



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

WE  
SECURE  
THE  
FUTURE

# CHECK POINT APPLIANCES

2016

TABLE OF CONTENTS

---

# CHECK POINT APPLIANCES

- 03** NEXT GENERATION THREAT PREVENTION
- 04** A SECURE OS, SIZED FOR YOU
- 05** SECURITY APPLIANCES
- 13** VIRTUAL APPLIANCES
- 14** MANAGEMENT APPLIANCES
- 15** DDoS PROTECTOR
- 16** SANDBLAST APPLIANCES
- 17** PROVEN SECURITY

## NEXT GENERATION THREAT PREVENTION



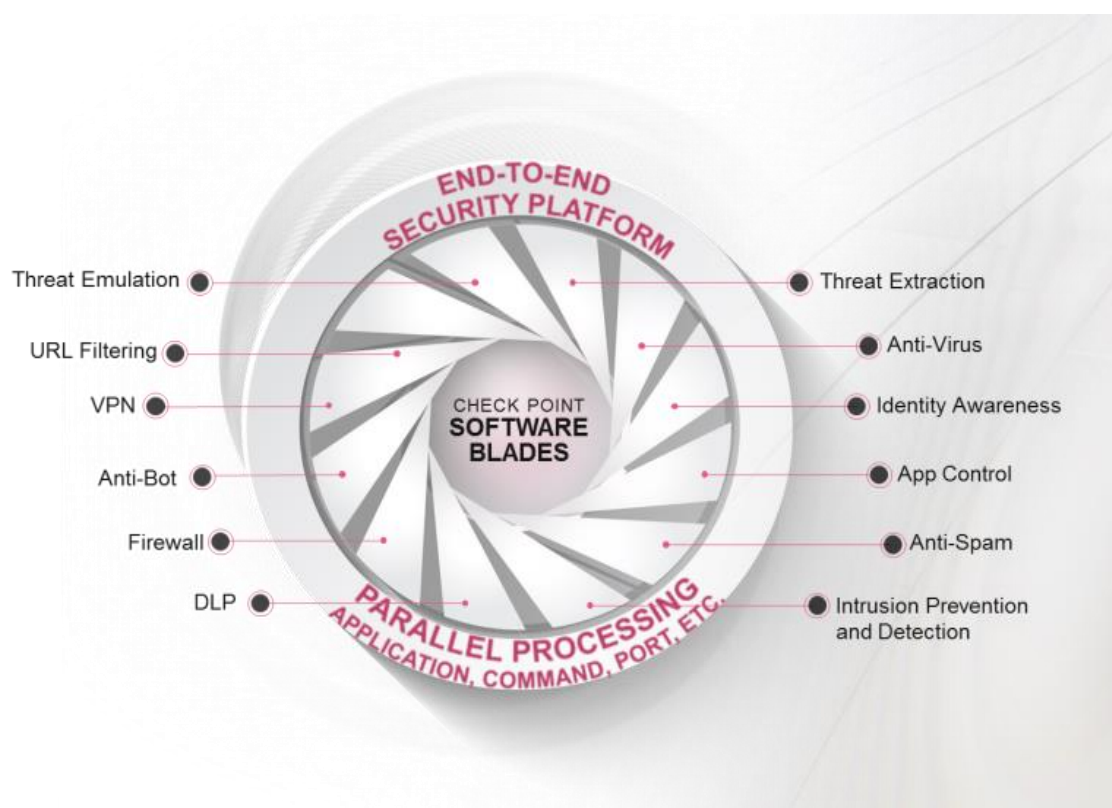
### COMPREHENSIVE THREAT PREVENTION

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.



## A SECURE NEXT-GEN OS SIZED FOR YOU



### GAIA – A UNIFIED SECURE OPERATING SYSTEM

Check Point GAIa™ is the next generation Secure Operating System for all Check Point Appliances, Open Servers and Virtualized Gateways. Customers benefit from the highly efficient 64-bit OS, improved appliance connection capacity and streamlined operational processes. GAIa simplifies management with segregation of duties among users with different privileges by enabling role-based administration. The automatic software update capabilities increases operational efficiency and the intuitive and feature-rich web interface allows for search of any command or property in a second. IPv4 and IPv6 networks are secure with acceleration and clustering technologies and support for the latest unicast and multicast routing protocols.

### TAP THE POWER OF VIRTUALIZATION

Check Point Virtual Systems enable organizations to consolidate infrastructure by creating multiple virtualized security gate ways on a single hardware device, offering significant cost savings with seamless security and infrastructure consolidation. The streamlined management of the virtualized gateways further improves the operational efficiency of a resource-challenged IT department, bringing the needed simplicity to network security.

### THE NEW WAY TO MEASURE THE REAL POWER OF SECURITY APPLIANCES

Unlike other vendors who provide performance numbers based upon optimal testing conditions and using a security policy that has only one rule, Accept Any, Check Point security appliance performance is based upon real-world customer traffic, multiple security functions and a typical security policy. SecurityPower™ provides an effective metric for selecting the right appliance that better predicts its current and future behavior under security attacks and in day to day operation. Customers are ensured they are getting a security appliance that meets their current needs and provides room for growth.





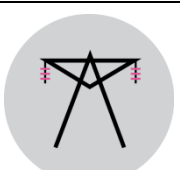


## SecurityPower

## SECURITY APPLIANCES



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.

 Branch Office	Deployment	Branch or Small Office	1100
	Form Factor	Desktop	1400
	Interfaces	1 GbE, Wi-Fi, 3G/4G support	2200
	FW Throughput	750 Mbps to 4 Gbps	3200
	Special Features	DSL, Web management	
 Enterprise	Deployment	Enterprise	4200, 4400
	Form Factor	1RU	4600, 4800
	Interfaces	1, 10 GbE	5200, 5400
	FW Throughput	3 to 35 Gbps	5600, 5800
	Special Features	Flexible IO options	12200
 Data Center	Deployment	Large enterprise, Data center	12400, 12600
	Form Factor	2RU	13500, 13800
	Interfaces	1, 10, 40 GbE	15400, 15600
	FW Throughput	25 to 128 Gbps	21400, 21700, 21800
	Special Features	Low latency, 40 GbE, LOM	23500, 23800
 Chassis Systems	Deployment	Data center, Telco, Carrier	41000
	Form Factor	6RU to 15RU	61000
	Interfaces	1, 10, 40 GbE	
	FW Throughput	80 to 400 Gbps	
	Special Features	Bladed, scalable platform, DC power	
 Rugged	Deployment	Harsh environments	1200R
	Form Factor	Desktop, DIN mount	
	Interfaces	1 GbE, 3G/4G support	
	FW Throughput	2 Gbps	
	Special Features	AC/DC power	

# 1400 APPLIANCES

## BRANCH OFFICE SECURITY



1430-1450 APPLIANCE  
(WIRELESS OPTION)



1470-1490 APPLIANCE  
(WIRELESS 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 to form a unified and total defense against potential threats. 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.

You can now protect your entire network from cyber threats with award-winning Check Point Threat Prevention — from the headquarters to the remote 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



All-Inclusive Next Generation Threat Prevention (NGTP): apply multiple layers of protection to prevent sophisticated cyber-threats — with Application Control, URL Filtering, IPS, Anti-Bot, Antivirus and Email Security.

### HIGH LEVEL COMPARISON

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

Maximum Capacities	1430	1450	1470	1490
Firewall production throughput (Mbps) <sup>1</sup>	750	1000	1500	2000
Threat prevention production throughput (Mbps) <sup>1</sup>	100	150	200	250
1 GbE ports	1x WAN, 1x DMZ, 8x LAN switch		1x WAN, 1x DMZ, 16x LAN switch	
Wi-Fi option	802.11 b/g/n/ac		802.11 b/g/n AND 802.11 n/ac	
Radio band	1: 2.4Ghz or 5Ghz		2 concurrent: 2.4Ghz and 5Ghz	

<sup>1</sup> performance with a real-world traffic blend, a typical rule-base, NAT and logging enabled and the most secure threat prevention

For more information: [www.checkpoint.com/products/1400-security-appliances](http://www.checkpoint.com/products/1400-security-appliances)

# 1200R RUGGED APPLIANCE

## SECURITY FOR HARSH ENVIRONMENTS



1200R APPLIANCE

### 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



NEXT GENERATION FIREWALL



THREAT PREVENTION

### HIGH LEVEL COMPARISON

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

Maximum Capacities	1200R
Firewall production throughput (Mbps) <sup>1</sup>	700
IPS production throughput (Mbps) <sup>1</sup>	60
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

<sup>1</sup> performance with a real-world traffic blend, a typical rule-base, NAT and logging enabled and the most secure threat prevention



# 3200 APPLIANCE

## ENTERPRISE SECURITY FOR BRANCH OFFICES



### OVERVIEW

Seamless security requires protection not only in the main corporate networks. The same level of protection is required for remote and branch offices—to form an unified and total defense against potential threats. The Check Point 3200 Appliance is an ideal solution for delivering security to small and branch offices.

The 3200 Appliance offers enterprise-grade security with leading price/performance in a compact desktop form factor. Its multi-core technology, six 1 Gigabit Ethernet ports and the full support of the Software Blade Architecture delivers a natural extension of corporate security to remote locations. Despite its small form factor, this powerful appliance provides a respectable 2.1 Gbps of real-life firewall throughput and 460 Mbps of real-life IPS throughput.

### ALL-INCLUSIVE SECURITY PACKAGES



THREAT PREVENTION



THREAT PREVENTION + SANDBLAST

### HIGH LEVEL COMPARISON

The compact design, multi-core technology and SandBlast Zero-Day Threat Prevention available in the 3200 Appliance make these gateways ideally suited for deployment in small offices and remote branch offices.

Maximum Capacities	3200
Firewall production throughput (Gbps) <sup>1</sup>	2.1
NGFW (Firewall, Application Control, IPS) production throughput (Mbps) <sup>1</sup>	260
Threat prevention throughput (Mbps) <sup>1</sup>	140
1 GbE ports (Copper)	6
RAM	8 GB
HDD	1x 320 GB
Enclosure	Desktop

<sup>1</sup> performance with a real-world traffic blend, a typical rule-base, NAT and logging enabled and the most secure threat prevention

For more information: [www.checkpoint.com/products/3200-security-appliances](http://www.checkpoint.com/products/3200-security-appliances)



# 5000 APPLIANCES

## ENTERPRISE SECURITY, FLEXIBLE NETWORK OPTIONS



5200 APPLIANCE



5400 APPLIANCE



5600 APPLIANCE



5800 APPLIANCE

### OVERVIEW

Security decisions no longer have to be a choice between features and performance. With the Check Point 5000 Appliances and the extensible Software Blade Architecture, customers can be confident that their security solution will meet their protection needs and also match the performance requirements of their enterprise network.

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 sixteen (26) 1 Gigabit Ethernet ports, redundant hot-swappable power supplies and an optional out-of-band LOM module into a compact 1U rack mountable form-factor. Supporting up to 22 Gbps of real-life firewall throughput and 3 Gbps of real-life IPS throughput, these appliances offer the best performance for its class.

### ALL-INCLUSIVE SECURITY PACKAGES



THREAT PREVENTION



THREAT PREVENTION + SANDBLAST

### HIGH LEVEL COMPARISON

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	5200	5400	5600	5800
Firewall production throughput (Gbps) <sup>1</sup>	5.3	10	17.5	22
IPS production throughput (Gbps) <sup>1</sup>	810 Mbps	1.08	1.9	3.05
1 GbE ports (Copper)	14	18	18	26
1 GbE ports (Fiber)	4	4	4	8
10 GbE ports (Fiber)			4	8
RAM	16 GB	16 GB	16 GB	16 GB
HDD	1x 500 GB	1x 500 GB	1x 500 GB	1x 500 GB
Power Supply Units	1	1	2	2
Lights Out Management	✓	✓	✓	✓
Network expansion slots	1	1	1	2

<sup>1</sup> performance with a real-world traffic blend, a typical rule-base, NAT and logging enabled and the most secure threat prevention

For more information: [www.checkpoint.com/products/5000-security-appliances](http://www.checkpoint.com/products/5000-security-appliances)

# 15000 APPLIANCES

## LARGE ENTERPRISE THREAT PREVENTION



15400 APPLIANCE



15600 APPLIANCE

### 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 real-world threat prevention throughput of up to 2.5 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 40 GbE, so are the 15000 Appliances. These are 2U appliances with three I/O expansion slots for high port capacity, redundant power supplies, a 2x 1TB RAID1 disk array, and Lights-Out Management (LOM) for remote management.

### ALL-INCLUSIVE SECURITY PACKAGES



THREAT PREVENTION



THREAT PREVENTION + SANDBLAST

### HIGH LEVEL COMPARISON

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
Firewall production throughput (Gbps) <sup>1</sup>	30	30
Threat prevention production throughput (Gbps) <sup>1</sup>	1.5	2.5
1 GbE ports (Copper)	26	26
1 GbE ports (Fiber)	12	12
10 GbE ports (Fiber)	12	12
40 GbE ports (Fiber)	4	4
RAM	24 GB	32 GB
HDD	2x 1TB	2x 1TB
Power Supply Units	2	2
Lights Out Management	✓	✓
Virtual Systems	40	80

<sup>1</sup> performance with a real-world traffic blend, a typical rule-base, NAT and logging enabled and the most secure threat prevention

# 23000 APPLIANCES

## DATA CENTER THREAT PREVENTION



23500 APPLIANCE



23800 APPLIANCE

### 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 real-world threat prevention throughput of up to 3.6 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 40 GbE, so are the 23000 Appliances. These are 2U appliances with five I/O expansion slots for high port capacity, redundant power supplies, a 2x 1TB RAID1 disk array, and Lights-Out Management (LOM) for remote management.

### ALL-INCLUSIVE SECURITY PACKAGES



THREAT PREVENTION



THREAT PREVENTION + SANDBLAST

### HIGH LEVEL COMPARISON

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
Firewall production throughput (Gbps) <sup>1</sup>	34	43
Threat Prevention production throughput (Gbps) <sup>1</sup>	2.9	3.6
1 GbE ports (Copper)	42	42
1 GbE ports (Fiber)	20	20
10 GbE ports (Fiber)	20	20
40 GbE ports (Fiber)	4	4
RAM	64 GB	64 GB
HDD	2x 1TB	2x 1TB
Power Supply Units	2	2
Lights Out Management	✓	✓
Virtual Systems	125	250

<sup>1</sup> performance with a real-world traffic blend, a typical rule-base, NAT and logging enabled and the most secure threat prevention

# 41000, 61000 SECURITY SYSTEMS

## SCALABLE MULTI-BLADE PERFORMANCE



41000 AND 61000 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 41000 and 61000 Security Systems is ideal for these environments. The platform provides scalable real-world firewall throughput up to 40 Gbps in the 41000 and up to 120 Gbps in the 61000 platform.

### ALL-INCLUSIVE SECURITY PACKAGES



All-Inclusive Next Generation Firewall (NGFW): identify and control applications by user and scan content to stop threats — with IPS and Application Control.

### HIGH LEVEL COMPARISON

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	41000	61000
Firewall production throughput (Gbps) <sup>1</sup>	up to 40	up to 120
IPS production throughput (Gbps) <sup>1</sup>	up to 25	up to 70
10 GbE ports (Fiber)	up to 30	up to 60
40 GbE ports (Fiber)	up to 4	up to 8
Security Switch Modules	1 to 2	2 to 4
Security Gateway Modules	1 to 4	2 to 12
Power Supply Units	3 AC or 2 DC	4 AC or 2 DC

<sup>1</sup> performance with a real-world traffic blend, a typical rule-base, NAT and logging enabled and the most secure threat prevention

## VIRTUAL APPLIANCES



### PUBLIC AND PRIVATE 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 CLOUD SECURITY CHALLENGES

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 vSEC delivers advanced threat protection and single pane-of-glass management for easily extending security to protect your data and assets in public cloud environments.

### PRIVATE CLOUD SECURITY CHALLENGES

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. And traditional approaches to security cannot keep pace with the dynamic nature of virtual environments where applications are constantly provisioned in and out.

Check Point vSEC seamlessly delivers advanced threat protections to private cloud infrastructure and provides the visibility and control effectively manage security in both physical and virtual environments—all from a single unified management solution.



**AMAZON WEB SERVICES**



**MICROSOFT AZURE**



**vSEC FOR VMWARE NSX**



**vSEC VIRTUAL EDITION**



**vSEC OPENSTACK**

# SMART-1 APPLIANCES

## CYBER SECURITY MANAGEMENT IN THE ERA OF BIG DATA



SMART-1 205, 210, 225, 3050, 3150 APPLIANCES

### OVERVIEW

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 the data and event management requirements of the Big Data era, 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 COMPARISON

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 12 TB of built-in storage as well as high-performance fiber channel connectivity to Storage Area Networks (SANs) for external storage.

Maximum Capacities	205	210	225	3050	3150
Managed Gateways	5	10	25	50	150+
Maximum Domains (Multi-Domain Management) <sup>1</sup>	x	x	x	50	200
Indexed Logs/Sec	3,000	5,000	11,000	26,000	44,000
SmartEvent Log Size/Day (GB)	3.5	6.5	13	40	100
HDD	1x 1TB	1x 2TB	2x 2TB	4x 2TB	12x 2TB
RAM	4 GB	8 GB	32 GB	256 GB	256 GB
Fiber Channel SAN Card	x	x	✓	✓	✓

# DDOS PROTECTORS

## STOP DENIAL OF SERVICE IN SECONDS



### 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 COMPARISON

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



# 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 COMPARISON

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
Recommended Files/Month	100K	250K	1M	2M
Recommended Users	up to 1,000	up to 3,000	up to 10,000	up to 20,000
Throughput	150 Mbps	700 Mbps	2 Gbps	4 Gbps
Number of Virtual Machines	4	8	28	56
10/100/1000Base-T RJ45	5	9	6	6
10 GBase-F SFP+	-	-	2	4
Enclosure	1U	1U	2U	2U
HDD	1x 1TB		2x 2TB RAID1	
Power Supply Units	1	2	2	2

For more information: [www.checkpoint.com/products-solutions/threat-prevention-appliances-and-software](http://www.checkpoint.com/products-solutions/threat-prevention-appliances-and-software)

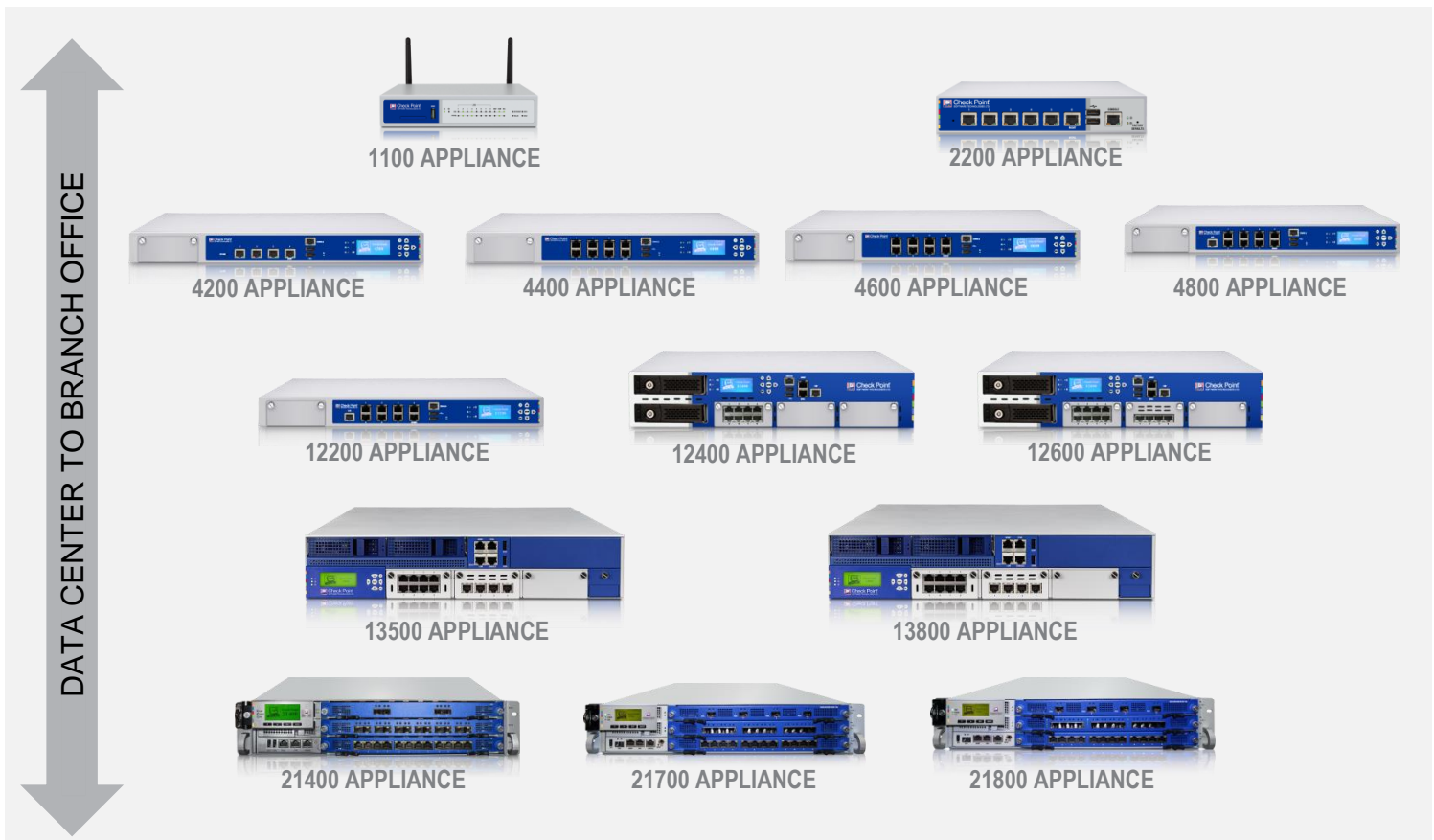
## PROVEN SECURITY



## RECOGNIZED LEADER

Whether you purchase one of our latest appliances or one of our Security Gateway appliances shown below, you can 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 such as Gartner, IDC, NSS Labs and Network World.

- Gartner Enterprise Network Firewalls Magic Quadrant Leader SINCE 1997 <sup>1</sup>
- Gartner Unified Threat Management Magic Quadrant Leader 5 YEARS IN A ROW <sup>2</sup>
- Leads the global market in combined Firewall and UTM appliance revenue share for 3Q 2015 <sup>3</sup>
- NSS Labs Recommend for IPS, NGFW and Breach Detection Systems



<sup>1</sup> Gartner, Inc., Magic Quadrant for Enterprise Network Firewalls, Adam Hills, Greg Young, Jeremy D'Hoinne, 22 April 2015.

<sup>2</sup> Gartner, Inc., Magic Quadrant for Unified Threat Management, Jeremy D'Hoinne, Adam Hills, Greg Young, Rajpreet Kaur, 27 August 2015.

<sup>3</sup> Source: IDC Worldwide Quarterly Security Appliance Tracker 3Q2015, December 14, 2015.

# 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

**Check Point**  
SOFTWARE TECHNOLOGIES LTD.

---

## CONTACT US

**Worldwide Headquarters** | 5 Ha'Solelim 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: 650-654-4233 | [www.checkpoint.com](http://www.checkpoint.com)