Check Point
SOFTWARE TECHNOLOGIES LTD

CHECK POINT ENTERPRISE SECURITY FRAMEWORK (CESF)

A Process-Driven Approach to
Building Enterprise Security Architecture

CHECK POINT
CESF
ENTERPRISE SECURITY FRAMEWORK

Abstract

This Check Point paper outlines a new process-oriented approach to developing enterprise security architecture. It draws from both well-known open frameworks as well as Check Point's rich experience in architectural design and development.

In this paper, we provide you with an overview that includes an architectural process, framework, and methodology. This is not, however, a "how-to" guide. By the time you reach the paper's conclusion, you should have a firm grasp of the various components of the Check Point Enterprise Security Framework (CESF), and how they form the foundation for your next enterprise architecture.

Audience

Architects, engineers, and designers engaged in security architecture will benefit from this paper. As a prerequisite, you should be well versed in network and security design concepts and generic security architectural concepts and frameworks.

TABLE OF CONTENTS

1 Introduction

Check Point has always believed in extending proper, correct, and impartial security advice to our customers, and the value in being trusted as security architectural advisors.

Our commitment to security architecture has resulted in Check Point supporting dedicated teams of security architects focused on advancing our clients' security posture. We designed this consultancy approach to deliver security based on real business requirements, and not just commercial motives.

Check Point has developed this approach into a complete architectural methodology and process framework. With great pride, we're excited to introduce this to a wider audience as the **Check Point Enterprise Security Framework - CESF.**

We know that organizations see value in a structured approach to security architecture, which is why Check Point developed the CESF process. This framework allows any enterprise security team to develop a secure architecture using a formulated, accountable, and comprehensive process.

WHY IS SECURITY ARCHITECTURE NECESSARY?

Before we explain how and why Check Point developed an enterprise security framework, let's discuss briefly, why it's important to understand the role of security architecture within an enterprise. Here are several reasons why you need security architecture:

- Building security without a carefully considered plan is at best complicated, and at worst can lead to a compromised security posture and increase your costs.
- CISOs need a way to communicate cyber risk to an organization's management team:
  — Does the current security posture align with common security standards?
  — Do the existing security controls complement the business needs?
  — Does the existing security infrastructure address all the business risks?
  — How to reduce TCO and operational efforts while enhancing the level of security?
  — How to implement new security innovations to support the wider business?
- Measuring the success of security spend is vital. Good security architecture adds structure to spending decisions and improves accountability.
- Check Point believes that security architecture should have a clear and concise methodology.

CHECK POINT ENTERPRISE SECURITY FRAMEWORK (CESF)

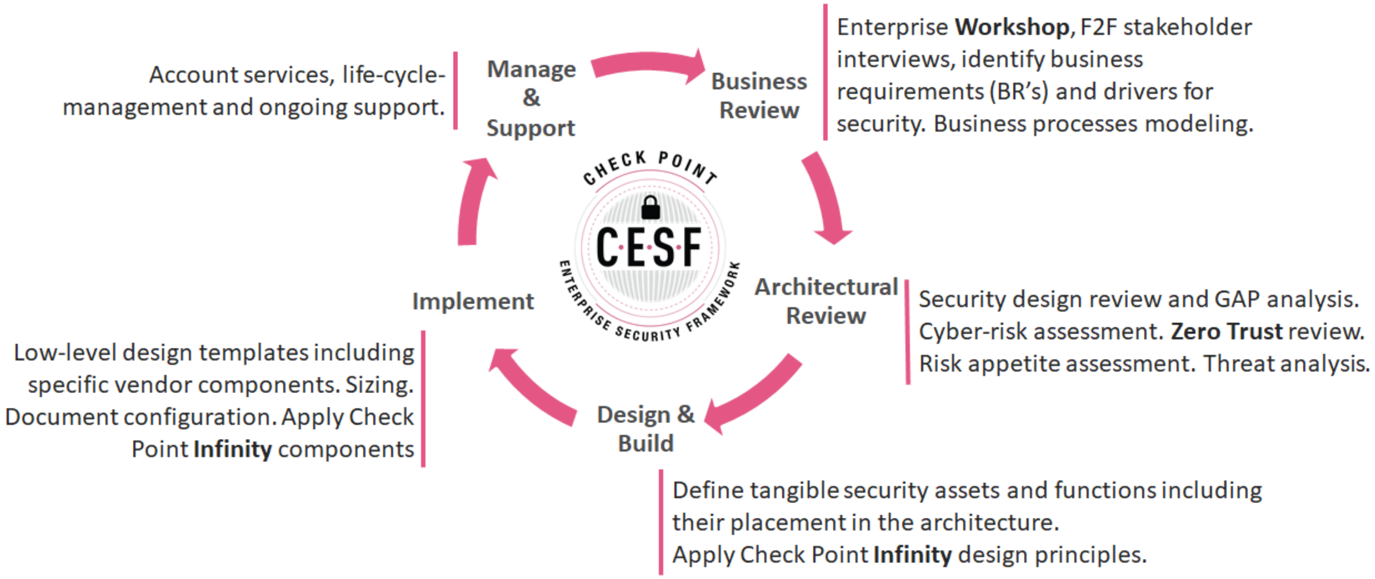
Check Point developed CESF as a customer-centric security framework to help our customers explain, develop, mature their security posture and align with security best practices. Through our process, architects are able to accurately capture and record business requirements and convert these into tangible Check Point solutions and advanced security solutions.

The CESF mission statement is to:

- Meet our customers' requirements for a structured and systematic approach to design, architecture, and digital transformation that results in a tangible implementable solutions.

- Respond to the challenges of transformation by reducing costs through careful design.
- Be a methodology that delivers digital transformation; from concept to the completion of real-world security solutions

The info-graphic below show the end-to-end process.



Enterprise **Workshop**, F2F stakeholder interviews, identify business requirements (BR's) and drivers for security. Business processes modeling.

Security design review and GAP analysis. Cyber-risk assessment. **Zero Trust** review. Risk appetite assessment. Threat analysis.

Define tangible security assets and functions including their placement in the architecture. Apply Check Point **Infinity** design principles.

Low-level design templates including specific vendor components. Sizing. Document configuration. Apply Check Point **Infinity** components

Account services, life-cycle-management and ongoing support.

WHAT CESF MEANS FOR OUR CUSTOMERS

Some key benefits include:

- **Accountability:** Using CESF ensures security spend is accountable and can be traced back to a business requirement.
- **Strategic:** The CESF helps define near, medium, and long-term goals, reducing technology overlap and unnecessary spend. Having a view of a long-term strategy reduces the need for point solutions and helps build a strong, complete, security ecosystem.
- **Complete:** The outcome of using the CESF is a security architecture roadmap and reference architecture, one designed to support the client's business while maturing the overall security posture.
- **Justified:** The CESF delivers a bespoke detailed design blueprint that enables clients to build a complete security ecosystem. Solutions and spend can be justified against measurable requirements. Solutions and spend can also be justified to the board.
- **Independent:** Because it is built and based on open standards, clients have full visibility of the decision making process and how the architectural solution was developed.
- **Professional:** A collaborative approach to developing security architecture brings Check Point and client architects into a closer working relationship.

CESF AS A PROCESS

We can explain the CESF process as a logical methodology that consists of a collection of phases. Each phase has a specific function and output. The combination of these phases allows us to deliver security architecture in a manner that is accountable, and fully documented. Expressing the CESF as series of linked phases helps simplify the process and means we can use different resources at different points of engagement.

The phases are:

- **Review and Architecture:** This phase of the process is for business and architecture reviews as part of a CESF workshop. This phase is for data-capture, business modelling and risk assessments.
- **Design and Build:** This phase is for CESF architects to develop a response to the requirements and to build customized logical design blueprints and recommendations.
- **Implementation:** This phase is for professional services, partners, etc. to add low-level design details and deliver statement-of-works for real-world solutions.
- **Service Management:** This phase is for continuous development and improvement of the security posture.

CESF FUNDAMENTALS

Before we look into the CESF process, it is important to understand the key components and drivers that have influenced its development; namely SABSA (Sherwood Applied Business Security Architecture) and Zero Trust.

SABSA is widely used outside of network or cyber security requirements to develop business-driven solutions and Zero Trust has become a mainstay of enterprise architecture. Both of these open frameworks are widely used and respected by the security industry for their approach and relevance. They are by their nature, both broad and, relevant to all disciplines of security.

Check Point's deep understanding these subjects has influenced and shaped the development of the CESF process:

- The CESF process has re-interpreted and reformatted these two key influences so that the CESF process is focused on delivering a holistic network and cyber security architecture relevant to our clients.
- The Check Point CESF process combines the best parts of these existing open frameworks with our world-class understanding of security, its design, implementation, development, and support.
- The CESF process is designed to deliver realistic, real-word security architecture and must result in blueprints and recommendations that are actionable and achievable.

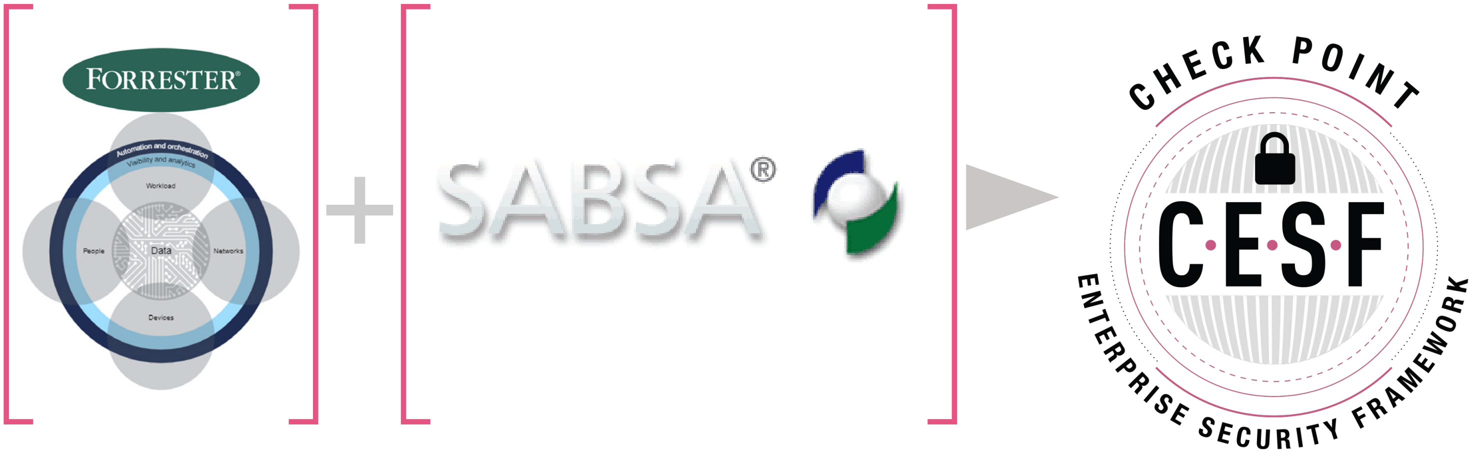


***Figure 2**: The key influences*

2 Frameworks

OVERVIEW

Let us look in more details at the SABSA open framework Check Point has used to develop CESF. SABSA is one of the most widely recognized security architectural methodologies. Its framework allows security architects to develop a business requirement into a security design, and then to manage implementation in a controlled manner while maintaining a business-driven focus. Every security solution is based on, and linked to, a business requirement. The key tools in delivering security architecture through SABSA are the use of the SABSA framework and SABSA views.

The SABSA methodology is to analyze the business requirements at the outset, and create a chain of traceability through to logical design and implementation. The main features of SABSA are the "views" and "layers" components of the SABSA framework. In the next section we will look at how these are used and their importance.

VIEWS

The first component of the SABSA process that we will look at is the SABSA *"view"* concept, which describes how the framework engages with different stakeholders as we move through the process of security architecture. The end-to-end process of building security needs to account for all points' of view. Each layer of the process is relevant to someone's point of view.

The table to the right shows the various layers of the SABSA design methodology and the *"views"* that are attributed to each layer.

For example, the *"Designer's View"* is concerned with logical architecture, and the *"Service Manager's View"* is concerned with the operational architecture.

SABSA View	Description
Business View	Contextual Architecture
Architect's View	Conceptual Architecture
Designer's View	Logical Architecture
Builder's View	Physical Architecture
Tradeperson's View	Component Architecture
Service Manager's View	Physical Architecture

Figure 3. *SABSA views*[1]

LAYERS

The SABSA framework is a top-down process that moves through a number of *"layers"*. Each layer has a specific purpose and has a specific *"view"* as seen above. When combined, they make up the entire SABSA process. Each *"layer"* has a specific job in the overall process and is a pre-requisite for the subsequent layers. Each *"layer"* represents a specific set of processes designed to elicit the data needed to complete the layer's objective. Each layer plays a fundamental part in the overall design process.

In the table to the right, we have listed the various layers and their function in the overall process.

SABSA View	SABSA Layer	Description
Business View	Contextual	Identify business risks and drivers and review architecture
Architect's View	Concept	Define security objectives
Designer's View	Logical	The security services that will be required
Builder's View	Physical	The tools, standards and physical devices
Tradeperson's View	Component	The specific vendor components and sizing
Service Manager's View	Management	The ongoing management and support

Figure 4. *SABSA framework*

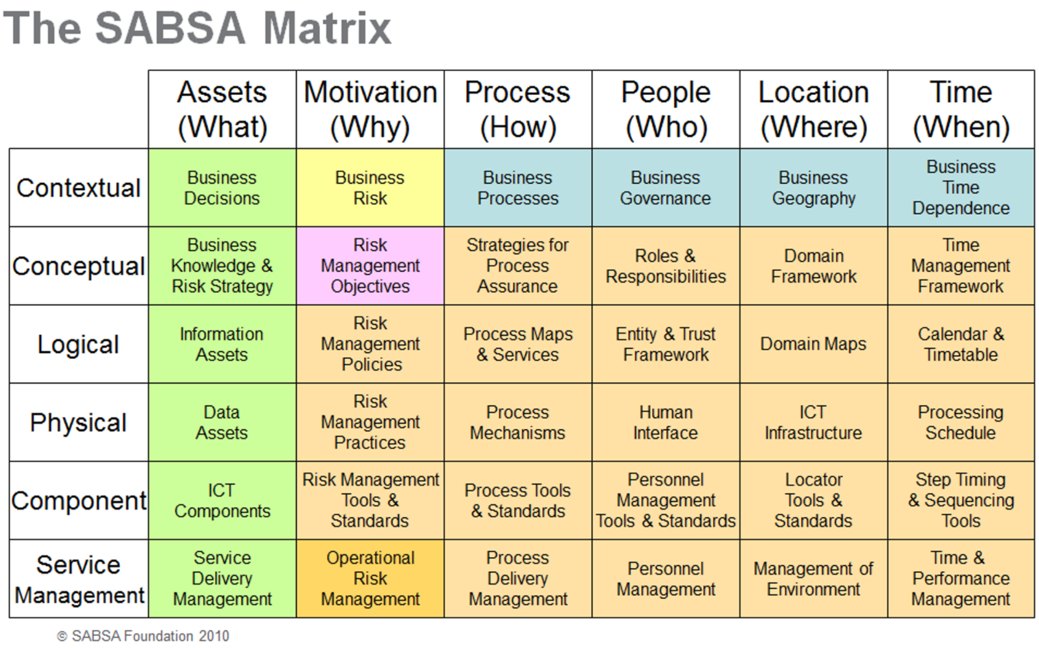
[1] Source: https://sabsa.org/sabsa-executive-summary/

THE SABSA FRAMEWORK

The cornerstone of SABSA is the SABSA framework. The framework gives the SABSA architect a structure by which to formulate the security architecture. It also structures how data is collected and the questions asked.

In its simplest form the SABSA framework is a roadmap to deliver business-driven accountable security by collecting answers and asking questions at each layer.

Key Point: *The framework starts at the 'contextual' layer and moves across and down.*



The SABSA Matrix

	Assets (What)	Motivation (Why)	Process (How)	People (Who)	Location (Where)	Time (When)
Contextual	Business Decisions	Business Risk	Business Processes	Business Governance	Business Geography	Business Time Dependence
Conceptual	Business Knowledge & Risk Strategy	Risk Management Objectives	Strategies for Process Assurance	Roles & Responsibilities	Domain Framework	Time Management Framework
Logical	Information Assets	Risk Management Policies	Process Maps & Services	Entity & Trust Framework	Domain Maps	Calendar & Timetable
Physical	Data Assets	Risk Management Practices	Process Mechanisms	Human Interface	ICT Infrastructure	Processing Schedule
Component	ICT Components	Risk Management Tools & Standards	Process Tools & Standards	Personnel Management Tools & Standards	Locator Tools & Standards	Step Timing & Sequencing Tools
Service Management	Service Delivery Management	Operational Risk Management	Process Delivery Management	Personnel Management	Management of Environment	Time & Performance Management

© SABSA Foundation 2010

Figure 5. *SABSA framework*[2]

SABSA AND CESF

Check Point has drawn inspiration from the SABSA framework and credits its influence in the creation of the CESF process. CESF borrowed, and adapted, the concepts of *"views"* and *"layers"* in its approach to develop a process specifically designed around network and cyber security.

Because SABSA has been designed to help in all fields of security architecture, Check Point chose to adopt some of its guiding principles but to tailor these specially for our own audience and customer-base. The result is a more targeted process designed to deliver on the requirements of Check Point customers.

Check Point's adoption of SABSA into the CESF process also means that we are able to borrow common terminology and act as an open framework.

[2] Source: The SABA framework - https://sabsa.org/sabsaoverview.pdf

3 Zero Trust

Zero Trust was introduced to the world as a model for security architecture in 2010 by John Kindervag of Forrester Research,[3] and it's another key influence on the CESF process.

In this section, we will explore Zero Trust as a wider concept and architectural methodology, before exploring how CESF uses Zero Trust.

A core premise of Zero Trust is that to think about cyber-risk correctly, we should first assume the internal network is compromised; we just do not know it yet. If we follow this assumption, we can conclude that internal connections must be authenticated before they are trusted.

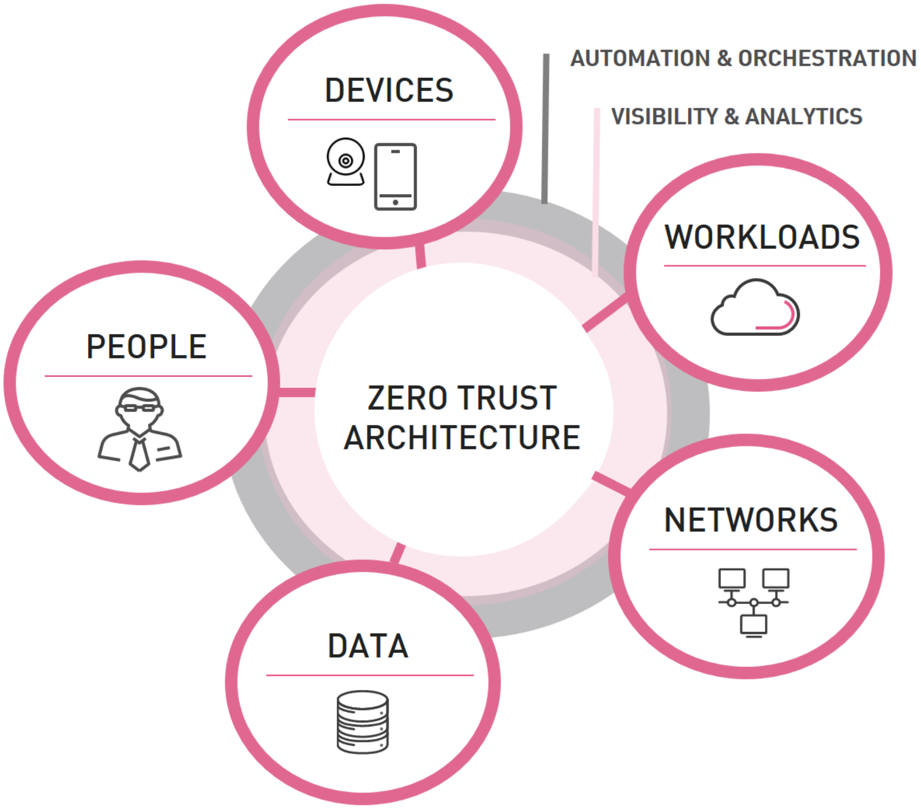


Figure 6. *Forrester: The seven pillars of Zero Trust architecture*

Zero Trust is now an industry standard design methodology. Its approach is a move towards a label-based architecture, which uses identity and connection-context to make access decisions for users, data, and networks irrespective of location.

In a true Zero Trust network, designers would approach the internal and external networks as essentially the same in terms of trust, risk, i.e., the internal and external networks are 'toxic'.

[3] Webinar: No More Chewy Centers: The Zero-Trust Model of Information Security," by John Kindervag, Forrester, August 9, 2010

DRIVERS FOR THE ZERO TRUST MODEL

As security professionals Zero Trust invites us to accept that a hard perimeter is ineffective against many attack vectors.

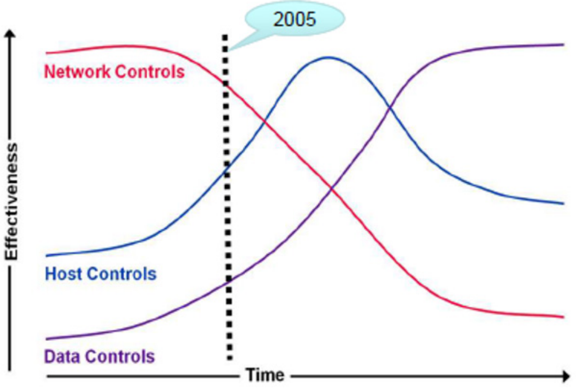
The following drivers are commonly quoted as reasons for adopting Zero Trust:

- Email, web access, and all encrypted traffic (VPN, SSL, SMTP-TLS, etc.) cannot be filtered efficiently or effectively at the corporate perimeter.
- Once inside the perimeter, those traffic items may carry hostile payloads that can work their way transversely to attack resources they were never intended to contact.
- A hard perimeter is at odds with modern business models; organizations are often disparate with users working from multiple locations.
- Cloud transformation is a key strategic goal for many organizations. This often means an organization's intellectual property and core workloads are now located in shared-ownership platforms. Traditional models of security aren't equipped to secure these business models.

PROCESS-CENTRIC SECURITY ARCHITECTURE

Zero Trust proposes that perimeters don't exist anymore and network is essentially borderless. Security professionals need to find alternatives to securing data, corporate assets and users. Modern thinking is to move away from a focus on networks, borders, and systems and address process and data-centric security requirements.

This paradigm shift is by no means complete but it means that security architecture needs to encompass a view of how data is secured irrespective of its location. How this manifests in real-world security architecture is a topic for the "build" and "design" CESF process; for now we will only acknowledge a move away from the network-centric to data-centric network design to a more process and data-centric view.



See: Dan Hitchcock, Evolution of Information Security Technologies, 2005 at http://movetheworld.wordpress.com

Figure 7. *Evolution of Information Security Technology* [4]

ZERO TRUST AND CESF

We have established that the principles of Zero Trust are mainstream and that Check Point has adopted these principles as a key design principle for CESF. The table on the right shows how the Zero Trust methodology is a critical component of the CESF process.

We consider Zero Trust a key component of CESF because:

- Zero Trust is used as a design principle integral to most modern secure networks. All security architectural papers and all Check Point design templates are built around Zero Trust, except in circumstances where this architecture doesn't apply or is counter-intuitive.

[4] Source: Dan Hitchcock, The SABSA Institute C.I.C. 2019

4 Check Point Enterprise Security Framework

THE CESF

This section introduces Check Point ENTERPRISE Security Architecture as a design process and the vehicle for building security architecture.

As previously discussed, CESF is the Check Point interpretation of the SABSA process combined with best practice and Zero Trust architecture. In this section, we will convert SABSA "views" and SABSA "layers" to CESF "views" and "layers", and incorporate Zero Trust into the CESF process.

We built CESF around number of layers, each with a specific goal and conducted sequentially. Each layer plays a role in collating and processing the client's business and security requirements in such a way as to arrive at the required output. The combination of these layers is a complete security architecture that is fully accountable to business requirement and fully documented.

SABSA TO CESF

Check Point's interpretation of the SABSA *"layers"* has resulted in the same amount of layers, but now described to be more relevant to our goal of building network and cyber security solutions. We will look at each layer in more detail in a later section of this paper. For now, it is important to understand the conversion that Check Point has made, as illustrated in the table on the right.

SABSA Layer	Check Point CESF Layer
Contextual	REVIEW
Concept	ARCHITECTURE
Logical	DESIGN
Physical	BUILD
Component	IMPLEMENT
Management	MANAGE

Figure 9. *Translating SABSA to CESF layers*

CESF VIEWS

CESF uses the principle of views in the same way as SABSA: a view describes the ownership for a layer. In the CESF framework, we can find the owner of the layer in the *"owner"* column, as shown in the table below. We will refer to CESF views throughout this paper, as they are a key part of the SABSA framework and CESF.

Key Point: *A difference between SABSA and CESF is that the CESF architect assumes responsibility for multiple views.*

CESF Layer	View / Owner
REVIEW	Client's View
ARCHITECTURE	Check Point Architect's View
DESIGN	
BUILD	
IMPLEMENT	Check Point SME, Professional Services
MANAGE	Check Point Account Management, Customer Success Team

Figure 10. *The CESF layers, views and owners*

CESF LAYERS

Like SABSA, CESF is comprised of a number of layers, each with a specific goal and conducted sequentially. Each layer plays a role in collating and processing the client's business and security requirements in such a way as to arrive at the required output.

The layers are as follows:

CESF Layer	Description
REVIEW	**Business-centric:** Understand the business context for security. Identify business requirements.
ARCHITECTURE	**Technology-centric:** Review the existing security architecture and understand business drivers for security. Define security attributes and map to security services.
DESIGN	**Logical design:** Define security services that will be required and how they are used in the design.
BUILD	**Build:** Defining the placement of security within the architecture. The tools, standards and physical devices that are used to meet the business requirements.
IMPLEMENT	**Low-level design:** The specific vendor components and sizing.
MANAGE	**Continuous improvement:** The ongoing management and support.

Figure 11. *The CESF layers and their descriptions*

CHECK POINT ENTERPRISE FRAMEWORK

As the name suggests the CESF is a framework, one that defines the structure by which we should conduct security architecture. The CESF provides a set of rules and principles that apply to the process of developing enterprise security solutions.

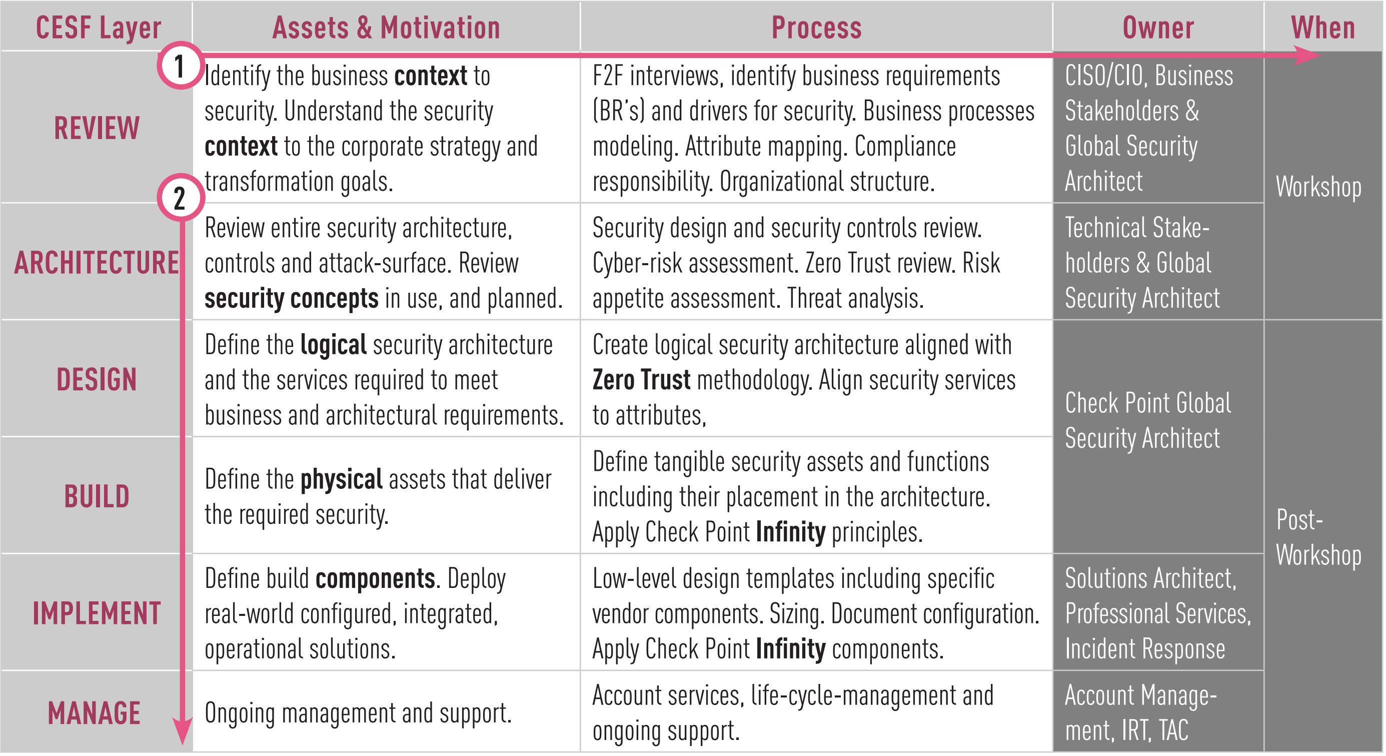
The framework below shows the complete CESF table and all its components; in the following sections, we will explore each layer and their respective inputs and outputs.

CESF Layer	Assets & Motivation	Process	Owner	When
REVIEW	Identify the business **context** to security. Understand the security **context** to the corporate strategy and transformation goals.	F2F interviews, identify business requirements (BR's) and drivers for security. Business processes modeling. Attribute mapping. Compliance responsibility. Organizational structure.	CISO/CIO, Business Stakeholders & Global Security Architect	Workshop
ARCHITECTURE	Review entire security architecture, controls and attack-surface. Review **security concepts** in use, and planned.	Security design and security controls review. Cyber-risk assessment. Zero Trust review. Risk appetite assessment. Threat analysis.	Technical Stakeholders & Global Security Architect	
DESIGN	Define the **logical** security architecture and the services required to meet business and architectural requirements.	Create logical security architecture aligned with **Zero Trust** methodology. Align security services to attributes,	Check Point Global Security Architect	Post-Workshop
BUILD	Define the **physical** assets that deliver the required security.	Define tangible security assets and functions including their placement in the architecture. Apply Check Point **Infinity** principles.		
IMPLEMENT	Define build **components**. Deploy real-world configured, integrated, operational solutions.	Low-level design templates including specific vendor components. Sizing. Document configuration. Apply Check Point **Infinity** components.	Solutions Architect, Professional Services, Incident Response	
MANAGE	Ongoing management and support.	Account services, life-cycle-management and ongoing support.	Account Management, IRT, TAC	

Figure 12. *The complete CESF showing the core and extended sections*

NAVIGATION

Before we discuss the various components of CESF it is important to understand how we navigate the table. We have divided the framework into a number of layers, with specific tools and deliverables at each phase. Each layer is addressed sequentially and from left to right, as shown below:



CESF Layer	Assets & Motivation	Process	Owner	When
REVIEW	Identify the business **context** to security. Understand the security **context** to the corporate strategy and transformation goals.	F2F interviews, identify business requirements (BR's) and drivers for security. Business processes modeling. Attribute mapping. Compliance responsibility. Organizational structure.	CISO/CIO, Business Stakeholders & Global Security Architect	Workshop
ARCHITECTURE	Review entire security architecture, controls and attack-surface. Review **security concepts** in use, and planned.	Security design and security controls review. Cyber-risk assessment. Zero Trust review. Risk appetite assessment. Threat analysis.	Technical Stake-holders & Global Security Architect	
DESIGN	Define the **logical** security architecture and the services required to meet business and architectural requirements.	Create logical security architecture aligned with **Zero Trust** methodology. Align security services to attributes,	Check Point Global Security Architect	Post-Workshop
BUILD	Define the **physical** assets that deliver the required security.	Define tangible security assets and functions including their placement in the architecture. Apply Check Point **Infinity** principles.		
IMPLEMENT	Define build **components**. Deploy real-world configured, integrated, operational solutions.	Low-level design templates including specific vendor components. Sizing. Document configuration. Apply Check Point **Infinity** components.	Solutions Architect, Professional Services, Incident Response	
MANAGE	Ongoing management and support.	Account services, life-cycle-management and ongoing support.	Account Manage-ment, IRT, TAC	

Figure 13. *The complete CESF showing how to navigate the layers and rows*

PROCESS AND TIMELINE

The final piece of information that we can gain from the framework is the order that we progress through the process. In the CESF we complete each layer at a specific time within the overall engagement.

This information is provided in the *"when"* column. The key data-gathering phase of the process is the workshop, which encapsulates the *"review"* and *"architecture"* layer. The post-workshop *"design"* and *"build"* layers follow the workshop. The CESF process then moves to the *"implementation"* and ongoing support layers.

CESF Layer	Assets & Motivation	Process	Owner	When
REVIEW	Identify the business **context** to security. Understand the security **context** to the corporate strategy and transformation goals.	F2F interviews, identify business requirements (BR's) and drivers for security. Business processes modeling. Attribute mapping. Compliance responsibility. Organizational structure.	CISO/CIO, Business Stakeholders & Global Security Architect	Workshop
ARCHITECTURE	Review entire security architecture, controls and attack-surface. Review **security concepts** in use, and planned.	Security design and security controls review. Cyber-risk assessment. Zero Trust review. Risk appetite assessment. Threat analysis.	Technical Stake-holders & Global Security Architect	
DESIGN	Define the **logical** security architecture and the services required to meet business and architectural requirements.	Create logical security architecture aligned with **Zero Trust** methodology. Align security services to attributes,	Check Point Global Security Architect	Post-Workshop
BUILD	Define the **physical** assets that deliver the required security.	Define tangible security assets and functions including their placement in the architecture. Apply Check Point **Infinity** principles.		
IMPLEMENT	Define build **components**. Deploy real-world configured, integrated, operational solutions.	Low-level design templates including specific vendor components. Sizing. Document configuration. Apply Check Point **Infinity** components.	Solutions Architect, Professional Services, Incident Response	
MANAGE	Ongoing management and support.	Account services, life-cycle-management and ongoing support.	Account Manage-ment, IRT, TAC	

Figure 14. *The CESF showing when the various layers are completed*

5 Using the CESF Process

INTRODUCTION

Now that we have introduced the framework, its conception and use we, can look at each layer of the framework in more detail. In this section, we'll explore the purpose of this layer, and how it contributes to the overall outcome of the CESF process. Each layer has a specific form and function that must be completed in order to progress. As discussed in the intro section, we have grouped some layers together in phases. Let's quickly go over the CESF phases, which are:

- **Review and Architecture:** Check Point teams capture requirements from the client though a tailored CESF workshop, during which we capture statements and data relating to business context, strategy, organizational aspirations and security posture. This phase centers on capturing requirements, problem statements as well as performing tasks such as risk and gap analysis.

- **Design and Build:** CESF architects develop recommended responses to the requirements that align with security best practices, open standards, such as Zero Trust and CESF design principles.

- **Implementation:** Professional services, partners and engineers are able to add low-level design details to the recommendations delivering on the business-driven solutions built through the CESF process. Engagement of specialist teams such as incident response and strategic alliance, and.vendor specific design patterns, such as the Check Point Infinity architecture, can be applied.

- **Service Management:** Continuous development and improvement of the security posture by Check Point. Account management and technical post-implementation support.

6 Review and Architecture Phase

OVERVIEW

This is the first stage of the CESF process and sets up the entire engagement. It contains two critical layers that are both of which are delivered as part of the CESF workshop. This phase consists of the following:

- **The Workshop** is the core, and only, vehicle for data-capture and discussion with the client. There is no way to complete the CESF process without a CESF workshop.

- **Review Layer** is used to capture the business requirements, risks, goals and strategy. The "review" layer is business-centric.

- **Architecture Layer** is used to capture security objectives and perform the required technology-centric analysis.

In terms of the CESF table, we are looking at the following layers:

CESF Layer	Assets & Motivation	Process	Owner	When
REVIEW	Identify the business **context** to security. Understand the security **context** to the corporate strategy and transformation goals.	F2F interviews, identify business requirements (BR's) and drivers for security. Business processes modeling. Attribute mapping. Compliance responsibility. Organizational structure.	CISO/CIO, Business Stakeholders & Global Security Architect	Workshop
ARCHITECTURE	Review entire security architecture, controls and attack-surface. Review **security concepts** in use, and planned.	Security design and security controls review. Cyber-risk assessment. Zero Trust review. Risk appetite assessment. Threat analysis.	Technical Stakeholders & Global Security Architect	
DESIGN	Define the **logical** security architecture and the services required to meet business and architectural requirements.	Create logical security architecture aligned with **Zero Trust** methodology. Align security services to attributes,	Check Point Global Security Architect	Post-Workshop
BUILD	Define the **physical** assets that deliver the required security.	Define tangible security assets and functions including their placement in the architecture. Apply Check Point **Infinity** principles.		
IMPLEMENT	Define build **components**. Deploy real-world configured, integrated, operational solutions.	Low-level design templates including specific vendor components. Sizing. Document configuration. Apply Check Point **Infinity** components.	Solutions Architect, Professional Services, Incident Response	
MANAGE	Ongoing management and support.	Account services, life-cycle-management and ongoing support.	Account Management, IRT, TAC	

Figure 15. *The CESF layers required for the workshop phase*

7 The Workshop

OVERVIEW

The CSF workshop is a core component of the CESF process. We consider it critical to the success of the process. Without the workshop, we are not able to collect the information required. The value of the workshop cannot be under-represented; consequently, they are always conducted face-to-face, in a forum format, designed to allow our clients a platform in which to articulate their organization's business and security requirements.

In this section, we will look at how the workshop is conducted, the people required to be present, and show some of the workshop components. We can describe a Check Point workshop as follows:

The Enterprise Architecture Workshop is an exclusive and focused single day meeting between the client and Check Point professionals to openly discuss, review and advise on all aspects of the existing, and future, security ecosystem.

As with any client-facing process, there is a specific engagement timeline as shown below. The key point is that the workshop is an open-forum, face-to-face exercise containing a significant whiteboard session that's followed by a report.

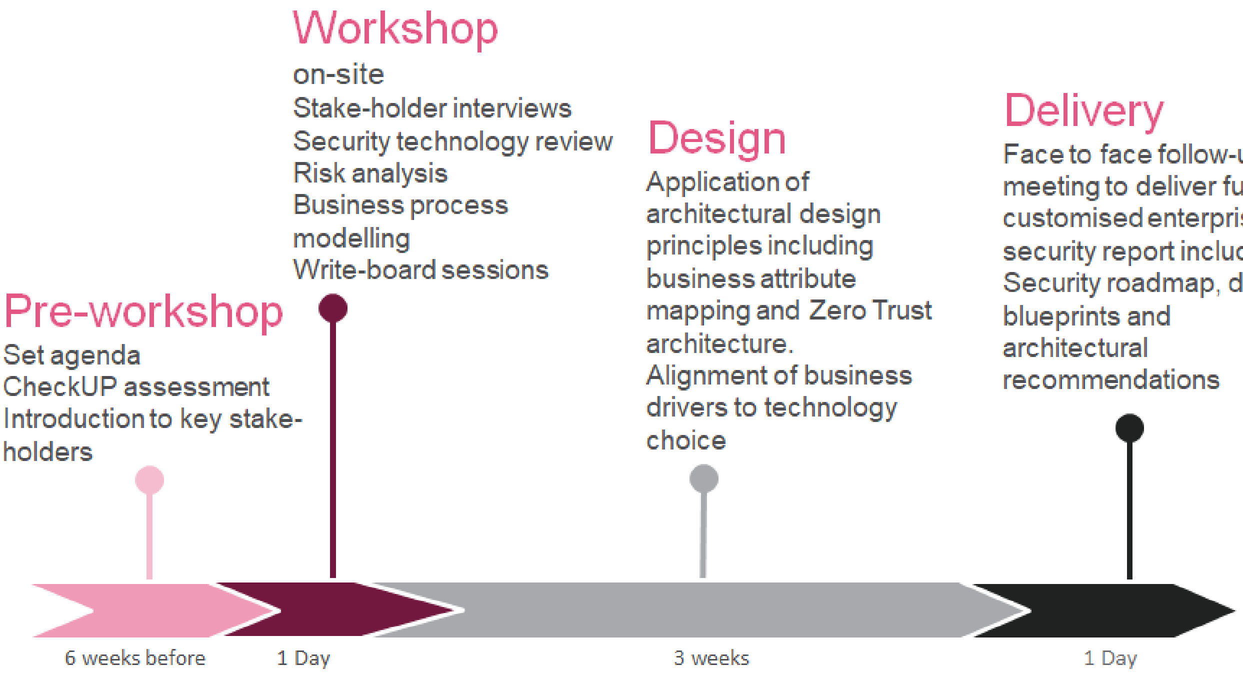

Workshop
on-site
Stake-holder interviews
Security technology review
Risk analysis
Business process modelling
Write-board sessions
Design
Application of architectural design principles including business attribute mapping and Zero Trust architecture.
Alignment of business drivers to technology choice
Delivery
Face to face follow-up meeting to deliver full customised enterprise security report including – Security roadmap, design blueprints and architectural recommendations
Pre-workshop
Set agenda
CheckUP assessment
Introduction to key stake-holders
6 weeks before
1 Day
3 weeks
1 Day

Figure 16. *The Check Point workshop timeline*

WORKSHOP PRINCIPLES

Onsite workshops are hosted by dedicated architects and are designed to systematically and methodically capture all the information required by the framework process. The guiding principles of the workshop are:

- An open, honest, and interactive one day session
- A vendor-neutral security best-practice discussion
- Business processes and context focused
- Security requirement and security concept focused
- Not a technical deep-dive

WORKSHOP GOALS

The workshop is the single most important point of contact between Check Point and the client. The main goals are:

- To better understand the client's business objectives and how this relates to their security technology choices
- Help clients achieve their architectural goals
- Challenge ideas and explore what is possible
- Help clients align with security best practices
- Write, record, report and present recommendations

OUTPUT

At the conclusion of the review we will have:

- A corporate strategy as it pertains to security
- The client's business and security drivers
- A collection of business processes and attributes
- The client's risk appetite
- An analysis of existing security controls and high-level security architecture
- Future or target architecture as the client sees it
- A complete business impact assessment

WORKSHOP STRUCTURE AND AGENDAS

The workshop agenda is written and agreed upon by the architect and client before they meet. Check Point CESF process can be used to assist customers who have a more focused agenda. In these cases the agenda can be changed. The most important consideration is that enough quality information is gathered to process to the *"design"* and *"build"* layers.

A sample of the topics covered is on the right.

Business Review	Architectural Review
Review Business Process Review Attribute Mapping Risk Appetite Assessment Business Impact Assessment (BIA)	Threat Environment Analysis Network Design Review Whiteboard Sessions Security Controls Review

Figure 16.
Most CESF workshops will contain these subjects at a minimum

The most important components of the workshop are:

Stakeholder Interviews

We always start by collaborating with senior security stakeholders to discuss the business drivers. The main vehicle for collecting requirements is through stakeholder interviews, conducted with senior managers, program managers, and C-level representatives. The interviews allows the architect to hear first-hand the client's business objectives and security challenges. These interviews are critical for establishing what really matters to the organization.

In this opening section of the workshop, the client's senior managers, program managers, etc. will articulate:

- What the business does and how it achieves its goals
- The key business process that the client is engaged in
- The impact of security on business functions
- The perception of security requirements to the business units
- Future business objectives
- The impact of change on the business

Complete Network Design Review

A significant part of the workshop process concerns the network design and security design review. This is where Check Point architects and the client map out the existing security environment, normally though a whiteboard session. The main components are:

- **Security architectural review:** Identify and cover immediate, mid- and long-term security challenges.
- **Security network and threat prevention design:** Provide a secured and flexible network and security design aligning with the security best practices.
- **Understand existing security controls:** The security infrastructure review session must capture the current state of the architecture to a sufficient technical depth, without unpacking the entire configuration. The architect will use a security control matrix to make sure all significant areas are covered.

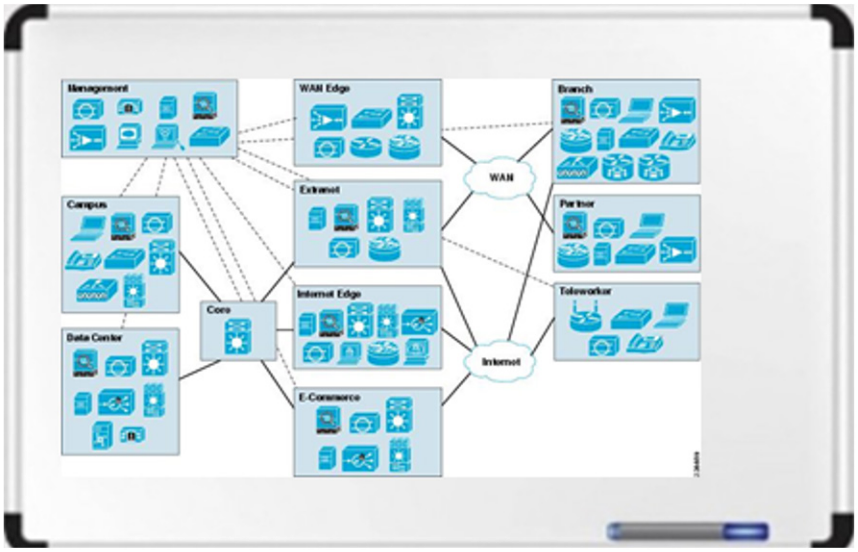


Figure 17. *Whiteboarding plays a large part in the workshop and is often the focus of discussion when reviewing the client's architecture*

Participation

The success of this phase is very much dependent on gaining the correct level of commitment and "buy-in" from the client.

The value of the designs developed though the CESF process is conditional on us collecting the correct level of information during the workshop. For example, in many organizations top-level managers can articulate the business strategy and future business aspirations, fundamental information for the CESF process. The most effective workshops are those that have the correct C-level sponsorship.

While every organization has its own internal structure, a good example of the various participants is in the table below.

Workshop Session	Participants
Business review session	Security Operations Managers / CISO Security and Network Architects
Whiteboard session – network architecture	Security and Network Architects / Experts / Engineers
Whiteboard session – threat environment	Security Team / SOC / Incident Response Team
Whiteboard session – cloud / data center security	Server Team Virtualization Team Application Team
Whiteboard session – security operations	Security Operations Representative Incident Response Team

Figure 18. *The recommended participants for a standard CESF workshop*

8 The Review Layer

OVERVIEW

The review layer is primarily concerned with capturing information that pertains to the client's business, both in terms of their general overall strategy, and the role security plays within the organization. We often refer to this as business modeling.

In the previous section, we discussed the workshop and the workshop process. We complete this layer during the workshop. This layer describes the process of capturing business objectives, requirements, aspirations, and near-, medium- and long-term goals. It is the only layer dedicated to the client's business and its objectives.

The layer is made up of the following steps:

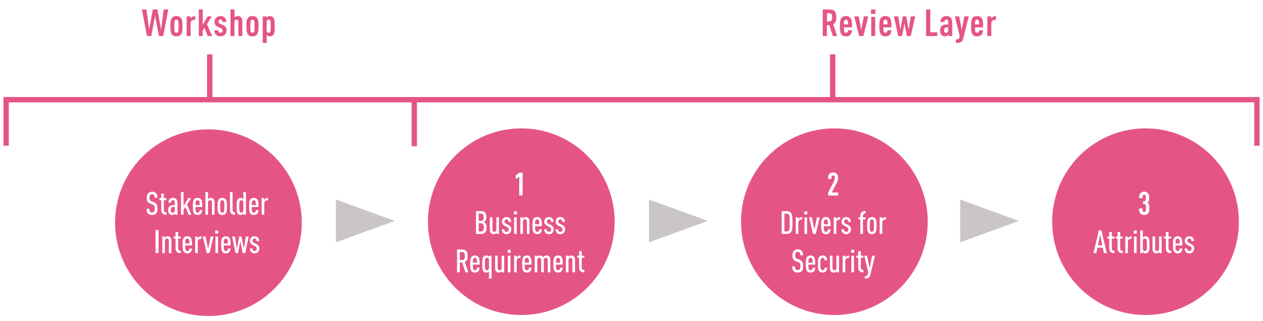


Figure 19. *The components of the review layer are all critical to understanding the client business requirements*

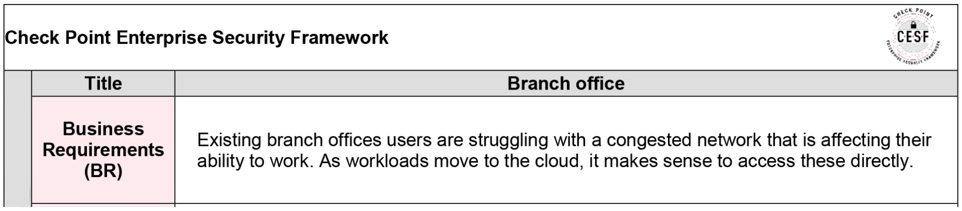
REVIEW LAYER PROCESS

The following section explains how the steps shown in Figure 19 are accomplished. This layer is a combination of three distinct processes. First, the architect will learn the client's business and identify requirements. Afterwards, they will be able to articulate 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.

1. Identifying Business Requirements (BRs)

We have already discussed the stakeholder interviews as a part of the workshop process. The outcome of these interviews should be a collection of business requirements.

Definition: A business requirement is a resource, process, or condition that is vital for the continued success and growth of a business. Below is an example of a business requirement captured in a data-capture template:



Check Point Enterprise Security Framework

Title	Branch office
Business Requirements (BR)	Existing branch offices users are struggling with a congested network that is affecting their ability to work. As workloads move to the cloud, it makes sense to access these directly.

Figure 20. *Example of a business requirement*

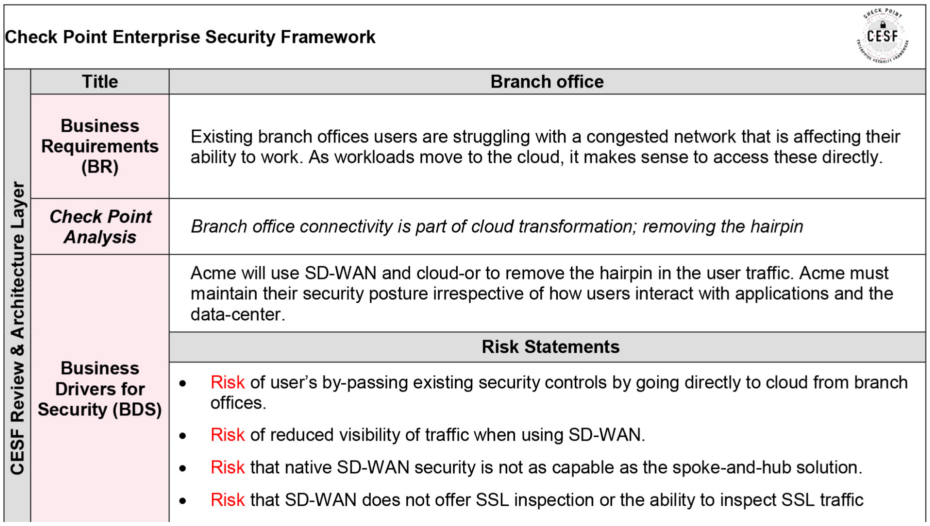
2. Identifying Business Drivers for Security (BDS)

During the stakeholder interviews, we will also gather the business drivers for security. These statements describe the requirements in the context of security. All requirements are relatable to security and this is what the BDS captures. In other words, the interview process will result in the CESF architect knowing exactly how to relate security to business requirements.

Business drivers for security are very specific to each client and it is only through the workshop interviews that we are able to capture these in detail. Often business requirements are too general in definition. The BDS gives them more focus and relevance to security architecture.

Key Point: *Business drivers for security are aways inked to the business requirements and processes. BDS's provide the security context to the BRs.*

Below is an example of a business requirement and its corresponding BDS.



Check Point Enterprise Security Framework

	Title	Branch office
CESF Review & Architecture Layer	**Business Requirements (BR)**	Existing branch offices users are struggling with a congested network that is affecting their ability to work. As workloads move to the cloud, it makes sense to access these directly.
	Check Point Analysis	*Branch office connectivity is part of cloud transformation; removing the hairpin*
	Business Drivers for Security (BDS)	Acme will use SD-WAN and cloud-or to remove the hairpin in the user traffic. Acme must maintain their security posture irrespective of how users interact with applications and the data-center. **Risk Statements** • Risk of user's by-passing existing security controls by going directly to cloud from branch offices. • Risk of reduced visibility of traffic when using SD-WAN. • Risk that native SD-WAN security is not as capable as the spoke-and-hub solution. • Risk that SD-WAN does not offer SSL inspection or the ability to inspect SSL traffic

Figure 21. *Example of a business requirement*

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 workshop.

We will discuss what an attribute is in the following section and they feature prominently in this paper. However, for now it is important to note that *"attributes"* play the role of providing a link between the requirement and the recommendation.

An attribute is a conceptual abstraction of a business requirement. The attributed terms are abstract in nature but 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. It is the CESF architect's responsibility to use attributes correctly.

Definition: SABSA defines an attribute as a conceptual abstraction of a real business requirement (the objectives, drivers and targets) which are modeled into a normalized language that articulates requirements and measures performance in a way that is instinctive to all stakeholders.

Key Point: *Defining attributes also helps us to prioritize the business requirements and security drivers. Attributes can be given different weightings. Later in the CESF we will use the attributes to define the security controls that are required.*

For the sake of simplicity we have borrowed the SABSA attribute table. However, it is possible for the architect to express their own attributes. The example below shows how we collect the attributes into our business process table.

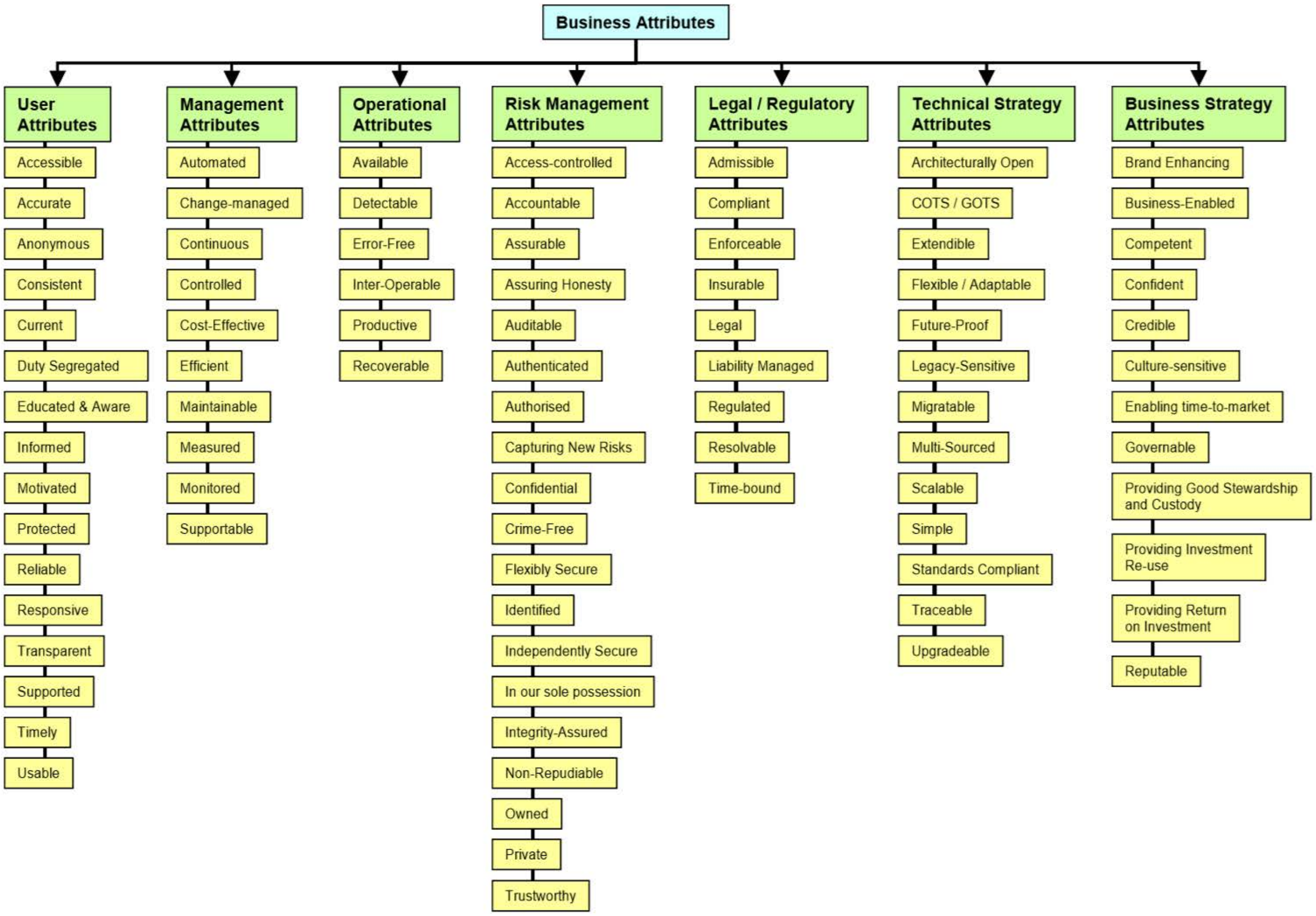


Figure 22. *A security attribute map used to link business requirements to business drivers for security*

ATTRIBUTE MAPPING

In complex cases it is common to find multiple attributes linking to multiple requirements. Another way to present these complexities is using an attribute map. The example below shows an enterprise's goals and security objectives connected to security attributes.

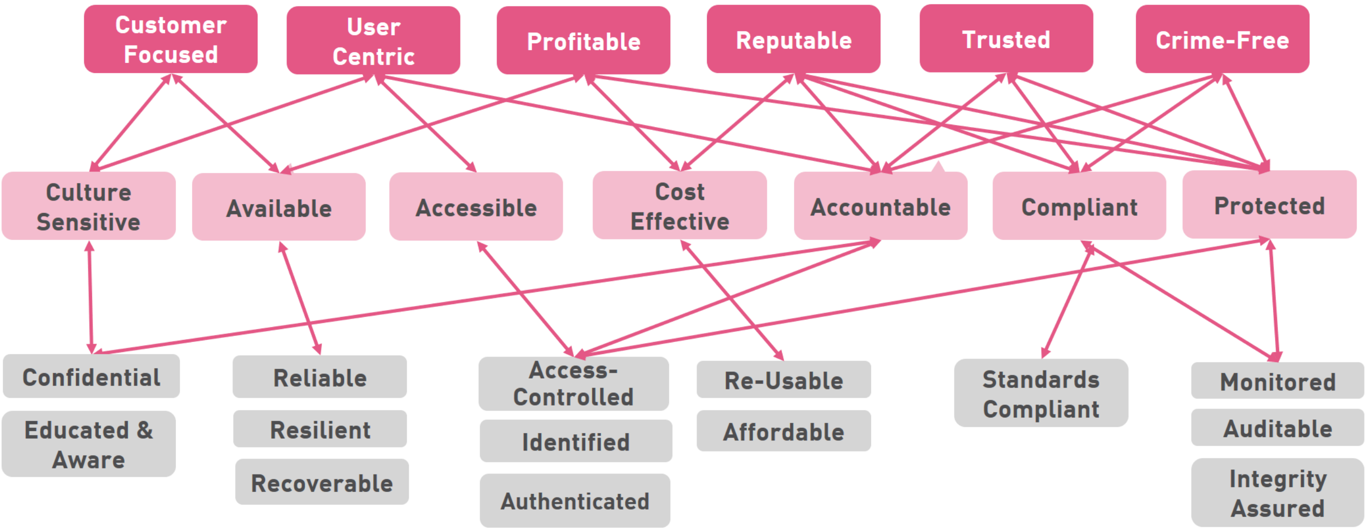
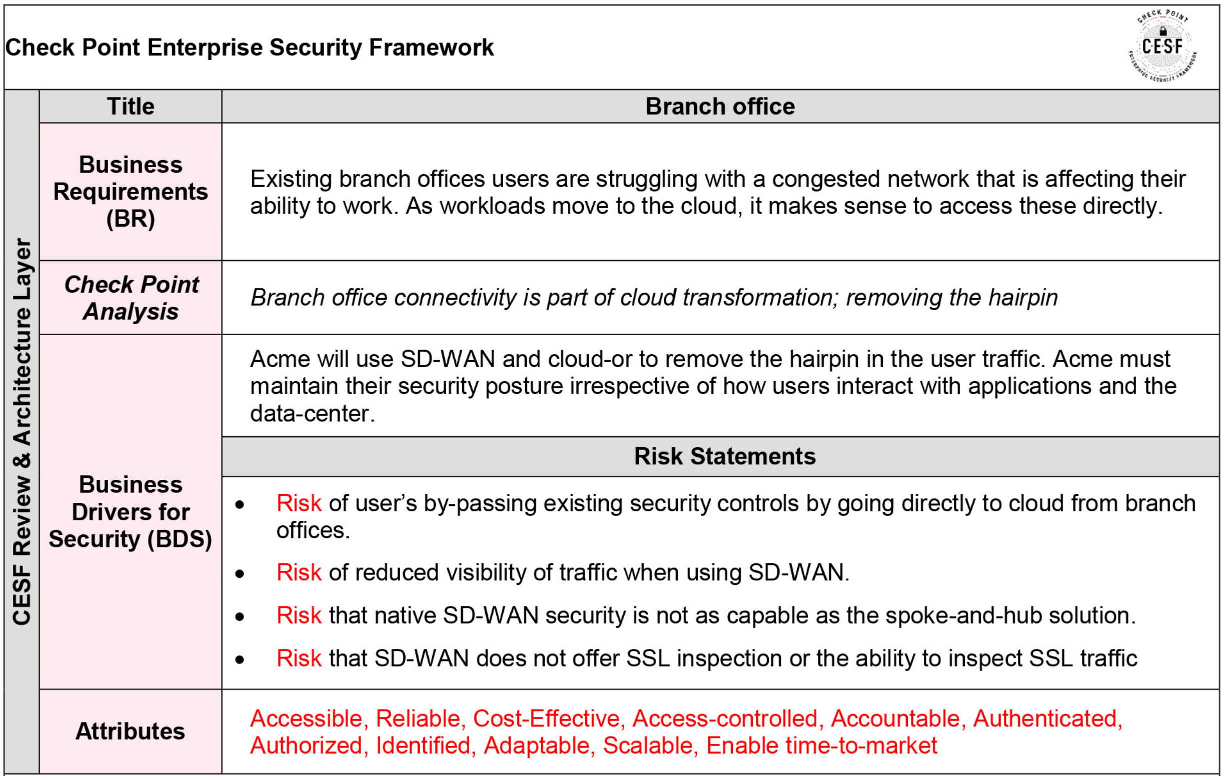


Figure 23. *A security attribute map used to link business requirements to business drivers for security*

Maps like the one shown above will be expanded on during the next phase of the CESF process, for now it is important to appreciate that a single attribute might decribe multiple requirements.

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



Check Point Enterprise Security Framework

CESF Review & Architecture Layer	Title	Branch office
	Business Requirements (BR)	Existing branch offices users are struggling with a congested network that is affecting their ability to work. As workloads move to the cloud, it makes sense to access these directly.
	Check Point Analysis	*Branch office connectivity is part of cloud transformation; removing the hairpin*
	Business Drivers for Security (BDS)	Acme will use SD-WAN and cloud-or to remove the hairpin in the user traffic. Acme must maintain their security posture irrespective of how users interact with applications and the data-center.
		Risk Statements
		• Risk of user's by-passing existing security controls by going directly to cloud from branch offices. • Risk of reduced visibility of traffic when using SD-WAN. • Risk that native SD-WAN security is not as capable as the spoke-and-hub solution. • Risk that SD-WAN does not offer SSL inspection or the ability to inspect SSL traffic
	Attributes	Accessible, Reliable, Cost-Effective, Access-controlled, Accountable, Authenticated, Authorized, Identified, Adaptable, Scalable, Enable time-to-market

Figure 24. *Example showing a business requirement and the attributes*

9 The Architecture Layer

OVERVIEW

The architecture layer is primarily concerned with capturing information that pertains to the client's security design, architecture, operations, and infrastructure.

Key Point: *This layer represents the workshop's architectural review process, and it should be considered one of the most important layers in the CESF process.*

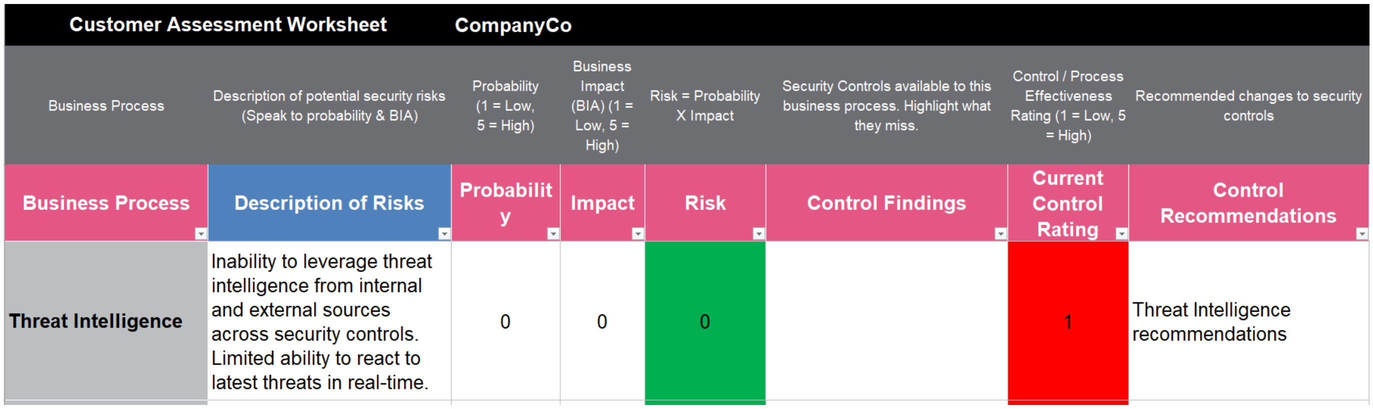
Combined with the review layer, the architecture layer will produce a complete business and technical data set on which the following phases will depend. In the following section, we will outline some of the key processes that define this layer.

RISK ASSESSMENT

A key component of this layer is performing a risk assessment that captures, in a systematic fashion, the various security components currently in the network. We use the risk assessment to measure and record the organization's security posture, in its current state.

The assessment is designed to probe the customer's security architecture. Through the assessment, the CESF architect can record how effective an attack might be and record the potential impact of a successful attack. This process analyses the risk and impact of various breach types, and the damage that would be caused.

The following table is an example of a risk assessment template.



Customer Assessment Worksheet	CompanyCo						
Business Process	Description of potential security risks (Speak to probability & BIA)	Probability (1 = Low, 5 = High)	Business Impact (BIA) (1 = Low, 5 = High)	Risk = Probability X Impact	Security Controls available to this business process. Highlight what they miss.	Control / Process Effectiveness Rating (1 = Low, 5 = High)	Recommended changes to security controls
Business Process	**Description of Risks**	**Probability**	**Impact**	**Risk**	**Control Findings**	**Current Control Rating**	**Control Recommendations**
Threat Intelligence	Inability to leverage threat intelligence from internal and external sources across security controls. Limited ability to react to latest threats in real-time.	0	0	0		1	Threat Intelligence recommendations

Figure 25. *Extract from a typical Risk Assessment Matrix*

A risk matrix gives us a structured method to work through various pre-defined controls and score them depending on the risk that a failure of this control would mean to the organization.

ZERO TRUST REVIEW

By taking a Zero Trust approach to the analysis of an existing network, architects and designers are able to probe the internal security functions and ask how capable the network is in defending itself from a breach. The Zero Trust approach takes the position that the internal network is already "toxic" or compromised, and invites us to assume the mindset of the attacker.

"A way to think about cyber threats is to assume you have already been compromised; you simply don't know it yet." Forrester[5]

Adopting this position allows for a higher degree of speculation about existing security postures, which results in a complete and thorough appraisal of the network. We will cover this topic in depth during the workshop stage of the CESF process.

RISK APPETITE ASSESSMENT

The risk appetite assessment is the process of quantifying a cyber risk. Making informed decisions about the cyber risk appetite could often be the difference between the success and failure for security projects, and if the organization will fulfill its strategic goals.

Risk appetite is the level of tolerance that an organization has for risk. One aspect of the definition is to understand how much risk an organization is willing to tolerate, and the other is thinking about how much an organization is willing to invest or spend to manage the risk. Risk appetite sets the boundaries for prioritizing which risks need to be treated.

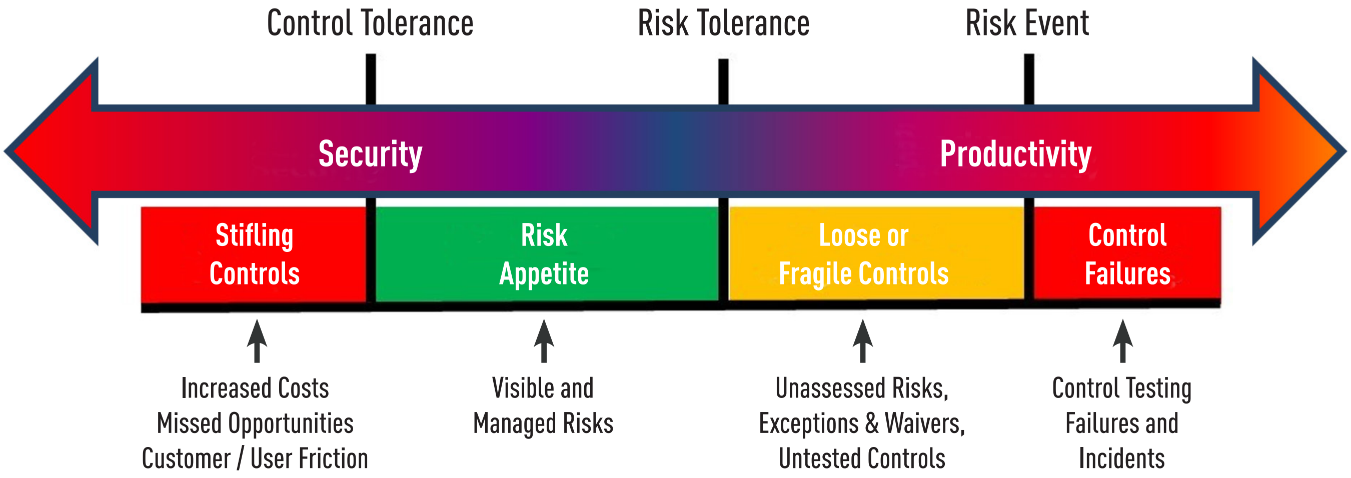


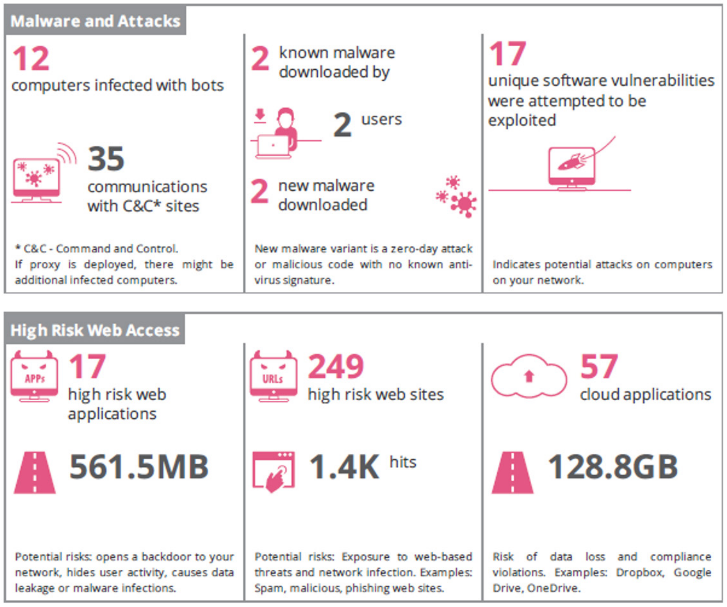
Figure 26. *The risk appetite scale*

Adopting this position allows for a higher degree of speculation about existing security postures, which results in a complete and thorough appraisal of the network. We will cover this topic in depth during the workshop stage of the CESF process.

[5] "Zero Trust," Forrester

THREAT ANALYSIS

A useful tool for analyzing a client's current architecture and security posture is through a managed Check Point CheckUp. We can use CheckUp results to understand network traffic and Internet usage. Often this level of insight can draw attention to operational issues, such as a lack of security visibility.



Malware and Attacks

12 computers infected with bots

35 communications with C&C* sites

* C&C - Command and Control. If proxy is deployed, there might be additional infected computers.

2 known malware downloaded by 2 users

2 new malware downloaded

New malware variant is a zero-day attack or malicious code with no known anti-virus signature.

17 unique software vulnerabilities were attempted to be exploited

Indicates potential attacks on computers on your network.

High Risk Web Access

17 high risk web applications

561.5MB

Potential risks: opens a backdoor to your network, hides user activity, causes data leakage or malware infections.

249 high risk web sites

1.4K hits

Potential risks: Exposure to web-based threats and network infection. Examples: Spam, malicious, phishing web sites.

57 cloud applications

128.8GB

Risk of data loss and compliance violations. Examples: Dropbox, Google Drive, OneDrive.

Figure 27. *Exampe of a CheckUp Report*

CONCLUSION: REVIEW AND ANALYSIS

We have completed the review and analysis of the client's business and security estate. This information will form the foundation of the entire engagement, which is why it is important that the work is thorough and professionally collected. The CESF architect will have a solid understanding of the business, its strategy and requirements, and how security is designed and managed. They will also have a good understanding of the client's appetite for change, their motivation, and capability.

At the conclusion of this phase, we will have:

A complete review layer

- All the required input from the client has been gathered
- Business drivers have been identified, captured, and recorded
- Business processes that influence the cyber security posture have been recorded
- Business attributes that reflect the business drivers have been identified

A complete architecture layer

- A detailed analysis of the existing network security posture has been performed
- A complete risk assessment
- A complete business impact assessment
- A record of the existing security controls

In the following phase, we will use this information to formulate a security architectural blueprint, roadmap and report.

10 Design and Build Phase

OVERVIEW

We will tackle the two layers *"design"* and *"build"* in a single phase. In this phase, the CESF architect will move from the business requirements (BRs) to the logical design and explain the security components used and why. This phase centers on designing and building a solution and a set of recommendations. At the completion of this phase, the CESF architect will have documented the whole process for delivery back to the client.

This phase consists of the:

- **Design Layer,** which uses Zero Trust, network segmentations, attribute mapping and security best-practices to define the security components required to meet the BRs.
- **Build Layer,** which pulls all the design components together into a logical security architecture blueprint and completes the reporting element of the process.

From the CESF table below, we see these phases complete post-workshop. They are the last layers under the CESF architect's complete ownership. Once the *"design"* and *"build"* layers are done, the design is passed to other teams for implementation.

CESF Layer	Assets & Motivation	Process	Owner	When
REVIEW	Identify the business **context** to security. Understand the security **context** to the corporate strategy and transformation goals.	F2F interviews, identify business requirements (BR's) and drivers for security. Business processes modeling. Attribute mapping. Compliance responsibility. Organizational structure.	CISO/CIO, Business Stakeholders & Global Security Architect	Workshop
ARCHITECTURE	Review entire security architecture, controls and attack-surface. Review **security concepts** in use, and planned.	Security design and security controls review. Cyber-risk assessment. Zero Trust review. Risk appetite assessment. Threat analysis.	Technical Stake-holders & Global Security Architect	
DESIGN	Define the **logical** security architecture and the services required to meet business and architectural requirements.	Create logical security architecture aligned with **Zero Trust** methodology. Align security services to attributes,	Check Point Global Security Architect	Post-Workshop
BUILD	Define the **physical** assets that deliver the required security.	Define tangible security assets and functions including their placement in the architecture. Apply Check Point **Infinity** principles.		
IMPLEMENT	Define build **components**. Deploy real-world configured, integrated, operational solutions.	Low-level design templates including specific vendor components. Sizing. Document configuration. Apply Check Point **Infinity** components.	Solutions Architect, Professional Services, Incident Response	
MANAGE	Ongoing management and support.	Account services, life-cycle-management and ongoing support.	Account Manage-ment, IRT, TAC	

Figure 28. *The CESF table showing the design and build phase*

THE DESIGN AND BUILD GOALS

The key goals of the phase are:

- To align business requirements with technology choices. All business requirements translate to security infrastructure or process improvements. All technology recommendations are justified and traceable back to the business requirements.
- If recommendations can be made to improve business processes, they will be delivered at this phase. Recommendations could include operational improvements or changes to the workflow. These recommendations are mapped to business requirements as are the technology choices.
- Convert the *“attributes”* into real-world security components.
- Complete the security architecture report, the overarching document that presents the CESF architects vision back to the client.

11 The Design Layer

OVERVIEW

This layer is the most complex to complete and requires knowledge of various security best practices and components. The outcome of this layer will depend on how the data from the previous layer was processed and the quality of the information collected during the *“review”* and *“architecture”* layers. The *“design”* layer covers all aspects of design, including the logical design of the security ecosystem as well as any relevant operational process designs.

The main **technology** deliverables from this layer are:

- Mapping business attributes to security controls and services
- Mapping security controls to physical components
- Applying Zero Trust design methods
- Applying Infinity architecture methods
- Maintaining the chain-of-responsibility between concept and logical design
- Adhering to the single platform of the Infinity architecture methodology

The main **operational/process** deliverables from this layer are:

- Operational efficiencies including organizational structures and separation of duties
- Operational efficiencies in the management of security events
- Efficiencies in the management of security policies
- Shared responsibility of security risk between business units and internal teams

The following techniques, processes and tools are used as part of this layer.

LOGICAL DESIGN

This section explains the technology design process. As explained in previous sections, the CESF architect will use information in the preceding layers, combine this with Zero Trust, reference architecture and best practices, and produce a design template and solution.

Before we can start building the logical design, we need to know what security components are required. For this, the architect will use the *"attribute-to-service"* mapping. This process is similar to the *"business-to-attribute"* mapping that we discussed in the review section. However, this time we are using the attribute to help define security services.

USING ATTRIBUTES

We first discussed attributes in the *"review"* layer and explained that each business requirement needs to have a number of them; a requirement would have between 2 and 20 attributes.

In this phase, we will map those attributes to specific security components and services. These components are key to the solution as they meet the needs of the various business requirements. This process does not let the CESF architect know where to put the component in the design, only that the component is required for the design to be complete.

Definition: A component is a vendor agnostic description of a thing that has a specific security function. For example, an IPS is a component.

It is the job of the CESF architect to consider each attribute and define the service, or controls, that are appropriate to meet the expectation of the attribute. As we have stated before, the attribute is the single most important link between the review and architecture layer and the design and build layers.

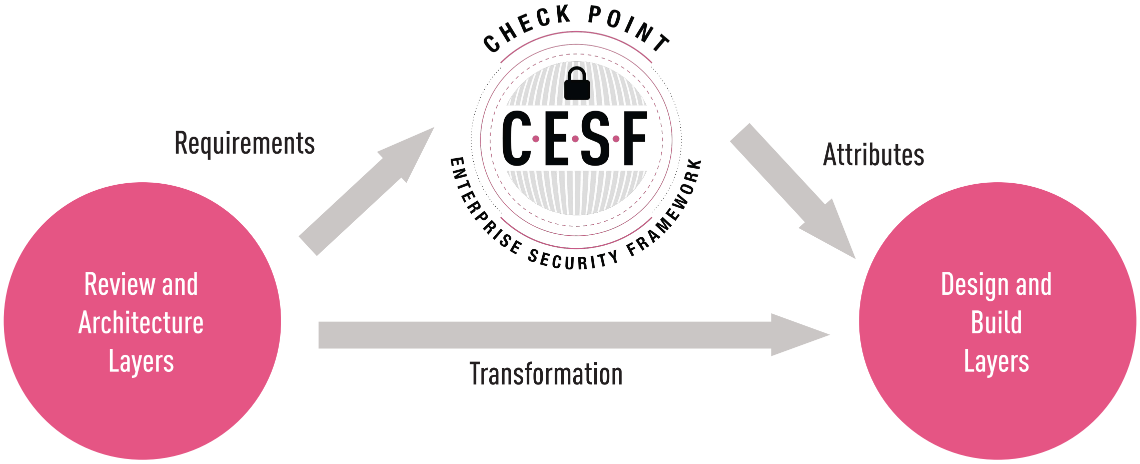


Figure 29. *Developing security architecture from business requirements*

SECURITY CONTROLS AND SERVICES

As with all design processes the language that is used is important. At the *"design"* layer, the "things" used in the design should be described as *"controls"* and not specific vendor competencies. This is because we can implement services in any number of different ways. It is only at the *"implementation"* layer that we define a specific vendor device and its configuration.

Definition: A security control is defined as a process, object or action that results in a specific security action or event.

In the context of the CESF framework, the design layer is only concerned with defining these controls and security services. Some examples are shown below:

CESF Layer	Description	Example
REVIEW	Business requirements and security focused drivers	Protect our hosted sites from external attacks so that business is not disrupted
ARCHITECTURE	The concepts that are used to define the business and security posture	Platform needs to be secure and accessible partially from Internet threat actors
DESIGN	Identifying the services that are required	An intrusion prevention service
BUILD	What is needed for the design to work	IPS software running on a gateway appliance
IMPLEMENT	What is needed to meet the physical requirements of the design	Check Point R80.40 IPS blade running recommended profile

Figure 30. *The language used to describe security things is different at each layer*

MAPPING ATTRIBUTES TO CONTROLS

With a complete list of business attributes, we are now able to do an attribute-to-security mapping. This process takes the attributes defined in the *"review"* phase and converts them to real-world technology that can be used in a logical design.

This step is critical for a completed architecture as it maps the attributes to real-world security technology and, where appropriate, to Check Point technology.

Key Point: *Mapping controls to business attributes means that we never loose focus on what is important to the business. Every control is there for a reason.*

Key Point: *CESF architects will use a list of known mappings. However, the main point to this process is being able to justify why a specific component, technology or service is being used.*

This process provides us with the list of security controls we will use in our design. In the map below, we can see how the security attributes that were collected as part of the previous phase are now mapped to security services and controls.

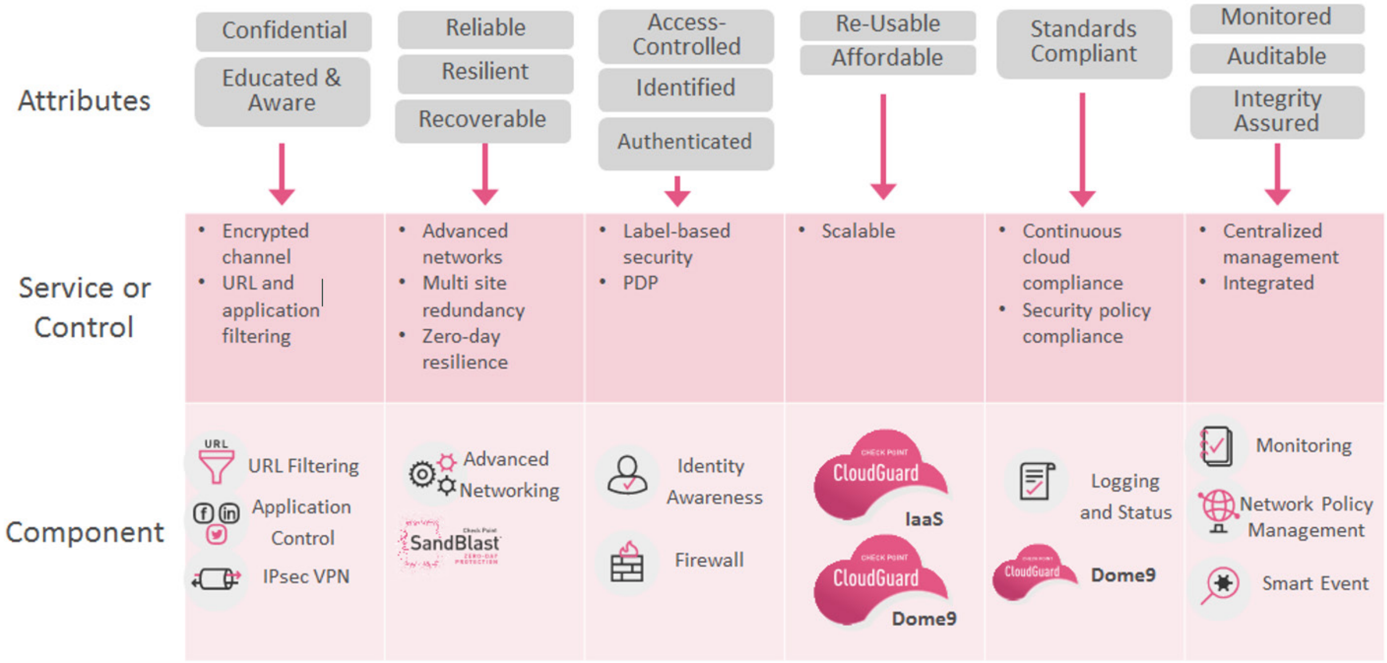


Figure 31. *The language used to describe security is different at each layer*

ZERO TRUST DESIGN

The following Zero Trust concepts are guiding principles for architects at the *"design"* layer. We consider Zero Trust as a gold standard in how to design secure networks, and how they should be segmented. CESF architects regard Zero Trust as a security best practice. Clearly, Zero Trust is not and cannot be applied to every solution. However, where applicable, CESF architects will use this as a core design principle.

In the following section, we will look at the building blocks of Zero Trust design, as defined by Forrester, and how we applied them to the CESF process.

Toxic networks – In Zero Trust architecture workloads should be available and accessible regardless of location. Zero Trust demands that security professionals protect internal data from insider abuse in the same manner as they protect external data on the public Internet. This has an impact on the security controls that we would use in the design.

Identity – Designing to Zero Trust standard means adopting the *"Principle of Least Privilege"* as the access control strategy. Zero Trust means strictly enforcing access control using identity. As a core principle of CESF we would expect the Zero Trust design to incorporate an identity source.

Key Point: *A Zero Trust design principle would be to restrict a user's access to only the resources they need to perform their job, and, instead of trusting everyone, we verify that they are the intended user for the resource.*

Audit and logging – Also aligned to Zero Trust principles is to perform logging on all traffic. This allows connections to be properly audited. It is therefore necessary for the CESF architecture to design a platform that is able to properly audit and log traffic, and to use this valuable data to enrich the overall security visibility.

Figure 32. *Control interactions between users, resources, data and applications*

MORE ZERO TRUST CONSIDERATIONS

The CESF architect will consider the following points, amongst others, when developing the recommended security architecture:

- **Encryption:** A key point that resonates with many security professionals is the percentage of encrypted traffic traversing perimeter gateways, and how effective perimeter security can be given the levels of encryption. For example, VPN, SSL, and TLS all traverse without inspection and to properly inspect this traffic will involve monetary and time resources.
- **Security effectiveness:** Zero Trust helps security architects deal with the role of network security in modern environments. The effectiveness of network controls is reduced due to end-to-end encryption and the ability to place network security controls in-path.
- **Micro-segmentation and visibility:** In order to keep threats isolated and any infection blast-radius contained, highly segmented or micro-segmented networks are needed. Increasing the amount of segments gives us more opportunity to monitor and record traffic. This should result in a high-degree of network visualization.
- **Flat networks:** Zero Trust can often be an effective way to address security in flat networks or where an organization wants to change fundamental ways of working, i.e., mobilization and worker agility. In such cases it can often be easier to move to a Zero Trust architecture that puts identity at its core, as opposed to creating traditional IP segmented networks.

DESIGNING OPERATIONAL PROCESSES

The *"design"* layer of the CESF is primarily concerned with making recommendations that advance the client's security posture through technology recommendations. However, there is also scope to assist clients outside of purely technological solutions.

Changes to operational and business processes can often lead to more secure and manageable security solutions. The CESF process acknowledges the value of such changes to the overall security architecture.

Workflow Process

How customers manage, their environment has a significant impact on the technology used. In some instances, the client may not have the capacity to manage a complex security ecosystem, so the architect might propose changes to the workflow process in order to enable a simpler, more manageable security.

Recommendations that address changes to workflow processes can often include use of new technology, such as automation, and:

- Simplification of the security policy
- Simplification of the change control process
- Sharing responsibility for the security policy with other teams, such as application owners

Operational Efficiency

How the client's operational team conducts the management of their security estate has an impact on security effectiveness. Often when security infrastructure becomes more complex, the size of a security team remains static. The CESF process recognizes this potential issue and is cognitive of the impact changes to security controls, services and processes can be.

We must consider the people and process component of security architecture as the part of the design process. Recommendations should be cognitive of the impact on the operational team's workload and responsibilities.

When relevant, the CESF architect will make recommendations to operational practices for the betterment of the overall security architecture. Often the CESF architect will be able to draw on first-hand experience of security operations (SOC) and share their relevant knowledge.

Examples of recommendations that might be included in the report include:

- Adoption of design templates from a pre-built service catalogue in order to reduce the design cycles.
- Changes to the change-control process so that pre-approved changes are allowed, resulting in security changes that can be implemented quicker.
- DevOps teams take control of intra-zone access control policies in order to reduce the change to implementation times.
- Assistance to help define the network as a cloud platform in order to help simplify cloud transition.

12 The Build Layer

OVERVIEW

We define the *"build"* layer as the layer at which the CESF architect will build a logical representation of the recommended architecture, including any changes to business processes and operations. The previous *"design"* layer gave us the principles and components that we can use. It is now time to pull these together into a working security architecture.

The design blueprints produced at this layer are a key deliverable handed back to the client, and define the CESF architect's vision for the client's architecture.

The main technology deliverables from this layer are the document;

- The placement of security controls into the security architecture
- The completed desgin blueprints and referance architecture
- The placement of components and services required to complete a Zero Trust design
- The use of the Check Point Infinity architecture

The main **operational/process** deliverables from this layer are:

- Document any recommendations to improve business processes that support the recommended architecture.

The following section will describe the techniques, processes, and tools used as part of this layer.

NETWORK SEGMENTATION AND TRUST ZONES

The process of network segmentation is a topic in its own right and we will not attempt to discuss it in full here. What is important to note is that at the completion of the design layer, a fully segmented architecture is defined. This logical design is aligned to Zero Trust architecture and our best practices.

The CESF process relies heavily on Zero Trust to inform how we approach segmentation. A key tenet of Zero Trust is to design a network that enables micro-segmentation for the purposes of increasing security visibility and reducing risk. Practitioners of cyber security will know the security benefits of moving to a properly segmented network and CESF architects will use segmentation best practice as a core design principle.

Key Point: *In some cases networks are suited to a more traditional segmentation approach. The approach is a product of the pervious layers of the CESF process.*

The graphic on the right shows some of the CESF design process:

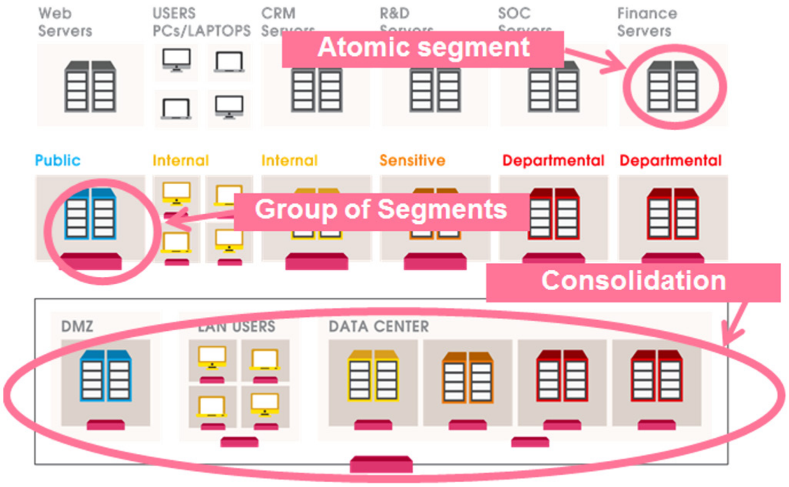


Figure 33. *Network segmentation practice in action*

ALIGNMENT WITH ZERO TRUST

In the previous section we looked at the various Zero Trust principles that make up a Zero Trust architecture, and we looked at the various design methodologies and the core features that need to exist in the Zero Trust design. We can now use these to influence where components are required, where they will be located, and how they will interact.

Key Point: *It's norma to find that organizations are not abe to immediatey convert to a compete Zero Trust architecture. However, because the architect knows the key attributes required in the design, they are abe to seect what components of Zero Trust are the most appropriate*.

Depending on the outcome of the workshop phase, the CESF architect would define one, or all, of the Zero Trust building blocks to be included in the final design. According to the principles of CESF, which we have discussed in previous sections, the design must be based on clear business requirements. Consequently, how Zero Trust is implemented is conditional on the outcome of the workshop. Below are the various Zero Trust designs that could be used.

- **Zero Trust Networks:** Reduce the risk of lateral movement with micro-perimeters and identity-based policies.
- **Zero Trust People:** Use multi-layer authentication to identify and verify all corporate access to any internal asset.

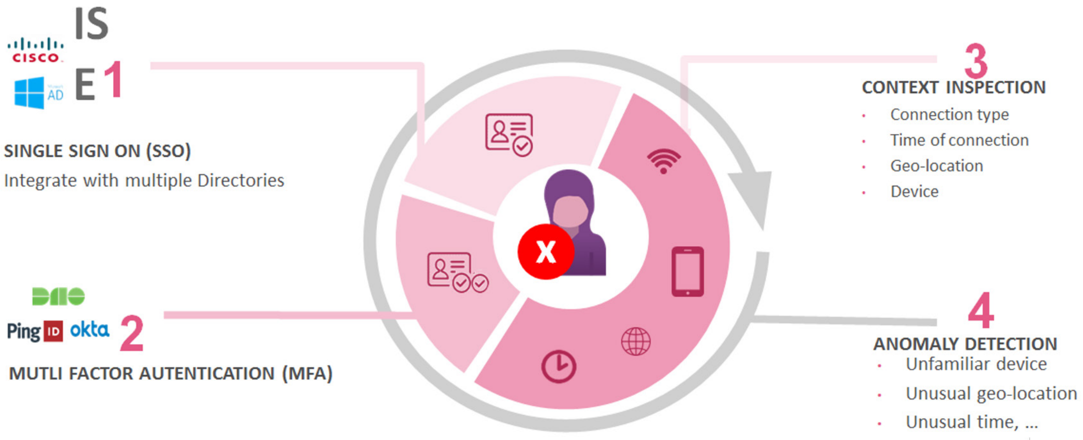
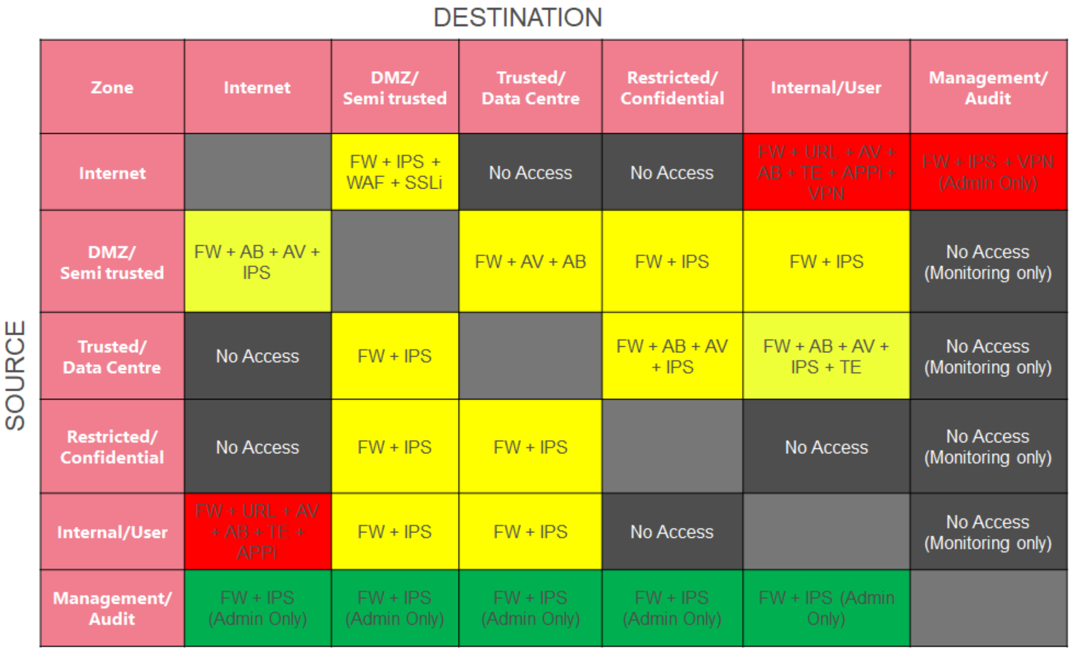


Figure 34. *The components required for Zero Trust people design*

- **Zero Trust Devices:** Secure, control, and isolate every device on your network.
- **Zero Trust Workload:** Secure data and applications in public clouds and data centers.
- **Zero Trust Data:** Keep data secure, anywhere, with comprehensive multi-layered protection.
- **Visibility and Analytics:** Full threat visibility with a single view into security risks, integrating Security Information Management (SIM) and more advanced security analytics platforms like Security User Behaviour Analytics (SUBA). Other analytics systems can also be enabled to know and understand what is taking place in the network.
- **Automation and Orchestration:** Automate all processes and tasks using flexible APIs and rich 3rd party integrations. Providing the ability to have positive command and control of the many components that are used as part of the Zero Trust strategy is a vital piece of the extended Zero Trust ecosystem.

DEFINING SECURITY CONTROLS

In the previous layer, we identified the various security components required to satisfy the business objectives. Now, we need to place these components into the network. This work is conducted by the CESF architect based on all the factors we have discussed previously, namely Zero Trust, best practice and business requirements. The example below shows security controls and their logical network positions.



DESTINATION

SOURCE

Zone	Internet	DMZ/ Semi trusted	Trusted/ Data Centre	Restricted/ Confidential	Internal/User	Management/ Audit
Internet		FW + IPS + WAF + SSLi	No Access	No Access	FW + URL + AV + AB + TE + APPi + VPN	FW + IPS + VPN (Admin Only)
DMZ/ Semi trusted	FW + AB + AV + IPS		FW + AV + AB	FW + IPS	FW + IPS	No Access (Monitoring only)
Trusted/ Data Centre	No Access	FW + IPS		FW + AB + AV + IPS	FW + AB + AV + IPS + TE	No Access (Monitoring only)
Restricted/ Confidential	No Access	FW + IPS	FW + IPS		No Access	No Access (Monitoring only)
Internal/User	FW + URL + AV + AB + TE + APPi	FW + IPS	FW + IPS	No Access		No Access (Monitoring only)
Management/ Audit	FW + IPS (Admin Only)	FW + IPS (Admin Only)	FW + IPS (Admin Only)	FW + IPS (Admin Only)	FW + IPS (Admin Only)	

Figure 35. *Security contro to network segment-mapping matrix*

DESIGN BLUEPRINTS

The completion of the build phase is the publishing of the Check Point workshop report, which we will discuss in the next section. A core component of the report is the design blueprints. These present the recommended logical security architecture, the security components, and their placement within the network.

The CESF architecture will draw on a number of resources in this part of the process. Some of these are:

- **Security Control Matrix:** The controls, components and services that were identified and linked to the business and architectural review will now be transposed to the design blueprints.
- **Best Practices:** Applying the industry and Check Point security best practice guides, as well as our own industry knowledge means that design blueprints are able to form the basis of any low-level design that might follow. The components are placed in the design relative to the required position and in relation to other security components.
- **Segmentation:** The segmentation architecture, including alignment with Zero Trust, as well as a proposal for segmentation rules.
- **Reference Architectures:** CESF architects have been conducting workshops for over five years. As a consequence the architects are able to draw on a design repository in the creation of the design blueprint and report. This allows designs to be referenced across industry verticals.

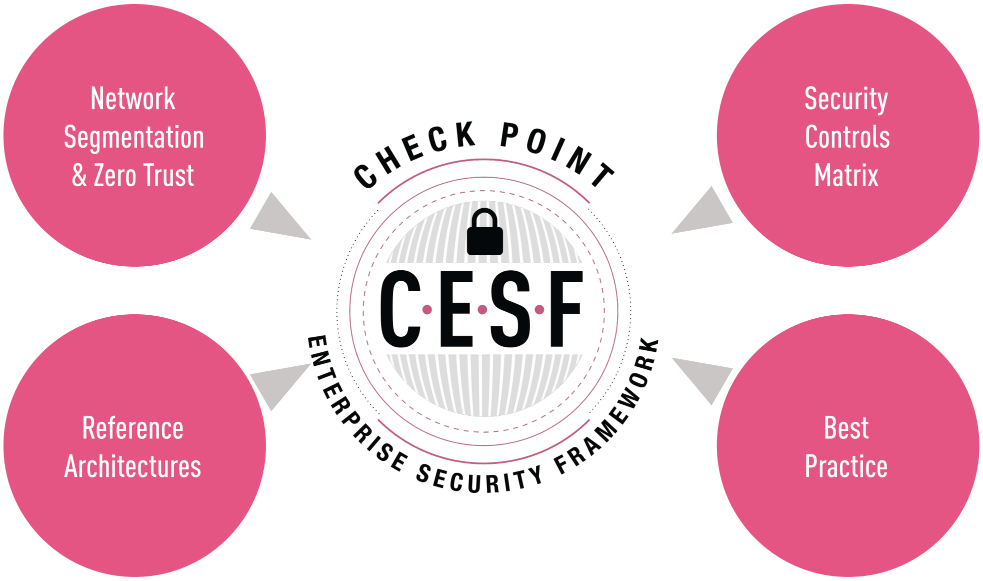


Figure 36. *Combining the various elements into the CESF process in order to define security architecture*

ZERO TRUST REFERENCE ARCHITECTURE

A highly segmented Zero Trust network means having security controls between all assets, reducing the ability of compromised assets to propagate malicious code, or for bad actors to pivot onto other machines and launch further attacks.

The graphic below shows a client's network in which multiple enforcement points have been established. As part of the CESF *"build"* layer, each of these enforcement points should be understood in the context of security and business re

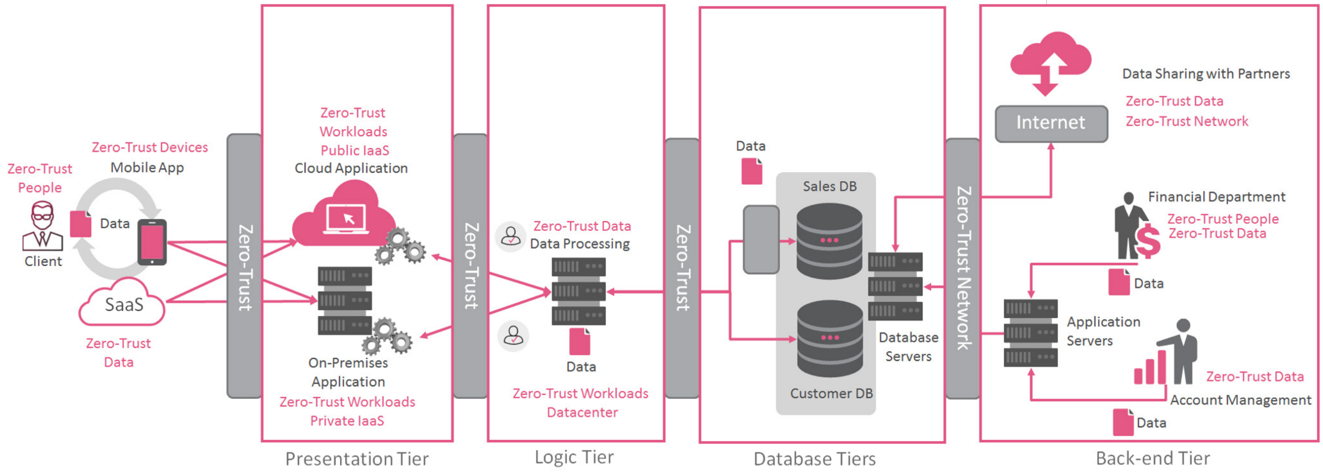


Figure 37. *A network segmented using Zero Trust principles*

INFINITY REFERENCE ARCHITECTURE

Check Point has always defined security architecture in a way that addresses all the components of a security ecosystem. Check Point Infinity architecture is a single-platform methodology whereby the entire security ecosystem is built on a common technology platform.

The key benefits of adopting this methodology are:

- **Attack Surface:** A single-platform approach where security products form each part of the network, including endpoint, cloud, and mobile, work together as a single security ecosystem.
- **Complexity:** Multiple security platforms normally means multiple management platforms, all of which need to be supported. Multiple point solutions can reduce overall security effectiveness. Building a security ecosystem means the sum of the total is more than that of the individual components.
- **Operational** and engineering teams are under increased pressure to deliver projects faster. Using the Infinity architecture approach means less complexity because the entire security infrastructure is managed from a centralized security policy.
- **Intelligence:** At the heart of Infinity architecture is the concept that by combining and sharing threat intelligence, from multiple sources, we are better able to protect the network, users and workloads.

Check Point Infinity architecture is described in the graphic below, where the entire security ecosystem is integrated with a cloud-based, threat-intelligence data store, and where management is consolidated.

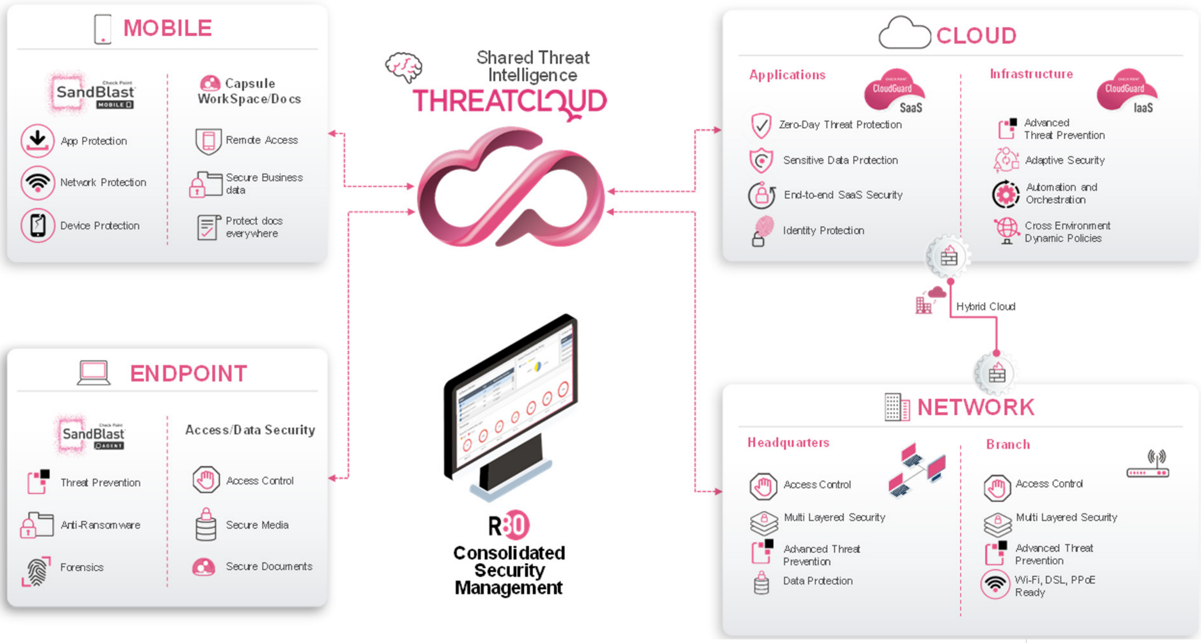


Figure 38. *The Check Point Infinity architecture*

Key Point: *Check Point Infinity is a cyber security architecture which future-proofs business and IT infrastructure across all networks, including cloud and mobile. The architecture is designed to resolve the complexities of growing connectivity and more challenging security.*

OTHER REFERENCE ARCHITECTURES

When developing a logical architecture, the CESF process allows for the use of any open and documented architectural reference guides. In some cases, there may be specialized technology or compliance references that can inform the architectural choices.

While the logical architecture must reflect business requirements, it should also be aligned with relevant architectural practices. For example, the Purdue model is widely used when developing SCADA security architecture.

THE REPORT

If the CESF process is going to be an effective means of communicating a long-term vision for better security, then it must be properly documented. At the completion of this layer, the architect will have created a bespoke report that outlines the key design and security concepts that Check Point would recommend for meeting the client's requirements.

The report is the only deliverable from the workshop that documents the design process from conception to completion.

Security Workshop Report

CUSTOMER

Version 2018.1
Updated 12/15/2018

XXXXXX XXXXXXXX,

Check Point Global Security Architect

generic logo company
Check Point SOFTWARE TECHNOLOGIES LTD.
We Secure the Internet.
Check Point SOFTWARE TECHNOLOGIES LTD.
TOC

Table of Contents

1. Executive Summary 3
2. Security Review 6
2.1. "CheckUp" Security Report 6
2.2. Network Security Design Review 6
2.3. Operations and Management review 8
3. Security Design Proposal 11
3.1. General Network Security Architecture 12
3.2. Security Segmentation 14
3.3. Network Security Recommendation 17
4. Security Management Design 20
4.1. Security Event Analysis 27
4.2. Best Practices and Policy Validation (Compliance) 28
5. Solutions Overview 30
5.1. Identity-based Access (IDA) 30
5.2. Internet access (Web Security) 38
5.3. Threat Emulation / Extraction (Zero-Day) and Data Loss Prevention 40
5.4. Mobile and Endpoint Security 42
5.4.1. Mobile Threat Prevention (SandBlast Mobile) 44
5.4.2. Endpoint Security 47
5.5. SCADA – Critical Infrastructure Protection 55
6. Check Point SaaS 62
7. Check Point IAAS 65

©2018 Check Point Software Technologies Ltd. All rights reserved
[Restricted] ONLY for designated groups and individuals
2

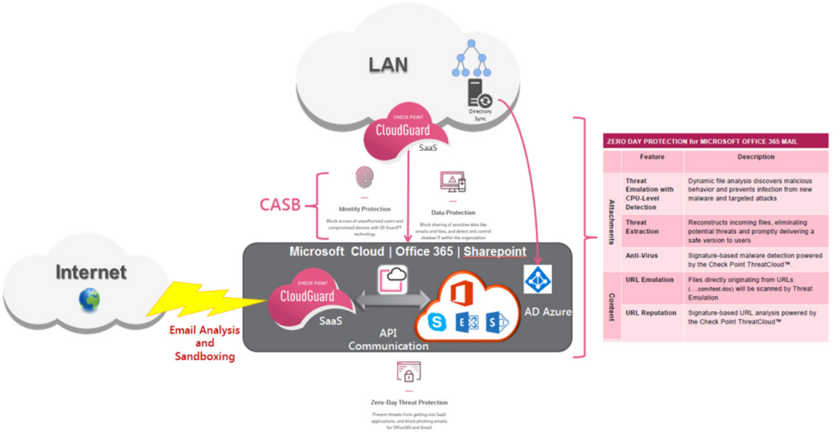
Figure 39. *Sample report*

REPORT CONTENTS

The standard report aims to be a single source of high-level design recommendations based on business requirements and security drivers. At a minimum, a report contains:

- **Review and Architecture:** What data was captured during the workshop and the existing network topology highlighting the components that should be considered as part of the overall security posture.
- **Best Practices:** The Check Point architect's methodology. This section explains how the various attributes have been assigned and why.
- **Conceptual Design:** A comprehensive, high-level security architecture report (50-80 pages) with findings and a recommended design. Personalized reports are crafted for each client.

- **Solution Overview:** An explanation of the components, which are included in the solution. The solution overview adds context to the personalized solutions presented in the recommendations section.
- **Operational Processes:** The report will often contain recommendations and advice that deals with improvements to the business process, workflow, or operational changes. These business consultancy recommendations are beyond pure technology recommendations.



Block access of unauthorized users and compromised devices with ID-Guard™ technology

Block sharing of sensitive data like emails and files, and detect and control shadow IT within the organization

Prevent threats from getting into SaaS applications, and block phishing emails for Office365 and Gmail

ZERO DAY PROTECTION for MICROSOFT OFFICE 365 MAIL

	Feature	Description
Attachments	Threat Emulation with CPU-Level Detection	Dynamic file analysis discovers malicious behavior and prevents infection from new malware and targeted attacks
	Threat Extraction	Reconstructs incoming files, eliminating potential threats and promptly delivering a safe version to users
	Anti-Virus	Signature-based malware detection powered by the Check Point ThreatCloud™.
Content	URL Emulation	Files directly originating from URLs (.....com/test.doc) will be scanned by Threat Emulation
	URL Reputation	Signature-based URL analysis powered by the Check Point ThreatCloud™

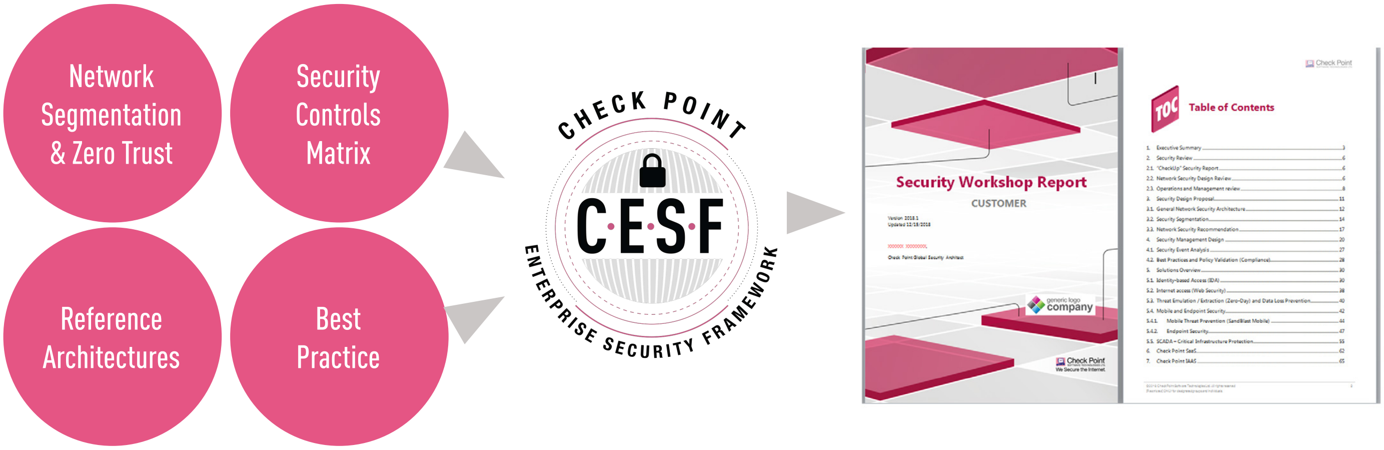
Figure 40. *Example taken from a workshop report.*

Key Point: *It's important to remember that the report is ony designed to give high-eve recommendations, design advice, and conceptua architecture, and not ow-eve design. The transition from high-eve concepts to ow-eve, impementabe, design is discussed in the next section.*

CONCLUSION: DESIGN AND BUILD

By applying Zero Trust design methods, leveraging industry recognized security best practices and interpreting the client's business requirements, the CESF architect is able to provide complete security architecture and solutions design. Blueprints and security services are documented in a bespoke report that, if required, can be moved to an implementation phase.

The architect has now finished the *"design"* and *"build"* phase of the client's security architecture.



Security Workshop Report

CUSTOMER

Version 2018.1
Updated 12/18/2018

XXXXXX XXXXXXXX

Check Point Global Security Architect

Table of Contents

1. Executive Summary 3
2. Security Review 6
2.1. "CheckUp" Security Report 6
2.2. Network Security Design Review 6
2.3. Operations and Management review 8
3. Security Design Proposal 11
3.1. General Network Security Architecture 12
3.2. Security Segmentation 14
3.3. Network Security Recommendation 17
4. Security Management Design 20
4.1. Security Event Analysis 27
4.2. Best Practices and Policy Validation (Compliance) 28
5. Solutions Overview 30
5.1. Identity-based Access (IDA) 30
5.2. Internet access (Web Security) 38
5.3. Threat Emulation / Extraction (Zero-Day) and Data Loss Prevention 40
5.4. Mobile and Endpoint Security 42
5.4.1. Mobile Threat Prevention (SandBlast Mobile) 44
5.4.2. Endpoint Security 47
5.5. SCADA – Critical Infrastructure Protection 55
6. Check Point SaaS 62
7. Check Point IAAS 65

Figure 41. *Taking the outcome from the review /architecture layers and producing a workshop report*

At the conclusion of this phase, we will have:

Completed the design layer:

- Mapped the business attributes to real-world security controls
- Completed the process of network segmentation
- Recommended changes to operational and business processes that would advance the security posture

Completed the build layer:

- Built the recommended security architecture
- Defined the placement of security controls
- Documented recommendations to business processes and operational efficiencies

Completed the workshop report:

- Combined the workshop blueprints and other requirements into a single security architecture package ready for low-level design and implementation
- The workshop report is presented to the client for approval and final sign-off

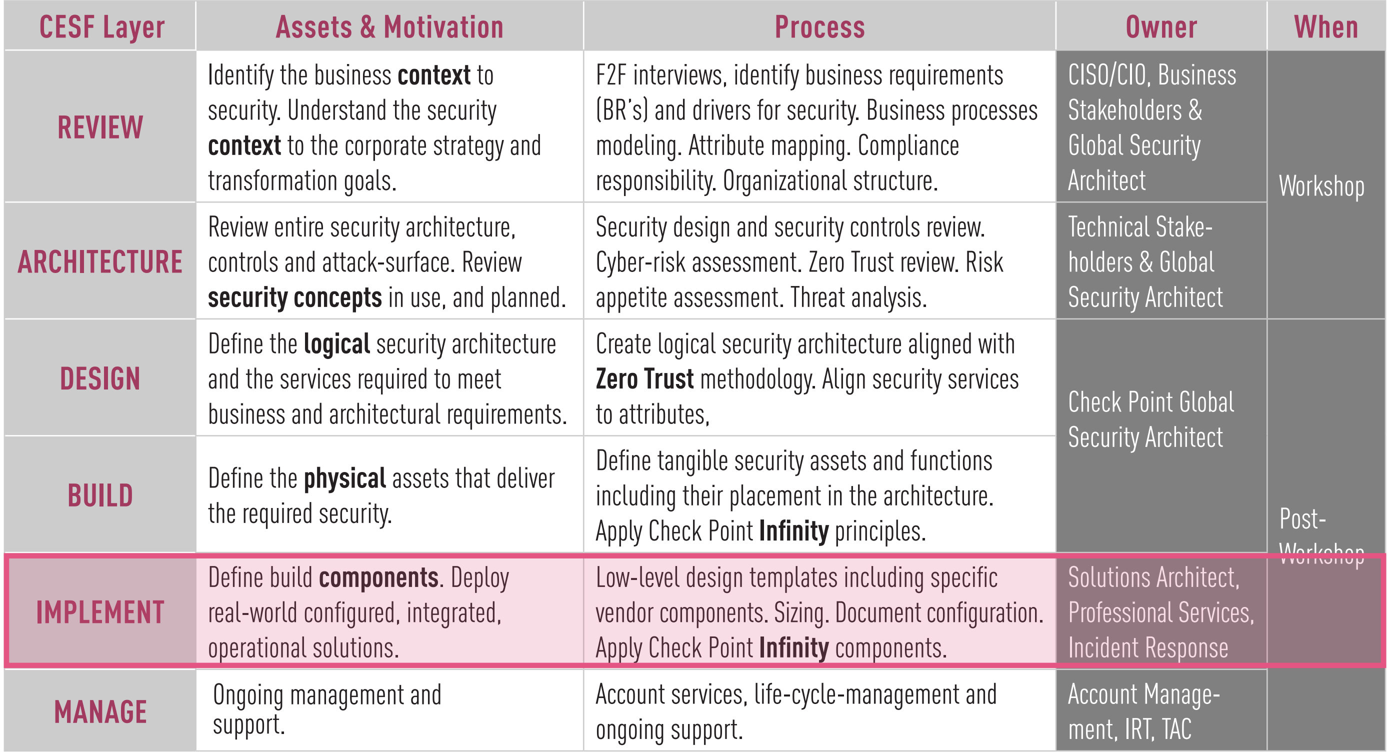
13 The Implementation Layer

OVERVIEW

We refer to this layer of the framework as the *"implementation"* layer in the CESF process. At this layer, the architect's design blueprints become a tangible working security ecosystem, one that respects the client's requirements.

In the *"implementation"* layer, the logical design is handed to other teams so that the various components, services, and processes can have real-world meaning and exist in the client's network or as part of the client's process.

We would expect that the recommendations are fully costed and that this is presented and agreed with the client.



CESF Layer	Assets & Motivation	Process	Owner	When
REVIEW	Identify the business **context** to security. Understand the security **context** to the corporate strategy and transformation goals.	F2F interviews, identify business requirements (BR's) and drivers for security. Business processes modeling. Attribute mapping. Compliance responsibility. Organizational structure.	CISO/CIO, Business Stakeholders & Global Security Architect	Workshop
ARCHITECTURE	Review entire security architecture, controls and attack-surface. Review **security concepts** in use, and planned.	Security design and security controls review. Cyber-risk assessment. Zero Trust review. Risk appetite assessment. Threat analysis.	Technical Stakeholders & Global Security Architect	
DESIGN	Define the **logical** security architecture and the services required to meet business and architectural requirements.	Create logical security architecture aligned with **Zero Trust** methodology. Align security services to attributes,	Check Point Global Security Architect	Post-Workshop
BUILD	Define the **physical** assets that deliver the required security.	Define tangible security assets and functions including their placement in the architecture. Apply Check Point **Infinity** principles.		
IMPLEMENT	Define build **components**. Deploy real-world configured, integrated, operational solutions.	Low-level design templates including specific vendor components. Sizing. Document configuration. Apply Check Point **Infinity** components.	Solutions Architect, Professional Services, Incident Response	
MANAGE	Ongoing management and support.	Account services, life-cycle-management and ongoing support.	Account Management, IRT, TAC	

Figure 42. *CESF showing the implementation layer and its owners*

THE IMPLEMENTATION LAYER

At this layer, the architect is not the owner. Check Point teams, partners and implementation engineers are now responsible for carrying out the physical implementation of the design.

Key Point: *Ownership of the process changes at this layer.*

Key Point: *When the overall design reaches this layer, the logical architecture would have been shared with the client and approved.*

COMPONENT AND PROCESS DESIGN

We would expect that all CESF designs and blueprints have physical components. The CESF architect would have produced a design blueprint to a level of detail required by the security engineering professional to translate it into a working solution.

Key Point: *At this layer, the logical architecture is now expected to become a reality.*

As part of the *"design"* and *"build"* layer, we have mapped the attributes to technology and operational processes. The *"implementation"* layer represents the process of further developing these choices into the physical security mechanisms and security services.

The table below shows how the CESF process expects the *"implementation"* layer to describe the design.

CESF Layer	Description	Example
REVIEW	Business requirements and security focused drivers	Protect our hosted sites from external attacks so that business is not disrupted
ARCHITECTURE	The concepts that are used to define the business and security posture	Platform needs to be secure and accessible partially from Internet threat actors
DESIGN	Identifying the services that are required	An intrusion prevention service
BUILD	What is needed for the design to work	IPS software running on a gateway appliance
IMPLEMENT	**What is needed to meet the physical requirements of the design**	**Check Point R80.40 IPS blade running recommended profile**

Figure 43. *The language used to describe security things is different at each layer*

If the design blueprints are to be stood up as a working solution, then professionals with working knowledge of the implementation must to do this. The Check Point teams that the CESF would expect to be engaged in this layer are:

- **Engineering –** Check Point's qualified engineers across all disciplines are able to address the low-level requirements of the design. These teams are critical to realizing the design in real-world terms. Specialist engineering teams will have practical working knowledge of the various components. Check Point engineers are also able discuss how Check Point products work "under-the-hood" and engage with the client on proof-of-concepts and product testing.

- **Professional Services –** For complex implementations, or where customizations are required, professional services can be used. These teams are able to translate the high-level design into a low-level implication plan and drive this to completion. These teams often communicate with R&D departments to find customized solutions, when required.

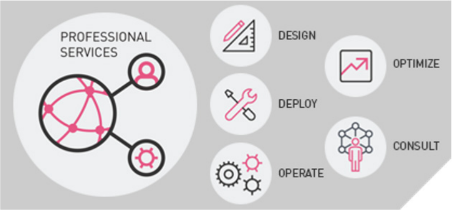


Figure 44. *Check Point Professional Services*

- **Incident Response –** Check Point security services, such as incident response teams, are included as there is often a business requirement for incident response and handling services.

- **Solutions Centre –** Where there is complexity in design, these specialist teams are able to craft non-standard services. For example, when a specific skill is required, the services of Check Point Solution Centre are available to create custom hot fixes.

Figure 45. *Check Point Incident Response Team*

- **Account Services –** Designs that have progressed to this layer are fully costed and this information is shared with the client. Ongoing service management is covered in the subsequent layer. However, professional services, incident response teams, and component costs are considered part of this layer.

SIZING AND SYSTEM INTERACTIONS

Implementation of any solution must address how components interact, their dependencies as well as configuration best practice. Subject matter experts will consult with engineers to make sure that the proposed solutions fit the design, and the logical design will become a physical architecture ready for implementing.

Key Point: *As with aengineering work, component sizing is a key consideration. The purpose of thisayer is to compete this process and to factor in elements such as future capacity requirements.*

OUTPUT AND DELIVERABLES

The diagram below shows how the implication layer deliverables are linked to the workshop report. It shows how the various layers of the CESF work together so that the output of this layer is low-level design.

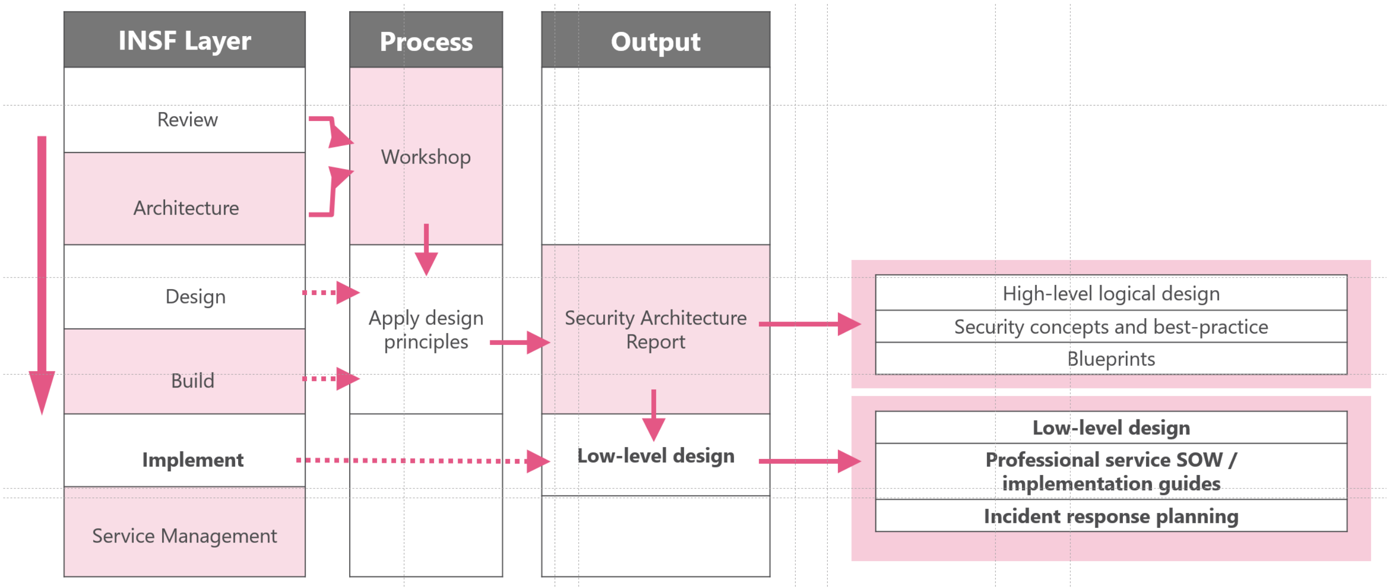
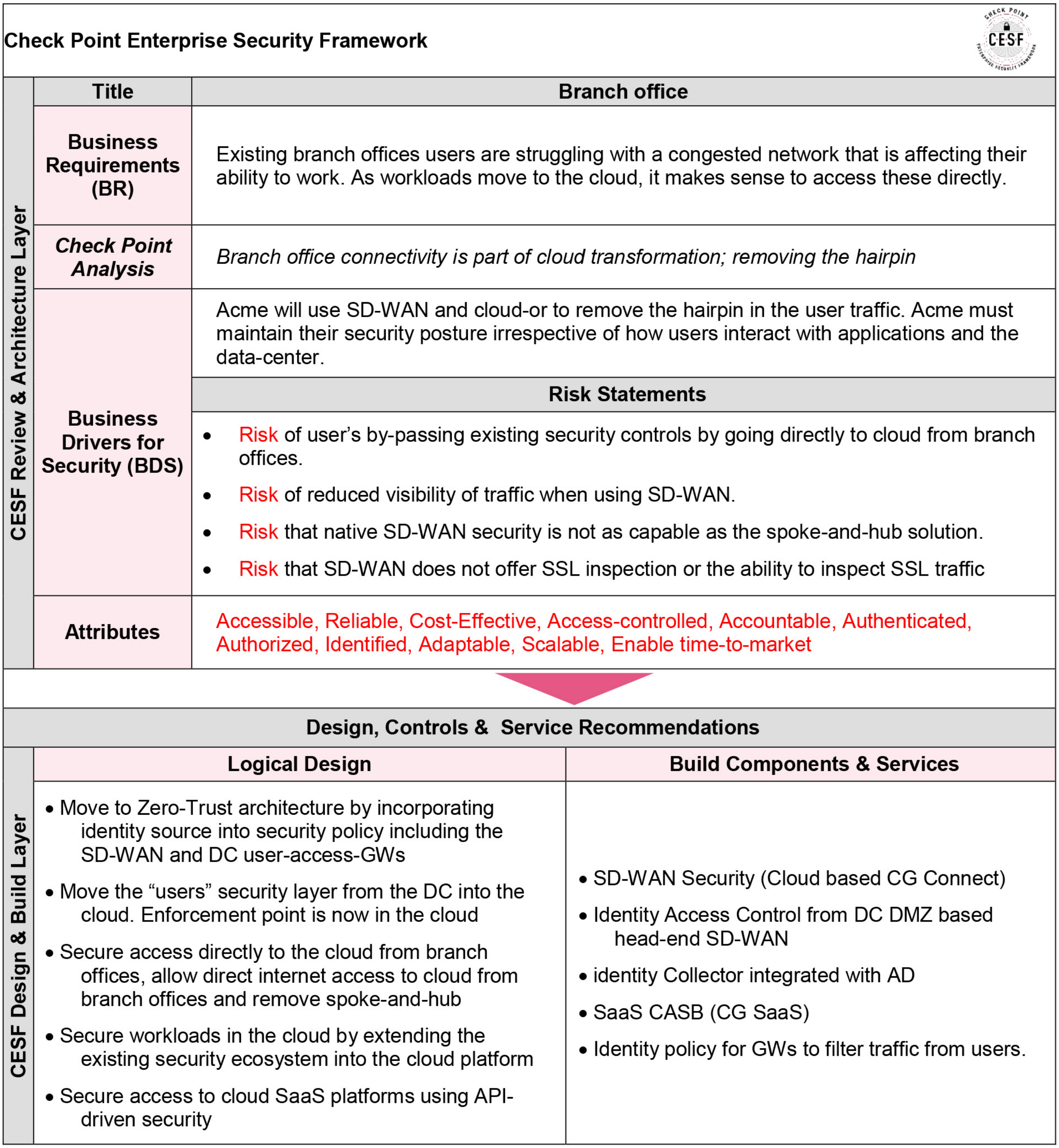

INSF Layer
Process
Output
Review
Architecture
Workshop
Design
Build
Apply design principles
Security Architecture Report
High-level logical design
Security concepts and best-practice
Blueprints
Implement
Low-level design
Low-level design
Professional service SOW / implementation guides
Incident response planning
Service Management

Figure 46. *The output from the implementation layer should be enough to complete a working design*

END-TO-END EXAMPLE

The following data-capture table shows a completed project whereby the business requirement has been translated to a design and set of Check Point components. Using data-capture forms allows the entire process to be viewed on a single page, albeit at a high-level.



Check Point Enterprise Security Framework

CESF

CESF Review & Architecture Layer	Title	Branch office
	Business Requirements (BR)	Existing branch offices users are struggling with a congested network that is affecting their ability to work. As workloads move to the cloud, it makes sense to access these directly.
	Check Point Analysis	*Branch office connectivity is part of cloud transformation; removing the hairpin*
	Business Drivers for Security (BDS)	Acme will use SD-WAN and cloud-or to remove the hairpin in the user traffic. Acme must maintain their security posture irrespective of how users interact with applications and the data-center. **Risk Statements** • Risk of user's by-passing existing security controls by going directly to cloud from branch offices. • Risk of reduced visibility of traffic when using SD-WAN. • Risk that native SD-WAN security is not as capable as the spoke-and-hub solution. • Risk that SD-WAN does not offer SSL inspection or the ability to inspect SSL traffic
	Attributes	Accessible, Reliable, Cost-Effective, Access-controlled, Accountable, Authenticated, Authorized, Identified, Adaptable, Scalable, Enable time-to-market

Design, Controls & Service Recommendations

CESF Design & Build Layer	Logical Design	Build Components & Services
	• Move to Zero-Trust architecture by incorporating identity source into security policy including the SD-WAN and DC user-access-GWs • Move the "users" security layer from the DC into the cloud. Enforcement point is now in the cloud • Secure access directly to the cloud from branch offices, allow direct internet access to cloud from branch offices and remove spoke-and-hub • Secure workloads in the cloud by extending the existing security ecosystem into the cloud platform • Secure access to cloud SaaS platforms using API-driven security	• SD-WAN Security (Cloud based CG Connect) • Identity Access Control from DC DMZ based head-end SD-WAN • identity Collector integrated with AD • SaaS CASB (CG SaaS) • Identity policy for GWs to filter traffic from users.

***Figure 47.** An end-to-end exampe of the CESF process*

14 Service Management

The final layer in the framework completes the CESF process. The service management layer is important as it sets up the ongoing process of design evaluation, in-flight account management, and the lifecycle management of the overall security architecture.

At this layer, we have completed the design and implementation of the logical architecture. Engineers now need to test and evaluate the solution.

The CESF owners for this layer are Check Point Professional Services, Check Point Incident Response Team, and account management teams.

CESF Layer	Assets & Motivation	Process	Owner	When
REVIEW	Identify the business **context** to security. Understand the security **context** to the corporate strategy and transformation goals.	F2F interviews, identify business requirements (BR's) and drivers for security. Business processes modeling. Attribute mapping. Compliance responsibility. Organizational structure.	CISO/CIO, Business Stakeholders & Global Security Architect	Workshop
ARCHITECTURE	Review entire security architecture, controls and attack-surface. Review **security concepts** in use, and planned.	Security design and security controls review. Cyber-risk assessment. Zero Trust review. Risk appetite assessment. Threat analysis.	Technical Stakeholders & Global Security Architect	
DESIGN	Define the **logical** security architecture and the services required to meet business and architectural requirements.	Create logical security architecture aligned with **Zero Trust** methodology. Align security services to attributes,	Check Point Global Security Architect	Post-Workshop
BUILD	Define the **physical** assets that deliver the required security.	Define tangible security assets and functions including their placement in the architecture. Apply Check Point **Infinity** principles.		
IMPLEMENT	Define build **components**. Deploy real-world configured, integrated, operational solutions.	Low-level design templates including specific vendor components. Sizing. Document configuration. Apply Check Point **Infinity** components.	Solutions Architect, Professional Services, Incident Response	
MANAGE	Ongoing management and support.	Account services, life-cycle-management and ongoing support.	Account Management, IRT, TAC	

Figure 48. *The service management layer*

15 The Service Management Layer

At this layer, the workshop report has been delivered and the technology has been implemented. In cases where Check Point advanced services are required by the design, then they would already be working with the account. When we get to this stage of the CESF process, both the architectural and implementation teams have completed their work.

It is now the responsibility of the other teams to maintain the momentum of the CESF process. The account service teams and technical support teams such as TAC and Diamond Services, who are responsible for the ongoing support of the implemented architecture, own this layer. These teams will work with the client for the duration of the solutions.

Key Point: *Account managers are responsible for restarting the CESF process.*

Account services and security engineers are in constant contact with the client, so it would be up to these teams to decide when to re-engage the architectural process. As the business requirements change, so too should the security architecture. The CESF process requires a Check Point representative to make sure the process does not stall and that the customer's solution is always relevant to their requirements.

The key features of this layer are:

- Understand and measure the success of the implemented solution
- Manage any support issues that arise
- Lifecycle management
- Quarterly business reviews
- Plan future workshops and subsequent CESF engagements

16 Summary and Conclusion

Check Point is pleased to present this paper as a new, innovative methodology for security architecture. We hope you have gained the insights as to why Check Point developed this framework and you understand how the process works.

Making informed architectural decisions based on clearly defined business requirements can help you understand the benefits and the context for why a specific solution is recommended.

All designers and architects strive to achieve completeness of vision in their solutions. Working within CESF means that only the requirements recorded are processed into solutions, allowing focus on solutions and justified results.

In addition, by developing a security architecture that is accountable and documented, the value of time spent designing and developing a security solution is justified.

We hope that by using the CESF process our clients can develop quicker solutions, create solutions that have a longer life cycle, and ensure that solutions are more efficient in terms of cost and security posture.

Worldwide Headquarters
5 Ha'Solelim 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; 650-628-2000 | Fax: 650-654-4233

www.checkpoint.com