CHECK POINT
ENTERPRISE SECURITY ARCHITECTURE WORKSHOP

JOINT COMMITMENT IS THE KEY TO SUCCESS

Active involvement from multiple disciplines and reporting levels help ensure that the workshop recommendations are accurate and effective. Check Point and the client should be represented by the following participants:

Check Point:

- Regional executive management
- Global security architects
- Accounts team
- Professional services
- Support engineers

Customer:

- Technology executives and business leaders
- Security and network architects, managers and engineers
- Risk professionals
- Operations managers and engineers

Agenda:

The workshop is a one day face-to-face engagement including the following:

- We review business processes, security strategy, operational, engineering and network architecture elements.
- We review technical controls: access control, virtualization, mobility, cloud and remote access.
- We actively participate in frramework, validation and conclusions taking business challenges into consideration.
- We deliver thorough and complete "before and after" recommendations based on all findings.

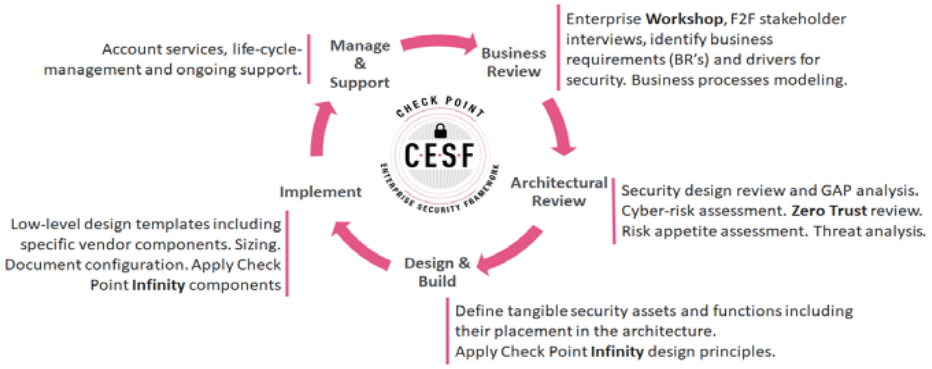
BETTER SECURITY BEGINS WITH A STRONG ARCHITECTURE

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. In scope are business processes, security strategy, deployment, design, and architecture, along with the day-to-day operational challenges unique to managing the client's security environment.

The result of the workshop is a customized security architecture that ensures our clients are protected by appropriate security controls through a proven and accountable design. The workshop report recommendations ways to lower operational costs, consolidate controls, and streamline operations regarding maintenance, monitoring and management.

BUILDING BUSINESS-DRIVEN SECURITY ARCHITECTURE

Enterprise architecture starts with a thorough understanding of the business, security and technology requirements. The workshop is based around open forum sessions with your cyber security stakeholders in order to complete a full business and architectural review.



CHECK POINT ENTERPRISE SECURITY FRAMEWORK

The workshop is built around the Check Point Enterprise Security Framework (CESF) and designed to meet our customers' requirements for accountable, actionable, holistic and vendor-agnostic architectural advice. The Check Point Enterprise Security Framework is built around the architectural methodology of SABSA, and the design principles of Zero Trust. The CESF allows Check Point to translate business requirements into working security solutions.

The motivation for **CESF** is to build a security architecture that is:

- **Strategic** – Defined long-term target architecture that minimizes overlapping technology and reduces spend.
- **Independent** – Solutions are be based on industry best practices, be open standards and customer-centric.

- **Justified** – Solutions must be traceable to business requirements. Security cost and decisions must be attributable and aligned.
- **Complete** – Proper analysis and alignment of corporate strategy with industry accepted frameworks ensure the solutions is built with no security gaps.

ZERO TRUST

The Check Point Enterprise Framework leverages Zero Trust as a core design principle. Zero Trust architecture is an IT security model that abolishes the idea of trust inside a corporate perimeter. Zero Trust requires strict identity verification for every person or device and includes all resources, regardless of where they reside in your network.

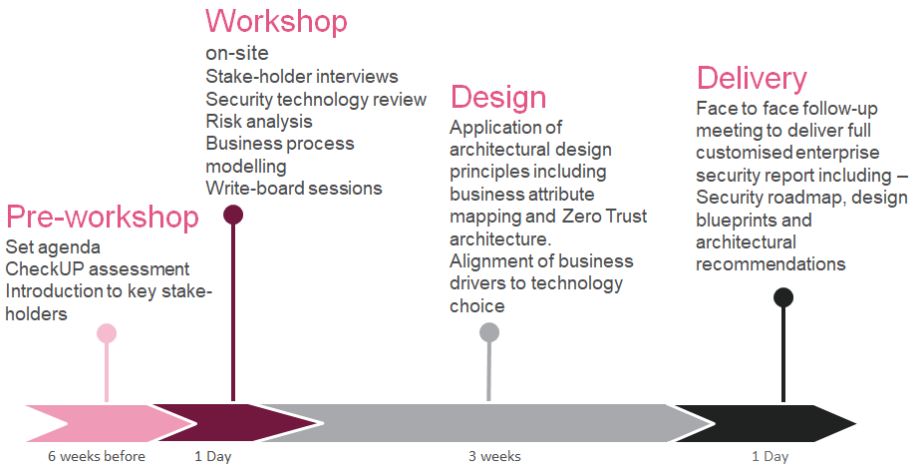
THE SECURITY ARCHITECTURE WORKSHOP

The Check Point Enterprise Architecture Workshop includes the following:

- **Business and Architecture Review**: Check Point teams capture multiple data-points relating to business context, strategy, organizational aspirations, security posture, etc. though a tailored face-to-face workshop. The framework is used because it meets the customers' requirements for a structured systematic approach to the design, architecture and ongoing digital transformation.

- **Design and Build Security Architecture**: Check Point architects develop a response to the business and security requirements that are aligned with security best practices and enable the clients' digital transformation. Open standards, such as Zero Trust, are used as architectural design principles. The Security Architecture Workshop and CESF process take a business requirement and translate it to a working, physical solution that protects the customer and reduces their cyber risk.

- **Timeline**: The infographic below show a typical workshop timeline.



ENTERPRISE SECURITY ARCHITECTURE REPORT

The result of the Enterprise Architecture Workshop is a report that contains the following:

- **Review and Architecture** – Review of the existing business processes, strategy and security estate, highlighting and documenting recommendations to improve the overall security posture.
- **Best Practices** – The Check Point architect's methodology. This section explains how the various security attributes have been assigned and why. Business requirements are aligned to known industry and security best practices.
- **Solution Overview and Recommendations** – Recommended solutions are presented as logical reference architectures and blueprints. Components are described in-terms of placement and accountability to the business requirements. These include Zero Trust, Purdue and Infinity aligned design patterns

For more information on CESF and the Check Point Enterprise Workshops please refer to:
https://www.checkpoint.com/support-services/security-workshop/