, spear phishing, and business systems compromise, are going to intensify using SaaS applications as the threat vector, with email being the primary means for attackers to target their prey.

The Evolving Insider Threat

Looking forward to 2025, the insider threat is going to continue and will only grow in frequency and difficulty to detect, due to the mobilization of the workforce. The movement of systems from on-premise to cloud applications makes it more difficult to detect an insider or threat agent posing as an insider. The data is not in the applications or organizations hosted, does not ride on the networks we built, and no longer resides in systems we own or control.

An insider can now be at our company or at the application provider's company. With the paradigm shift in the consumption and delivery of business systems and data, one would think the programs would need to have rapid change as well. While there is rapid change in the technology, there is no rapid change needed in the program and approach.

Insiders are largely triggered by emotional events. While these events are not ones that a company can easily support, the identification, education, and systems to support a strong insider threat program cannot be any easier to deploy. First, strong background checks, general awareness, and targeted education to high-value employees is key in turning an insider from a malicious one to a ***benign*** one. The systems most of us have can let users know while we don't always see them, our systems, processes, and culture does. Alerts, daily action reports, and notices to users on their behavior will make them think twice about their actions. It can also be leveraged to coach an unknowing or untrained user to do the right action like leverage a secure file transfer system provisioned by the company over email or other systems. This awareness will also help users identify if they have been targeted, as they know their actions better than we do.

Analytics for Insider Threat

Another control we all can leverage, and historically have not been able to use, is analytics. Systems using strong statistical analysis are a huge game-changer. These systems are only becoming smarter as they are supercharged with AI and ML analytics and engines which can learn what is and isn't normal. While these technologies and approaches are at your fingertips the trick is executing the pivot your program must take to get the visibility, control, and ability to notify the users of their actions. Start by taking a look at your systems and adjust your strategy for insider threat management to include the growing evolution of the threat from "Cloud First" or "Cloud Only" IT strategies and how this impacts your security strategy. Next evaluate your ability to do deep analysis on the traffic understanding the user, the data, the actions, the source, and the destination. These are your context for baseline in your analytic systems but also the baseline for education and awareness. Lastly, make sure you have inline support to stop and, in some cases, get justification for the users' actions. Many times this simple step will stop the user from proceeding, but it also will break many automated scripts that are trying to exfiltrate data to cloud systems.

Force 6: Government and Industry Regulations

Regulatory authorities are still trying to catch up with cloud computing let alone the revolution that business digitalization is causing as there is no longer a data center to audit or a firewall log to review.

Cloud Impact on Regulations

As the cloud reduces physical perimeters for organizations, the cloud also reduces and blurs the digital divide between countries and nations. For many organizations, knowing where their data is located should be a fundamental requirement, yet for many, it's not always obvious. Responding to a government or a regulator request that our data "is in the cloud" is not perhaps the correct response. Instead, the regulator has made it clear in recent data protection law revisions, such as the EU GDPR, that organizations must know where their data is located. It is a legal requirement and as we see updated regulations introduced across the globe, this requirement will be mandatory for most organizations.

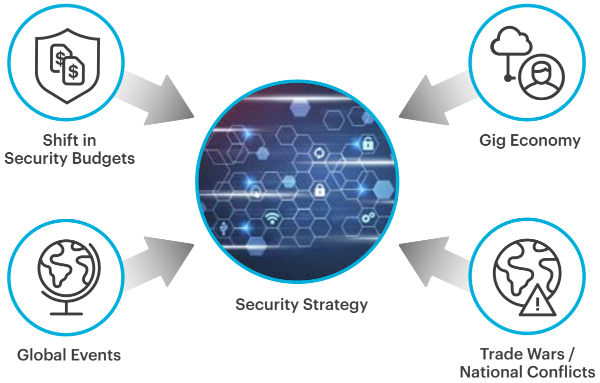
Geolocation Impact on Regulations

Not only is geolocation of the data a requirement but also an understanding of why the organization has this data, how long they can retain it, what organizational and security controls are required, and what agreements are in place to transfer this data cross-border to other data controllers and data processors. These are all questions the organization should be able to easily answer. As we see a consolidation of these requirements, we also see an acceleration in consumers being aware of their rights under new data protection and privacy Laws. GDPR, LGPD, CCPA, and POPIA are just some national or state examples whereby the national authorities have made it clear that consumer data protection is critical and they are willing to take action against even the largest organizations that do not take their obligations seriously.

Across the globe, countries and unions have applied aggressive mandates to control and protect data in and out of the country. For these countries, cross border connectivity must be controlled with organizations relying on valid agreements to be in place. The complexity of the rules in place continues to impact both global data protection and security teams that need visibility and control over their network and systems and to not run foul of these laws. For many of these laws, there is no simple answer as rules and guidelines continue to be developed to best support the government's intentions to support both their economy and their trade arrangements.

Recommendations to best manage these regulatory minefields include mapping the organizational data flows to truly understand where your organization may need to deal with these issues before they negatively impact the organization. Understanding where employees connect to and from cloud services, as an example, will help with maintaining a cross-border inventory of the locations that may need additional control and/or analysis. Sharing this information will provide greater visibility across the whole organization and can help support legal, risk, and audit teams in their understanding of the requirements. Building a strong coalition alongside the security team that factors into the location variable that cloud computing brings is a good first step to manage these forces.

Force 7: Global Social and Economic Forces



A security strategy should also be implemented to be aware of outside influences, such as global social and economic forces. Employees may not always give a second thought to these forces that may influence their favorite collaboration application. How would they know that they are using storage where the provider has terms that allow for this data to be used for secondary purposes? It is so easy to sign up for a new application completely unaware of the potential ramifications. Another aspect is the use of this data to train existing algorithms that can be used to enhance an understanding of behavior. All good vendor assurance and third-party risk assessments should uncover the potential of this, however, if the organization has embraced an acceptance of shadow IT, who is responsible for these checks and balances? These forces and influences should be considered and embedded into a strategy focusing on protecting both the employees from misguided information and to protect the organization from potentially losing value from their data.

The Shift in Security Budgets

The movement to cloud applications is also having a major impact on investment dollars of security budgets. By 2024 investments in cloud security will shift from the current ~20% of the budget to over ~60% of the security budget[6]. Major investments will be moving away from on-premise appliance-based secure web gateways (SWG) to software-based Next Generation SWGs that combine the functionality of data leakage prevention (DLP), web security, and cloud access security broker (CASB) into one platform. When implemented inline, the technologies can monitor and protect the information flowing to and from all critical business systems.

By 2024 investments in cloud security will shift from the current ~20% of the budget to over ~60% of the security budget.

Global Events

Often global events will impact the security strategy in unforeseen ways. The COVID-19 virus made almost every business continuity plan obsolete. Prior to COVID-19, if you went to your executive team and said *"I want to create a plan with enough secure network capacity, and mobile endpoint security to allow for the entire workforce to go remote all at once,"* you would have been laughed out of the office. Now that a global remote workforce is a reality, better security organizations have ramped up from a capacity perspective and are quickly redoing their network and endpoint security control structures to enable visibility and control for their remote workers.

[6] Source: Cowen, *Evolution of Security Creates Interesting Opportunity*, May 2019

Gig Economy

Outside of the pandemic, the economic forces have been changing for the past few years since the last financial crisis. Organizations have seen the rise and value of the gig economy which is based on flexible, temporary, and/or freelance workers that utilize technology and platforms to deliver projects and digital transformation. In the U.S, it's estimated that over half (53%) of Generation Z workers are freelancers[7], a number that is projected to grow in the next five years across all generations. With this growth in mind, organizations are moving away from traditional types of business processes to be more open and flexible and will expect a greater collaboration of tools and technology between permanent and freelance employees.

In the U.S, it's estimated that over half (53%) of Generation Z workers are freelancers[7], a number that is projected to grow in the next 5 years across all generations.

This move will push security teams to better understand and deal with a dynamic workforce whereby behaviors will need to be aligned and monitored. Gone are the days of spending time with a permanent team and providing security education and raising security awareness. Instead, more agile and real-time security awareness training is required that can educate an employee or a freelancer when they make a decision that introduces a high level of risk to the organization. This form of education strengthens the approach and allows for the flexibility of supporting a workforce that could change monthly, weekly, or even daily without damaging their productivity.

Trade Wars and National Conflicts Impact on Security Strategy

The security strategy is also impacted by trade wars and national conflicts. It is not uncommon to see an increase in cyberattacks during and immediately following a trade war or national conflict. In recent history, we have seen this in action in Asia and the Middle East. Shortly after the national event, a significant increase in cyber-attacks followed.

Whilst preparing for the next event, better security organizations are tracking national events and then adjusting their kill chain analysis, threat watch, and monitoring rules to prepare for and react to the next potential threat. Considerations should be made to the supply chain as although most organizations may not be the direct target, a disruption in the supply chain could have the same effect. Understanding which services your organization consumes and for what purpose and understanding the needs of your organization to supply goods and services to your customers is key.

[7] Source: *Freelancing in America* study by Upwork and Freelancers Union, 2019
https://adquiro-content-prod.s3-us-west-1.amazonaws.com/documents/19-0919_r3_Freelancing+in+America+2019+Infographic.pdf

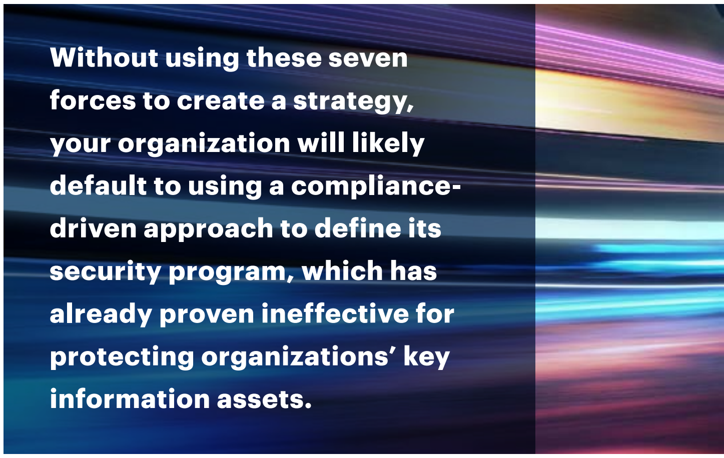
CONCLUSION

Business digitalization and the new mobile workforce are driving the biggest shift we have ever seen in network traffic and threats. The attack surface is now larger and the techniques to reduce the attack surface have changed. Managing dwell time is more important than ever and requires close monitoring of the cloud service applications for security compromises.

The SASE architecture represents a significant change in the traditional hub-and-spoke network architecture of the past and the inversion of network traffic from direct-to-internet connections requires the opportunity to completely rethink your network security strategy. The first step in the journey of implementing a SASE architecture is to implement a Next Generation Secure Web Gateway and a Zero Trust Network Access solution. Then continue down the journey to simplify your network and security controls and realize all the benefits of moving to the SASE architecture.

Obtaining and retaining visibility into your risk levels, cloud services being used, attack surface, and movement of data across the cloud services demands a new data protection strategy and network monitoring. Expect to continue seeing shifts in the attacks from cyber adversaries, and in turn, you should monitor the threat reports and adjust your security strategy and controls accordingly.

Evaluate your security strategy and make changes now. Continuing to invest in appliance-based, on-premise controls will leave you lacking visibility and impact the workforce experience, as you wait for these investments to fully depreciate. During your next cycle look at cloud-based, microservice-based systems that can easily upgrade as threats and solutions evolve.



Without using these seven forces to create a strategy, your organization will likely default to using a compliance-driven approach to define its security program, which has already proven ineffective for protecting organizations' key information assets.

Far too few enterprise-level organizations have been given the kind of opportunity we're seeing now to create a security strategy in the face of evolving threats and an ever-changing world. Without using these seven forces to create a strategy, your organization will likely default to using a compliance-driven approach to define its security program, which has already proven ineffective for protecting organizations' key information assets. Break the mold from cookie-cutter approaches with your security strategy, and use all seven of these forces to transform your security strategy for the better in the SASE-enabled, next generation of cloud security.