ABSOLUTE ZERO TRUST SECURITY
WITH CHECK POINT INFINITY

ABSOLUTE ZERO TRUST SECURITY

A practical. holistic approach to implementing zero trust security, based on a consolidated Security Architecture, Check Point Infinity.

Implement All of the Zero Trust Principles

- Zero Trust Networks
- Zero Trust Workloads
- Zero Trust People
- Zero Trust Devices
- Zero Trust Data
- Visibility & Analytics
- Automation & Orchestration

Efficiently Manage Zero Trust

- Centralized Security Management
- Unified Policy

Empower Zero Trust with Threat Prevention

- Globally Shared Threat Intelligence
- SandBlast Zero–day Protection
- 64 Different Security Engines

BACKGROUND

An ever-evolving IT environment and cyber-threat landscape have made legacy security infrastructures ineffective. Based on the outdated assumption that anything within the security perimeter can be trusted, they leave organizations exposed to cyber-attacks. As evidence, 34% of cyber attacks in 2018 were perpetrated by insiders.[1] Across the industry, security professionals are shifting to a Zero Trust security paradigm to close these security gaps. The *Extended Zero Trust Security model*, introduced by Forrester analysts, enables the adoption of a security posture of "Default Deny" where systems are isolated until a level of trust is established.

A PRACTICAL HOLISTIC APPROACH TO ZERO TRUST SECURITY

Rebuilding security infrastructure around a Zero Trust approach using point solutions may lead to complex deployment and inherent security gaps. To avoid that, Check Point offers a more practical and holistic approach to implement Zero Trust, based on single consolidated cyber-security architecture, Check Point Infinity.

Absolute Zero Trust Security, delivered by Check Point Infinity, offers a complete, efficient, and preventive implementation of the Zero Trust model.

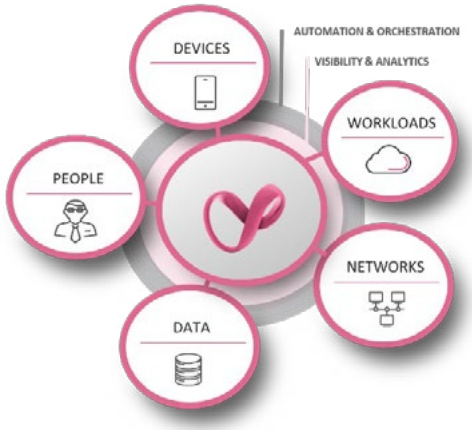

Figure 1: Absolute Zero Trust Security

COMPLETE ZERO TRUST

The Check Point Infinity architecture consolidates a wide range of security functions and solutions that enable you to implement all of the seven principals of the Extended Zero Trust Security model.

ZERO TRUST NETWORKS: *Check Point Security Gateways* enable you to create granular network segmentation across public/private cloud and LAN environments. With detailed visibility into the users, groups, applications, machines and connection types on your network, you can set and enforce a "Least Privileged" access policy, so only the right users and devices can access your protected assets.

ZERO TRUST WORKLOADS: *Check Point CloudGuard IaaS*, and *CloudGuard Dome 9* secure workloads, particularly those which are running in the public cloud. Seamless integration with any public or private cloud infrastructure provides you full visibility and control over these ever-changing environments; including AWS, GCP, Microsoft Azure, Oracle Cloud, IBM Cloud, Alibaba Cloud, NSX, Cisco ACI, Cisco ISE, OpenStack, etc.

[1] Verizon Data Breach Incident Report 2019

ZERO TRUST PEOPLE: *Check Point Identity Awareness,* and *Check Point CloudGuard SaaS* ensure that access to your data is granted only to authorized users, and only after their identities have been strictly authenticated; using Single Sign-On, Multi-Factor Authentication, context-aware policies (e.g., time and geo-location of the connection), and anomaly detection.

ZERO TRUST DATA: Check Point Infinity delivers multi-layered data protection that preemptively protects data from theft, corruption, and unintentional loss, wherever it is.

1. **Data Encryption** — *Check Point Full Disk Encryption, Check Point Media Encryption, and Check Point IPsec.*
2. **Data Loss Prevention** — *Check Point Data Loss Prevention.*
3. **Data Management Categorization and Classification** — *Capsules Docs*, and *Capsules Workspace*.

ZERO TRUST DEVICES: Check Point solutions enable you to block infected devices from accessing corporate data and assets, including employees' mobile devices and workstations, IoT devices, and Industrial Control Systems. Also, *Check Point SandBlast Agent* and *SandBlast Mobile* protect employees' devices at all times and maintain your corporate security policy on untrusted networks.

VISIBILITY AND ANALYTICS: Check Point Infinity is managed via *R80 Centralized Security Management* and *Check Point Smart Event* which provide full visibility into your entire security posture, so you can quickly detect and mitigate threats in real-time. View and analyze billion of log records with *Smart Log.* Investigate events with real-time forensics using the *Cyber Attack Dashboard.* Follow compliance with corporate policy and Data Protection Regulations with *Check Point Compliance*.

AUTOMATION AND ORCHESTRATION: Check Point Infinity includes a rich set of APIs that support automated integration with the organization's broader IT environment to enable speed and agility, improved incident response, policy accuracy, and task delegations. These APIs are used by over 160 Check Point's technology partners to develop integrated solutions.

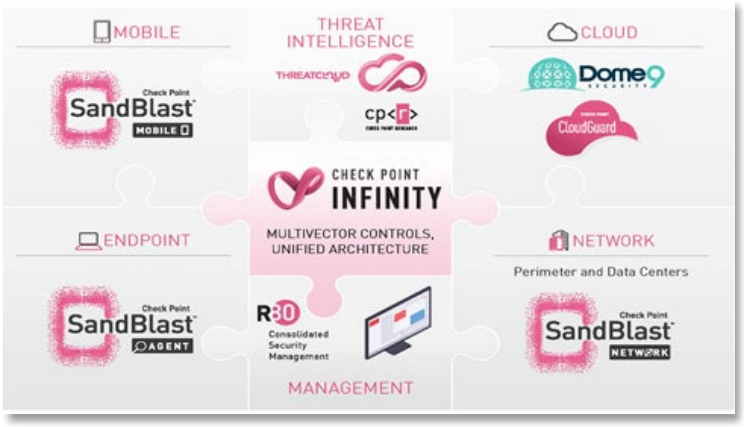

Figure 2: Check Point Infinity – A Consolidated Zero Trust Security Architecture

EFFICIENT ZERO TRUST

Check Point Infinity is managed centrally through the Check Point R80 centralized Security Management. With one console, security teams can manage all aspects of security from access policy to threat prevention – across the entire organization – on both physical and virtual environments.

PREVENTIVE ZERO TRUST

Focused on threat Prevention instead of detection, Check Point Infinity uses 64 different security engines to protect against known and unknown threats across all networks, endpoints, cloud, mobile, and IoT. It leverages globally shared threat intelligence powered by *ThreatCloud* to provide threat prevention technologies with the industry's best catch rate. Including the *Check Point SandBlast Zero-day Protection* product suite that delivers advanced protection against Zero-day malware with technologies such as threat emulation (sandboxing), threat extraction (safe content delivery), anti-phishing, endpoint forensics, and anti-ransomware.

THE INDUSTRY'S FIRST ZERO TRUST SECURITY WORKSHOP

To help you start adopting Zero Trust Security approach Check Point offers the industry's first Zero Trust workshop. During this two day workshop, Check Point Security Architects will plan a Zero Trust strategy customized for your business needs, along with a detailed implementation plan and a blueprint.

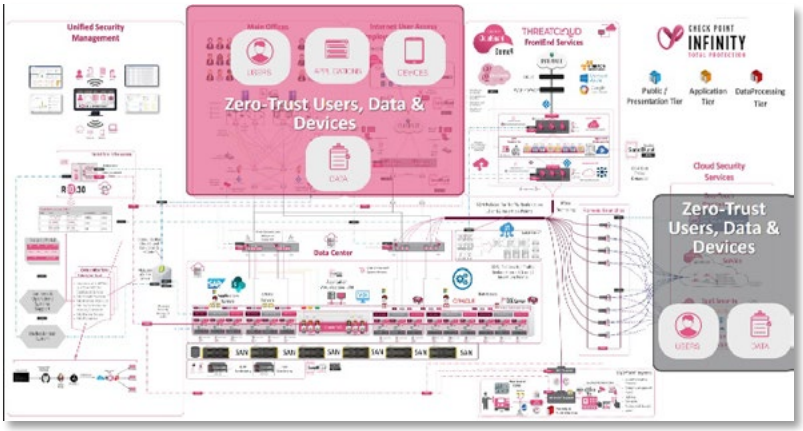

Figure 3: Zero Trust Architecture Blueprint example designed by Check Point Security Architecture team.