Check Point®
SOFTWARE TECHNOLOGIES LTD

ABSOLUTE ZERO TRUST SECURITY

WITH CHECK POINT INFINITY ARCHITECTURE

Are you designing or rebuilding your security infrastructure around a Zero Trust approach?

Learn how to implement Zero Trust security,
based on a single consolidated security architecture, Check Point Infinity.

TABLE OF CONTENTS

Introduction 3

Absolute Zero Trust Security with Check Point Infinity 4

Start Your Journey to Absolute Zero Trust 5

Complete Zero Trust 6

- Zero Trust Networks 6
- Zero Trust Workloads 7
- Zero Trust People 8
- Zero Trust Devices 9
- Zero Trust Data 10
- Visibility and Analytics 11
- Automation and Orchestration 13

Efficient Zero Trust 14

Preventive Zero Trust 15

Summary 17

INTRODUCTION

Cyber threats exist within and outside of the traditional secure enterprise perimeter. In 2018, 34% of cyber attacks were perpetrated by insiders[1].

In the face of this new reality, legacy perimeter focused security approaches have become ineffective. The outdated assumption that everything inside the security perimeter can be trusted leaves organizations exposed.

A new security paradigm closes these security gaps. Across the industry, security professionals are shifting to a Zero Trust Security state-of-mind: No device, user, workload or system should be trusted by default, regardless of the location in which it operates from, neither inside or outside the security perimeter.

The Zero Trust Extended Security model, introduced by Forrester analysts, offers seven key principles of implementation that organizations should focus on when moving toward a Zero Trust security model. Implementing these principles enables the adoption of a security posture of "Default Deny" where systems are hardened and isolated until a level of trust is established.

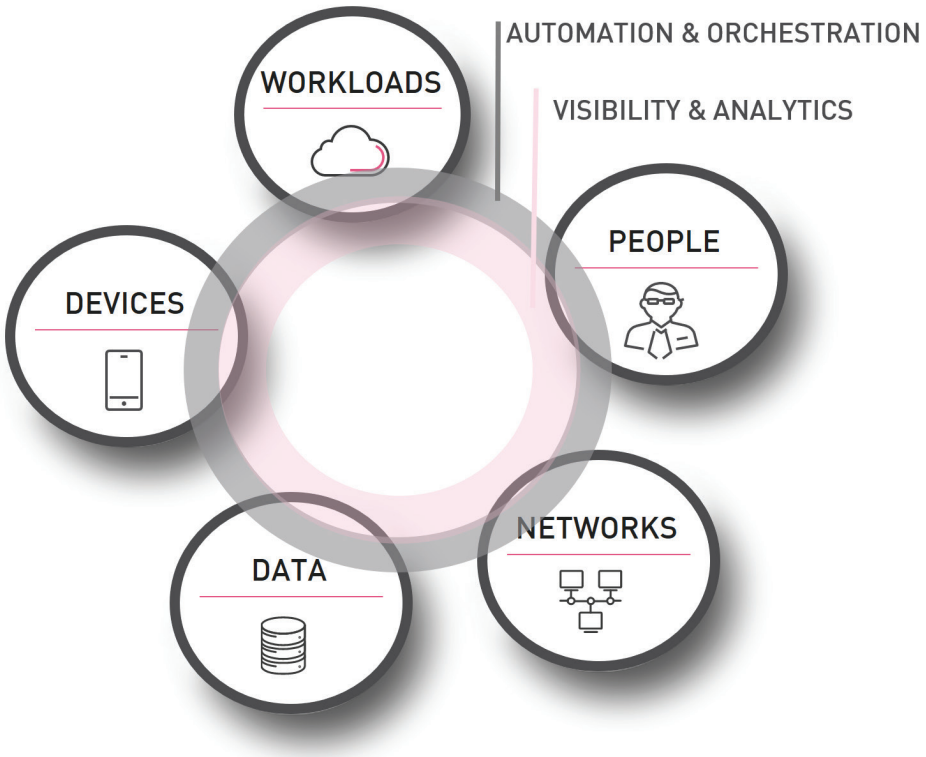

Figure 1: The Forrester Zero Trust Extended Security Model

[1] Verizon DBIR 2019

ABSOLUTE ZERO TRUST SECURITY WITH CHECK POINT INFINITY

A PRACTICAL HOLISTIC APPROACH TO ZERO TRUST SECURITY

Rebuilding your security infrastructure around a Zero Trust approach using disparate technologies might lead to complexities 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.

The Check Point Infinity security architecture enables organizations to fully implement all of the Zero Trust principles. Focused on threat prevention and centrally managed through a centralized security console, it empowers Zero Trust implementations with unparalleled security and efficiency.

COMPLETE

Accomplishes all of the Zero Trust principles

EFFICIENT

Centrally managed using a single console and a unified policy

PREVENTIVE

Focused on threat preventiion and protects from zero-day attacks

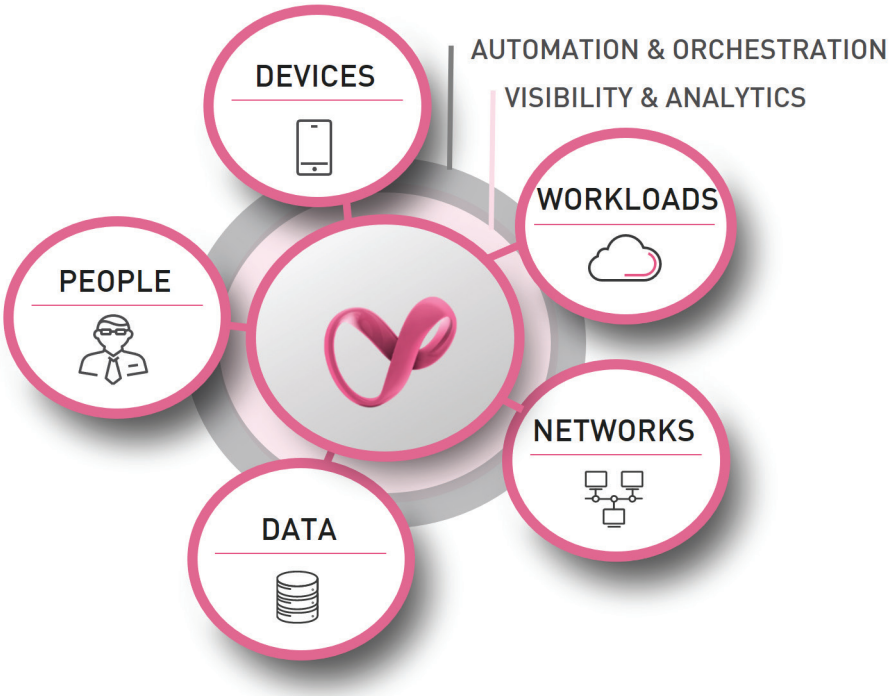

Figure 2: Absolute Zero Trust with Check Point Infinity

START YOUR JOURNEY TO ABSOLUTE ZERO TRUST

THE INDUSTRY'S FIRST ZERO TRUST SECURITY WORKSHOP

To help you start a safe journey to implement a Zero Trust approach, Check Point offers the industry's first Zero Trust Security workshop. Led by a team of Security Architects who are specialized and experienced in designing and implementing Zero Trust Security models for companies of different sizes and industries.

In this two-day workshop, we will review all aspects of your existing security infrastructure and design a customized Zero Trust Security Strategy and implementation plan for your business needs. Workshop benefits include:

- A Zero Trust Security deployment blueprint designed to ensure that all critical assets are protected by the appropriate security controls.
- Recommendations also address ways to lower operational costs, consolidate controls and reduce operational time around maintenance, monitoring and management.
- Executive level summary of the short and long term issues that need to be addressed
- Detailed technical solution offering that is based on the workshop discussions and understanding
- A bill of materials that includes refreshing and/or consolidating the entire security solution estate over a multi-year period
- A total cost of ownership calculation to assist with budgetary planning

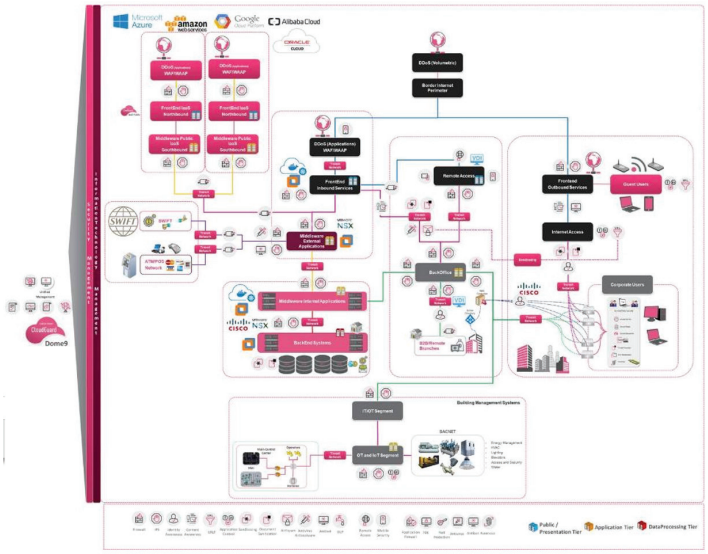

Figure 3: A Zero Trust Architecture Blueprint example designed by Check Point Security Architecture team

COMPLETE ZERO TRUST

FULLY IMPLEMENT ALL OF THE ZERO TRUST PRINCIPLES WITH CHECK POINT INFINITY

The Check Point Infinity architecture consolidates a wide range of security functions and solutions that enable you to implement all of the zero trust principals.

We have described below the principals of the Extended Zero Trust Security Model and the technologies included within the Check Point Infinity architecture that support their implementation.

ZERO TRUST NETWORKS

PREVENT MALICIOUS LATERAL MOVEMENT WITH GRANULAR NETWORK SEGMENTATION

When moving toward Zero Trust Security, it is crucial you "Divide and Rule" your network. Identifying your valuable assets and defining "Micro-segments" around them create multiple junctions and inspection points that block malicious or unauthorized lateral movement, so that In the event of a breach, the threat is easily contained and isolated.

Check Point Security Gateways enable you to micro-segment the network across your entire IT infrastructure, and across private/public cloud and corporate network environments. They also enable you to apply a unified policy for users, devices applications, and zones.

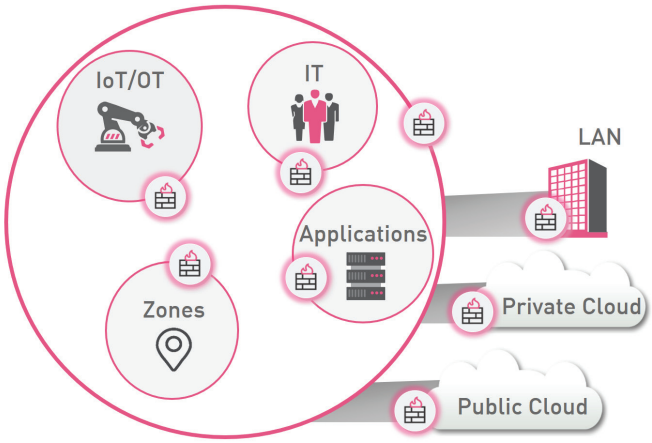

Figure 4: Granular Micro-segmentation with Check Point Security Gateways

Integration with **Check Point Identity Awareness** and **Application Control** enables you to set and enforce a granular policy that is context- identity-aware; and achieve a "Least Privileged" access control. For example, you can limit access to specific users, on specific devices, time, and geo-location. You can limit the usage of applications and features within them, and to limit access to specific elements of data, e.g., credit card, source code, or Social Security numbers.

With full control of all east-west traffic, at the application level, these gateways accurately inspect and block unauthorized traffic between segments; while allowing only the absolute minimum, legitimate traffic.

ZERO TRUST WORKLOADS

PROTECT YOUR WORKLOADS IN PRIVATE AND PUBLIC CLOUD WITH EXTENDED VISIBILITY AND ADAPTABLE POLICY

Securing workloads, particularly those who are running in the public cloud, is essential since these cloud assets (e.g. containers, functions and VM's) are vulnerable, and attractive target to malicious actors.

Check Point CloudGuard IaaS and **Check Point CloudGuard Dome 9** seamlessly integrate with any cloud infrastructure and provide you with 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.

- Construct a real-time topology of your cloud assets, security groups, instances, and firewalls
- Facilitate an adaptable access policies that are automatically adjusted to any changes in workloads
- Enforce compliance, detect and remediate misconfigurations
- Provide threat prevention layer using engines such as IPS, Malware detection, and Threat Emulation

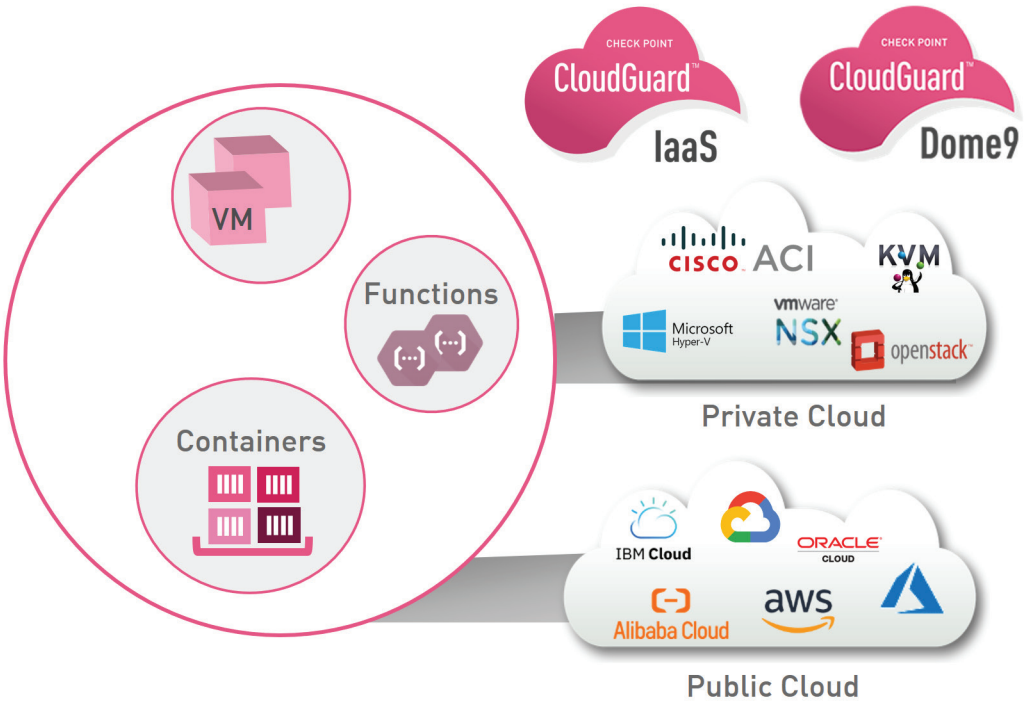

Figure 5: Secure Workloads with Check Point CloudGuard

ZERO TRUST PEOPLE

USE CONTEXT-AWARE AUTHORIZATION TO PROTECT AGAINST IDENTITY THIEVES

With 81% of data breaches involving stolen credentials[2], it is clear that username and passwords no longer prove the identity of a user. Identities are easily compromised, so access control to your valuable assets must be strengthened.

Check Point Identity Awareness enables granting access to your data only to authorized users, and only after their identities have been strictly authenticated.

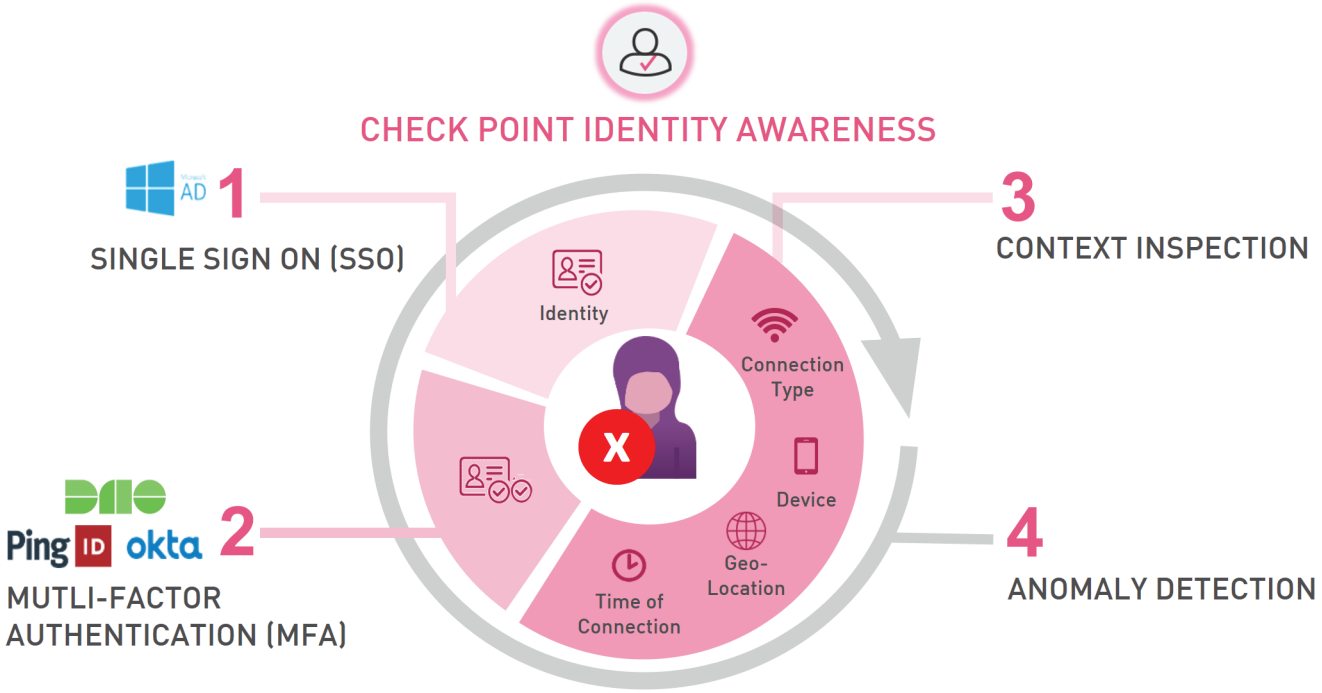

Figure 6: Check Point Infinity context-aware Authorization

- **SSO and MFA:** integrating with a broad range of third-party identity and multi-factor authentication services providers, such as Okta, Ping, Microsoft AD, Cisco ISE, and more
- **Context-aware policy**: that can be set based on the full context of the connection attempt, including time, geo-location, device type, and connection type (e.g., VPN, wireless network, other).
- **Anomaly Detection**: analysis of anomalies such as multiple unsuccessful login attempts, unrecognized devices, unusual times and locations, and more.

[2] Verizon DBIR 2019

ZERO TRUST DEVICES

PROTECT ALL DEVICES FROM THREATS, AND ISOLATE THEM IF COMPROMISED

With 70% of breaches involving compromised devices[1], every device connected to your network is a threat vector, whether it's a workstation, a mobile or an IoT/OT device. The following solutions and products included in the Check Point Infinity architecture prevent from cyber-criminals from maliciously using devices to gain privileged access or to infect other systems with:

- **Check Point SandBlast Agent** and **Check Point SandBlast Mobile** –
  - Protect employees' mobile devices and workstations from advanced attacks, zero-day malware, malicious app installation, and more.
  - Prevent infected devices or devices with security vulnerabilities from accessing corporate apps by providing the gateways full visibility into their security posture. This includes information about whether the devices are infected by malware, jailbroken or rooted, and the security status, e.g., is antivirus or data encryption installed, and more.
- **IoT/OT Security Solution** – Discovers all IoT/OT devices connected to your network and automatically separates them from other IT systems and devices with automated network segmentation. Allows only minimal and legitimate communication to and from these devices with an adaptive policy that is tailored by proprietary device attributes, communication patterns, and methods, etc.
- **Network-based Threat Prevention** – Protects devices from threats that are coming from the network and vice versa.

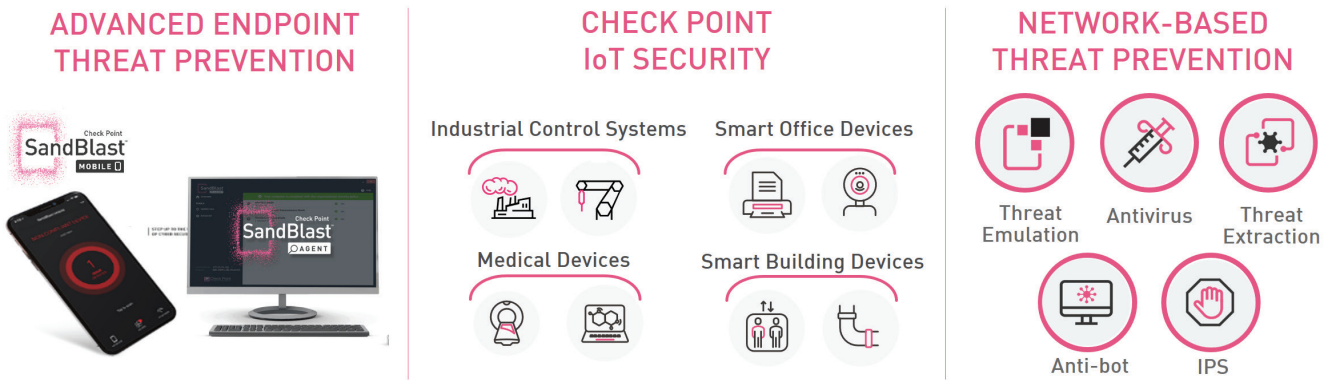

Figure 7: Check Point Infinity Secures Every Workstation, Mobile and IoT Device

1 2017 IDC research

ZERO TRUST DATA

CLASSIFY, PROTECT AND ENCRYPT YOUR DATA, WHEREVER IT IS

Zero Trust is all about protecting the data while it is shared continuously between workstations, mobile devices, application servers, databases, SaaS applications, and across the corporate and public networks. Check Point delivers multi-layered data protection, that preemptively protects data from theft, corruption, and unintentional loss, wherever it is.

1. **Data Encryption** that renders the information useless in the case of a breach:
    - **Full Disk Encryption** of all information on endpoint hard drives, including user data and operating system files.
    - **Media Encryption** enforces encryption of all removable storage media.
    - **Site-to-site and Client-to-site Virtual Private Networks (VPN)** secure and encrypt communication tunnels between the corporate networks and remote and mobile users, branch offices, and business partners.
2. **Data Management Categorization and Classification:**
    - **Capsule Docs** enables employees to classify and protect documents by limiting permissions (i.e., view, share, and edit) to specific user or groups. That security follows the documents everywhere they go, inside and outside your organization.
    - **Capsule Workspace** is a secure business environment where users have one-touch access from their mobile devices to corporate email, files, directories, corporate contacts, and calendars. Data is kept encrypted and stored in a password-protected container.
3. **Check Point Data Loss Prevention (DLP)** tracks and controls data movements across the network to ensure sensitive information does not leave the organization or is exposed to unauthorized users whether via email, web browsing or file-sharing services.
    - **Content Awareness** provides an accurate and automated identification of sensitive data types (e.g., credit card, bank statement).

- **Compliance** dynamically updates the DLP policy based on corporate policy or relevant data protection regulation.
- **CloudGuard SaaS** extends DLP policies to protect data in SaaS applications.

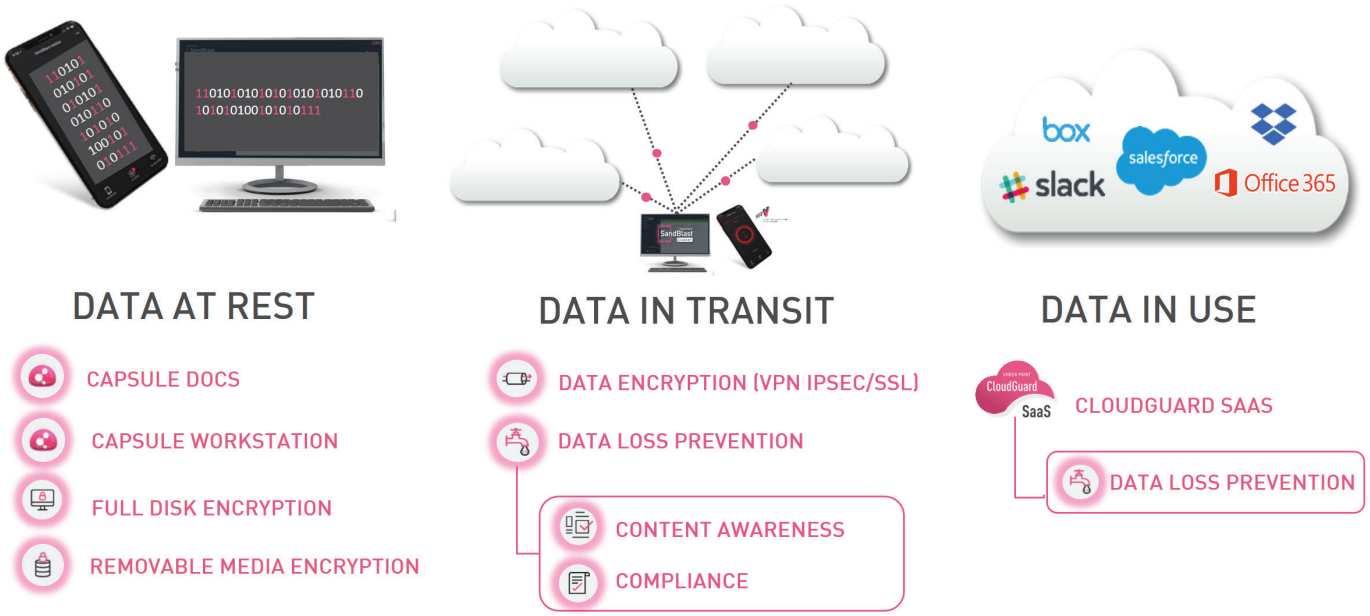

Figure 8: Check Point Infinity Delivers a Multi-layered Data Protection

VISIBILITY AND ANALYTICS

A SINGLE, COMPLETE VIEW INTO SECURITY RISKS

You can't protect what you can't see or understand. A ZeroTrust Security model constantly monitors, logs, correlates, and analyzes every activity across your network.

Check Point Infinity is managed via a single and a centralized security console, **Check Point R80 Smart Console** which includes event monitoring. **Smart Event** correlates all types of events from all enforcement points, including endpoints and mobile devices, to identify suspicious activity and track threat trends. It provides security teams with full visibility into their entire security posture so they can quickly detect and mitigate threats in real-time using advanced and visual dashboards.

1. **Cyber Attack Dashboard** allows immediate response to security incidents and provides real-time forensics to investigate events.

2. **Smart Log** provides real-time visibility into billions of log records over multiple periods and domains.

3. **Check Point Compliance** examines your environment's security gateways, software modules, policies, and configuration settings in real-time. With over 300 Security Best Practices, it detects poor configurations and provides instant remediation tips to ensure your business stays secure and compliant with different and complex regulations such as GDPR, HIPAA, and CPI.

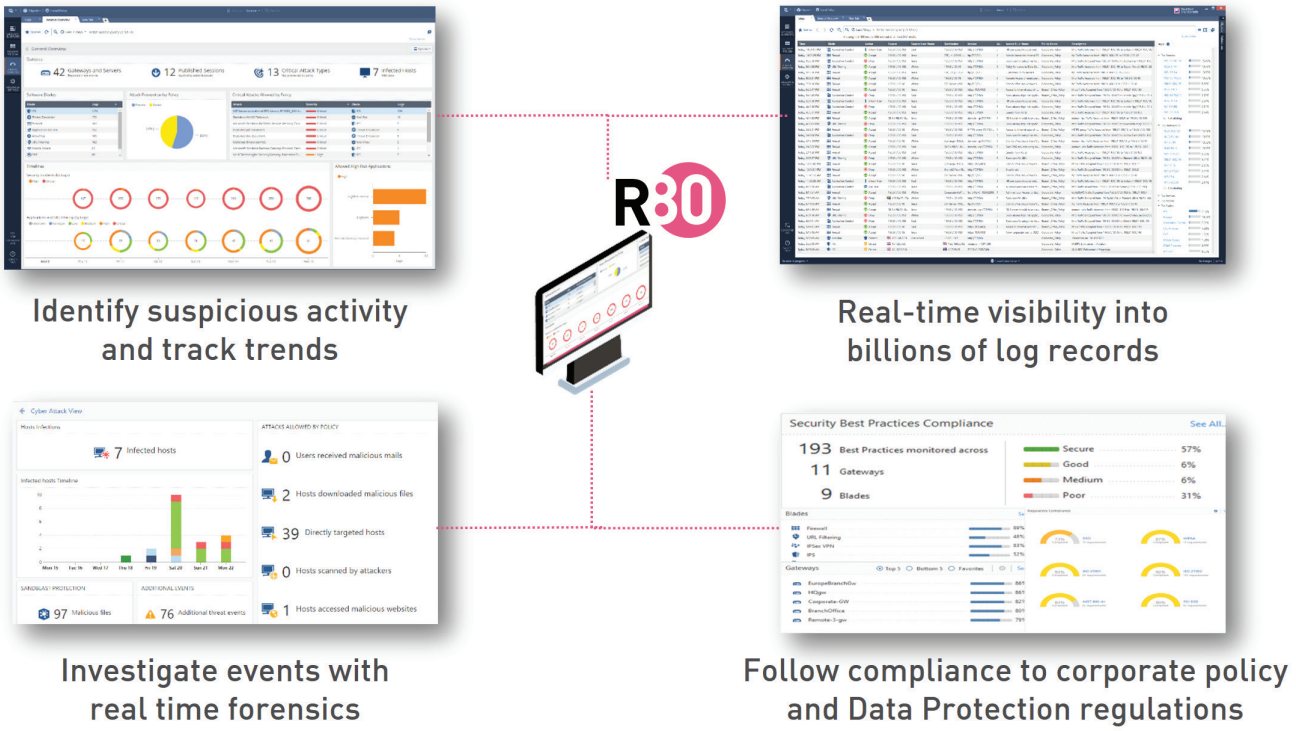

Figure 9: Check Point Infinity Delivers a Multi-layered Data Protection

AUTOMATION AND ORCHESTRATION

AUTOMATE ALL SECURITY TASKS TO IMPROVE INCIDENT RESPONSE AND AGILITY

A Zero Trust Security Architecture must automatically integrate with the organization's broader IT environment to enable speed and agility, improved incident response, policy accuracy, and task delegations. Check Point Infinity architecture includes a rich set of APIs and automation tools that support these goals, including:

1. **Reduce security admin workload:**
    - **Security procedure automation:** converting repetitive and tedious security tasks into customized workflows that are executed automatically, scheduled, or event-driven.
    - **Update of objects and policy rules:** dynamically linking objects in the security policy to external object stores (such as Microsoft Active Directory, Cisco ISE) to free up significant staff time and decrease the chance of mistakes due to human error.
    - **Admin role delegation:** delegating policy management to relevant organization to reduce unnecessary communication and coordination.
2. **Automated incident detection and remediation:**
    - **Check Point R80 Centralized Security Management** uses algorithms and best practices to identify security incidents and incorporate remediation via changes of access policy rules; or by quarantining devices/user via integration with network controllers such as Cisco ISE and other NAC solutions.
    - **Incident Response (IR) and Ticket Enrichment:** deep integration with industry-leading SIEM vendors provides the SIEM deep insight information on security incidents such as event logs and threat Intelligence data powered by ThreatCloud (More information in the next pages). The SIEM perform analysis and trigger policy changes or provides IoC's (Indication of Compromise) for enforcement.
3. **API Eco-system:** Check Point Infinity architecture includes a rich set of APIs used by over 160 technology partners to develop integrated solutions. Example use cases include SIEM, network management, security assessment, identity awareness, compliance testing and auditing, ticket and workflow management, etc.

To support our customer's efforts to use our APIs, Check Point hosts Checkmates, where our community members can ask questions, interact with their peers, share code, and collaborate with Check Point R&D. The section dedicated to API developers can be accessed **here**.

EFFICIENT ZERO TRUST

CENTRALIZED SECURITY MANAGEMENT AND A UNIFIED POLICY

Efficient Zero Trust Security Management must also consolidate the policy across network, cloud, and mobile, rather than depending on security operations to manually align policy across multiple point solutions. 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 policy to threat prevention – across the entire organization – on both physical and virtual environments.

ELEMENT	EXAMPLES
User or Group	Joe, Marketing Group, Summer Interns
Application	Twitter, Instagram
Data and Content	Credit Card Numbers, ABA Bank Routing
Target for Enforcement	Amazon AWS, VMware Cluster, Mobile

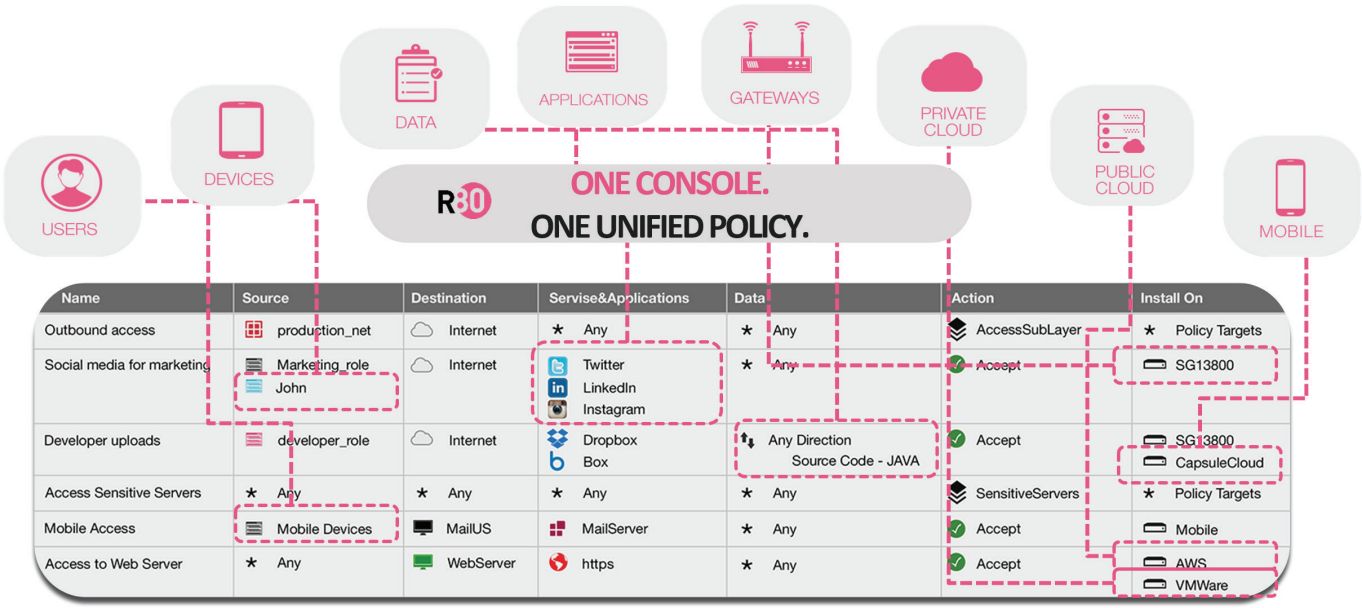

Figure 10: Check Point R80 Centralized Security Management Offers a Unified Policy Across the Different IT Domains

PREVENTIVE ZERO TRUST

FOCUS ON THREAT PREVENTION AND ZERO-DAY PROTECTION

As cyber-threats grow in quantity and complexity, you must be able to continuously monitor your network, identify the most important threats, and effectively prevent them. The following components of Check Point Infinity empower Zero Trust implementations with threat prevention against fifth-generation of cyber attack.

GLOBALLY SHARED THREAT INTELLIGENCE

IMMEDIATELY TRANSLATED INTO PROACTIVE SECURITY PROTECTIONS

Check Point Infinity breaks down security silos by ensuring comprehensive and timely intelligence across the entire infrastructure. **Check Point ThreatCloud** is the world's largest threat intelligence database aggregating threat intelligence data from a broad array of sources, including 100 million gateways across the world. It emulates more than 4 million files per day, Stops 7,000 zero-day attacks per day and processes 86 billion IoCs per day.

ThreatCloud continuously collects and analyzes new threat indicators for malware, threat behavior, and network addresses associated with each identified attack. These indicators are then fed into the global ThreatCloud platform, which automatically translates them into security protections and distributes them to enforcement points around the world.

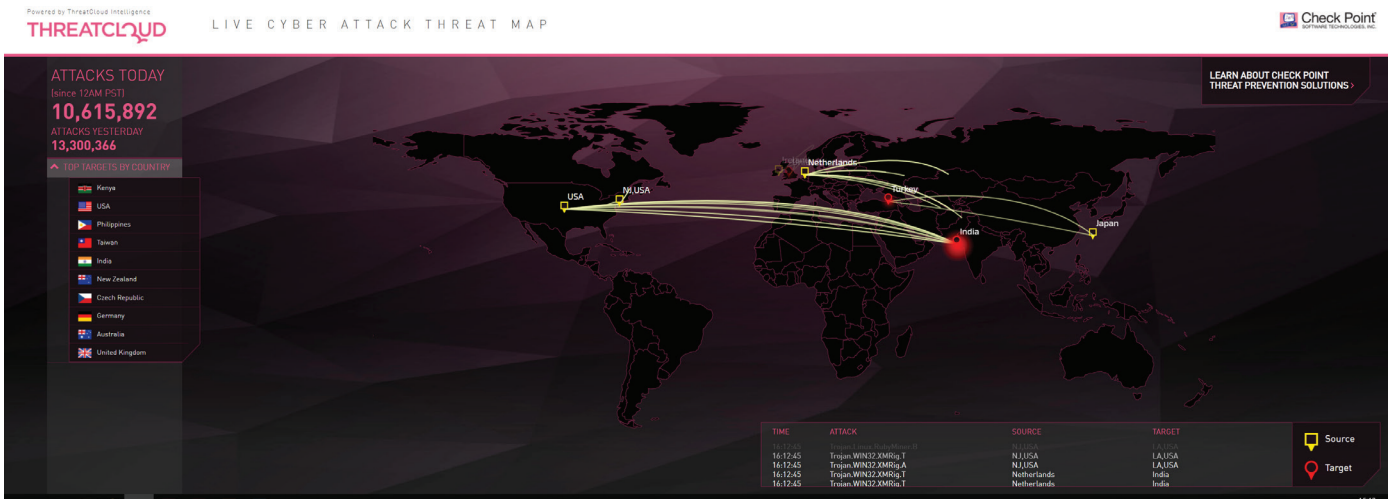

Figure 11:
Check Point ThreatCloud aggregates threat intelligence from a broad array of sources including Check Point Research, sandboxing analysis, Incident Response, security gateway appliances, Computer Emergency Readiness Teams (CERTs) and Computer Security Incident Response Teams (CSIRTs), security product vendors and other organizations within the security community.

64 DIFFERENT SECURITY ENGINES POWERED BY THREAT INTELLIGENCE

PROTECT AGAINST KNOWN AND UNKNOWN THREATS

Check Point Infinity uses ThreatCloud threat intelligence to provide threat prevention technologies with the industry's best catch rate. With 64 different security engines, Check Point Infinity protects against known and unknown threats across all networks, endpoints, cloud, mobile, and IoT. Also, **Check Point SandBlast Zero-day Protection** provides 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.

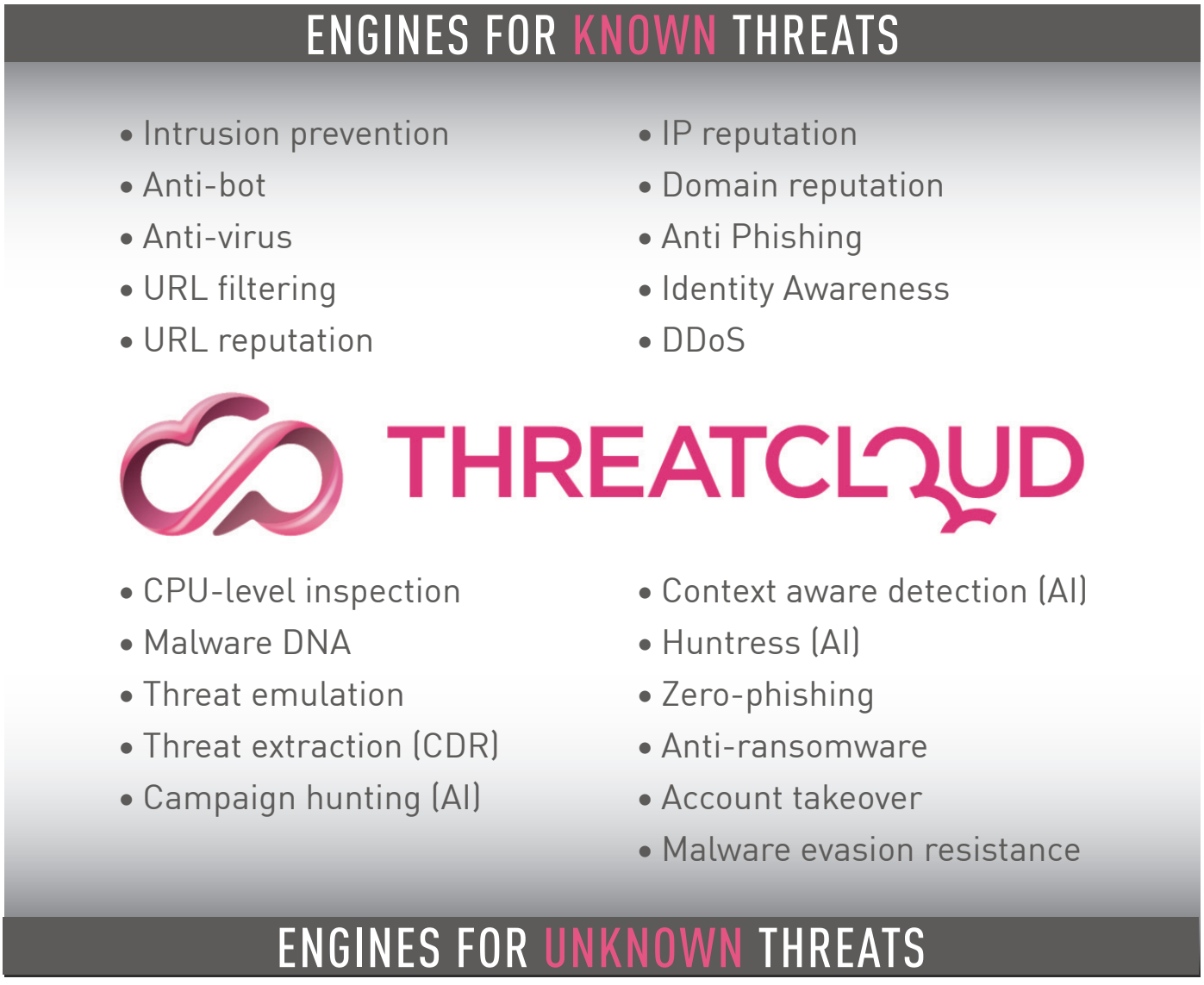

Figure 12: Check Point Infinity has 64 security engines powered by global threat intelligence data.

SUMMARY

While implementing Zero Trust using point solutions might add complexities and risk, 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 by Check Point infinity enables you to:

- Fully implement all of the principles of the Zero Trust Security model
- Increase operational security efficiency using single centralized security management and a unified policy
- Future proof your business against the increasing sophistication of cyber-attacks with real-time threat prevention.

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 13: Check Point Infinity – A Consolidated Zero Trust Security Architecture

Learn more about Absolute Zero Trust with Check Point Infinity

checkpoint.com/solutions/zero-trust-security

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

© 2019 Check Point Software Technologies Ltd. All rights reserved.