Check Point®
SOFTWARE TECHNOLOGIES LTD

SECURE CLOUD TRANSFORMATION

Managing the journey to cloud-centric security

ABSTRACT

Moving to the cloud is more than a technical transition to a new platform. It is a core part of an enterprise's growth strategy and while strategically important, it can also be potentially disruptive.

For security experts and security architects, the most critical challenge in cloud adoption is handling complex technical scenarios where the mix of traditional and cloud-driven infrastructures must be integrated and aligned with the security needs of the organization.

For cloud transformation to be successful, enterprises must be aware of their organizational and technology challenges, and security teams must carefully plan their strategy and approach.

Cloud transformation is a huge opportunity not without risks. At Check Point, our goal is to support decision-makers navigating the challenges of defining their cloud transformation strategy. This paper provides an evidence-based approach to planning, designing, and implementing the transition, with the goal of reducing design cycles and the overall cost of your cloud transformation.

AUDIENCE

CISO, security officers, architects, and designers engaged in cloud security architecture will benefit from this paper. As a prerequisite, you should be well versed in cloud and security design concepts and generic security architectural concepts and framework.

TABLE OF CONTENTS

INTRODUCTION

Moving to the cloud takes careful consideration. Merely copying an existing setup and moving it off-premises (referred to as a "lift & shift") is usually the least preferred option. In order to successfully transition to the cloud, organizations must find cloud computing technologies that best fit their business needs.

As we shift towards cloud-based architectures, security must not be an afterthought, it should be embedded in all services rather than "sprinkled" on the architectural blueprints of a newly approved cloud-based data centre.

Cloud transformation goals

Cloud transformation is going to touch all organizations. In this paper, we share our experience, discuss our understanding and present our thoughts.

Although any organizations rational for cloud transformation is defined by their own very specific business goals, at some level we expect that most will align with a set of common architectural trends and that these will shape the majority of end-state architectures.

Gartner's *"Top Security and Risk Management Trends"*[1] report highlighted three important trends, referred to as the building blocks of cloud transformation – Zero-Trust, Cloud Native Security and SASE.

The convergence of these trends is a unified view for a cloud centric security strategy, one that should be considered by each and every enterprise as a target cloud security architecture and used for their digital transformation journey.

We can describe the contribution of each trend as follows;

Cloud Native Security
Cloud native means building applications architected for, and in, the cloud on services such as containers and Kubernetes. Cloud native security is delivered by solutions built in the cloud and designed for the unique security challenges the cloud presents, including CI/CD development processes along with advanced security-operational model - DevSecOps.

Secure Access Service Edge (SASE)
SASE means de-centralisation of the data centre-centric architecture and moving users outside of the traditional perimeter, allowing them to consume Internet and corporate services directly from the cloud as SaaS or X'aaS. Security is provided as a service that is built on cloud native technology and delivered as an OPEX model.

Zero Trust
Underpinning both these design concepts is a principle that teaches us to approach networks as inherently untrusted and to leverage identity and trust as key components. "Never trust, always verify" has become a driving design principle and industry standard to which all cloud architecture should be measured.

[1] https://www.gartner.com/doc/reprints?id=1-1YKW4MUN&ct=200310&st=sb

CLOUD TRANSFORMATION DRIVERS

There are many reasons why an enterprise should adopt a cloud transformation project or strategy, and it is outside the scope of this paper to attempt to explain all the intricacies behind such a decision. In the following section, we look at some of the more common reasons behind an enterprise's decision to embark on such a journey.

We have defined the following key drivers as the main reasons for cloud transformation: business opportunity, operational agility, and security gains. Understanding these drivers will help enterprises and cloud architects define their target cloud architecture and cloud transformation strategy.

Business Opportunity	**Competitive advantage**	Early adoption of cloud technology and the ability to leverage cloud native feature-sets can reduce time-to-market and positivity impact competitive advantage.
	Flexibility	Shifting infrastructure responsibility, and some security risk, to a cloud service provider means more time and budget for core business needs.
	Availability	Cloud means high availability of mission critical apps
Operational Agility	**Branch offices / remote workers**	Shifting security for remote workers and branch offices to the cloud is cost effective and efficient.
	Mobility	Cloud-centric security enables all employees to securely access corporate data and applications, regardless of location.
	Pay-as-you-grow model/ cost reduction according to business needs	• The upfront cost is much lower • There are no hidden costs for unused features • The CAPEX is lower as overprovisioning is avoided; the capacity is purchased before it is used • Easy scaling: capacity upgrades do not translate to downtime, unlike most hardware-based solutions.
Security Gains	**Disaster recovery**	Most large enterprises spend time, effort, and money maintaining a resilient data center infrastructure. Moving to the cloud means this responsibility is transferred to the service provider.
	Unified management	It is important for enterprises to manage cloud security infrastructure the same way they manage on premise assets.
	Zero Trust alignment	One of the core principles of Forrester's Zero Trust Model is that network access should be user, device, and application-centric rather than relying on IP information or geographical location. Moving apps to the cloud and using an identity broker means these conditions are met adequately. Zero Trust is a component of a Secure Access Service Edge architecture and ensures the confidentiality and integrity of the data exchanged, a critical factor when assuming the network is inherently hostile.
	Controlled access	When workloads and data are stored in the cloud, there is a physical separation between employees, vendors, and visitors.
	Frequent auditing	Cloud service providers are required by law to undergo yearly audits designed to prevent flaws in their security systems.
	Physical security	Unlike traditional IT environments, the cloud service provider's data centres *always* have multi-layered security defences, including security guards, fences, barbed wire, surveillance cameras, concrete barriers, etc.

Budget Optimization

One of the key cloud transformation drivers is the shift from a CAPEX to an OPEX cost model. Moving to cloud computing and services inadvertently means making this accounting shift, for example, assets that are normally obtained as CAPEX can now be consumed as an OPEX service cost.

We believe that further cost optimization can be gained from a hybrid model that mixes different computing models (IaaS-PaaS, IaaS-PaaS-SaaS, PaaS-FaaS, etc.) allowing the optimization of day-to-day expenses. The infographic below shows some of these options and how they impact IT spend.

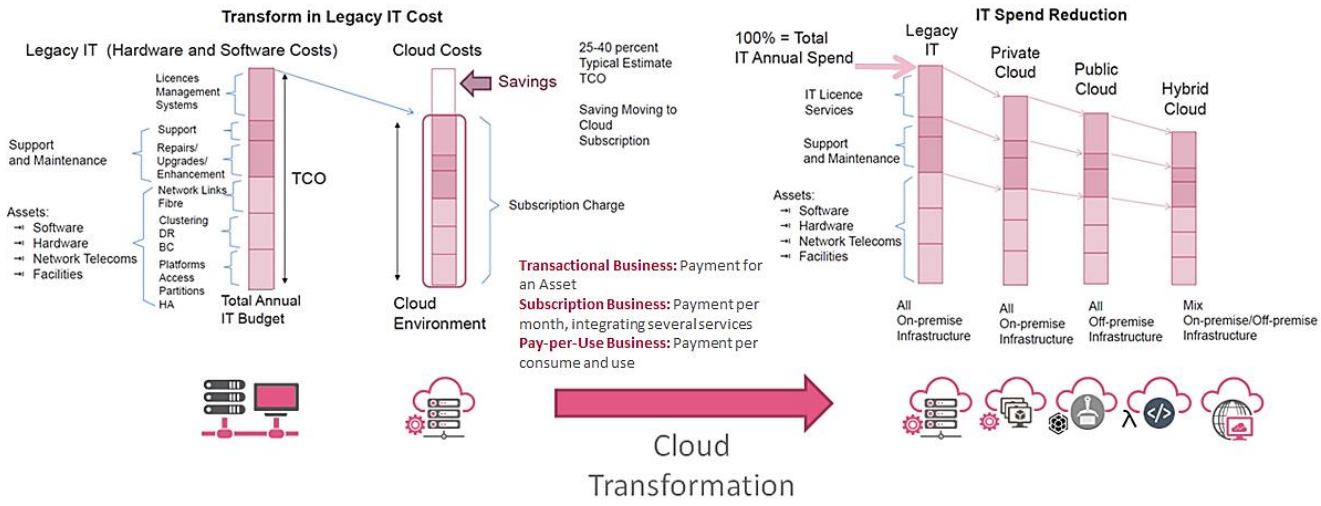


Figure 1: *The transition from CAPEX to OPEX in cloud transformation*[2]

SHARED RESPONSIBILITY

At some point, enterprises are likely to use all the available cloud services, including the public IaaS, PaaS, FaaS and SaaS. The issue is all these platforms have different operational benefits, shared responsibilities, and security challenges.

In traditional IT environments, the enterprise owns the whole stack and the dedicated security team make the necessary infrastructure changes. In the cloud, some responsibilities are transferred to cloud service providers, and some are transferred to application owners. Shared responsibility models challenge the traditional models of security implementation, management, and administration.

Leading research and advisory company, Gartner, stated that "*through 2020, 95% of cloud security failures will be the customer's fault."* Our own analysis also concludes that customer misconfiguration is the most common reason behind cloud security breaches. We believe this is partly due to customers thinking the cloud provider has secured, monitored, and appropriately configured the environment.

Enterprises must be aware that when they implement cloud-native security controls and integrate with solutions such as FaaS, PaaS, and SaaS, they need to take responsibility for the new cloud security policies such as access control, data protection, application activity visibility, content-awareness, and threat prevention.

In the example below we show how security responsibility is shared between the organization and the cloud provider and also between Application teams and traditional Security teams.

[2] Cloud Credential Council, ITpreneurs Nederland B.V. | CAPEX to OPEX transition analysis for Hybrid Clouds)

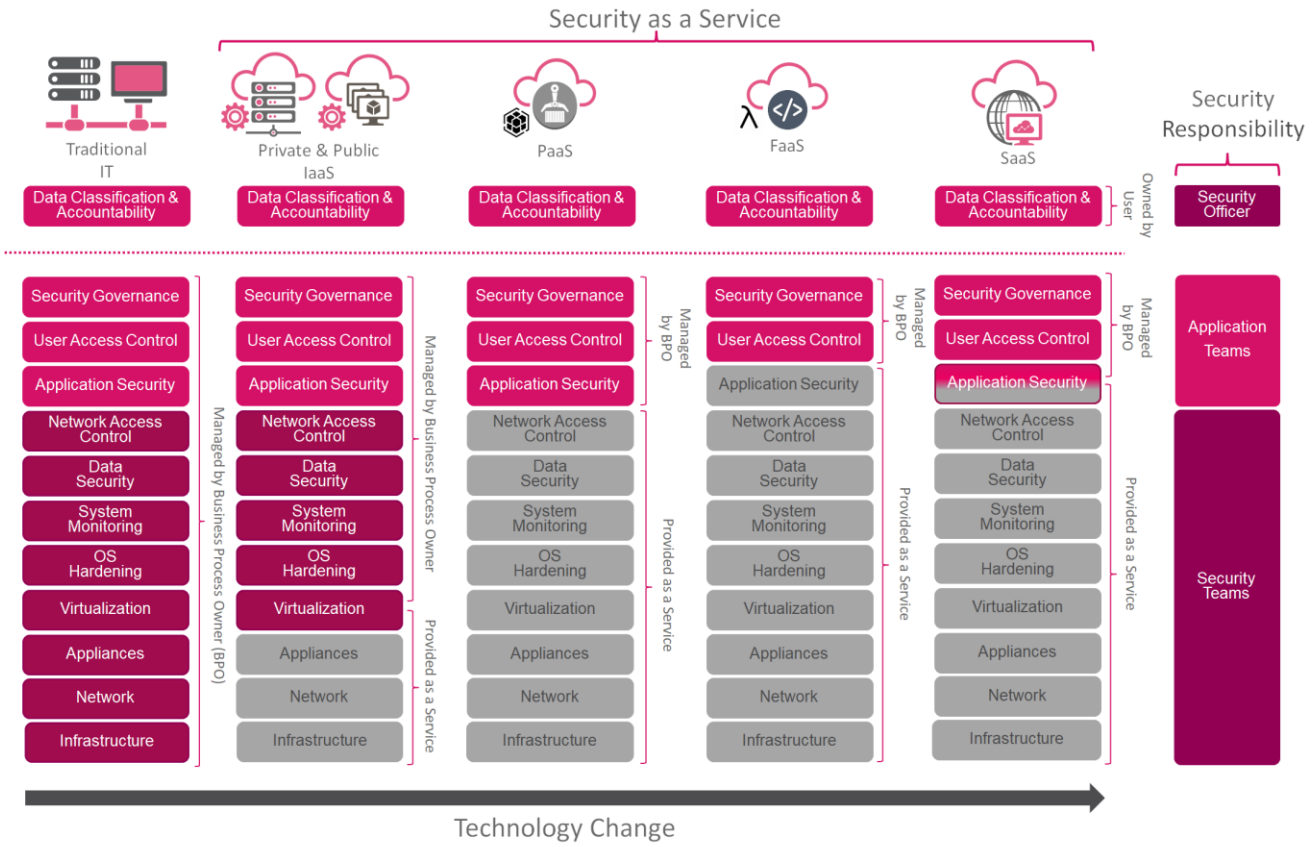


Figure 2: *Shared responsibility for the user and business process owner between the cloud computing models*

Security Responsibility and Security Oversight

We believe as organizations shift towards SaaS and FaaS services, security responsibility will change and traditional technology teams will have a different role to play in enforcing the organizational security policy. There are a number of different ways we see this happening; either through the assimilation of existing DevOps teams to form DevSecOps teams, or by moving into security assurance and responsibility roles.

This shift in security responsibility means that although the Security team still has overall responsibility for the security posture, the implementation of security is done by Application and DevOps teams. Therefore, it is important for the cloud transformation process to capture who is actually going to own the implementation of security and who is responsible for its management.

For example, an existing DevOps team is responsible for securing their application and moving the app to a PaaS platform. They have to abide by the organizational security policy of installing the Check Point WAAP agent into the ingress node. The responsibility for this install is with the DevOps team. Once the install is complete, the Security team will monitor the traffic.

The graphic below shows an example of the various cloud technology services and how security responsibility is shared between the Security team, Network team and Application teams as organisations move towards full cloud native technology and development practices.

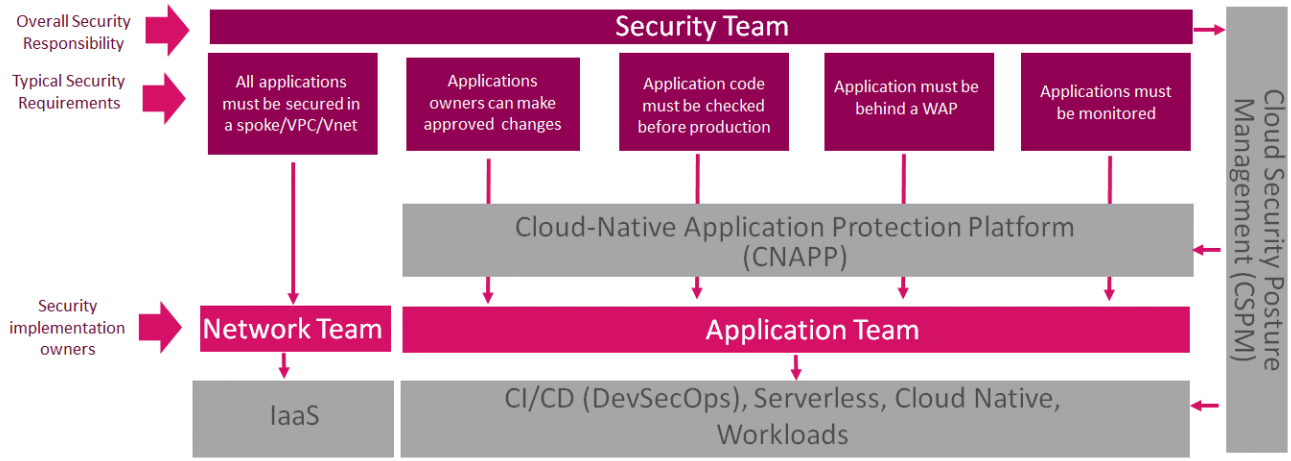


Figure 4: *Security oversight and shared security responsibility in cloud native environments*

Managing Cloud Security

Another way to visualize how roles change during the transformation process is to relate this to the CISO role. As we can see from the table below, the CISO needs to understand the different threat models and attack vectors associated with each cloud computing technology. For the CISO, this approach should create the right balance between the security needs, while maintaining business agility.

As the enterprise moves towards PaaS/FaaS, the security technologies are being changed from traditional (e.g. Firewalls/IPS etc.) to API-based, Posture Management and code-analysis driven.

	Traditional Data Centers	Virtualization (Private IaaS)	Public Cloud IaaS	Containers (PaaS)	Serverless (FaaS)	SaaS
Infrastructure needed	Huge	Large	Medium	Small	Very Small	Not Required
Security	Physical Perimeters Server & Network Security Security Appliances DDoS Appliances SSL Decryptors	Segments/Zones Virtual Firewall/ Virtual IPS Antibot/Antivirus Sandboxing	Microsegments Virtual Firewall Virtual IPS WAF	Posture Security • Configuration Management • Access-Control • API Security • Application Flows	Static-Code Analysis Run-Time Analysis DevSecOps	Identity Access Management API Security Data Security
Units of Computation	Physical Servers (Monolithic/Single Units)	Virtual Machines (Coarse-grained)	Computing Instances (Coarse-grained)	Applications & Libraries (Fine-Grained)	Code executed through libraries disregarding OS (Fine-Grained)	Cloud Computing Driven
Data Transport	Packets, Connection per Second/Throughput	Traffic Flows Hypervisor	Traffic Flows VPCs	Application Flows	Execution Code	API Flows
Deployment	Months	Hours	Minutes	Seconds	Milliseconds	Minutes
Best fit	Highly transactional operations, low latency	Resource optimization	Resource optimization, Delegate-Risk	Agile, Fast and Elastic Services for Time to Market	Micro services Enabled for IoT devices	IT Commodity Services replacement
Price	$$$$$$	$$$$$	$$$$	$$	$	$$

Figure 5: *New technology and changing roles*

SECURE CLOUD TRANSFORMATION

In the introduction, we presented a vision of the future in which most enterprises embrace cloud native architectural principles.

In most cases, it is not practical to expect all enterprises to move to this state immediately, which is why we have devised a set of transformation phases. These are simple design templates that can help enterprises understand their current position relative to a future cloud-centric state and SASE driven architecture.

Before we discuss the transformation phases, it is important to understand the various Check Point technology sets and how they fit into the cloud transformation process.

CloudGuard Overview

From private cloud data centre to public cloud, PaaS, FaaS, and SaaS application migrations, Cloud Guard provides comprehensive cloud security solutions to keep enterprise data, assets, and apps protected against even the most sophisticated attacks. Whether one's business strategy centres on cloud-enabling applications and platforms, public and hybrid infrastructure, or a multi-cloud approach, Cloud Guard ensures all assets are adequately protected while supporting the flexible, dynamic, and cost-effective nature of the cloud.

Figure 6: *Check Point CloudGuard*

The table below shows the major technology areas in the cloud supported by Check Point.

CLOUD PLATFORM	CHECK POINT APPROACH
IaaS	Check Point's flagship CloudGuard IaaS Cloud Security solution is designed to keep data in public, private and hybrid cloud networks safe from even the most sophisticated attacks. CloudGuard IaaS: Enhances native micro-segmentation and elastic networking of cloud environments to dynamically deliver advanced security and consistent policy enforcement that automatically grows and scales with cloud environments. Secures workloads and applications running in hybrid and public cloud environments such as Microsoft Azure, Amazon AWS, and GCP, mitigating risks from breaches, data leakage and zero-day threats. Supports leading network virtualization solutions such as VMware NSX and Cisco ACI. Check Point CloudGuard IaaS enhances native micro-segmentation capabilities to provide proactive protections for East-West traffic inside virtual data centres.
SaaS	Check Point offers CloudGuard SaaS – a cloud service that prevents attacks on enterprises using SaaS applications: • Prevents malware and zero-day threats from attacking SaaS users • Stops sophisticated phishing attacks on Office365 and Gmail accounts • Eliminates the top SaaS threat by blocking account hijacks • Provides instant visibility into unauthorized SaaS activity • Protects shared files and sensitive business data
Security as a Service	CloudGuard Connect is a cloud-hosted network threat prevention service offering a maintenance-free, comprehensive, affordable security solution for remote sites and roaming users. CloudGuard Connect supports adding advanced threat prevention capabilities on top of existing routers or SD-WAN deployments, connecting to the corporate resources in the Public / Private IaaS and SaaS applications in the Internet.
Cloud Security Posture Management	CloudGuard Dome9 delivers full lifecycle security for cloud native applications from development through runtime. With CloudGuard Dome9, organizations can gain complete control and visibility of their cloud native applications and functions, across cloud providers. Dome9 integrates with Azure NSG and AWS security groups allowing full control and viability using cloud native controls.
Serverless / Cloud Workload Protection Platform	CloudGuard Dome9 automates the entire security lifecycle of serverless FaaS applications, from development to runtime. CloudGuard Dome9 detects and alerts on security posture issues, as well as providing corrective remediation prior to deployment – saving developers' time and assuring no vulnerabilities reach the live environment with seamless CI/CD integration. During runtime, the CloudGuard Workloads agentless Function-Self-Protection (FSP) layer detects and blocks OWASP TOP 10 attacks at the function level, like injection, broken authentication, excessive permissions, and sensitive data exposure, while generating a highly accurate behavioural profile for each function in order to stop anomalies.
Management as a service	Check Point offers all-inclusive security management as a service (MaaS) designed to manage security across on-premises appliances, Networks, Cloud, Mobile and IoT.

Figure 7: *Check Point CloudGuard products*

Transformation Phases

In this section, we present a visual representation of the three distinct cloud maturity levels after the traditional data centre approach, each representing a defined phase of cloud adoption.

All transformation processes require several steps. By defining these into phases we can quickly visualize the current levels of cloud adoption and efficiently design the target architecture. Most customers are already in phase 1. However, some will be aiming to adopt phase 3, while other business models may only require phase 2 adoptions.

Phase I: Network and Infrastructure Centric

This phase is the starting point for an enterprise to define the different transition steps.

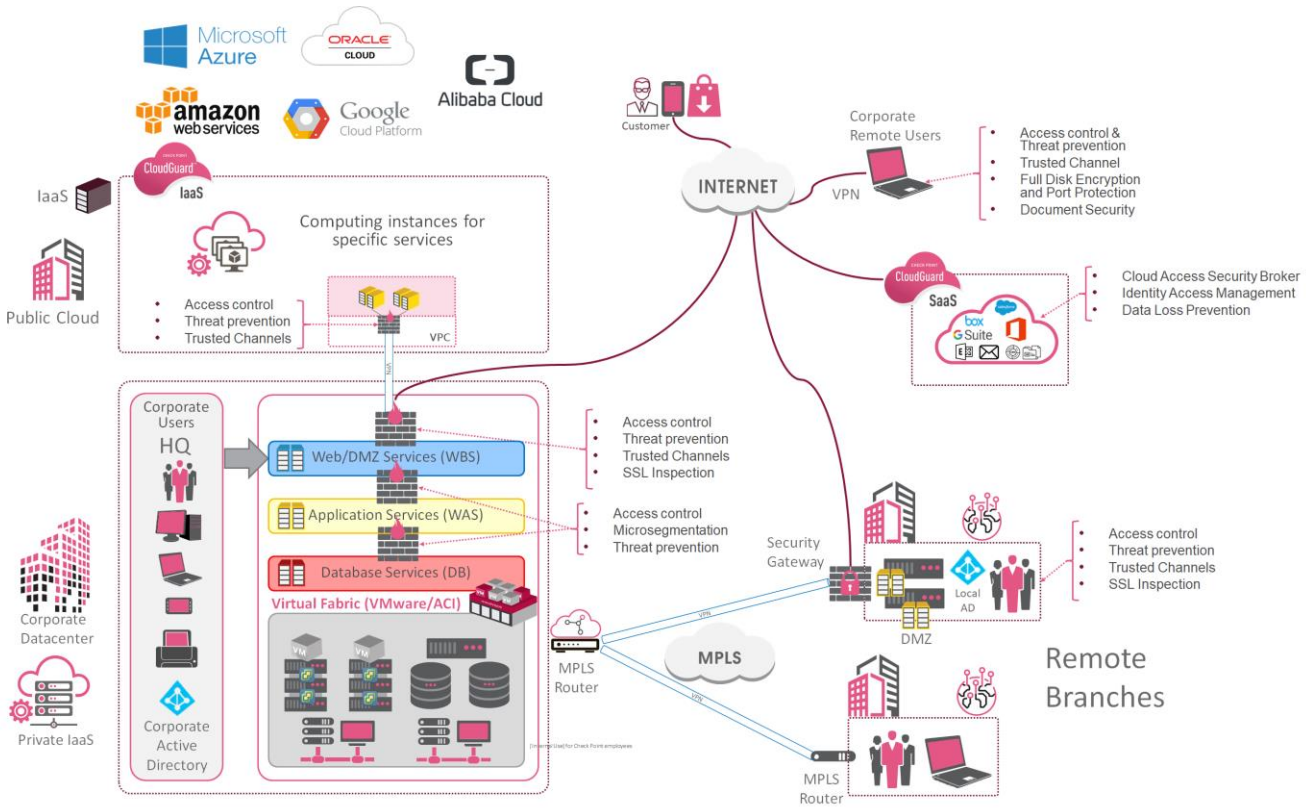


Figure 8: *Network and Infrastructure centric approach, the current situation for most enterprises*

This diagram shows the current situation for most enterprises when they start to deploy computing instances in the cloud to begin their transformation. A shift towards the partial public and private cloud usage has been made, yet most users still connect to resources in the on-premises data centre. The Internet egress point and corresponding policy are controlled centrally, and there is no way to avoid it. Most, if not all, remote sites connect to HQ via a traditional WAN link, and do not have a local Internet breakout.

While this traditional architecture is common, there are several significant challenges enterprises face:

- The cost of running an on-premises data center is significantly higher than outsourcing it to public cloud providers, regardless of the type of service.
- As there is still a large amount of bare metal in the data center, the only way to truly microsegment is to combine hypervisor-level security, with security in the switch fabric using Cisco ACI (Application Centric Infrastructure). This comes at a high cost, especially from an operational point of view.
- The Internet-bound traffic originating from remote sites is backhauled to the data center where the Internet breakout is located. This leads to additional latency, decreased application performance for cloud-based apps, and unnecessarily expensive Internet access pipes. This is especially true when an IPSec VPN is used without split tunneling for remote sites. Traffic enters the HQ in an encrypted way and leaves unencrypted, thereby doubling the throughput requirement of the access pipe. This type of architecture has several names: traffic hair pinning, trombone, and backhauling. The disadvantages outnumber the advantages.
- SD-WAN technologies are not yet in place. Expensive MPLS (Multiprotocol Label Switching) circuits are a significant cost factor in the organization's telco OPEX.
- Response times for SaaS applications are subpar because of the traffic hair pinning.
- Some remote sites may already have a local Internet breakout, however if the same level of security needs to be enforced as in the HQ's Internet breakout point, the same security controls need to be in place in remote sites. This refers to local appliances capable of running the full threat prevention stack of controls, including SSL inspection. This is an expensive approach, especially if many remote sites have a local Internet breakout.

Phase II: Transitional and Hybrid

In the above example, the enterprise has made some significant changes towards cloud usage, but they rely heavily on on-premises infrastructure in the data centre. The organization is now in a hybrid cloud model.

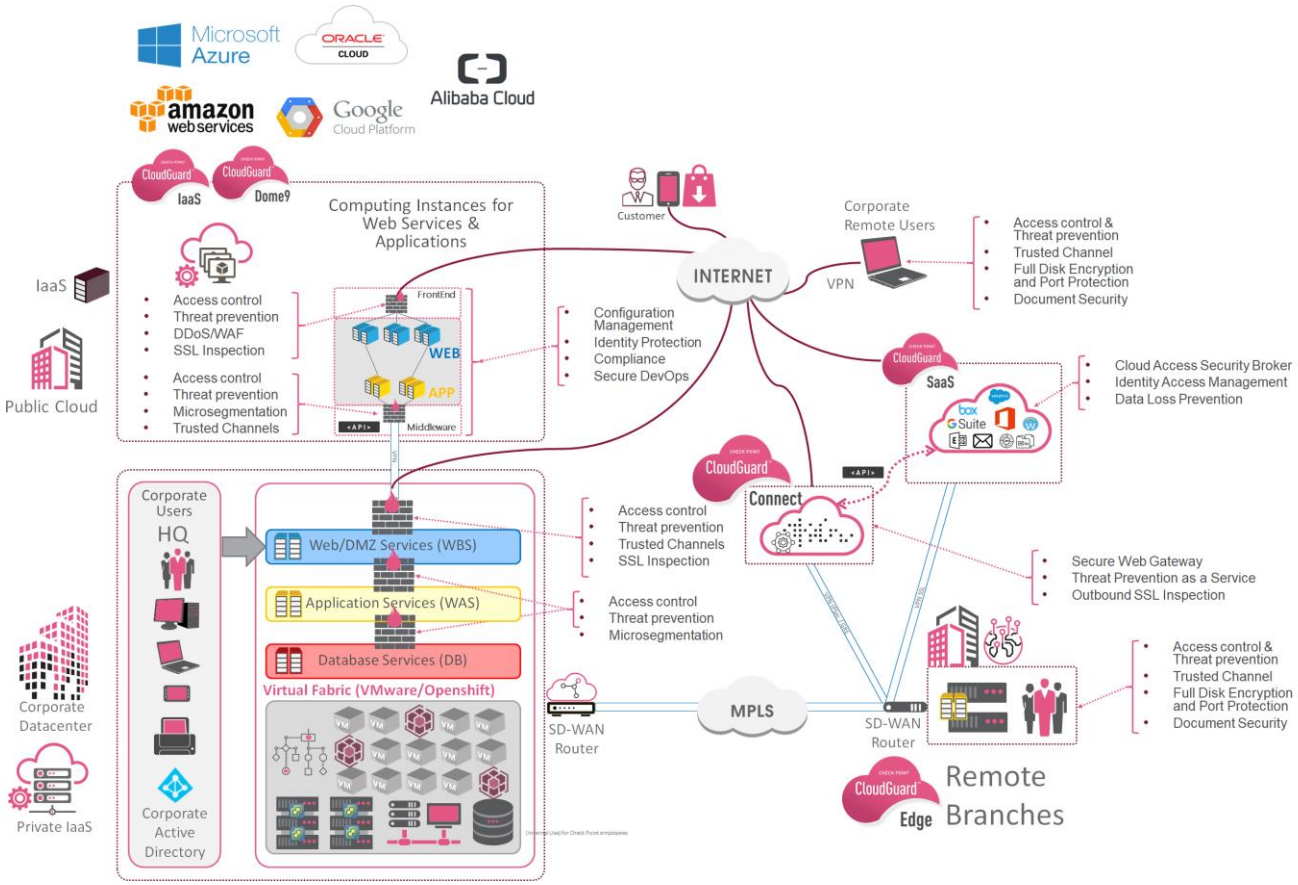


Figure 9: *Ongoing migration to the cloud*

Enterprises in this phase typically have the following characteristics:

- The remote sites have been moved to an SD-WAN architecture and have a local Internet breakout in order to improve the performance of SaaS applications, which reduces the cost of the WAN services such as MPLS. The secured access is being provided through the Security as a Service in the cloud.
- MPLS circuits are still in used to offer QoS for specific HQ-bound applications like VoIP and videoconferencing.
- Most of the bare metal in the data center has been moved to virtualized instances, leading to significant cost reductions and the option being to truly microsegment the on-premise workloads.
- The majority of workloads have moved off-premise, some public services are still hosted in the data center, which is not cost-effective and does not auto-scale.

Phase III: Cloud Centric

In order to successfully complete the move to the cloud, organizations must find cloud computing technologies that best fit their business needs.

Regardless of how long it takes for the transformation process to move all workloads and security to the cloud, it will inevitably happen. Having a vision of the end-state architecture will help organizations to execute their cloud transformation strategies.

Phase III describes a target architecture that is premised on SASE and Zero Trust design principles meaning decentralised users, consumption of SaaS and a paradigm shift in how we secure enterprise networks.

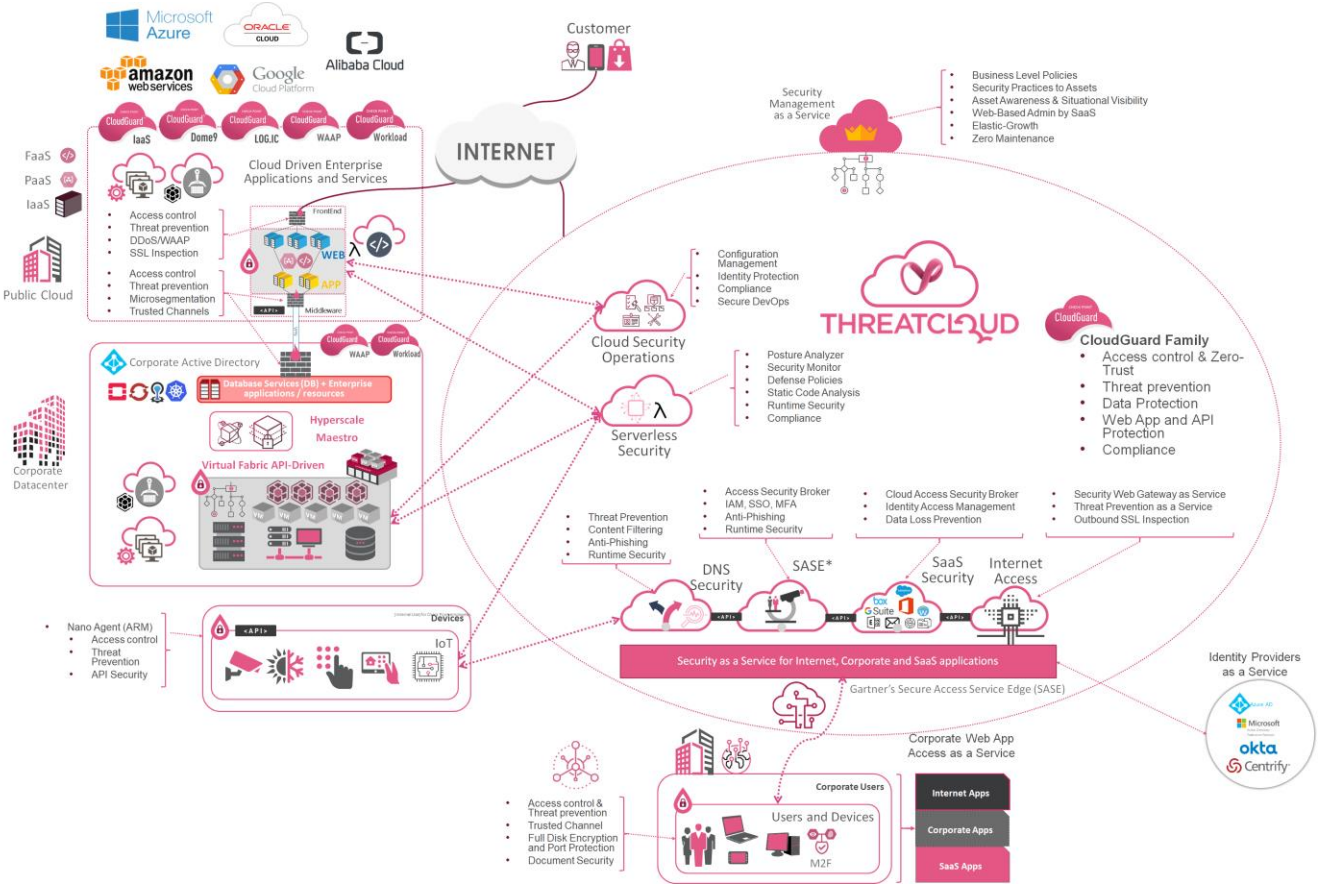


Figure 10: *Full cloud centric architecture with Security as a Service and SASE*

Cloud Centric Overview

The target architecture described in Phase III is conditional on factors such as application maturity and the organisational appetite to change and risk. In order to articulate the characteristics of this phase of transformation we use the following architectural and design principles;

Architecture

- Cloud Security Centric with the main focus on the security as a service provided through the cloud service - SASE
- Hybrid cloud data center where the frontend and applications infrastructure located in the cloud and the backend remain at the data center on prem.
- Reducing amount of security hardware presence at remote offices and sites, shifting to the cloud-based secure access to the Internet and Data Center.

Services

- X-as-a-service first, where possible all services are subscription based.
- Shift from CAPEX to OPEX.

Branch Offices

- Reduced the on-premise appliances footprint according to the needs of internal site security, e.g. OT/IT isolation and segregation.
- Secure branch office egress Internet-bound traffic in the cloud.
- Branch office primary transport network is the internet.
- If optimization is required SD-WAN is used.

Data Center

- Web and Applications tiers complete migration from the data center to the Public cloud IaaS.
- Leveraging Zero-Trust security design modeling to protect access the public cloud data center and perform macro and micro-segmentation.
- Resources such as mainframes and high-value databases remain on-premise, connected to the public cloud IaaS through the VPN direct links secured by the single layer of the Firewalls located at the perimeter of the on-premise Data Center.
- The data center is no longer the core of the organization.
- The hair-pining of traffic thought the DC has been removed.

Cloud Native Security

- Cloud Native Security – Private and Public IaaS security leveraging a modern approach such as Cloud Native Application Protection Platform (CNAPP) and Posture Management with Cloud Workload Protection Platform (CWPP) for K8s/Containers and DevSecOps.

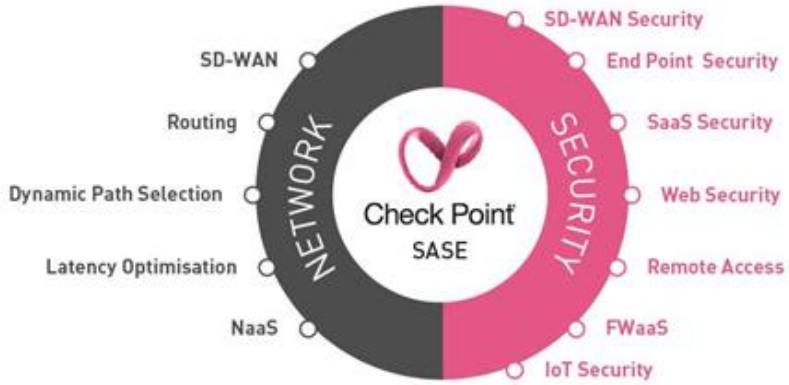
Users and devices (IoT)

- All users and devices are secured by SASE components and can access the Internet directly.
- The users accessing corporate applications via Remote Access VPN capabilities provided by SASE service regardless the location.

SASE

The SASE model described a change in architecture that no longer places the traditional on-premise data center at the core of the infrastructure and shifts the focus to decentralization. SASE is all about distributing access to (corporate) resources instead of consolidating them.

SASE is an architectural model consisting of several products, whose goal is to allow users to access applications with the best possible user experience and the highest level of security, all depending on the user's identity.



Any user, regardless of their location and the device they are using should be able to access any application, corporate or public, in a secured way. Versatility, scalability and user experience are of paramount importance.

Rather than routing traffic originating from branch offices and remote users to the data center where the internet egress point was typically located, SASE dictates users and branches should all break out to the internet directly. In any case, most resources are moving from the traditional data center to the cloud.

The SASE model covers a wide range of functionalities, ranging from layer 3 in the OSI model up to the application layer, as depicted in the graphic above on the left-hand side.

The Check Point SASE model covers 2 aspects – network and security:

SASE building blocks		
Security	SD-WAN Security	Allows companies dealing with a significant amount of legacy infrastructure in branch offices to stop backhauling all internet-bound traffic to the regional hub site without having to upgrade the legacy gateways, saving WAN costs without compromising security.
	Firewall as a Service (FWaaS)	A cloud-based Next-Generation Firewall is a scalable, application-aware solution allowing enterprises to eliminate the challenges of legacy appliance-based solutions
	Web Security	Secures Internet access to Web applications and resources leveraging unified Threat Prevention solutions, such as URL Filtering, Anti-Virus, IPS, Anti-Bot, and Zero-Day attack prevention.
	End Point Security	Security for mobile and portable devices to protect against loss of corporate data and to mitigate modern-day malware such as ransomware, zero-day attacks, phishing, etc. so you can safely navigate today's menacing threat landscape.
	Secure Remote Access to corporate resources	Replacing traditional remote access solutions where the VPN was terminated in an on premise data center, SASE Remote access no longer requires the traffic to be backhauled, improving the user experience.
	SaaS security	Secure access to SaaS applications like Office 365, Google suite, etc. using a Cloud Access Security Broker (CASB)

	IoT security	SASE enables IoT devices to break out to the internet directly in a secure way.
Network	Latency Optimisation	Optimizing access to the Internet and Data Canters by allowing branch offices and users to break out to the internet directly and securely, significantly improving the user experience.
	Routing	Elements like routing, dynamic path selection, NaaS, and latency optimization are all essential networking features of SD-WAN, laying the foundations on which security is built.

The Check Point SASE solution places security as a service in the cloud in a distributed fashion instead of enforcing it the legacy way on gateways, on-premise Data Centers and branches.

The infographic below shows a high-level representation of the key SASE components.

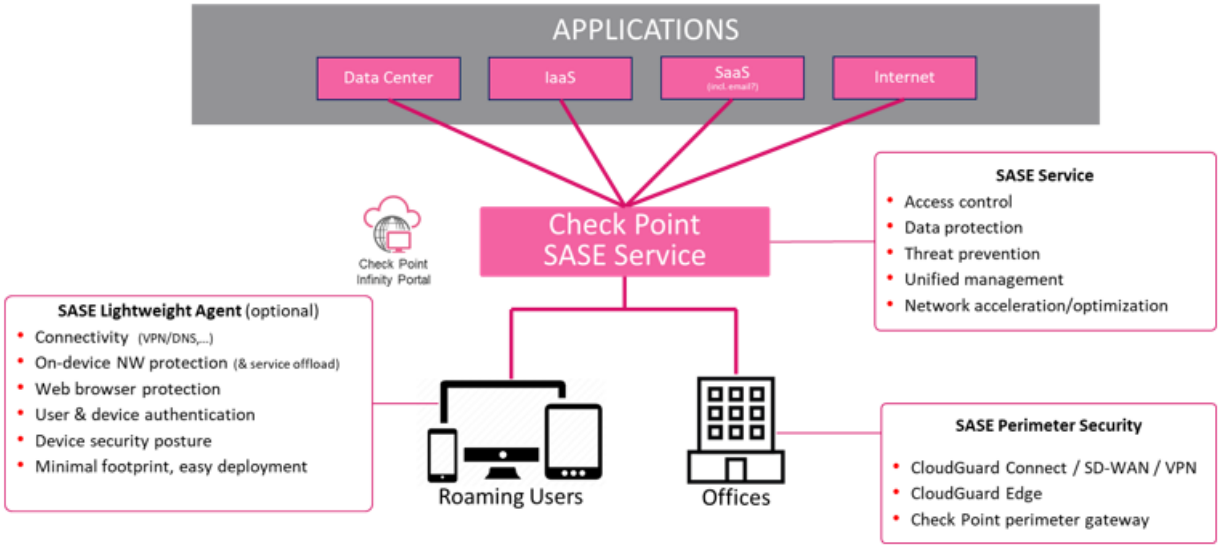


Figure 11: *Check Point SASE components*

CLOUD TRANSFORMATION FRAMEWORK

Check Point has created a set of transformation principles to help enterprises shape their cloud strategy and transformation process. We have captured these into a framework which we present below. These high-level architectural principles also form the foundation of our *"Cloud Transformation Workshops"* and are designed to support the planning and execution as well as give some structure to the overall process.

Overview

Unlike other frameworks, Check Point's cloud transformation framework is a collection of principles, analyses, and recommendations presented as a single process. Our experience of working with enterprises has led to the understanding that teams, strategies and internal processes are usually at very different stages. Consequently, when we discuss the topics below with customers, some topics are well developed and allow us to move directly to recommendations, while others require a deeper analysis, and some are mainly aspirational.

The overall goal of the framework is to understand our customer's current position, explain our understanding of a holistic target architecture, and make recommendations that help them achieve their strategic vision.

Check Point has identified the following key principles for cloud transformation:

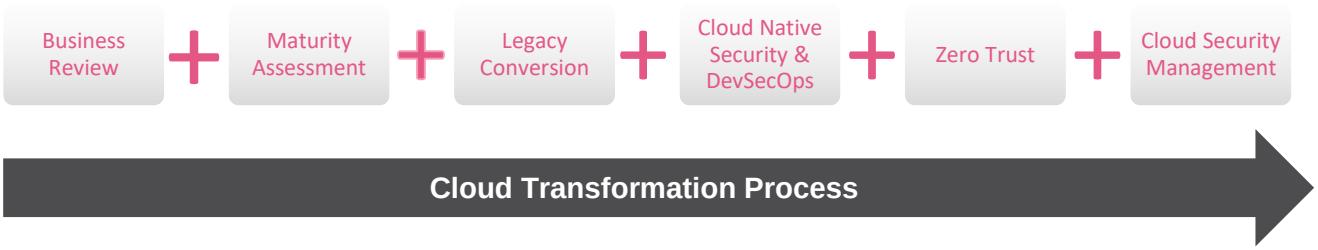


Figure 12: *The Check Point Cloud Transformation Framework*

Business Review

The first step in the cloud transformation journey is the business review. It is focused on capturing information that pertains to the enterprise's business, both in terms of strategy and the role security plays within. We often refer to this as security business modelling. This is an essential stage to learn business needs and identify precise requirements for the cloud strategy. Afterwards, it will be easy to understand the influence of security on these requirements. The final step is to express these requirements as attributes, i.e. labels that describe what is required of the security architecture.

This process is described in more detail in the Check Point Enterprise Security Framework (CESF) that can be found here: https://www.checkpoint.com/downloads/products/checkpoint-enterprise-security-framework-whitepaper.pdf

1. Identifying Business Requirements (BRs)

To begin the process, information is collected through interviews with key stakeholders, such as the CISO, cloud architects, and security officers. The outcome of these interviews should be a collection of business requirements. A business requirement is a resource, process, or condition that is vital for the continued success and growth of a business.

2. Identifying Business Drivers for Security (BDS)

Business drivers for security are very specific to each enterprise and it is only through the interviews that we are able to capture these in detail. Often business requirements are too general in definition, which is why we use 'Business Drivers for Security' to give the 'business requirements' more relevance to security architecture. Business Drivers for Security are always linked to the business requirements and provide the security context to the BRs.

3. Attributes

The next and final stage is "business attribute mapping." This is the process of assigning a number of attributes to each requirement identified during the review stage. "Attributes" play the important role of providing a link between the requirement and the recommendation.

An attribute is a conceptual abstraction of a real business requirement (the objectives, drivers, and targets), which is modelled into a normalized language that articulates requirements, and measures performance in an instinctive way for all stakeholders. Although the attributed terms are abstract in nature, they are an excellent mechanism to map out security controls. There are no fixed rules on how attributes are used and their use is often subjective.

Defining attributes also helps us to prioritize the business requirements and security drivers, as attributes can be given different weightings.

Business Review Example

In the following example, we have added the attributes to the data-collection table.

<table>
<tr><th colspan="2">CHECK POINT ENTERPRISE SECURITY FRAMEWORK</th></tr>
<tr><td>Title</td><td>Public IaaS/PaaS for e-commerce Services</td></tr>
<tr><td>Business Requirements (BR)</td><td>Enable Acme business growth through elastic, agile and scalable technology.
Enable e-commerce services to be provided through computing resources
Improve time-to-market requirements deploying public and private cloud IaaS/PaaS, performing a combination between Microsoft Azure and Red Hat Openshift etc.</td></tr>
<tr><td>Security Analysis</td><td>Data and information in the cloud are exposed to the same threats as traditional infrastructures. However, due to the large amount of data processed in cloud computing, data leaks can lead to a chain of unfortunate events for IT companies and Infrastructure as a Service (IaaS).
• External Exposure – Cloud services are typically accessed from any location and any device. All that’s needed is an Internet connection. While ease of access can boost company agility, services running in the cloud versus those on premise are more likely to be breached.
• Only Default Security – Typically, cloud services are provided with only basic security, which allows unrestricted open Internet file sharing. This vulnerability can open the door to any number of malware attacks.
• Cloud services are vulnerable across three main attack vectors:
1. Account Hijacks – Gaining unauthorized access to an individual or organization’s email or computer account for malicious purposes. In a Check Point survey, account hijacks were the most significant concern amongst customers and partners.
2. Malware Delivery – Propagation, primarily through in-app file-sharing services, such as Drop Box or One Drive cloud apps, to commit a variety of cybercrimes.
3. Data Leaks – Whether intentionally or unintentionally, data leakage occurs with the seamlessness of sharing information using cloud services.</td></tr>
<tr><td rowspan="2">Business Drivers for Security (BDS)</td><td>To meet these requirements the organization will need to adopt a significant amount of cloud technology, which needs to on-board in a secure manner. The attack surface will change when workloads are moved to the cloud.</td></tr>
<tr><td>Risk Statements
Risk: Lack of visibility in the cloud virtual network (Vnet) can lead to a sensitive problem if one of the computing instances is compromised to extract information.
Risk: Lack of identity management in the public cloud IaaS can lead to an employee accidentally modifying the logic of the configuration template, and impacting the services.
Risk: Lack of lateral protections can lead to a compromised computing instance, which can impact the customer’s services, and, consequently, the business’s reputation.
Risk: Lack of visibility in the encrypted communications from public cloud IaaS can lead to malicious code gaining access to the data centre’s resources.
Risk: Time-to-market requirements can lead to mistakes in the configurations of the workloads.
Risk: The company reputation can be impacted by compromised content in the public/ private workloads that aren’t protected in public networks.</td></tr>
<tr><td>Attributes</td><td>Accessible, Reliable, Cost-Effective, Elastic, Agile, Access-controlled, Accountable, Authenticated, Authorized, Identified, Adaptable, Scalable, Enables Time-to-Market</td></tr>
</table>

Figure 13: *Example of using the CESF process to define risk statements for IaaS*

Cloud Maturity Assessment

Understanding an enterprise's existing and aspirational cloud maturity is critical to the cloud transformation process. Check Point breaks this down into application maturity and the transformation phase.

A cloud maturity assessment and security controls review, provides a simple way to assess the existing level of cloud security capability. Understanding cloud maturity helps define the starting point for cloud transformation and breaks it down into several migration steps moving towards a cloud-centric operations and security model.

In the introduction to this paper we discussed the various phases Check Point proposes as part of any enterprise's cloud transformation. The following figure represents the three main phases of cloud transformation as previously described.

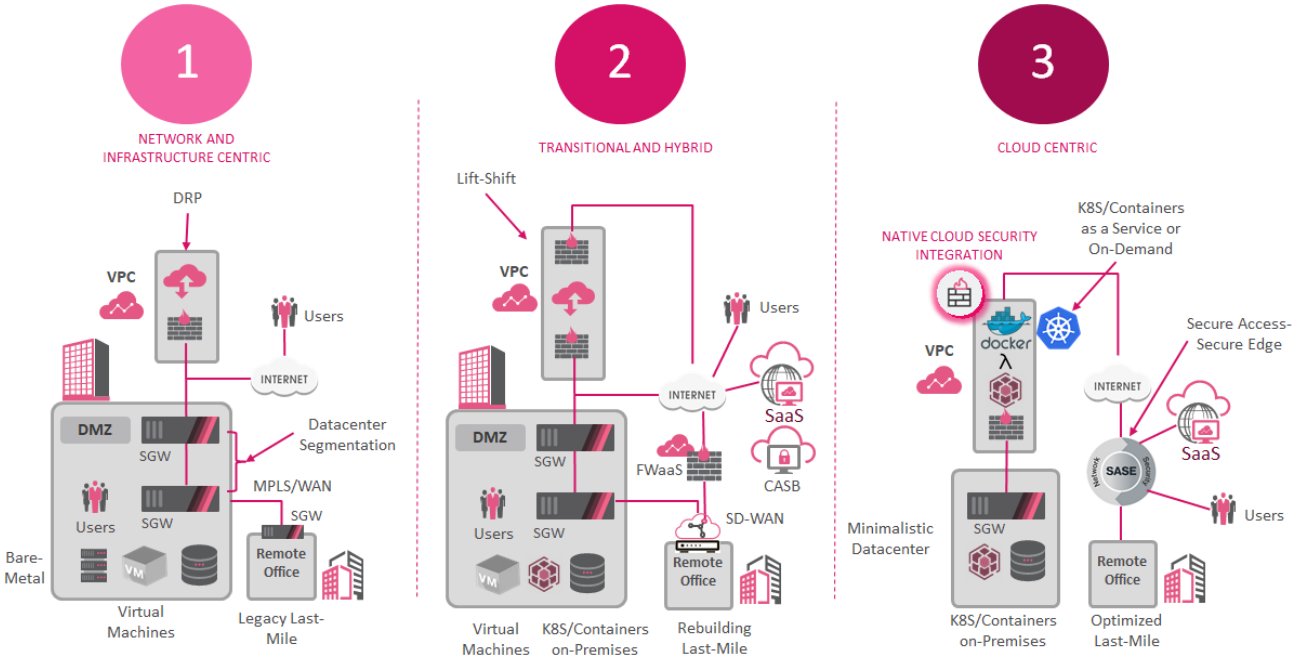


Figure 15: *Cloud Transformation phases*

Phase 1: Applications are primarily hosted on-site with a few instances in the cloud. Remote users are connected to DC using MPLS. Applications are developed and deployed into the on premise DC and any cloud deployments are done using IaaS virtual machines.

Phase 2: Applications have moved to the cloud with the majority of applications existing as SaaS and IaaS services. Those applications that are in cloud DC's are protected by an IaaS perimeter gateway and follow a spoke-and-hub cloud architecture. SD-WAN has replaced some of the MPLS circuits.

Phase 3: Full SASE architecture. It is important to note that at this phase these is still hybrid cloud architecture.

Applications have b been refactored or re-build using cloud native solutions such as serverless and containers by dedicated DevSecOps teams.

Legacy to Cloud-Native Analysis and Mapping

A core component of planning and executing a successful cloud transformation is to understand which applications and resources within the enterprise will be migrated to cloud technologies, and which will remain, leveraging either legacy platforms or advanced virtualization fabrics in the private IaaS.

Mapping the legacy assets and processes to be transformed to the cloud allows enterprises to understand which cloud security technologies should be implemented.

The following diagram show the four types of services associated with the different business processes commonly found in any enterprise. As part of the analysis, we need to understand and explain which type of workloads are suitable for which type of private, hybrid, or public cloud service. We should also see what is realistic and practical to move and what is not.

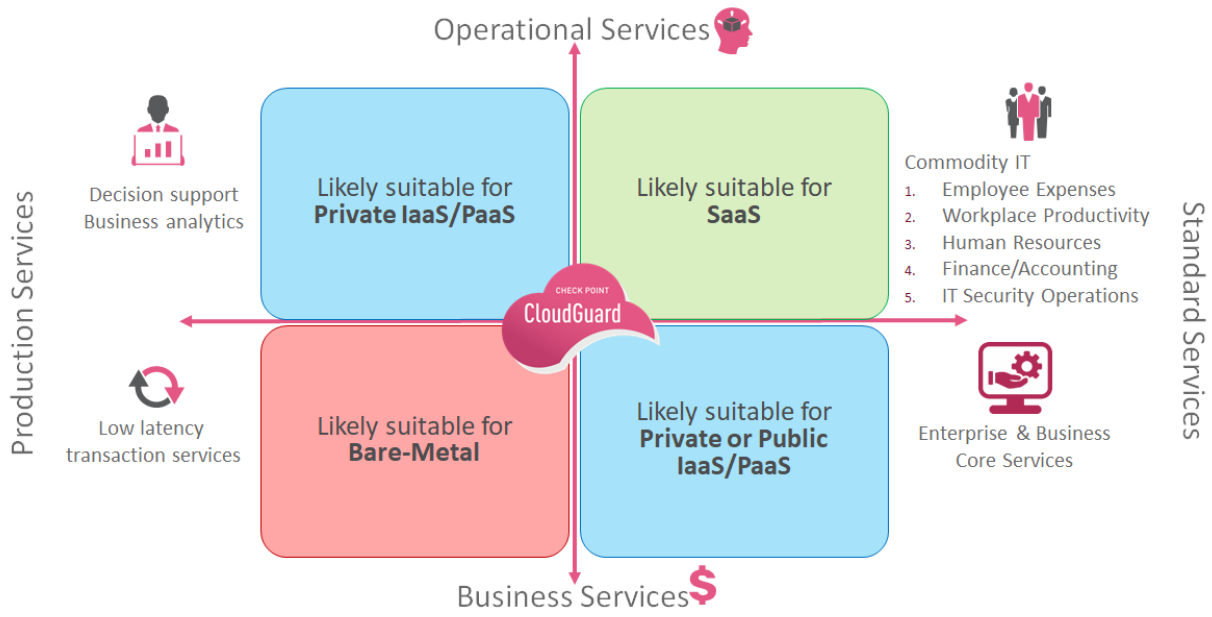


Figure 16: *Magic quadrants for business process analysis. Used for categorization of cloud computing enterprise needs*[3]

The goal behind using quadrant analysis, as shown above, is to help us visualize which existing technologies and services suit what cloud technologies. Typically, organizations will have a mix of cloud platforms and technologies depending on the workload:

We expect that most enterprises will continue to use legacy hardware, custom developments, enterprise applications, and operations. Digital transformation does not mean moving everything. The transformation process should go through several phases and place workloads where they are the best fit.

[3] Cloud Credential Council, https://www.cloudcredential.org/

Migrating Security Controls to the Cloud

The following figure shows how the various components of a legacy environment can be translated into their equivalent cloud assets by integrating different security components.

Our approach has always been to fully understand the existing security controls and then to map these to their cloud equivalent as and if required. This exercise means that we have a clear appreciation of what we will be leveraging in the cloud and how we are going to manage it.

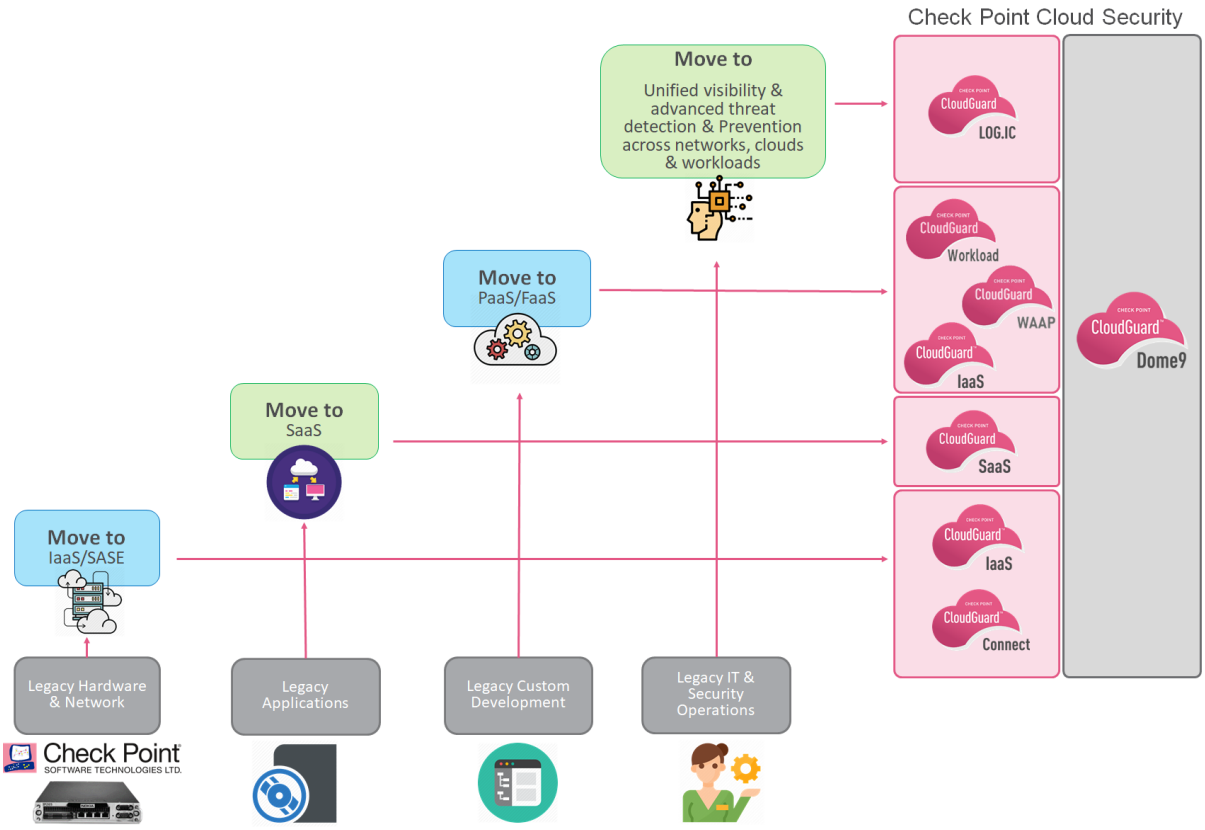


Figure 17: *How different security components are migrated to the cloud*

Cloud transformation involves more than just data centre and workload migration; it includes aspects such as SD-WAN and adoption of network-based SASE solutions. As part of the transformation process it is important to have a firm grasp of what form the exiting security control will, if any, take in the cloud.

Depending on what is being hosted and the DevSecOps-readiness of the organization we would anticipate a “where it make sense” approach to the uptake of cloud native services such as containers and serverless.

One of the key security challenges that we often face as part of cloud transformation is how to manage security when adopting cloud native services and cloud native working practices such as micro-services and DevSecOps.

In the following section we will look at this topic in more detail and explore some of Check Points approach to securing cloud native workloads.

Cloud Native Security

Cloud-native applications use containers/K8s, micro services, serverless functions, and code. They represent infrastructure native cloud technologies that aim to accelerate software development and enable world-class enterprises to create reliable, easily manageable, transparent applications with dynamic scalability.

DevOps Risks and Challenges

A DevOps approach implements security checks at the final stages of the software development lifecycle, while the DevSecOps concept automates all security checks, codifying them in unit tests and using them from the very beginning of software development, on each and every stage of the CI/CD pipeline.

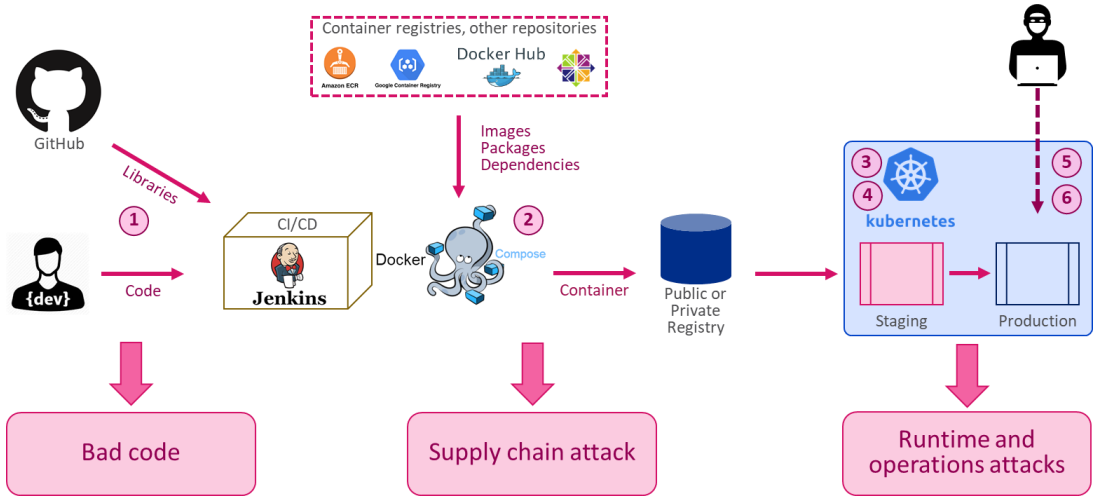


Figure 20: *Various risks attributable to CI/CD pipeline development process*

Some of the most common security challenges and risks are;

- Company software developers can write code containing vulnerabilities. They can use external libraries (for example, downloaded from GitHub), which brings additional risk (poor code quality or even specially crafted backdoors).
- Containers built on top of images from public registries and added packages from public repositories. They can be compromised intentionally and replaced by hackers after they hack the registry (for example 190K accounts on the Docker Hub were compromised in 2019, images may have been tampered with). The use of repositories (RPM's and other dependencies) may not be safe either.
- Improper environment configuration (file permissions, access rights, etc.) could have a serious negative impact. There are many benchmarks (for example the CIS Kubernetes Benchmark) that provide lists of hundreds of items to check, which is often too difficult to be done manually on a regular basis.
- The environment could have its own vulnerabilities (multiple CVEs for Docker, Kubernetes and plugins like "execute code", "bypass something", and "gain privilege").
- Ephemerality on the containers (start/ stop/ create/ delete/ change IP) makes traditional IP-based firewall policies useless.

Cloud-Native Application Protection Platform (CNAPP)

The concept of a single cloud-native security platform or, as Gartner describes, a Cloud-native application protection platform (CNAPP), is the combination of the cloud workload protection (CWPP) and cloud posture management (CSPM) into a single platform.

This approach aligns with Check Point's vision of a single over-arching security platform in, and on which, all cloud native security functions are built. The infographic below shows this approach whereby Check Point Cloud Guard Dome9 becomes the CNAPP.

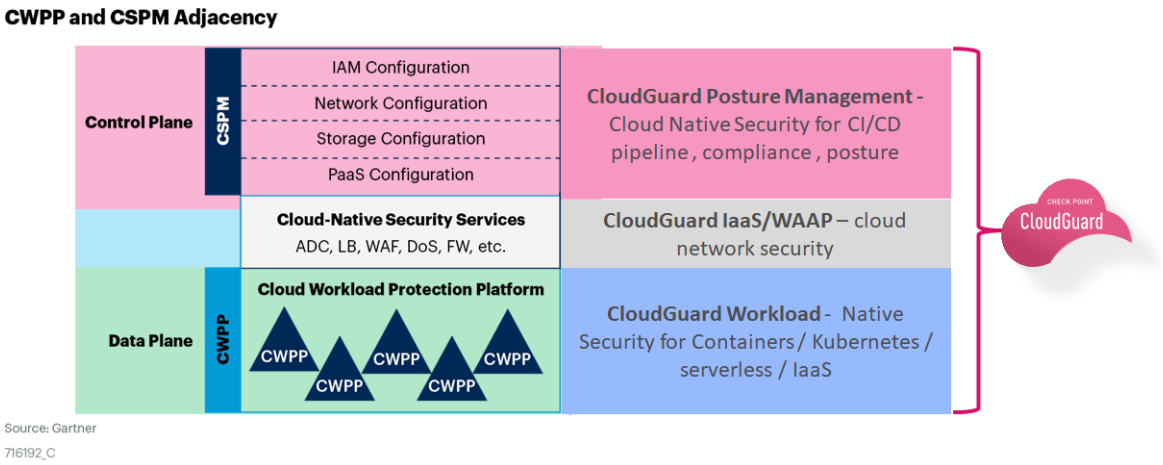


Figure 18: *The cloud-native application protection platform*

Cloud Native Security for Serverless

Serverless functions represent a growing component of an organizations' cloud native technology mix but are, at the time of writing, the most ephemeral in terms of security, maintaining the correct level of security around their use is a key concern for all security teams who need to be fully aware of the security requirements and implications.

The infographic below shows Check Points approach to serverless security whereby the security is done using a combination of posture management and workload protection at various stages of the development and runtime.

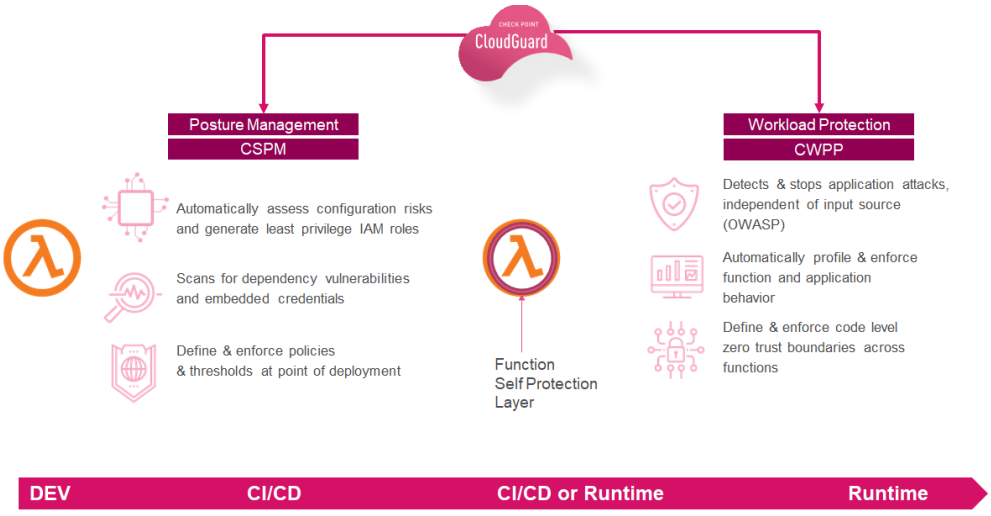


Figure 19: *Check Point serverless security*

Check Point Cloud Native Security

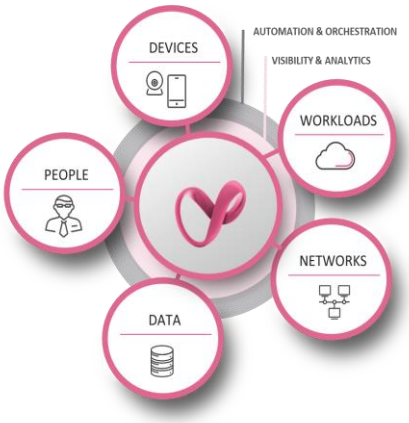
Check Point enables DevSecOps to incorporate cloud native security and compliance into how they build, deploy, and run applications, without sacrificing agility. With the added power of Check Point's automated DevSecOps tools, teams can not only test, but they can also enforce security policies and prevent threats. The following are four ways in which DevSecOps teams can automate security and strengthen their applications with Check Point.

Check Point Cloud Native Security	Cloud Security Posture Management	**CloudGuard Dome9**	Continuous analysis of multi cloud security posture from CI/CD to Production. Prevents configuration errors (CIS Kubernetes and other benchmarks).
	IaaS Security	**CloudGuard IaaS**	Delivers automated and elastic security for your cloud networks in order to keep assets and data protected, while meeting the dynamic needs of your cloud environment. Supports cloud and k8s aware policies
	Web Application and API Protection	**CloudGuard WAAP**	WAF and REST API protection; bot mitigation.
	Container and Serverless Security	**CloudGuard Workload**	Secures serverless applications (in Java, Node.js, Python, C#, etc.). Multi-layer security, leveraging machine learning to profile and protect workloads. Enforce granular security policies during CI/CD and production
	Cloud Intelligence & Threat Hunting	**CloudGuard Log.ic**	Log analysis; detects suspicious and dangerous patterns in the network and other activities; forensics and incident investigation; mitigation using CloudBots.

Zero Trust Modelling

Based on Check Point's experience of cloud transformation and feedback from customers, Zero Trust is high on the agenda as a guiding architectural principle that must be considered. A seismic shift of workloads to the cloud means that Zero Trust architecture can become a reality for users and workloads.

According to Forrester's Zero Trust Extended, to achieve full Zero Trust, we need to focus on the protection of data by following the five layers of protection:



- **The Data:** the core of the business
- **The Workloads:** that process and transform data into information
- **The Networks:** that transport the data and information using end-to-end encryption mechanisms
- **The Devices:** endpoints or IoT devices that upload or access data
- **The People:** that consume information using applications

In order to achieve this goal, the process should start with the analysis of all the applications and their relationships. Emphasis should be placed on creating an 'assets and applications' inventory that should be grouped into classes based on complexity, dependencies, data classification and interdependencies.

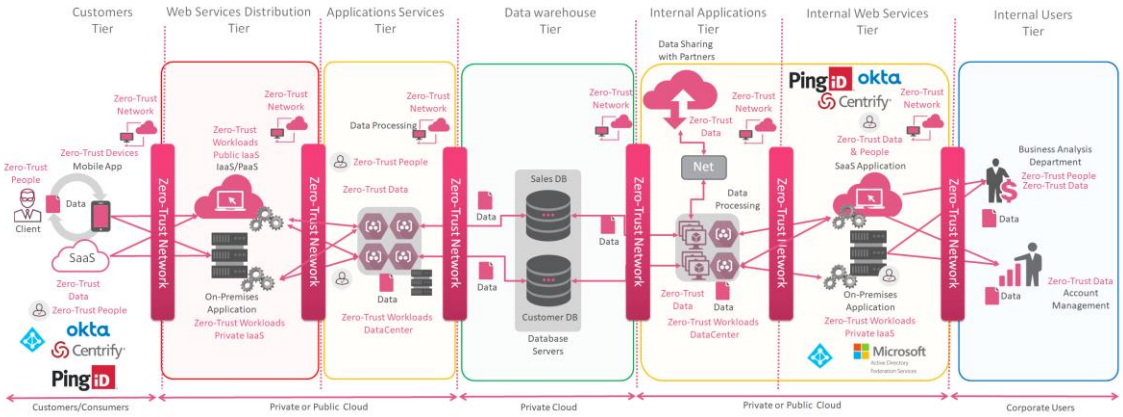


Figure 22: *An enterprise-wide Zero-Trust architecture*

Completing this analysis will provide macro and micro segmentation planning and define security access roles, and assets security classification to create Zero-Trust based policies.

The analysis should consider the following:

- The real business context, i.e. what role does technology play in the business
- Data has to be transformed and structured to have business meaning and relevance through intelligent analysis and synthesis
- Raw facts and quantities that form the inputs and outputs of all business processes, and are processed and stored during process execution
- Data classification, which is defined as the process of organizing data in different and relevant categories to be used and protected more efficiently. Also, it is an essential component for risk management, compliance, and data security

- Data flows related to stream processing or reactive programming to which all business processes are related

Secure Cloud IaaS; Public and Private

Our approach to Zero Trust is based on being able to build solutions that can adapt dynamically to workload changes, are able to ingest tag information from the service account or the enterprise's platform, and are able to build micro-perimeters and micro-segments.

Protecting Public Cloud Workload (IaaS)

Check Point's CloudGuard IaaS and CloudGuard Dome 9, secure workloads for seamless integration with public or private cloud infrastructure.

They provide **micro-segmentation** within the virtual fabric with full visibility and control of North-South and East-West traffic; including AWS, Microsoft Azure, NSX, etc.

Protecting Private Cloud Workload (IaaS)

For **Check Point VMware NSX-T security** integration, please refer to the following best practices document:

https://www.checkpoint.com/downloads/products/check-point-cloudguard-iaas-for-vmware-nsx-v-and-nsx-t.pdf

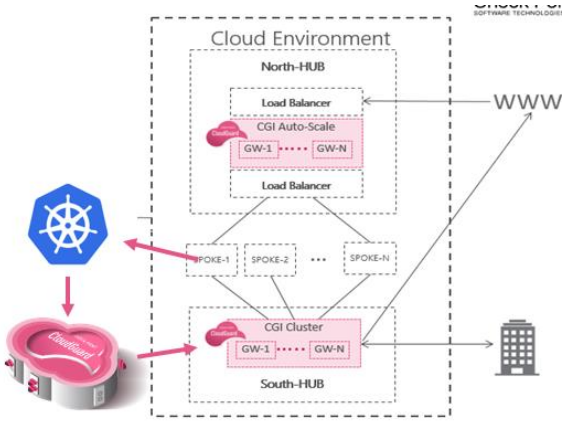


Figure 23: *Integration with the K8 orchestrator to provide micro-segmentation*

Cloud Security Management

Deploying architectural models such as Zero Trust in the cloud is made a lot easier if cloud security controls and technologies can seamlessly integrate with any cloud infrastructure and provide full visibility and control over these ever-changing environments. This includes a variety of cloud environments such as: AWS, GCP, Microsoft Azure, Oracle Cloud, IBM Cloud, Alibaba Cloud, NSX, Cisco ACI, Cisco ISE, OpenStack, etc.

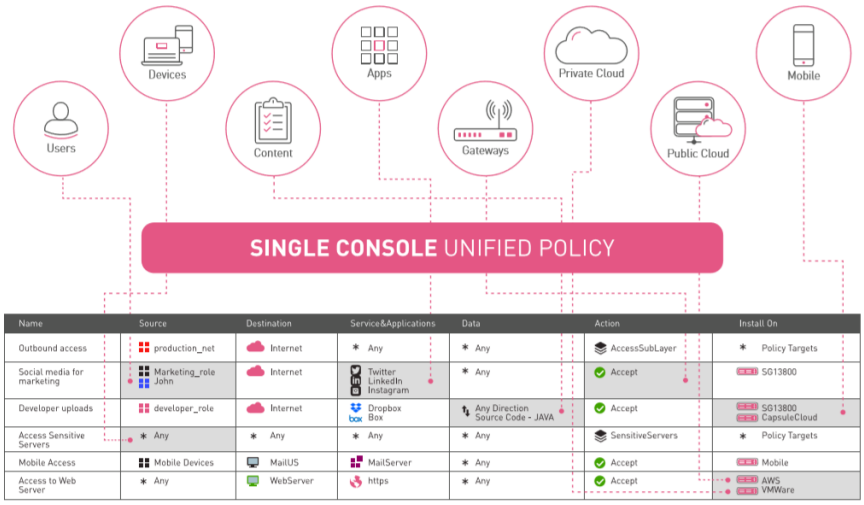
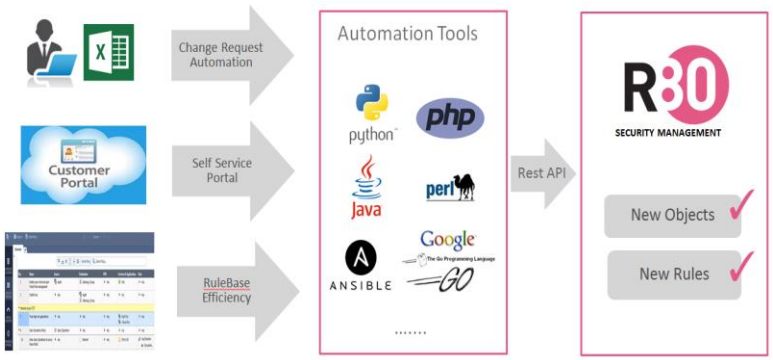


Figure 24: *The Check Point console showing identity as a key component of the security*

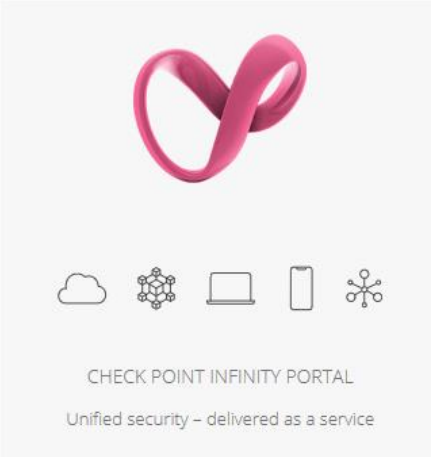


As organisations move to the cloud, we believe enterprises will adopt an integrated security managed architecture that incorporates a security ecosystem driven through APIs. Enterprises will use service chains built on APIs from Check Point and other vendors to drive efficiencies in security management and deployment. This example shows how changes to a security policy can be done by a number of mechanisms.

Check Point Infinity Portal

The adoption of cloud technology is also very relevant to how organizations manage their security posture; especially when considering the requirements for managed endpoints. Clearly when the majority of user endpoints sit outside the traditional campus network then it make more sense to manage these from a cloud-based platform.

SASE security concepts lend themselves to a cloud-centric approach to management.



Check Point Infinity Portal is the Check Point cloud web-based management platform for hosting the Check Point Security-as-a-Service (SaaS) services, such as CloudGuard, MaaS and Mobile Security.

TRANSFORMING CLOUD SECURITY WITH CHECK POINT

Check Point understands that cloud transformation is a complex undertaking, and knows the value our customers place in our architectural workshops. Because of this, Check Point now offers a Cloud Transformation Security Consultancy service designed specifically around cloud transformation.

The service is based on the core principles defined in the Check Point Enterprise Security Framework (CESF).

The Check Point Enterprise Security Framework is built around the architectural methodology of SABSA, and the design principles of Zero Trust. The CESF allows Check Point to translate business requirements into practical security solutions.

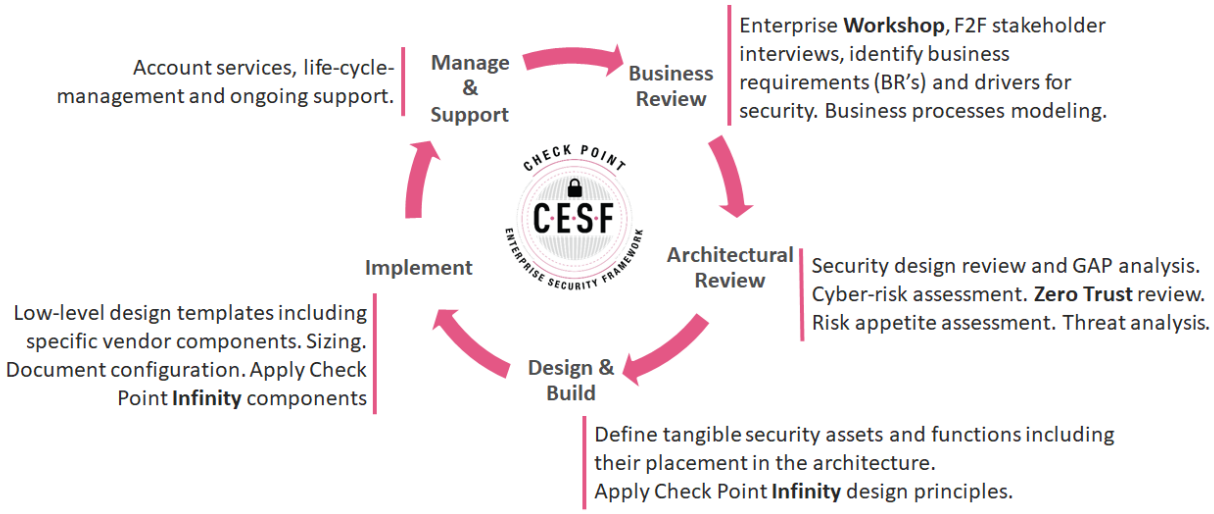


Figure 29: *Check Point Enterprise Security Framework for enterprise architecture*

Cloud Transformation Workshop

The security cloud transformation workshop - this is a focused, single-day meeting between the client and Check Point architects to openly discuss, review, and capture all aspects of the existing, and future, security ecosystem of your business.

The process begins with a series of interviews with key stakeholders and moves into a detailed review of the current and future security posture and network topology. A key component of the workshop is to fully understand the drivers and the challenges to cloud transformation, starting from the business perspective and then the technology perspective.

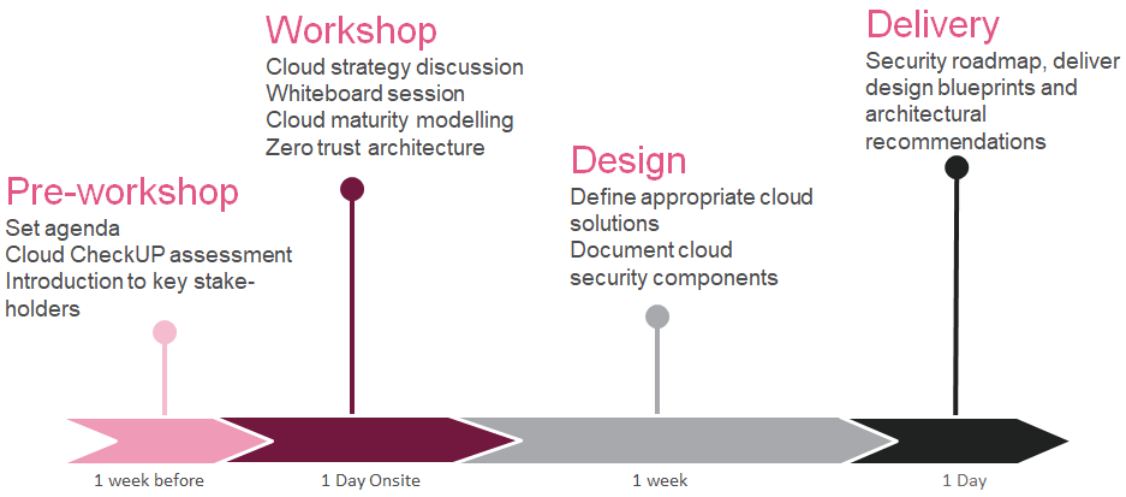


Figure 27: *The stages of a CESF cloud transformation workshop*

Reporting

We believe this process is an effective means of communicating a long-term vision for better security architecture. In order for this message to be accurately delivered, the workshop process culminates in a bespoke report that outlines the key design concepts and recommendations. Upon completion, we will deliver an architectural report that includes a customized transformation blueprint and recommendations that we align to your business objectives.

Digital and cloud transformation requires careful planning and a long-term vision. It is not enough to choose a collection of cloud technologies without having a solid understanding of the why, what, and how they will be used. From experience, it is known that enterprises see value in a more structured approach, which is why Check Point have developed a unique enterprise security framework.

A Process-Driven Approach to Security Architecture

The digital future is challenged by existing long-held operational models and established fundamental business processes. Check Point believes to navigate these, organizations should adopt a structured, methodological approach that translates defined business requirements into strategic security solutions.

To help tackle these challenges, Check Point have developed an enterprise security framework capable of managing the process of transformation, end-to-end.

CONCLUSION

Cloud transformation is in every enterprise's pipeline. However, it can easily disrupt day-to-day business.

Check Point understands the complexity of these architectural engagements and has therefore derived best practice strategies and approaches. Check Point's vision for this paper was to present an approach to cloud transformation, from conception to completion, based on the real-world experiences of our customers' transitions to the cloud.

The 'phases and transitions approach' acknowledges that enterprises don't arrive at their target architecture overnight, and that successful transition to the cloud requires careful planning and a long-term vision. We hope that this paper has provided you with an honest approach to planning, designing, and implementing the transition, and has helped to reduce your design cycles, as well as the eventual overall cost of your cloud transformation.

APPENDIX

EXAMPLE: ECOMMERCE SECURITY MODELING

This is a working example of a secure digital transformation:

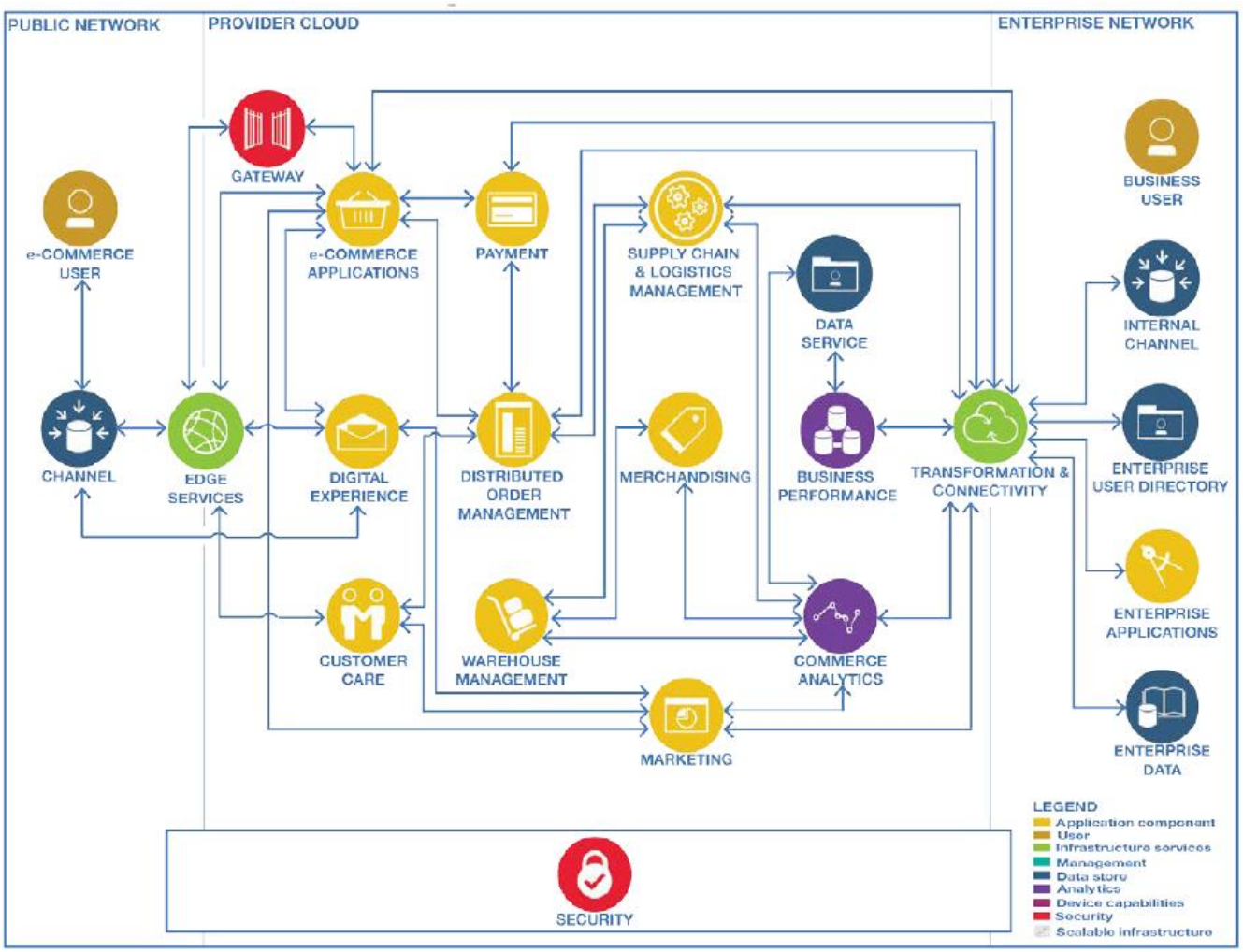


Figure 31: *Example of a cloud solution template that we will use in this example*

In the following example, we demonstrate how the CESF process delivers complete enterprise security solutions. The example describes a typical case of an enterprise adopting eCommerce for their business and then needing to move some components from the on-premise data centre to computing instances in the cloud.

We will use the reference architecture documented by The Cloud Standards Customer Council for eCommerce[4] use case as a guideline in the analysis, and help to put all the different elements together in a secure way using the hybrid cloud model.

According to the Cloud Standards Customer Council for eCommerce use-case, “The public network domain contains commerce users and their eCommerce channel for interaction with the enterprise. The public network also includes communication with peer clouds. The edge services handle traffic between the pubic network and the cloud.”

CHECK POINT ENTERPRISE SECURITY FRAMEWORK		
CESF Review & Architecture Layer	**Title**	<<ACME>> Public IaaS/PaaS for eCommerce Services
	Business Requirements (BR)	Enable eCommerce services, improving time-to-market requirements, deploying public and private cloud IaaS/PaaS, doing a combination of public cloud data centre with Microsoft Azure and Red Hat Openshift data centre.
	Check Point Analysis	Data and information in the cloud are exposed to the same threats as traditional infrastructures; however, due to a large amount of data processed in cloud computing, data leaks can lead to a chain of unfortunate events for IT companies and infrastructure as a service (IaaS). • **External Exposure –** Cloud services are typically accessed from any location and any device. All that’s needed is an Internet connection. While ease of access can boost company agility, services running in the cloud versus those on premise are just as likely to be breached. Furthermore, since cloud and internal physical networks are frequently tightly integrated, a breach on either network will likely affect both systems. • **Restricting Security to Native Cloud Tools –** Typically, cloud providers offer an extensive range of security solutions and services that are natively bundled with their systems. While many of these tools are very capable, they do not address the entire range of attacks and vulnerabilities found in today’s information systems. This sometimes leads to a false sense of security and leaves cloud systems under-protected. Cloud services are vulnerable across three principal attack vectors: • **Account Hijacks –** Gaining unauthorized access to an individual’s or organization’s email or computer account, for malicious purposes. In a Check Point survey, account hijacks were the most significant concern amongst customers and partners. • **Malware Delivery –** Propagation, primarily through in-app file-sharing services, such as Box or One Drive cloud apps, to commit a variety of cybercrimes. • **Data Leaks –** Whether intentionally or unintentionally, data leakage occurs with the seamlessness of sharing information with cloud services. • **Code Vulnerabilities –** Public applications hosted in the cloud are by their very nature accessible to everyone. This access allows for attacks that target known and unknown vulnerabilities, which form part of the code or underlying operating system.
	Business Drivers for Security (BDS)	The attack surface changes when workloads are moved to the cloud. These are some of the vectors likely to be exploited that should therefore be protected vigilantly.

[4] Cloud Customer Architecture for eCommerce , URL: https://www.omg.org/cloud/deliverables/cloud-customer-architecture-for-ecommerce.htm

	Risk Statements
Business Drivers for Security (BDS) (Continuation)	**Risk:** Lack of visibility inside a VNET/VPC can allow breached systems or misconfigurations to remain undiscovered. Even if visibility exists, it must be monitored by a human or an automated system. **Risk:** Lack of proper identity management in the public cloud IaaS (such as granting too much access or permitting too little access) can lead to breaches or service interruptions. **Risk:** Lack of lateral protections could allow intruders (that gain access to one internal system), to propagate their level of access laterally throughout the unmonitored sections of the internal network and remain undetected for long periods. **Risk:** Lack of visibility inside encrypted communications can render deep inspection systems ineffective and allow intruders to move undetected inside of the network. Over 80% of breaches in the last few years were utilizing encrypted protocols for communication. **Risk:** Time constraints and hasty learning curves can lead to mistakes in the configurations of topologies, security systems and workloads. This makes posture analysis and configuration control essential to reduce accidental or malicious misconfigurations. **Risk:** Zero-day attacks embedded in data files. If you host VDI users in the cloud, or if your public applications accept document uploads (i.e. resumes, documentation for loans, proposals, photos, etc.) your ingress traffic could include files infected with zero-day malware. WAFs generally do not inspect payloads for infection. **Risk:** Lack of threat analysis on API traffic can allow attacks against the cloud control plane. **Risk:** No visibility into Bastion Host traffic and activities. Bastion hosts usually have admin access levels, and actions performed by users connected to a Bastion host are not always tracked. **Risk:** Lack of capability to block certain file types from moving internally between restricted cloud zones (i.e. moving documents containing credit card information to another section of the cloud that may not be fully PCI compliant). **Risk:** Lack of threat analysis on serverless traffic, which can lead to embedded commands that include attacks or be used to leverage other vulnerabilities. **Risk:** Lack of log and workload analysis can allow attacks or breaches that managed to elude or bypass network security and remain undetected. **Risk:** Egress traffic should be URL filtered and analysed for Bot C&C traffic to prevent outbound traffic from connecting to malicious sites.
Attributes[5]	Accessible, Reliable, Cost-Effective, Elastic, Agile, Access-controlled, Accountable, Authenticated, Authorized, Identified, Adaptable, Scalable, Enables Time-to-Market

Figure 12: *Example of an end-to-end solution architecture*

[5] According to the Security Business attributes described in the ANDRITZ Financial Report 2019 - https://www.andritz.com/resource/blob/340670/5bb77db191467e3f3eabd0322a70582d/andritz-annual-financial-report-2019-data.zip

DESIGN, CONTROLS & SERVICE RECOMMENDATIONS

CESF Design & Build Layer

Logical Design	Build Security Components & Services

• Security segmentation and visibility are highly relevant to the business requirements and must feature in the cloud security architecture
• It is essential to complete VPC/VNET segmentation that defines a web tier, business logic tier and data-tier.
• Design must include cloud Configuration management and identity management.
• Keep and maintain the same security level and posture in the cloud and data center using the unified security approach.
  ○ Network: Reduce risk of lateral movement with micro-perimeters and identity-based policies.
  ○ Workloads: Secure data and applications in public clouds and data centres
  ○ Data: Keep data safe, anywhere, with comprehensive multi-layered security architecture
  ○ Visibility and Analytics: Full threat visibility with single view into security risks.
  ○ Automation and Orchestration: Automate all processes and tasks using flexible APIs and rich 3rd party integrations.
	Network Security
	• CloudGuard IaaS for Public Cloud
	• Microsoft Azure
	• Security hubs for macro-segments:
	  ○ Inbound Hub
	  ○ E-W Traffic Hub
	  ○ Outbound Hub
	  ○ VPN Hub
	CloudGuard IaaS for Private Cloud
	• NSX-T 2.5
	• Express Route or VPN IPSec
	• Security Gateways with R80.x
	Cloud Workload Protection Platforms
	• CloudGuard WAAP
	• CloudGuard Workload
	• SourceGuard (For CI/CD)
	Cloud Posture Security Management
	• CloudGuard Dome9 for Azure and Kubernetes On-Premise
	• CloudGuard Log.IC

Figure 22: *Example of an end-to-end solution architecture*

In this analysis, we can see advanced access control and threat prevention for enterprise networks in public and private clouds, native security, compliance across the public cloud, the prevention of targeted attacks on SaaS applications and cloud-based email.

Whether a business strategy centres on cloud-enabling applications and platforms, public and hybrid infrastructure or a multi-cloud approach, CloudGuard ensures all assets are fully protected, while supporting the flexible, dynamic, and cost effective nature of the cloud.

By analysing this use case, an architecture can be built using the Check Point CloudGuard portfolio, which integrates several components to create a secure eCommerce site.

The diagram below is the result of the analysis above. The requirements have been developed into a working design blueprint that can now be moved to an implementation stage.

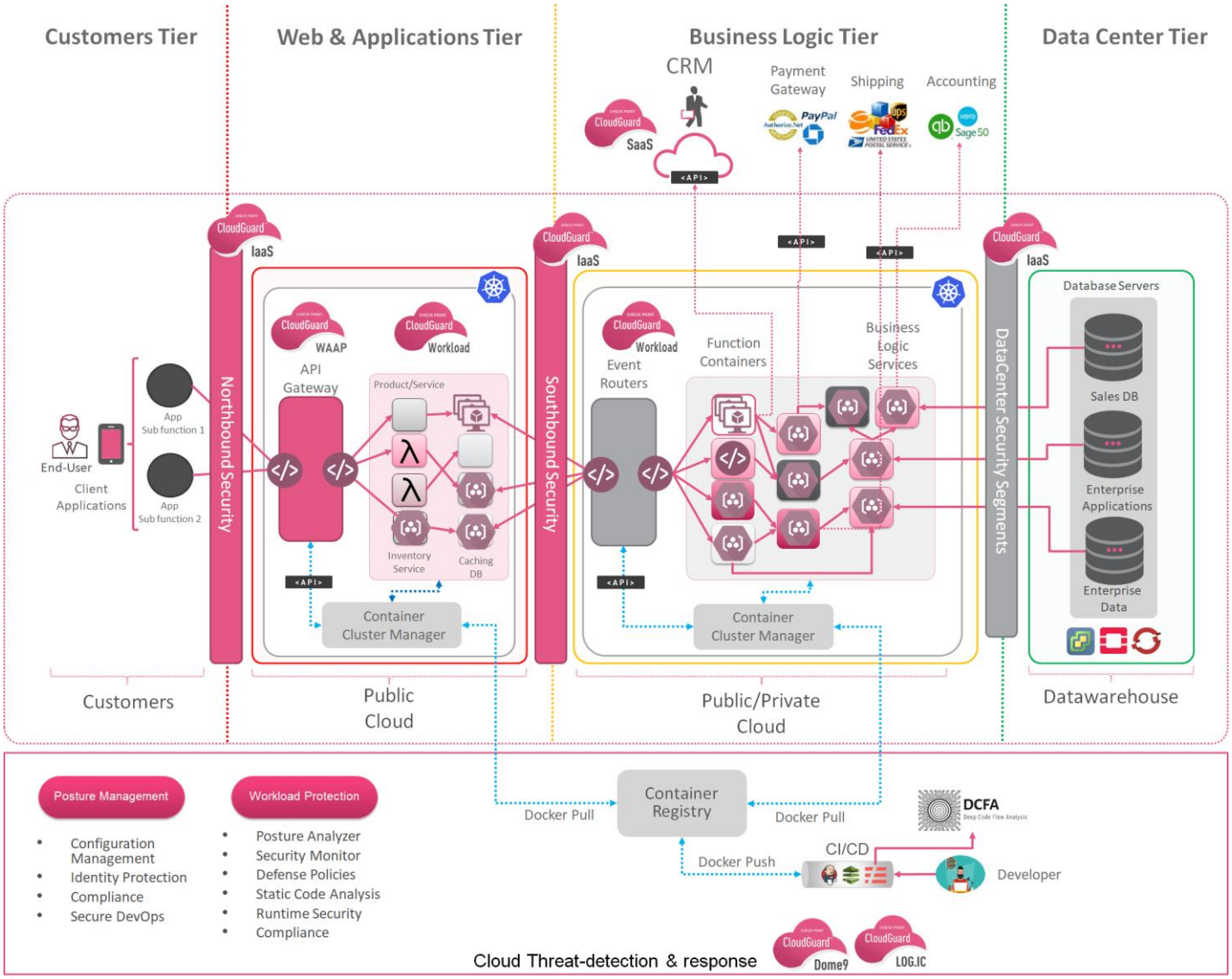


Figure 32: *eCommerce use-case secured by the CloudGuard portfolio*

CONTACT US

Worldwide Headquarters | 5 Shlomo Kaplan Street, Tel Aviv 67897, Israel | Tel: 972-3-753-4555 | Fax: 972-3-624-1100 | Email: info@checkpoint.com **U.S. Headquarters** | 959 Skyway Road, Suite 300, San Carlos, CA 94070 | Tel: 800-429-4391; 650-628-2117 | Fax: 650-654-4233 | www.checkpoint.com