



**Check Point**<sup>®</sup>  
SOFTWARE TECHNOLOGIES LTD.

# CHECK POINT APPLIANCES

2019

TABLE OF CONTENTS

---

# CHECK POINT APPLIANCES

- 03** CHECK POINT INFINITY ARCHITECTURE
- 04** NEXT GENERATION THREAT PREVENTION
- 05** SECURITY GATEWAYS
- 15** VIRTUAL APPLIANCES
- 16** MANAGEMENT APPLIANCES
- 17** DDoS PROTECTOR
- 18** SANDBLAST APPLIANCES
- 19** PROVEN SECURITY

WELCOME TO THE FUTURE OF CYBER SECURITY



## THE CYBER SECURITY ARCHITECTURE OF THE FUTURE

MOBILE



NETWORK



CLOUD



ENDPOINT



### ONE SECURITY PLATFORM

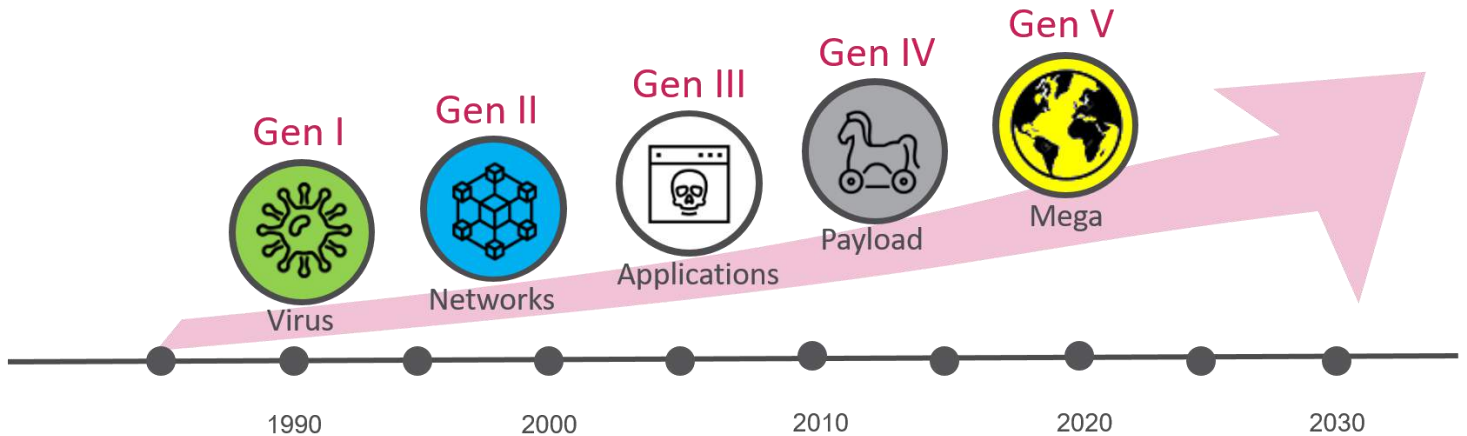
Leveraging unified threat intelligence and open interfaces

### REAL-TIME THREAT PREVENTION

Blocking the most sophisticated attacks before they infiltrate the network

### CONSOLIDATED MANAGEMENT

Single management, modular policy management and integrated threat visibility



## BACKGROUND

As the world becomes more connected and networks continue to evolve, securing IT environments is becoming more complex than it once was. We are now facing Gen V (5<sup>th</sup> Generation) of cyberattacks, large scale attacks that quickly spread and move across attack vectors and industries. Gen V attacks are more sophisticated than ever, crossing mobile, cloud and networks, and bypassing conventional defenses that are based on detection.

Separate IT environments often drive businesses to apply different point solutions, many of which are focused on detection and mitigation rather than prevention. This reactive approach to cyberattacks is costly and ineffective, complicates security operations and creates inherent gaps in security posture, leaving you unprotected from sophisticated Gen V attacks.

It's time to step up to Gen V of cyber security, with the architecture that truly protects your entire IT infrastructure.

## SOLUTION

Check Point Infinity is the only fully consolidated cyber security architecture that protects your business and IT infrastructure against Gen V mega cyberattacks across all networks, endpoint, cloud and mobile.

The architecture is designed to resolve the complexities of growing connectivity and inefficient security. It provides complete threat prevention which seals security gaps, enables automatic, immediate threat intelligence sharing across all security environments, and a unified security management for an utmost efficient security operation. Check Point Infinity delivers unprecedented protection against current and potential attacks—today and in the future.

WELCOME TO THE FUTURE OF CYBER SECURITY

# NEXT GENERATION THREAT PREVENTION



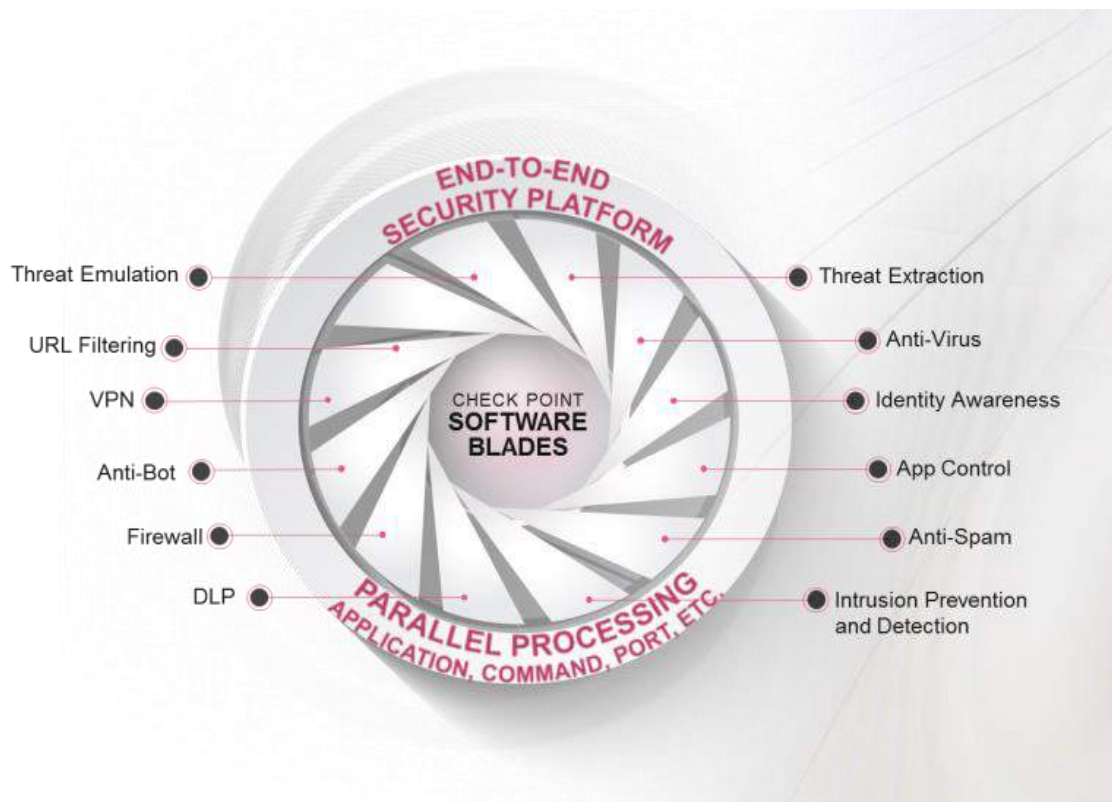
## COMPREHENSIVE THREAT PREVENTION

The rapid growth of malware, growing attacker sophistication and the rise of new unknown zero-day threats requires a different approach to keep enterprise networks and data secure. Check Point delivers fully integrated, comprehensive Threat Prevention to combat these emerging threats while reducing complexities and increasing operational efficiencies. The Check Point Threat Prevention solution includes powerful security features such as firewall, IPS, Anti-Bot, Antivirus, Application Control, and URL Filtering to combat known cyber-attacks and threats – now enhanced with the award-winning SandBlast™ Threat Emulation and Threat Extraction for complete protection against the most sophisticated threats and zero-day vulnerabilities.

## PREVENT KNOWN AND ZERO-DAY THREATS

As part of the Check Point SandBlast Zero-Day Protection solution, the cloud-based Threat Emulation engine detects malware at the exploit phase, even before hackers can apply evasion techniques attempting to bypass the sandbox. Files are quickly quarantined and inspected, running in a virtual sandbox to discover malicious behavior before it enters your network. This innovative solution combines cloud-based CPU-level inspection and OS-level sandboxing to prevent infection from the most dangerous exploits, and zero-day and targeted attacks.

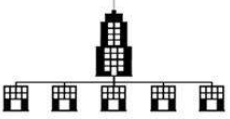




Furthermore, SandBlast Threat Extraction removes exploitable content, including active content and embedded objects, reconstructs files to eliminate potential threats, and promptly delivers sanitized content to users to maintain business flow.



# SECURITY GATEWAYS



Check Point provides customers of all sizes with the latest data and network security protection in an integrated next generation threat prevention platforms, reducing complexity and lowering the total cost of ownership. Whether you need next-generation security for your data center, enterprise, small business or home office, Check Point has a solution for you.

 <b>Branch Office</b>	<p>Deployment: Branch or Small Office</p> <p>Form Factor: Desktop</p> <p>Interfaces: 1 GbE, Wi-Fi, 3G/4G, DSL, PoE</p> <p>FW Throughput: 750 Mbps to 14.5 Gbps</p> <p>Special Features: Web management</p>	<p>1400</p> <p>3100, 3200</p> <p>5100</p>
 <b>Enterprise</b>	<p>Deployment: Enterprise</p> <p>Form Factor: 1RU</p> <p>Interfaces: 1, 10, 40 GbE</p> <p>FW Throughput: 16 to 52 Gbps</p> <p>Special Features: Flexible IO options, LOM</p>	<p>5200</p> <p>5400, 5600</p> <p>5800, 5900</p> <p>6500, 6800</p>
 <b>Data Center</b>	<p>Deployment: Large enterprise, Data center</p> <p>Form Factor: 2RU</p> <p>Interfaces: 1, 10, 25, 40, 100 GbE</p> <p>FW Throughput: 25 to 128 Gbps</p> <p>Special Features: 25/40/100 GbE, DC power, LOM</p>	<p>15400, 15600</p> <p>23500, 23800, 23900</p>
 <b>Chassis Systems</b>	<p>Deployment: Data center, Telco, Carrier</p> <p>Form Factor: 6RU to 16RU</p> <p>Interfaces: 1, 10, 40, 100 GbE</p> <p>FW Throughput: 335 to 800 Gbps</p> <p>Special Features: DC power, scalable platform</p>	<p>44000</p> <p>64000</p>
 <b>Rugged</b>	<p>Deployment: Harsh environments</p> <p>Form Factor: Desktop, DIN mount</p> <p>Interfaces: 1 GbE, 3G/4G support</p> <p>FW Throughput: 2 Gbps</p> <p>Special Features: AC/DC power</p>	<p>1200R</p>

WELCOME TO THE FUTURE OF CYBER SECURITY

# 1400 APPLIANCES

## BRANCH OFFICE SECURITY



1430-1450  
(WI-FI OPTION)



1470-1490  
(WI-FI OPTION)

### OVERVIEW

Enforcing consistent network security throughout an enterprise is challenging when the enterprise border extends to remote and branch offices where there are a few users with little to no IT expertise. Remote and branch offices require the same level of protection from sophisticated cyber-attacks and zero-day threats as main corporate offices. The Check Point 1400 Appliances are a simple, affordable and easy to deploy all-in-one solution for delivering industry leading security to protect the weakest link in your enterprise network — the remote branch offices.

The 1400 Appliances are ideal for small offices. For local management and support in a small office environment, an easy and intuitive web-based local management interface is available. Enterprises who want to manage security from a central office can leverage Check Point Security Management or Multi-Domain Security Management to remotely manage and apply a consistent security policy to hundreds of devices across the field offices.

### ALL-INCLUSIVE SECURITY



THREAT PREVENTION



THREAT PREVENTION + SANDBLAST

### HIGH LEVEL OVERVIEW

A wide variety of network interface options are available including 1GbE Ethernet ports, DSL, PoE, 802.11b/g/n/ac WiFi with guest access, 3G and 4G wireless connections.

Maximum Capacities	1430	1450	1470	1490
NGFW + IPS	300 Mbps	490 Mbps	625 Mbps	800 Mbps
Threat prevention	225 Mbps	400 Mbps	500 Mbps	550 Mbps
1 GbE ports	1x WAN, 1x DMZ, 6x LAN switch		1x WAN, 1x DMZ, 16x LAN switch	
Wi-Fi option	802.11 b/g/n/ac, single band 2.4 or 5GHz		802.11 b/g/n/ac, dual band 2.4 and 5GHz	
PoE option	x		✓	
DSL option	✓		x	
3G, 4G/LTE modem support	Yes, see sk92809			

For more information: [www.checkpoint.com/products/branch-office-security/](http://www.checkpoint.com/products/branch-office-security/)



WELCOME TO THE FUTURE OF CYBER SECURITY

# 1200R RUGGED APPLIANCE

## SECURITY FOR HARSH ENVIRONMENTS



1200R

### OVERVIEW

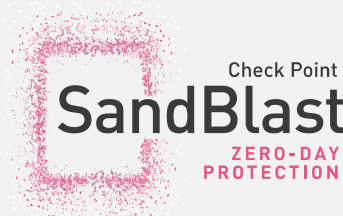
Protecting critical infrastructure from cyberattacks poses unique challenges. The environments can be harsh and systems often use specialized protocols. Check Point's ICS/SCADA cyber security solutions provide advanced threat prevention paired with ruggedized appliance options and comprehensive protocol support to ensure vital assets such as power generation facilities, traffic control systems, water treatment systems and factories are never compromised.

The 1200R appliance complements our extensive appliance family to support a diverse range of deployment environments and meet specialized requirements. For instance, the 1200R complies with industrial specifications such as IEEE 1613 and IEC 61850-3 for heat, vibration and immunity to electromagnetic interference (EMI). In extreme temperatures from -40°C to 75°C where other appliances would fail, this appliance keeps you secure.

### ALL-INCLUSIVE SECURITY PACKAGES



THREAT PREVENTION



THREAT PREVENTION + SANDBLAST

### HIGH LEVEL OVERVIEW

Copper and fiber 1GbE Ethernet ports are included as is 3G and 4G wireless connection support through compatible USB modems.

Maximum Capacities	1200R
Firewall throughput	2 Gbps
VPN throughput	450 Mbps
WAN	1x 10/100/1000BaseT RJ45 or 1x 1000BaseF port
DMZ	1x 10/100/1000BaseT RJ45 or 1x 1000BaseF port
LAN	4x 10/100/1000BaseT RJ45 ports
Mount Options	DIN rail or rack mount
Industrial Certifications	IEEE 1613, IEC 61850-3
Power	AC or DC

WELCOME TO THE FUTURE OF CYBER SECURITY

# 3000 APPLIANCES

## ENTERPRISE SECURITY FOR BRANCH OFFICES



3100



3200

### OVERVIEW

Seamless security requires consistent protections across all locations, not just at the main corporate network. The same level of protection is required for remote and branch offices—to form a unified and total defense against potential threats. The Check Point 3000 Appliances are an ideal solution for delivering security to small and branch offices.

The 3000 Appliances offer enterprise-grade security without compromise in a compact desktop form factor. Multi-core technology, six 1 Gigabit Ethernet ports and advanced threat prevention capabilities easily extends robust security to remote branch locations and small offices. Despite the small form factor, these powerful appliances provide up to 1.15 Gbps of Next Generation Firewall throughput and up to 740 Mbps of threat prevention throughput.

### ALL-INCLUSIVE SECURITY PACKAGES



THREAT PREVENTION



THREAT PREVENTION + SANDBLAST

### HIGH LEVEL OVERVIEW

The compact design, multi-core technology and SandBlast Zero-Day Protection available in the 3000 Appliances make these gateways ideally suited for deployment in small offices and remote branch offices.

Maximum Capacities	3100	3200
NGFW with IPS throughput <sup>1</sup>	850 Mbps	1.15 Gbps
VPN throughput	1.7 Gbps	2.25 Gbps
Threat prevention throughput <sup>1</sup>	340 Mbps	385 Mbps
1 GbE ports (Copper)	6	
RAM	8 GB	
Storage	1x 320GB (HDD) or 1x 240GB (SSD)	
Enclosure	Desktop	
Power Consumption (Max)	29.5W	

<sup>1</sup> Measured with the Enterprise testing conditions



WELCOME TO THE FUTURE OF CYBER SECURITY

# 5000 APPLIANCES

## ENTERPRISE SECURITY, FLEXIBLE NETWORK OPTIONS



### OVERVIEW

Security decisions no longer have to be a choice between features and performance. The purpose-built Check Point 5000 appliances provide the most advanced threat prevention security without compromise for demanding small to midsize enterprise networks.

The Check Point 5000 Appliances combine multiple network interface options with high-performance multi-core capabilities — delivering exceptional multi-layered security protection without compromising on performance. The 5000 Appliances pack a maximum of twenty-six (26) 1 Gigabit Ethernet ports, redundant hot-swappable power supplies and an optional Lights-out Management (LOM) module into a compact 1U rack mountable form-factor. Supporting up to 7.25 Gbps of Next Generation Firewall throughput and 3.95 Gbps of threat prevention throughput, these appliances offer the best performance for its class.

### ALL-INCLUSIVE SECURITY PACKAGES



THREAT PREVENTION



THREAT PREVENTION + SANDBLAST

### HIGH LEVEL OVERVIEW

The modular design and the wide variety of network options available in the 5000 series of appliances not only provides a rich set of connectivity options for these gateways, they also make the gateways highly customizable to be suited for deployment in any network environment.

Maximum Capacities	5100	5200	5400	5600	5800	5900
NGFW with IPS (Gbps) <sup>1</sup>	2.1	2.52	3.4	5.1	6	7.25
Threat prevention (Gbps) <sup>1</sup>	700 Mbps	840 Mbps	980 Mbps	1.85	2.75	3.95
1 GbE ports (Copper)	14	14	18	18	26	26
1 GbE ports (Fiber)	4	4	4	4	8	8
10 GbE ports (Fiber)				4	8	8
RAM	16 GB	16 GB	32 GB	32 GB	32 GB	32 GB
Storage	1x 1TB (HDD) or 1x 240GB (SSD)					2x drives
AC or DC Power Supplies	1	1	1	2	2	2
Lights-out Management	✓	✓	✓	✓	✓	✓
Network expansion slots	1	1	1	1	2	2

<sup>1</sup> Measured with the Enterprise testing conditions

WELCOME TO THE FUTURE OF CYBER SECURITY

# 6000 APPLIANCES

## ENTERPRISE THREAT PREVENTION



6500



6800

### OVERVIEW

Security decisions no longer have to be a choice between features and performance. The purpose-built Check Point 6000 appliances provide the most advanced threat prevention security without compromise for demanding enterprise networks.

The 6500 and 6800 offer a fully integrated, unified solution tuned to deliver maximum security against 5th generation threats without compromising performance. The 6000 Security Appliances pack a maximum of eighteen (18) or twenty-six (26) 1 Gigabit Ethernet ports, redundant hot-swappable power supplies and a Lights-out Management (LOM) module into a compact 1U rack mountable form-factor. Supporting up to 15 Gbps of Next Generation Firewall throughput and 8.9 Gbps of threat prevention throughput, these appliances offer the best performance for its class.

### ALL-INCLUSIVE SECURITY PACKAGES



THREAT PREVENTION



THREAT PREVENTION + SANDBLAST

### HIGH LEVEL OVERVIEW

The modular design and the redundant options available in the 6000 series of appliances not only provides a rich set of connectivity options for these gateways, they also make the gateways suitable for deployment in any enterprise network environment where redundancy is required.

Maximum Capacities	6500	6800
NGFW with IPS (Gbps) <sup>1</sup>	6.8	15
Threat prevention (Gbps) <sup>1</sup>	3.4	8.9
1 GbE ports (Copper)	18	26
1 GbE ports (Fiber)	4	8
10 GbE ports (Fiber)	4	8
RAM	32 GB	64 GB
Storage	1x 1TB (HDD) or 1x 240GB (SSD)	2x 1TB (HDD) or 2x 480GB (SSD)
AC or DC Power Supplies	2	2
Lights-out Management	✓	✓
Network expansion slots	1	2

<sup>1</sup> Measured with the Enterprise testing conditions

WELCOME TO THE FUTURE OF CYBER SECURITY

# 15000 APPLIANCES

## LARGE ENTERPRISE THREAT PREVENTION



### OVERVIEW

Large enterprises have uncompromising needs for performance, uptime and scalability. The 15000 Appliances combine the most comprehensive security protections with purpose-built hardware. These powerful security appliances are optimized to deliver threat prevention throughput of up to 7.4 Gbps to secure your most critical assets.

The Check Point 15000 Appliances are ideal for large enterprise networks that require high performance and flexible I/O options. If you're ready to move from 10 to 25, 40 or 100 GbE, so are the 15000 Appliances. These are 2U appliances with three I/O expansion slots for high port capacity, redundant AC or DC power supplies, a 2x 1TB (HDD) or 2x 480GB (SSD) RAID1 disk array, and Lights-out Management (LOM) for remote management.

### ALL-INCLUSIVE SECURITY PACKAGES



THREAT PREVENTION



THREAT PREVENTION + SANDBLAST

### HIGH LEVEL OVERVIEW

The modular design and the wide variety of network options available in the 15000 series of appliances not only provides a rich set of connectivity options for these gateways, they also make the gateways highly customizable to be suited for deployment in any network environment.

Maximum Capacities	15400	15600
NGFW with IPS (Gbps) <sup>1</sup>	7.7	10.5
Threat prevention (Gbps) <sup>1</sup>	4.05	7.4
1 GbE ports (Copper)	26	
10 GbE ports (Fiber)	12	
40 GbE ports (Fiber)	6	
100/25 GbE ports (Fiber)	6	
RAM	64 GB	
Storage	2x 1TB (HDD) or 2x 480GB (SSD)	
AC or DC Power Supplies	2	
Lights-out Management	✓	
Virtual Systems	40	80

<sup>1</sup> Measured with the Enterprise testing conditions

WELCOME TO THE FUTURE OF CYBER SECURITY

# 23000 APPLIANCES

## DATA CENTER THREAT PREVENTION



23500



23800



23900

### OVERVIEW

Data centers have uncompromising needs for performance, uptime and scalability. The 23000 Appliances combine the most comprehensive security protections with purpose-built hardware. These powerful security appliances are optimized to deliver threat prevention throughput of up to 14.6 Gbps to secure your most critical assets.

The Check Point 23000 Appliances are ideal for data center networks that require high performance and flexible I/O options. If you're ready to move from 10 to 25, 40 or 100 GbE, so are the 23000 Appliances. These are 2U appliances with five I/O expansion slots for high port capacity, redundant AC or DC power supplies, a 2x 1TB (HDD) or 2x 480GB (SSD) RAID1 disk array, and Lights-out Management (LOM) for remote management.

### ALL-INCLUSIVE SECURITY PACKAGES



THREAT PREVENTION



THREAT PREVENTION + SANDBLAST

### HIGH LEVEL OVERVIEW

The modular design and the wide variety of network options available in the 23000 series of appliances not only provides a rich set of connectivity options for these gateways, they also make the gateways highly customizable to be suited for deployment in any network environment.

Maximum Capacities	23500	23800	23900
NGFW with IPS (Gbps) <sup>1</sup>	12.6	20.4	24
Threat prevention (Gbps) <sup>1</sup>	9.7	10.5	14.6
1 GbE ports (Copper)		42	
10 GbE ports (Fiber)		20	
40 GbE ports (Fiber)		6	
100/25 GbE ports (Fiber)		6	
RAM	128 GB		
Storage	2x 1TB (HDD) or 2x 480GB (SSD)		
AC or DC Power Supplies	2		
Lights-out Management	✓		
Virtual Systems	125	250	250

<sup>1</sup> Measured with the Enterprise testing conditions

WELCOME TO THE FUTURE OF CYBER SECURITY

# 44000, 64000 SECURITY SYSTEMS

## SCALABLE MULTI-BLADE PERFORMANCE



44000 AND 64000 SECURITY SYSTEM

### OVERVIEW

When it comes to protecting the most demanding network environments of data centers, telecommunication and cloud service providers, security and performance are two critical factors that cannot be compromised. The multi-blade hardware and software architecture in the 44000 and 64000 Security Systems is ideal for these environments. The platform provides scalable firewall throughput up to 335 Gbps in the 44000 and up to 800 Gbps in the 64000 platform.

### ALL-INCLUSIVE SECURITY PACKAGES



THREAT PREVENTION



THREAT PREVENTION + SANDBLAST

### HIGH LEVEL OVERVIEW

Designed from the ground-up to support the reliability, availability and serviceability requirements of data centers and service providers, the carrier-grade ATCA chassis runs in High Availability and Load Sharing modes among Security Gateway Modules in one chassis. Add another chassis operating in High Availability mode to further improve redundancy — ensuring mission-critical assets are always available and protected.

Maximum Capacities	44000	64000
Firewall throughput (Gbps) <sup>1</sup>	up to 335	up to 800
100 GbE ports (Fiber)	up to 4	up to 4
40 GbE ports (Fiber)	up to 12	up to 12
10 GbE ports (Fiber)	up to 64	up to 64
Security Switch Modules	1 to 2	2
Security Gateway Modules	1 to 6	2 to 12
Power Supplies	4 AC	6 AC or 2 DC

<sup>1</sup> Measured with the Enterprise testing conditions

For more information: [www.checkpoint.com/products/high-performance-scalable-platforms/](http://www.checkpoint.com/products/high-performance-scalable-platforms/)

WELCOME TO THE FUTURE OF CYBER SECURITY

# MAESTRO

## HYPERSCALE SECURITY ORCHESTRATION



MAESTRO HYPERSCALE ORCHESTRATOR 140 | 170

### OVERVIEW

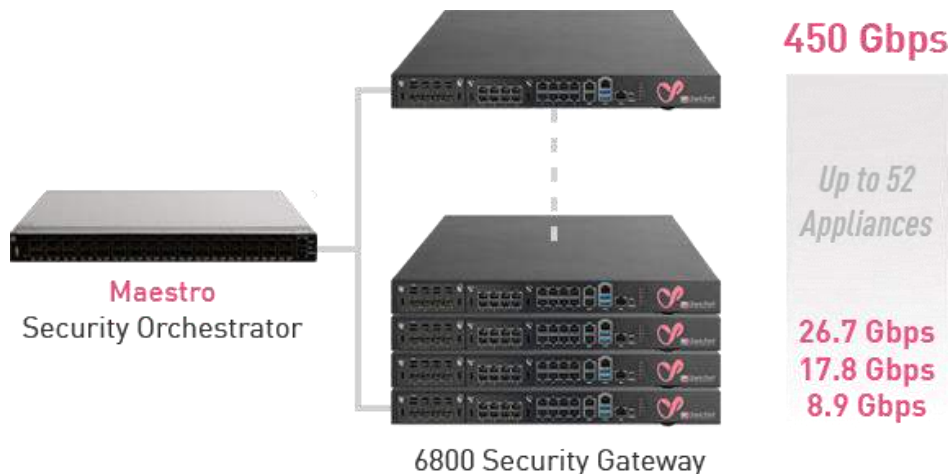
Check Point Maestro brings scale, agility and elasticity of the cloud on premise with efficient N+1 clustering based on Check Point HyperSync technology, maximizing the capabilities of your existing security gateways. Create your own virtualized private-cloud on premise by stacking multiple Check Point security gateways together. Group them by security feature set, policy or the assets they protect and further virtualize them with virtual systems technology.

With the Maestro Hyperscale Orchestrator, businesses of all sizes can have cloud-level security on premise. Add compute to meet your needs using the Maestro Web UI or RESTful APIs – all while minimizing the risk of downtime and maximizing your cost efficiency.

### COST-EFFICIENT N+1 DEPLOYMENT THAT SCALES

Efficient N+1 clustering is now available under one unified system with Check Point Maestro. When a gateway is added to the system, it's configuration, policy and software version are updated and aligned with the existing deployment. Within 6 minutes the new gateway is an active member, increasing your overall system capacity.

In an example deployment using our 6800 model, you can start with one gateway that delivers 8.9 Gbps of threat prevention throughput. Then easily add existing AND new gateways to create a security solution that delivers up to 450 Gbps of threat prevention throughput, simply by using Check Point Maestro.





WELCOME TO THE FUTURE OF CYBER SECURITY

## VIRTUAL APPLIANCES



### CLOUD SECURITY

The wide adoption of cloud architectures—whether public, private or hybrid—is being driven by the desire to transform businesses for greater efficiency, speed, agility and cost controls. While the cloud offers many advantages over traditional infrastructure it also exposes your company to whole new set of security challenges. Check Point offers a complete public and private cloud security portfolio that seamlessly extends security protections to any cloud environment, so you can feel as confident about the cloud as you do about your physical environment.

### PUBLIC IaaS SECURITY

When you move computing resources and data to the public cloud, security responsibilities become shared between you and your cloud service provider. The loss of control in moving applications and data out of the enterprise to a cloud provider—such as Amazon Web Services or Microsoft Azure—and the resulting challenges in monitoring and governing those resources, create a variety of security concerns. This is especially true because of the anonymous, multi-tenant nature of the public cloud. Many companies use hybrid clouds to maintain control of their private cloud infrastructure and protect confidential assets while outsourcing other aspects to public clouds. With the hybrid cloud the new challenge is to protect data as it moves back and forth from the enterprise to a public cloud.

Check Point CloudGuard delivers automated and elastic security to keep assets and data protected while staying aligned to the dynamic needs of public cloud environments.



### PRIVATE IaaS SECURITY

As enterprises adopt Software-defined networking and private cloud environments, the increased agility and efficiency has been a boon to the business but has led to dramatic increases in network traffic going east-west within the data center. This shift in traffic patterns introduces new security challenges. With few controls to secure east-west traffic, threats can travel unimpeded once inside the data center.

Check Point CloudGuard delivers dynamic security within virtual datacenters to prevent the lateral spread of threats while consolidating visibility and management across physical and virtual networks.



For more information: [www.checkpoint.com/products/cloud-security/](http://www.checkpoint.com/products/cloud-security/)



WELCOME TO THE FUTURE OF CYBER SECURITY

# SMART-1 APPLIANCES

## CYBER SECURITY MANAGEMENT IN THE ERA OF BIG DATA



### OVERVIEW

Growing networks, disruptive technologies, and the proliferation of interconnected devices demand a new approach to managing security. Check Point Infinity architecture consolidates management of multiple security layers, providing superior policy efficiency and enabling you to manage security through a single pane of glass. The single management centrally correlates all types of events across all network environments, cloud services and mobile infrastructures.

In order to manage the security environment efficiently and effectively, organizations need security management solutions to also be efficient, effective and to process more data faster than ever before. Check Point Smart-1 Appliances consolidate security management, including logging, event management, and reporting into a single dedicated management appliance. Organizations can now efficiently manage their data and event management requirements across networks, cloud and mobile – gaining centralized visibility into billions of logs, visual indication of risks, and the ability to quickly investigate potential threats.

### UNIFIED, INTELLIGENT SECURITY MANAGEMENT

- 

**SINGLE DOMAIN SECURITY MANAGEMENT**
- 

**MULTI-DOMAIN SECURITY MANAGEMENT**
- 

**MULTI-DOMAIN LOG MANAGEMENT**
- 

**SMARTEVENT EVENT MANAGEMENT**

### HIGH LEVEL OVERVIEW

Organizations can leverage Smart-1 Appliances to manage from 5 to 5,000 gateways. With Smart-1 Multi-Domain Management you can segment the network into as many as 200 independent domains. In addition Smart-1 Appliances provide up to 48 TB of built-in storage and up to 256 GB of Random Access Memory (RAM).

Maximum Capacities	405	410	525	5050	5150
Managed Gateways	5	10	25	50	150+
Maximum Domains (Multi-Domain Management)	x	x	x	50	200
Peak Indexed Logs/Sec	6,000/400 <sup>1</sup>	10,000/600 <sup>1</sup>	14,000/1,600 <sup>1</sup>	27,000/7,500 <sup>1</sup>	40,000/12,000 <sup>1</sup>
Sustained Indexed Logs/Sec	3,000/200 <sup>1</sup>	5,000/300 <sup>1</sup>	7,000/800 <sup>1</sup>	15,000/3,750 <sup>1</sup>	22,000/6,000 <sup>1</sup>
Log Size/Day (GB)	88/0.36 <sup>1</sup>	147/0.55 <sup>1</sup>	205/1.5 <sup>1</sup>	440/6.8 <sup>1</sup>	645/11 <sup>1</sup>
HDD	1x 1TB	1x 2TB	2x 4TB	4x 4TB	12x 4TB
RAM	16 GB	32 GB	64 GB	128 GB	256 GB
Hot Swappable Power Supplies	x	x	✓	✓	✓

<sup>1</sup> Single or Multi-domain/dedicated SmartEvent configuration

WELCOME TO THE FUTURE OF CYBER SECURITY

# DDOS PROTECTORS

## STOP DENIAL OF SERVICE IN SECONDS



506 / 1006 / 2006



4412 / 8412 / 12412



10420 / 20420 / 30420 / 40420

### OVERVIEW

Denial of Service (DoS) and Distributed Denial of Service (DDoS) attacks are increasing in number, speed and complexity in recent years. These attacks are relatively easy to carry out, and can cause serious damage to companies who rely on web services to operate. Many DDoS protection solutions are deployed by an Internet Service Provider, offering generic protections against network layer attacks. However today's DDoS attacks have become more sophisticated, launching multiple attacks at network and application layers. Successful DDoS solutions will offer companies the ability to customize their protections to meet changing security needs, fast response time during an attack, and a choice of deployment options.

DDoS Protector Appliances offer flexible deployment options to easily protect any size business, and integrated security management for real-time traffic analysis and threat management intelligence for advanced protection against DDoS attacks. Check Point also provides dedicated 24/7 support and resources to ensure up-to-the-minute protections.

### MULTI-LAYERED PROTECTIONS



NETWORK & TRAFFIC FLOOD



APPLICATION BASED DOS/DDOS

### HIGH LEVEL OVERVIEW

Check Point DDoS Protector™ Appliances block Denial of Service attacks within seconds with multi-layered protection and up to 40 Gbps of performance. DDoS Protectors extend company's security perimeters to block destructive DDoS attacks before they cause damage.

Maximum Capacities	Enterprise	Data Center	Carrier
Throughput (Gbps) <sup>1</sup>	500 Mbps to 2 Gbps	4 to 12 Gbps	10 to 40 Gbps
Max Concurrent Sessions	2,000,000	4,000,000	6,000,000
Max DDoS Flood Attack Prevention Rate (pps)	1,000,000	10,000,000	25,000,000
Latency	< 60 microseconds		
10/100/1000 Copper Ethernet	4	8	
10 GbE (SFP+)			20
40 GbE QSFP			4
Network Operation	Transparent L2 Forwarding		
High Availability	Active-Passive Cluster		

<sup>1</sup> Throughput is measured with behavioral IPS protections and signature IPS protections using ecommerce protection profile

WELCOME TO THE FUTURE OF CYBER SECURITY

# SANDBLAST APPLIANCES

## PRIVATE CLOUD ZERO DAY THREAT PREVENTION

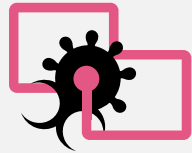


### OVERVIEW

With the increase in sophistication of cyber threats, many targeted attacks begin with exploiting software vulnerabilities in downloaded files and email attachments. These threats include new exploits, or even variants of known exploits unleashed almost daily with no existing signatures and therefore no standard solutions to detect those variants. New and undiscovered threats require new solutions that go beyond signatures of known threats.

Check Point SandBlast Zero-Day Protection, with evasion-resistant malware detection, provides comprehensive protection from even the most dangerous attacks while ensuring quick delivery of safe content to your users. At the core of our solution are two unique capabilities – Threat Emulation and Threat Extraction that take threat defense to the next level.

### STOP NEW AND UNKNOWN THREATS



THREAT EMULATION



THREAT EXTRACTION

### HIGH LEVEL OVERVIEW

We offer a wide range of SandBlast Appliances. These are perfect for customers who have regulatory or privacy concerns preventing them from using the SandBlast Threat Emulation cloud-based service.

Maximum Capacities	TE100X	TE250X	TE1000X	TE2000X
Unique Files/Hour	450	1,000	2,800	5,000
Throughput	150 Mbps	700 Mbps	2 Gbps	4 Gbps
Number of Virtual Machines	4	8	28	56
10/100/1000Base-T RJ45	13	17	14	14
10GBase-F SFP+	-	-	6	8
Bypass (Fail-Open)	Optional 4x 1GbE copper or 2x 10GbE			
Enclosure	1U	1U	2U	2U
HDD	1x 1TB		2x 2TB RAID1	
Power Supplies	1	2	2	2



## PROVEN SECURITY

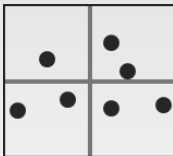
### RECOGNIZED LEADER

When you purchase a Check Point product, rest assured that you are buying a product from a leader in the security industry and a product recognized by leading test and analyst firms.

#### GARTNER

ENTERPRISE NETWORK FIREWALLS

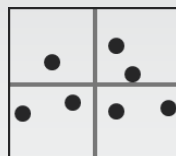
Leader Since 1997<sup>1</sup>



#### GARTNER

UNIFIED THREAT MANAGEMENT

Leader 7 Years in a Row<sup>2</sup>



#### NSS LABS

RECOMMENDED (17 since 2011)

- Firewall
- Next Generation Firewall
- IPS
- Breach Detection Systems



Additional certifications include; NATO Information Assurance Product Catalogue, Common Criteria Medium Robustness, Defense Information Systems Agency (DoD certification of firewall, VPN, IDS and IPS), Commercial Solutions for Classified Program, IPv6 Ready, VPN Consortium. Learn more at [www.checkpoint.com](http://www.checkpoint.com).

<sup>1</sup> Gartner, Inc., Gartner Magic Quadrant for Enterprise Network Firewalls, Adam Hills, Jeremy D'Hoinne, Rajpreet Kaur, Greg Young, 25 May 2016.

<sup>2</sup> Gartner, Inc., Magic Quadrant for Unified Threat Management, Jeremy D'Hoinne, Adam Hills, Greg Young, Rajpreet Kaur, 21 June 2017.

# Contact Check Point Now

[www.checkpoint.com/about-us/contact-us](http://www.checkpoint.com/about-us/contact-us)

By phone in the US: 1-800-429-4391

1-650-628-2000



---

## CONTACT US

**Worldwide Headquarters** | 5 Shlomo Kaplan Street, Tel Aviv 67897, Israel | Tel: 972-3-753-4555 | Fax: 972-3-624-1100 | Email: [info@checkpoint.com](mailto:info@checkpoint.com)  
**U.S. Headquarters** | 959 Skyway Road, Suite 300, San Carlos, CA 94070 | Tel: 800-429-4391; 650-628-2000 | Fax: 650-628-2117 | [www.checkpoint.com](http://www.checkpoint.com)