CHECK POINT ENTERPRISE SECURITY FRAMEWORK (CESF)

A PROCESS-DRIVEN APPROACH TO SECURITY ARCHITECTURE

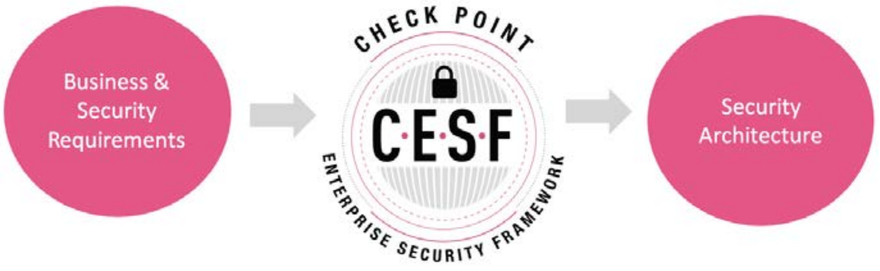
Signs of the digital transformation are everywhere. As security professionals, it's the defining statement of our time, quickly re-shaping the cyber security landscape. A complex digital future challenges our existing, long-held operational models and established business processes.

Check Point believes navigating this future requires the adoption of a structured methodical approach to transformation. It's simply not enough to choose a collection of technologies without a firm understanding of the why, what, and how they are used.

To help you tackle these challenges, Check Point developed an enterprise security framework capable of managing the process of transformation, end-to-end; and one that encompasses necessary security changes.

MANAGING CYBER SECURITY CHANGE

This paper outlines our new process-oriented approach to enterprise security architecture, drawing from well-known open frameworks, such as SABSA and Zero Trust. It also envelops Check Point's rich experience in delivering business-centric, strategic security solutions.


Business & Security Requirements
CHECK POINT
CESF
ENTERPRISE SECURITY FRAMEWORK
Security Architecture

Organizations can use CESF to translate requirements to solutions

Our process has taken the best parts of existing generic open frameworks and incorporated them into a process designed to produce real-world cyber solutions aligned to strategic goals. Solutions that are fully justified in-terms of cost and effort.

Our Check Point Enterprise Security Framework (CESF) allows us to provide you with an architectural service that extends cyber security effectiveness with these benefits:.

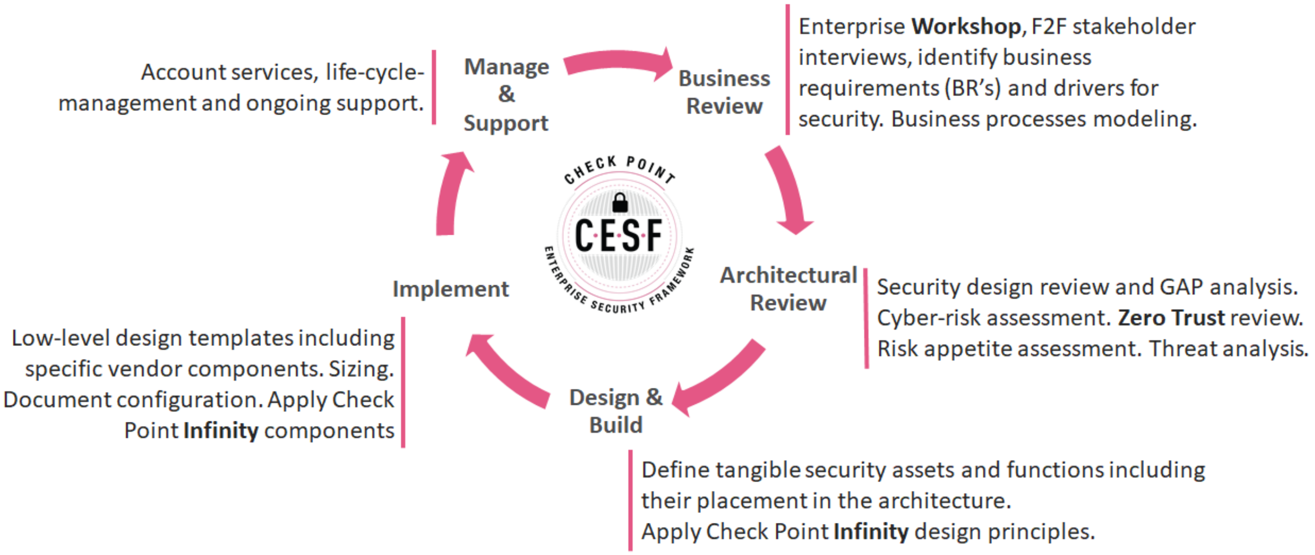
- **Accountable**: We build solutions around business requirements meaning full accountability and traceability.
- **Strategic**: The process delivers long-term strategic solutions, not just tactical point-solutions.
- **Complete** Building complete security ecosystems means starting with carful and thorough analysis.
- **Independent**: we build solutions aligned with industry best practice and our framework is open meaning more transparency in designs and justification.

THE CHECK POINT PROCESS

We define the Enterprise Security Framework as a set of open architectural principles for managing cyber security transformation. The framework is a model-driven process that takes business and security analysis, combined with security best practice and translates this into security solutions. The process starts with a detailed enterprise security workshop. Once completed, we move into a design phase where suitable solutions are developed and aligned with best practices such as Zero Trust and the Check Point Infinity architecture.

Only after you have approved the solutions, do they move to the implementation phase, where our partners and professional services can help implement our blueprints.

The infographic below shows the whole CESF 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.

THE CHECK POINT ENTERPISE SECURITY FRAMEWORK

We designed CESF to be open and accessible to all cyber security professionals. The table below shows how we capture the views of multiple teams and how all these different views contribute toward the end-state architecture.

We built CESF around these layers, each with a specific goal. They are conducted sequentially. Each layer helps collate and process your business and security needs as required. These layers offer you a complete, fully documented security architecture that meets your business requirements.

Customers view	CESF Layer	CESF Owner
Business View	**Review**	Clients view
Architect's View	**Architecture**	Check Point Architects
Solution designer's View	**Design**	
Engineer's View	**Build**	
Implementation Team's View	**Implement**	Pro Services & Partners
Service Manager's View	**Manage**	Incident response, TAC

SECURITY ARCHITECTURE WORKSHOP

As with most processes, there is a beginning and an end. Our process starts with a series of key stakeholder interviews and moves onto a detailed review of the current, future, and target security architecture. A key component of the workshop is to understand fully the drivers and the challenges to transformation, starting from the business perspective and then, to the technology perspective.

The Architecture Review Workshop is an exclusive, one-to-two-day customer engagement to openly discuss and review all aspects of existing security services. It also includes discussions deployment, design, architecture, along with the day-to-day operational challenges unique to managing the customer environment.

REPORTING

The CESF process is an effective means of communicating a long-term vision for improving security architecture and it culminates in a bespoke report that outlines the key recommended design concepts.

On completion, we will deliver an architectural report Blueprint designed to ensure that all critical assets are protected by the appropriate security controls. Our recommendations also address ways to lower operational costs, consolidate controls, and reduce operational time with maintenance, monitoring, and management.

CONCLUSION

Check Point believes that informed architectural, business-driven decisions are not only more cost-effective, but provides longer-lasting security than with un-planned point solution designs.

We believe cyber architects strive to achieve a completeness of vision in their solutions. Working within the Check Point Enterprise Security Framework allows you to meet what you require in your solution. This means you get a highly focused scope of work.

In addition, by developing a security architecture that’s fully accountable and well-documented, the benefits of a expertly designed security solution far outweighs the time and resources you spend.