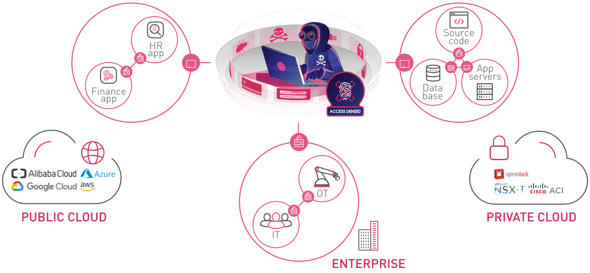
9 STEPS TO ABSOLUTE ZERO TRUST SECURITY

WITH CHECK POINT INFINITY

01 ZERO TRUST FOR NETWORKS

Prevent malicious lateral movement with granular network segmentation


HR app
Finance app
ACCESS DENIED
Source code
Data base
App servers
Alibaba Cloud
Azure
Google Cloud
aws
PUBLIC CLOUD
OT
IT
ENTERPRISE
openstack
NSX-T
cisco ACI
PRIVATE CLOUD

CHECK POINT SECURITY GATEWAYS

Set and enforce a unified access policy for users, devices, applications and zones across all environments

CHECK POINT APPLICATION CONTROL

Limit usage of ~8000 applications, and features within them

CHECK POINT IDENTITY AWARENESS

Allow access only to specific users

02 ZERO TRUST PEOPLE

Use context-aware authorization to protect against identity-thieves

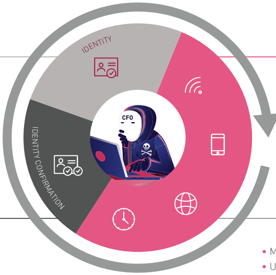
Single Sign On (SSO)

01

Seamless integration with a broad range of third-party identity and Multi-Factor Authentication service providers.

Multi Factor Authentication (MFA)

02


IDENTITY
IDENTITY CONFIRMATION
CFO

Context Inspection

03

- Device Identity
- Geo-Location
- Time of connection
- Connection type (VPN, wireless)

Anomaly Detection

04

- Multiple unsuccessful login attempts
- Unrecognized device
- Unusual time and location
- And more...

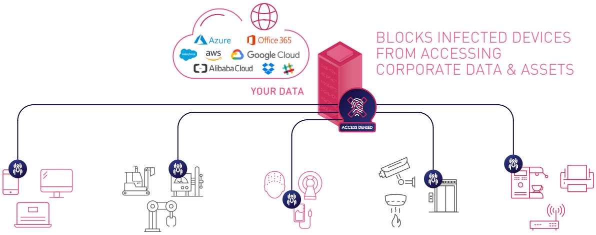
CHECK POINT IDENTITY AWARENESS

Granting access to your data only to authorized users, and only after their identities have been strictly authenticated.

03 ZERO TRUST DEVICES

Check Point SandBlast MOBILE AGENT

Protect all devices from threats, and isolate them if compromised


Azure
Office 365
aws
Google Cloud
Alibaba Cloud
YOUR DATA
ACCESS DENIED

BLOCKS INFECTED DEVICES FROM ACCESSING CORPORATE DATA & ASSETS

EMPLOYEES' ENDPOINTS

INDUSTRIAL CONTROL SYSTEMS

MEDICAL DEVICES

SMART BUILDING DEVICES

SMART OFFICE DEVICES

SANDBLAST AGENT & SANDBLAST MOBILE

Protect employees' mobile devices and workstations from advanced attacks, zero-day malware, malicious app installation, and more.

INFINITY FOR IoT

Automatically discovers and protect smart office and building devices, Industrial Control Systems (ICS) and medical devices.

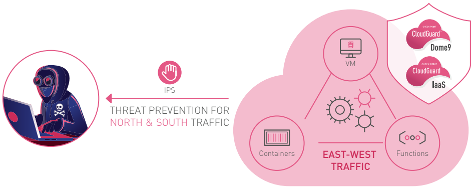
NETWORK-BASED THREAT PREVENTION

- Threat emulation
- Threat extraction
- Anti-virus
- Anti-bot
- IPS

04

ZERO TRUST WORKLOADS

Protect your workloads with extended visibility and adaptable policy


IPS
VM
CloudGuard
Dome9
CloudGuard
IaaS
Containers
Functions

THREAT PREVENTION FOR NORTH & SOUTH TRAFFIC

EAST-WEST TRAFFIC

CloudGuard Dome9
CloudGuard IaaS

✓ SEAMLESS INTEGRATION

With any cloud infrastructure

Azure NSX-T cisco ACI Google Cloud aws openstack

✓ VISIBILITY INTO THE CLOUD INFRASTRUCTURE

Identifies misconfigurations and security gaps

✓ FULL CONTROL OVER EAST-WEST TRAFFIC

Enables to define micro-perimeters

✓ ADAPTIVE ACCESS POLICY

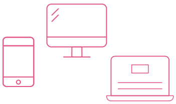
Responsive to cloud environmental changes

05

101110
010011
110100

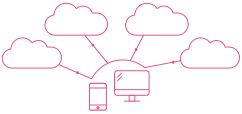
ZERO TRUST DATA

Classify, protect and encrypt your data, wherever it is



DATA AT REST

- Capsule docs
- Capsule workspace
- Full disk encryption
- Removable media encryption



DATA IN TRANSIT

- Data encryption (VPN IPSEC/SSL)
- Data loss prevention
  - Content awareness
  - Compliance

salesforce
slack
box
Office 365

DATA IN USE

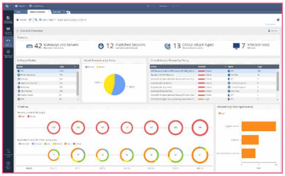
- Cloudguard SAAS
  - Data loss prevention

06

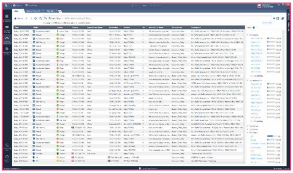
VISIBILITY & ANALYTICS

Quickly detect and mitigate threats
with a single view into security risks

Identify suspicious activity and track trends

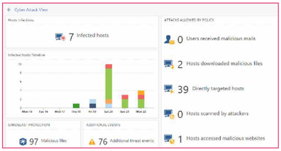

General Overview
Statistics
42 Gateways and Servers
12 Published Sessions
13 Critical Attack Types
7 Infected Hosts
Software Blades
Attack Prevention by Policy
Critical Attacks Allowed by Policy
Timeline
Allowed High Risk Applications

Real-time visibility into billions of log records



**CHECK POINT R80
CENTRALIZED SECURITY
MANAGEMENT**

Investigate events with real time forensic


Cyber Attack View
Hosts Infections
Infected hosts Timeline
10
8
6
4
2
0
Mon 15
Tue 16
Wed 17
Thu 18
Fri 19
Sat 20
Sun 21
Mon 22
SANDBLAST PROTECTION
ADDITIONAL EVENTS
ATTACKS ALLOWED BY POLICY

7 Infected hosts

0 Users received malicious mails

2 Hosts downloaded malicious files

39 Directly targeted hosts

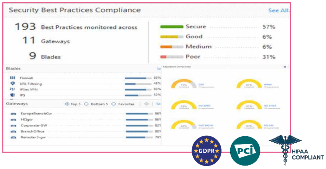
0 Hosts scanned by attackers

1 Hosts accessed malicious websites

97 Malicious files

76 Additional threat events

Follow compliance to corporate policy and data protection regulations


See All.
Blades
Gateways
Top 5
Bottom 5
Favorites
GDPR
PCI
HIPAA COMPLIANT

Security Best Practices Compliance

193 Best Practices monitored across
11 Gateways
9 Blades

Secure	57%
Good	6%
Medium	6%
Poor	31%

Firewall	89%
URL Filtering	48%
IPSec VPN	83%
IPS	52%

EuropeBranchGw	86%
HQgw	86%
Corporate-GW	82%
BranchOffice	80%
Remote-3-gw	79%

07

AUTOMATION & ORCHESTRATION

Use rich API's to automate security
tasks and incident response

Asset and workload discovery in cloud-based data centers (IaaS) and virtualization

Incident response (IR) ticket enrichment

CHECK POINT INFINITY OFFERS RICH **API'S** USED BY OVER **160 TECHNOLOGY PARTNERS**

Dynamic update of objects and policy rules

Automation of security operational tasks

Automated incident remidiation

08

THREAT PREVENTION

Protect from known and unknown threats

64 DIFFERENT SECURITY ENGINES

POWERED BY GLOBALLY SHARED
THREAT INTELLIGENCE

Engines for **KNOWN** threats

- Intrusion prevention
- Anti-bot
- Anti-virus
- URL filtering
- URL reputation
- IP reputation
- Domain reputation
- Anti phishing
- Identity awareness
- DDoS

THREATCLOUD

Emulates more than 4 million files per day

Stops 7,000 zero-day attacks per day

Passes 86 billion IOCs per day

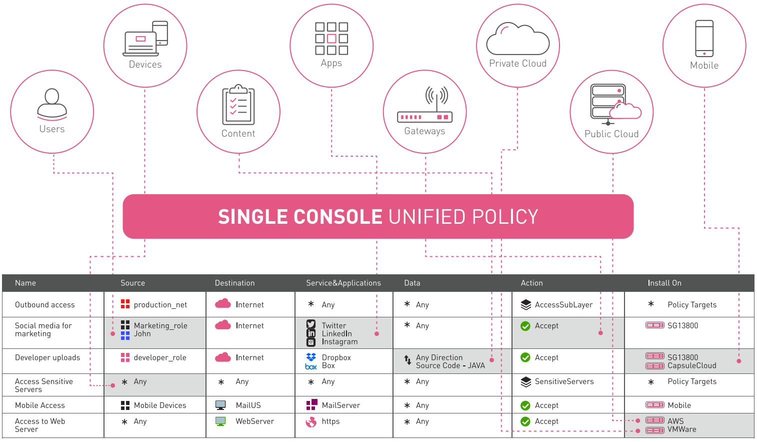
Engines for **UNKNOWN** threats

- CPU-level inspection
- Malware DNA
- Threat emulation
- Threat extraction (CDR)
- Campaign hunting (AI)
- Context aware detection (AI)
- Huntress (AI)
- Zero-phishing
- Anti-ransomware
- Account takeover
- Malware evasion resistance

09

CENTRALIZED SECURITY MANAGEMENT

Efficiently manage Zero Trust security
with a single console and a unified policy


Devices
Apps
Private Cloud
Mobile
Users
Content
Gateways
Public Cloud
SINGLE CONSOLE UNIFIED POLICY

Name	Source	Destination	Service&Applications	Data	Action	Install On
Outbound access	production_net	Internet	* Any	* Any	AccessSubLayer	* Policy Targets
Social media for marketing	Marketing_role John	Internet	Twitter LinkedIn Instagram	* Any	✓ Accept	SG13800
Developer uploads	developer_role	Internet	Dropbox Box	Any Direction Source Code - JAVA	✓ Accept	SG13800 CapsuleCloud
Access Sensitive Servers	* Any	* Any	* Any	* Any	SensitiveServers	* Policy Targets
Mobile Access	Mobile Devices	MailUS	MailServer	* Any	✓ Accept	Mobile
Access to Web Server	* Any	WebServer	https	* Any	✓ Accept	AWS VMWare

R80 UNIFIED POLICY

CHECK POINT
INFINITY

ABSOLUTE ZERO TRUST SECURITY WITH CHECK POINT INFINITY

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 single consolidated 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.

Learn more about Absolute Zero Trust with Check Point Infinity
Checkpoint.com/solutions/Zero-Trust-Security

CHECK POINT™