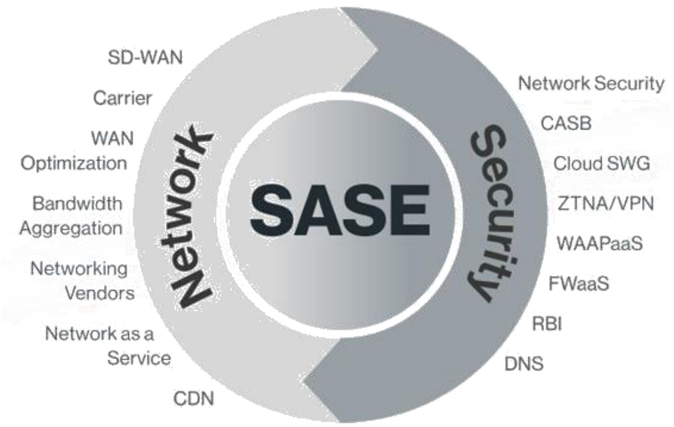
Cloud Transformation Security Consultancy

The Cloud Transformation Journey

Cloud transformation is all around us. For security professionals, it's a defining statement of our time, shaping the cyber security landscape. Nevertheless, cloud transformation is complex and challenging, with long-held operational models and fundamental business processes.

Today, organizations are looking towards a future where all workloads are in the cloud and where networks and users exist in a secure access secure edge (SASE) architecture. At Check Point we aim to extend architectural assistance to organisations to support their development a proper strategy for this journey.



> "By 2024, at least 40% of enterprises will have security strategies that will require the SASE model. The concept is to create and provide a secure cloud environment that is fully integrated into one's network."
>
> Gartner, 2019

A good cloud transformation strategy should enable decision makers, and allow enterprise architects to navigating the challenges of defining and executing their cloud strategy.

In this paper we will highlight some of the common security challenges that our enterprise architecture teams encounter as part of our cloud transformation engagements, and through our cloud transformation workshops.

Cloud Business Drivers

There are many reasons for organizations to adopt a cloud transformation project or strategy.

Check Point has defined the following as some of the key business drivers for cloud adoption:

Business Expansion	Operations	Security
Competitive advantage • Moving to the cloud offers improved business agility **Flexibility and availability** • Automatic software updates in the cloud • Cloud service providers have a worldwide presence • Availability of new services	• Branch offices and homeworking are increasing quickly • Some applications are better suited to cloud deployment e.g. mobile apps • Single vendor architecture • Pay as you grow model/ cost reduction according to the business needs • Operational efforts decrease in the cloud vs. traditional IT	• Quick disaster recovery • Unified management • Zero Trust alignment • Controlled access • Frequent auditing • Physical security

The Cloud Transformation Challenge

Transitioning security from an infrastructure-driven approach to a cloud and workload-centric approach is a considerable challenge. Organizations must find the correct cloud security technologies to fit their business needs, and address the following challenges during the cloud transformation process:

- Cloud means a new approach to operations and administration. This can lead to misconfiguration that impacts the overall security posture, and can lead to cyber breaches.
- On the one hand, a significant shift in the security shared responsibility model reduces operational efforts from the security team, however, on the other hand, it requires a proper trust model between the customer and the cloud provider be defined.
- Cloud security architecture is conceptually different from traditional IT security architecture.
- New application development technologies, such as DevOps, are based on the containers and Kubernetes that require a complete rethink and different approach to security. Conversely, common security controls, like firewalls, won't be effective and sometimes may not even be applicable.
- Security teams must be knowledgeable enough to face new cloud technology implementations and align with cloud IT and development teams.

Cloud Transformation Principles

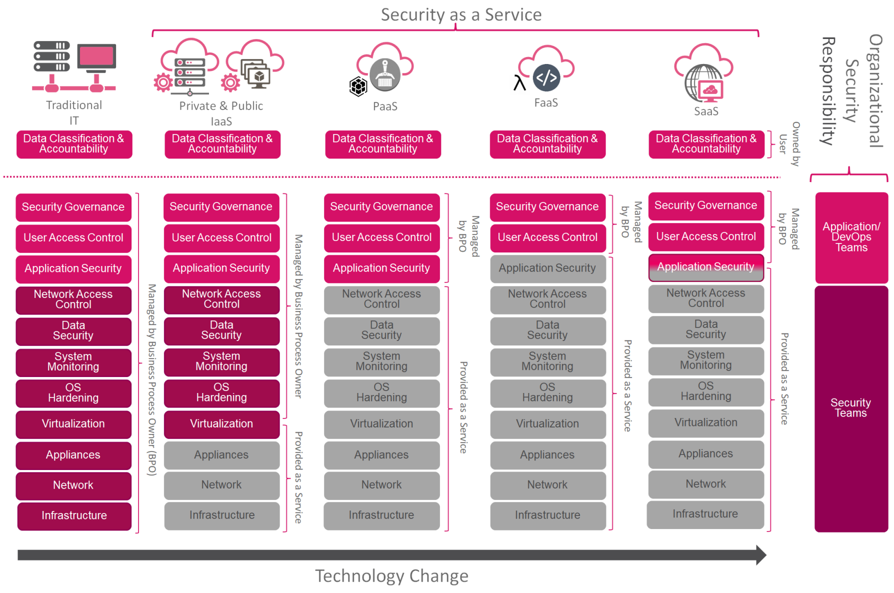
In order to help organizations with their transformation journey, we have created a set of transformation principles to inform and help shape this process. These high-level architectural principles form the foundation of our *"Cloud Transformation Workshops"* and are designed to support the planning and execution of a cloud transformation strategy.

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

- Analysis of business security drivers.
- Assessment of existing cloud maturity, and a security controls review.
- Mapping of legacy infrastructure to cloud-native controls (DevOps, APIs, Containers, etc.).
- Using Zero Trust security modeling and architecture.
- Appreciation of cloud security operations and management.

Shared Responsibility

In traditional IT environments, the organization owns the whole stack; however, in the cloud, some responsibilities are transferred to cloud service providers.

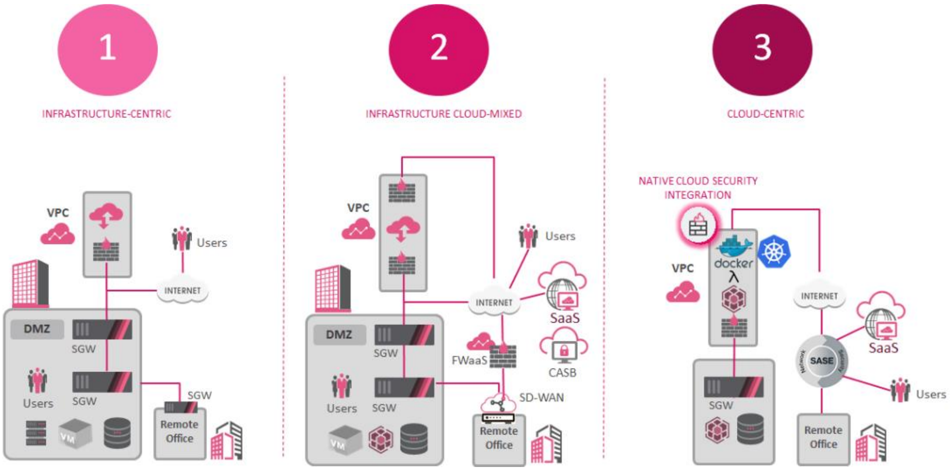


We predict that, at some point, all enterprises will leverage most currently available cloud platforms, including the public IaaS, PaaS, FaaS and SaaS. The challenge is that all these platforms have different operational benefits, shared responsibilities, and security challenges.

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 that the cloud provider has secured, monitored, and appropriately configured the environment.

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

Cloud Maturity



Check Point’s cloud transformation principles help organizations design their move to the cloud. However, it is also important that organizations have a vision of the transformed end-state architecture.

It is not enough to start a cloud transformation journey without knowing where it is leads. A clearly defined strategy and vision are important and cannot be underestimated.

In order to help organizations visualize this end-state architecture, Check Point has developed the following phases, each one describing a step in the cloud transformation journey:

Phase 1 - Infrastructure-Centric
Phase 2 - Infrastructure-Cloud Mixed
Phase 3 - Full Cloud-Centric Security Architecture

Cloud-Centric Security as a Service Architecture

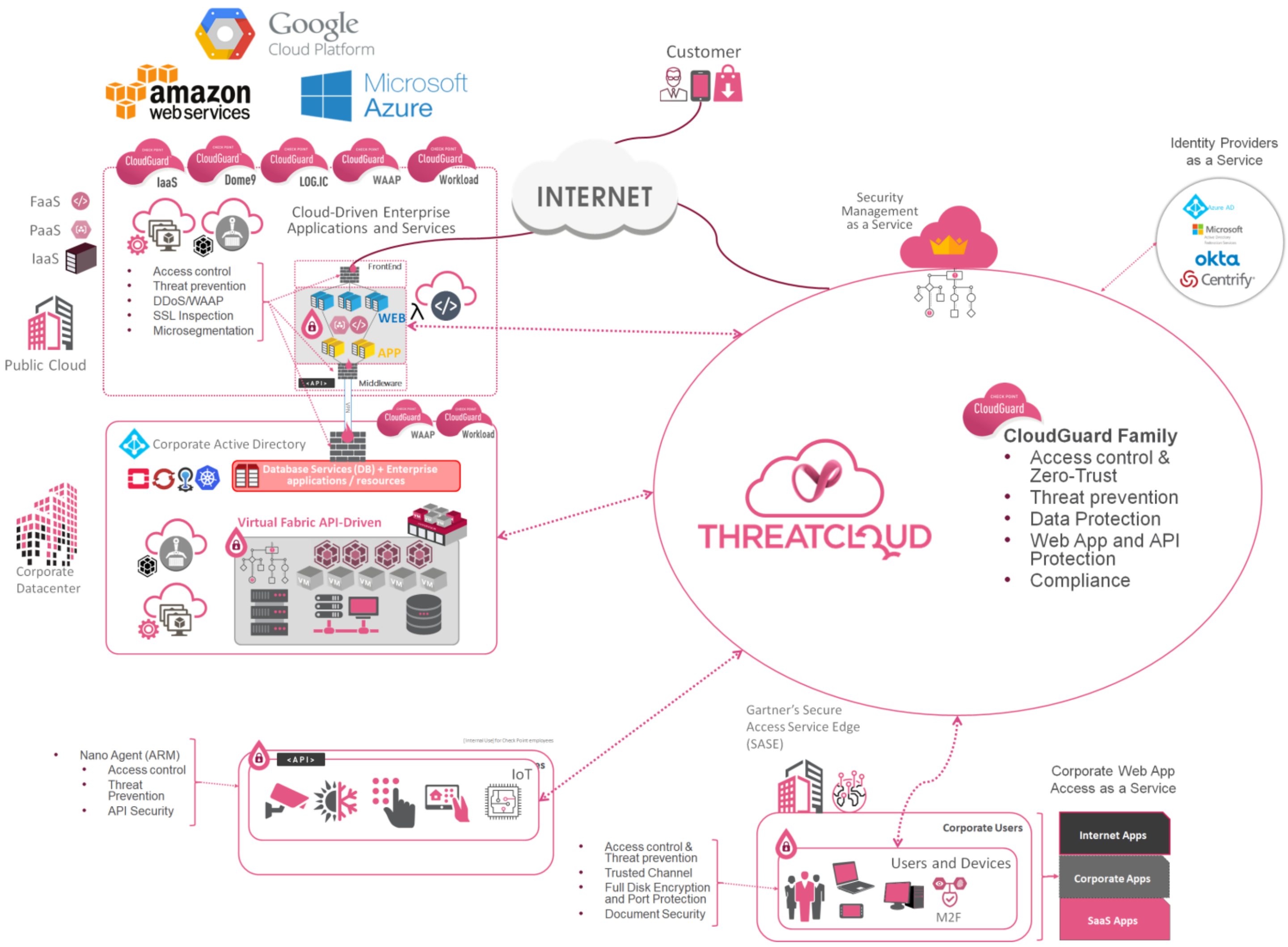
As previosuly stated we believe that all orginzations are on a trajectory towards full SASE architecture. SASE architectural principles describe a set of network security functions and security capabilities defined by Gartner[1]. Check Point’s vision is to leverage this approach in our third phase, which is a full cloud-centric driven approach where the majority of security components are represented “as-a-Service”.

Organization adopting SASE architecture display the following characteristics:

- Minimizing the amount of hardware security appliances on-site
- Understand that the majority of corporate resources are SaaS platforms or hosted in the cloud where they are accessed by remote branches, users, and IoT
- Specifying the few resources remaining in the on premise data center; mostly legacy applications that cannot be virtualized
- Identifying that the majority of workloads have been virtualized to instances in the public cloud, containers, or serverless functions

[1] https://blogs.gartner.com/andrew-lerner/2019/12/23/say-hello-sase-secure-access-service-edge/

- Acknowledging that cloud security is natively integrated with cloud application technologies (e.g. containers, Kubernetes, etc.)
- Highlighting that the data center is no longer the core of the organization; neither is it the place where the Internet egress point is located
- Noting that access to applications is achieved at the application edge, i.e. via API integration.



To learn more about the Cloud Transformation phases and the Check Point approach, please review our **Cloud Transformation Whitepaper** paper located at https://www.checkpoint.com/architecture/best-practices/.

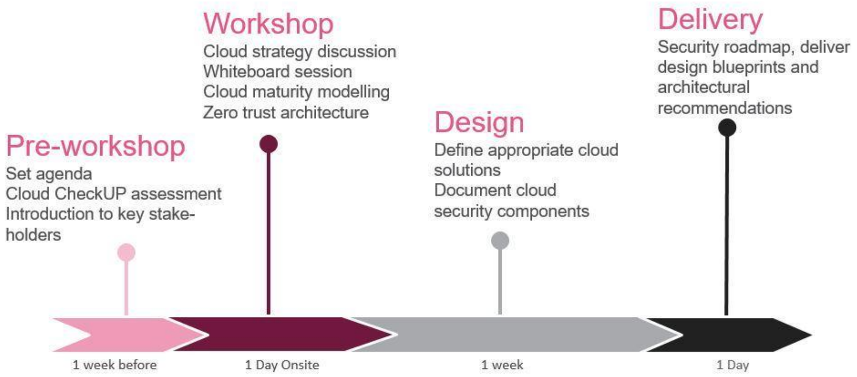
Cloud Transformation Workshops

From experience, we know that organizations value a structured approach to security architecture and want to plan their cloud transformation initiatives carefully.

In order to meet this requirement, Check Point has developed dedicated Cloud Transformation Workshops that follow proven architectural design principles and focus on delivering cloud transformation blueprints and architecture guidance.

The Cloud Transformation Workshop is a one-day session with a Check Point enterprise architect. The workshop is open-forum and designed to fully understand the cloud vision and strategy.

On completion, we will deliver an architectural report blueprint designed to ensure that all critical assets are protected by the appropriate security controls.


Pre-workshop
Set agenda
Cloud CheckUP assessment
Introduction to key stake-holders
Workshop
Cloud strategy discussion
Whiteboard session
Cloud maturity modelling
Zero trust architecture
Design
Define appropriate cloud solutions
Document cloud security components
Delivery
Security roadmap, deliver design blueprints and architectural recommendations
1 week before
1 Day Onsite
1 week
1 Day

The Check Point architect will deliver a customized cloud transformation report that includes:

- An existing environment review
- Cloud architecture blueprints
- Cloud best-practices
- A recommended solution, including products and services.

For more information about the Cloud Transformation Workshops program, please visit our site at https://www.checkpoint.com/support-services/security-workshop/