NETWORK SECURITY

2022

TABLE OF CONTENTS

CHECK POINT NETWORK SECURITY

CHECK POINT™

YOU DESERVE THE BEST SECURITY

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 VI (6th 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.

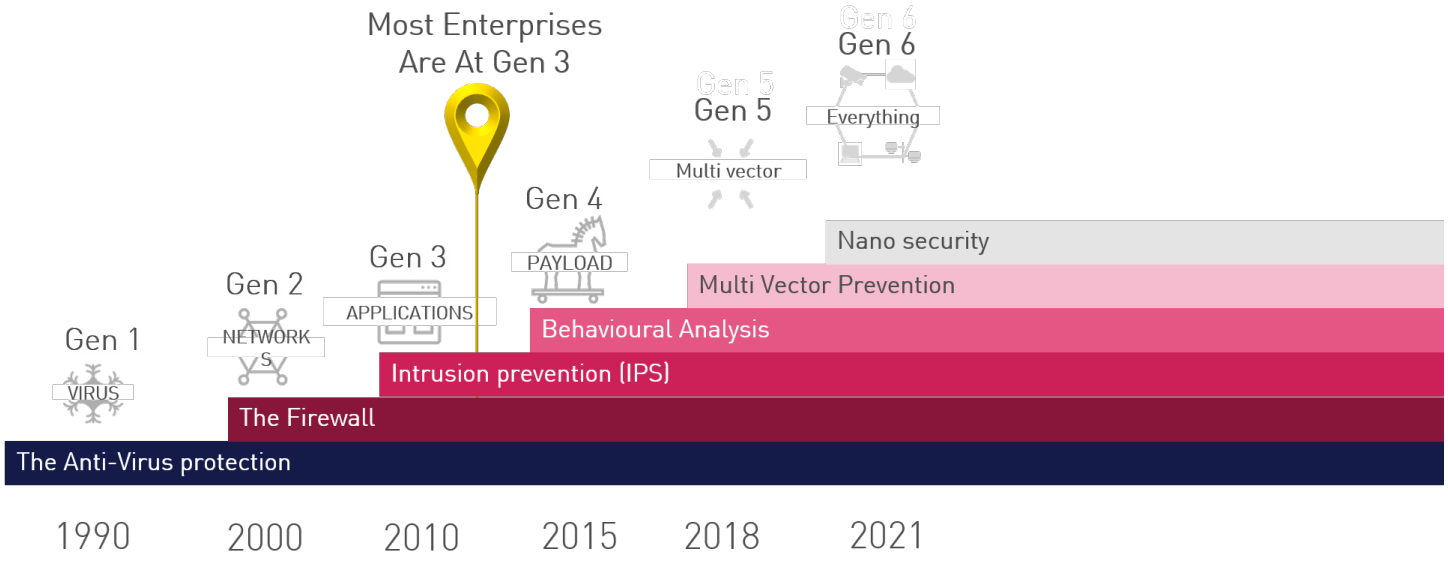
Separate IT environments often drive businesses to apply different point solutions, many of which are focused on detection and mitigation rather than prevention. This reactive approach to cyberattacks is costly and ineffective, complicates security operations and creates inherent gaps in security posture,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

It's time to step up to Gen VI 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 VI 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.



NEXT GEN
THREAT PREVENTION

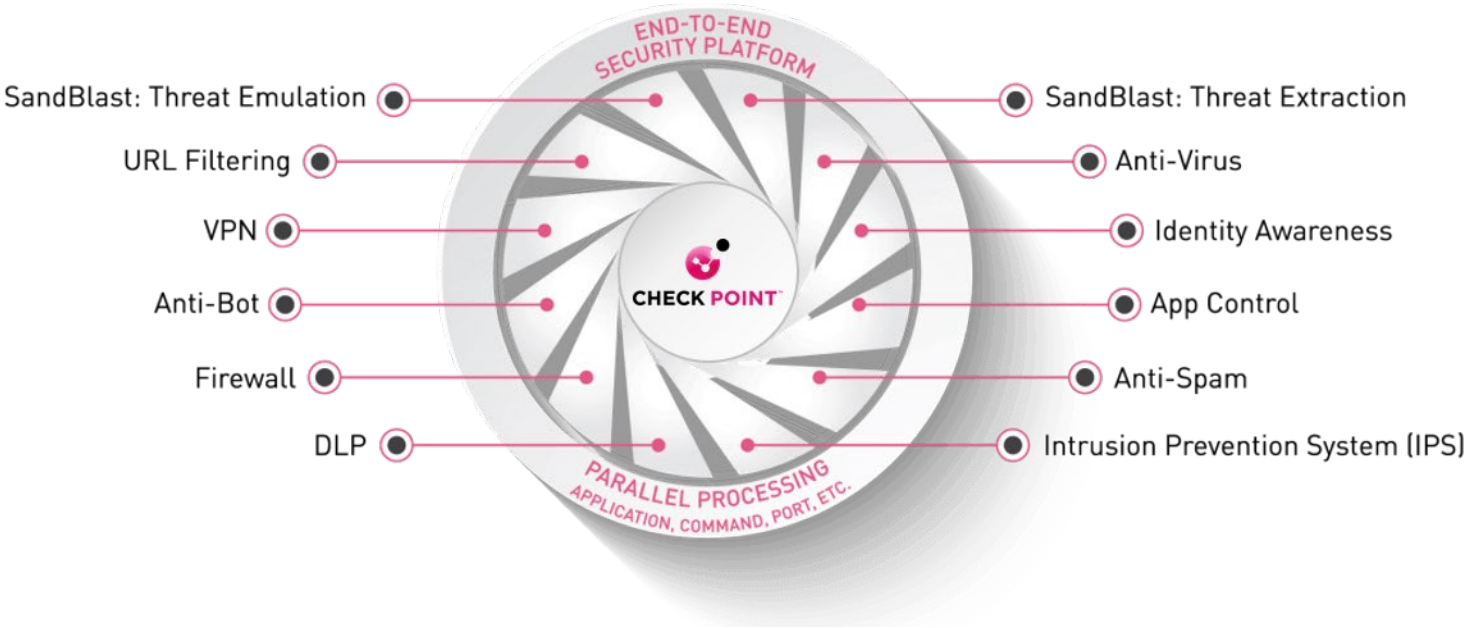
COMPREHENSIVE THREAT PREVENTION

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 – enhanced with the award-winning SandBlast™ Threat Emulation (sandboxing) and Threat Extraction (Content Disarm & Reconstruction) 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 in email and web, 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.

 Scalable Platforms	Deployment Form Factor Interfaces Throughput Special Features	Data center, Telco, Carrier 4RU and up 1, 10, 40, 100 GbE Up to 1,500 Gbps Threat Prevention DC power, Active/Active Clustering	Maestro
 Data Center	Deployment Form Factor Interfaces FW Throughput Special Features	Large enterprise, Data center 2RU 1, 10, 25, 40, 100 GbE 78.3 to 800 Gbps 25/40/100 GbE, DC power, LOM	Lightspeed Firewalls 28000 26000 16200
 Enterprise	Deployment Form Factor Interfaces FW Throughput Special Features	Enterprise 1RU 1, 10, 40 GbE 9 to 48 Gbps (Enterprise Test) Flexible IO options, LOM	7000, 6900 6700, 6600 6400, 6200
 Branch, Small Office	Deployment Form Factor Interfaces FW Throughput Special Features	Branch or Small Office Desktop 1 GbE, Wi-Fi, DSL, 3G/4G/LTE 1 to 7.5 Gbps (Enterprise Test) Web management	3800, 3600 1800, 1600 1500
 Rugged	Deployment Form Factor Interfaces FW Throughput Special Features	Harsh environments Desktop, DIN and wall mount 1 GbE, 3G/4G/TE support 4 Gbps AC/DC power	1570R

QUANTUM MAESTRO

HYPERSCALE SECURITY ORCHESTRATION

Quantum Maestro Hyperscal Orchestrator 140 | 175

OVERVIEW

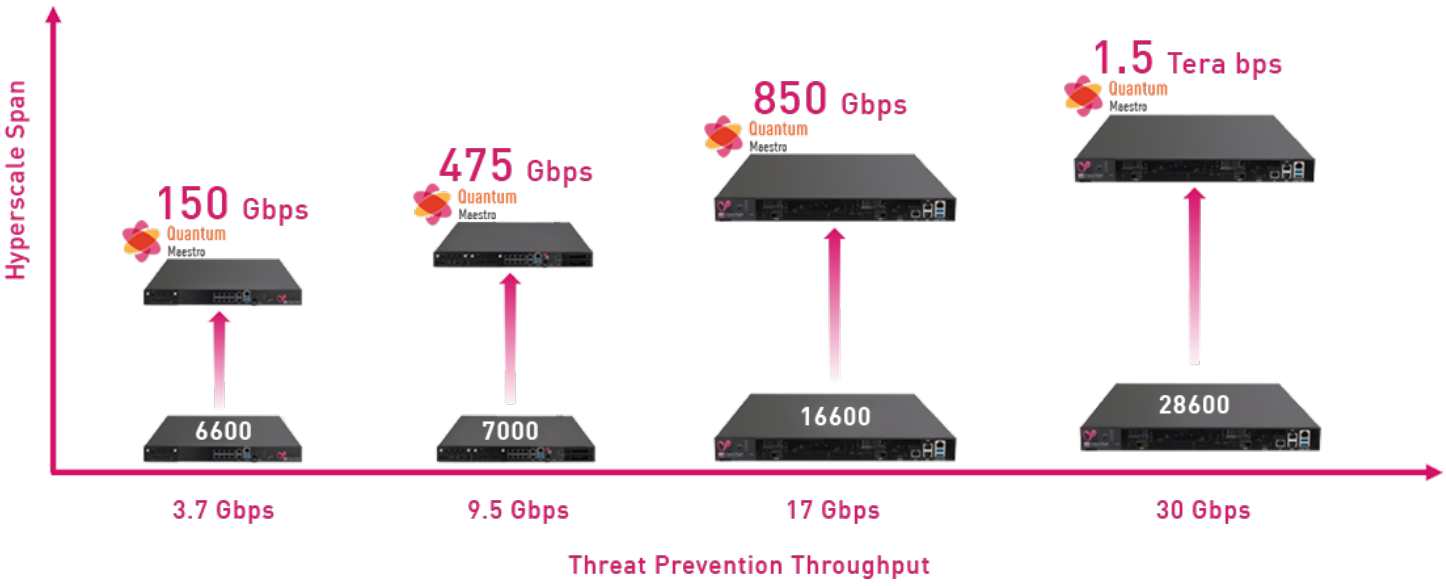
Check Point Maestro brings scale, agility and elasticity of the cloud on premise with efficient N+1 clustering based on Check Point HyperSync technology, maximizing the capabilities of your existing security gateways. Create your own virtualized private-cloud on premise by stacking multiple Check Point 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 16600HS model, you can start with one gateway that delivers 17.6 Gbps of threat prevention throughput. Then easily add existing AND new gateways to create a security solution that delivers up to 850 Gbps of threat prevention throughput, simply by using Check Point Maestro.



QUANTUM LIGHTSPEED

HYPER-FAST, ULTRA-LOW LATENCY FIREWALL

QLS250 QLS450 QLS650 QLS800

OVERVIEW

Enterprises need data center security to perform at the speed of the network, to enable the transfer of hundreds of terabytes of data in minutes instead of hours, provide low latency for high frequency financial transactions, while scaling on demand to support high growth businesses like online commerce. Check Point Quantum Lightspeed firewalls are custom designed to meet and exceed these requirements at a very competitive price-performance.

Quantum Lightspeed sets the standard in data center firewall security, delivering 20x better security price performance than competing solutions. Quantum Lightspeed hyper-fast firewalls deliver 5 times the security throughput, scales up to 3 Tbps per system (800 Gbps per single gateway), while delivering 3 microseconds of ultra-low latency. They also support up to 100G elephant flows. These are characterized by a large, continuous flow that stays open and occupies a disproportionate share of the total bandwidth of a network link for a long duration.

ALL-INCLUSIVE SECURITY PACKAGES

3 µSEC ULTRA-LOW LATENCY FIREWALL

Check Point SandBlast™

ZERO-DAY THREAT PREVENTION

HIGH LEVEL OVERVIEW

The Lightspeed family is 4 models; the QLS250, QLS450, QLS650 and the QLS800 which range in throughput from 250 Gbps to 800 Gbps of firewall throughput. Firewall throughput depends upon the number of accelerated 100GbE ports in the QLS model. Each 100GbE NIC has 2x 100G QSFP28 ports and delivers nearly 200G of aggregate firewall throughput.

Maximum Capacities	QLS250	QLS450	QLS650	QLS800
Firewall throughput (Gbps)[1]	250	450	650	796
Firewall Latency	3µSec	3µSec	3µSec	3µSec
Accelerated 100 GbE ports	2	4	6	8
10 GbE ports	8	8	8	-
Memory	128 GB	192 GB	192 GB	192 GB
Power Supplies	Redundant hot-swap power supplies			
Storage	2x 960GB SSD RAID1 array			
Lights-out Management	✓	✓	✓	✓

[1] Measured with 1518B UDP

For more information: checkpoint.com/quantum/next-generation-firewall/

QUANTUM 28000, 26000

HIGH-END ENTERPRISE THREAT PREVENTION

Quantum 26000, 28000

OVERVIEW

Check Point Quantum 26000 and 28000 Security Gateways combine the most comprehensive protections with data center-grade security and hardware to maximize uptime and deliver up to 30 Gbps of threat prevention performance for securing data centers.

The Check Point Quantum 26000 and 28000 Security Gateways are ideal for data center networks that require high performance and flexible I/O options. These are 3U appliances with eight I/O expansion slots for high port capacity, redundant AC 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

NEXT-GEN FIREWALL

Check Point SandBlast™

ZERO-DAY THREAT PREVENTION

HIGH LEVEL OVERVIEW

Maximum Capacities	26000	28000
Threat prevention (Gbps)[1]	24	30
NGFW with IPS (Gbps)[1]	40.5	51.5
1 GbE ports (Copper)	up to 66x 10/100/1000 Base-T	
1, 10, 40, or 100/25 GbE ports (Fiber)	up to 32x 1GbE, 32x 10GbE, 16x 40GbE or 16x 100/25 GbE ports	
I/O expansion slots	8	
Memory	128 GB	
Storage	2x 480GB SSD RAID1 array	
Power Supplies	3x redundant hot-swap power supplies	
Lights-out Management	✓	

[1] Measured with the Enterprise testing conditions

For more information: checkpoint.com/quantum/next-generation-firewall/

QUANTUM 16000

LARGE ENTERPRISE THREAT PREVENTION

Quantum 16200

OVERVIEW

Check Point Quantum 16200 Security Gateways combine the most comprehensive protections with data center-grade security and hardware to maximize uptime and deliver up to 15 Gbps of threat prevention performance for securing large enterprises.

The Check Point Quantum 16200 Security Gateways are ideal for large enterprise networks that require high performance and flexible I/O options. These are 2U appliances with four I/O expansion slots for high port capacity, redundant AC power supplies, a 2x 480GB SSD RAID1 disk array, and Lights-out Management (LOM) for remote management.

ALL-INCLUSIVE SECURITY PACKAGES

NEXT-GEN FIREWALL

Check Point SandBlast™

ZERO-DAY THREAT PREVENTION

HIGH LEVEL OVERVIEW

Maximum Capacities	16200
Threat prevention (Gbps)[1]	15
NGFW with IPS (Gbps)[1]	27
1 GbE ports (Copper)	up to 34x 10/100/1000 Base-T
1, 10, 40, or 100/25 GbE ports (Fiber)	up to 16x 1GbE, 16x 10GbE, 8x 40GbE or 8x 100/25 GbE ports
I/O expansion slots	4
RAM	128 GB
Storage	2x 480GB SSD RAID1 array
AC Power Supplies	2x redundant hot-swap power supplies
Lights-out Management	✓

[1] Measured with the Enterprise testing conditions

For more information: checkpoint.com/quantum/next-generation-firewall/

QUANTUM 7000

ENTERPRISE THREAT PREVENTION

Quantum 7000

OVERVIEW

Large enterprises have uncompromising needs for performance, uptime and scalability. The 7000 Security Gateways combine the most comprehensive security protections with purpose-built hardware. These powerful security appliances are optimized to deliver threat prevention throughput of up to 9.5 Gbps to secure your most critical assets.

The Check Point 7000 Security Gateways are ideal for enterprise networks that require high performance and flexible I/O options. These are 2U appliances with two I/O expansion slots for high port capacity, redundant AC or DC power supplies, a 2x 480GB SSD RAID1 disk array, and Lights-out Management (LOM) for remote management.

ALL-INCLUSIVE SECURITY PACKAGES

NEXT-GEN FIREWALL

Check Point SandBlast™

ZERO-DAY THREAT PREVENTION

HIGH LEVEL OVERVIEW

The modular design and the wide variety of network options available in the 7000 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	7000
Threat prevention (Gbps)[1]	9.5
NGFW with IPS (Gbps)[1]	22
1 GbE ports (Copper)	26
10 GbE ports (Fiber)	8
40 GbE ports (Fiber)	4
RAM	64 GB
Storage	2x 480GB SSD RAID1 array
AC Power Supplies	2x redundant hot-swap power supplies
Lights-out Management	✓

[1] Measured with the Enterprise testing conditions

For more information: checkpoint.com/quantum/next-generation-firewall/

QUANTUM 6000

SMALL TO MID-ENTERPRISE THREAT PREVENTION

Quantum 6200,

Quantum 6600,

Quantum 6900

OVERVIEW

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

The Quantum 6000 Security Gateways come standard with 10x 1 Gigabit Ethernet ports, and support redundant power supplies and Lights-out Management (LOM) in a compact 1U rack mountable form-factor. Supporting up to 17 Gbps of Next Generation Firewall throughput and 7.4 Gbps of threat prevention throughput, these appliances offer best-in-class performance.

ALL-INCLUSIVE SECURITY PACKAGES

NEXT-GEN FIREWALL

Check Point SandBlast™

ZERO-DAY THREAT PREVENTION

HIGH LEVEL OVERVIEW

The one expansion slot available in the Quantum 6000 security appliances, 2 in the 6900, provides a rich set of connectivity options for these gateways. Redundant power supplies ensure continuous power in the event of a power source failure.

Maximum Capacities	6200	6400	6600	6700	6900
Threat Prevention (Gbps)[1]	1.8	2.5	3.7	5.8	7.4
NGFW with IPS (Gbps)[1]	3.72	5.5	6.2	13.4	17
1 GbE ports (Copper)	18				26
1 GbE ports (Fiber)	4				8
10 GbE ports (Fiber)	4				8
RAM	32				64
Storage	1x 240GB SSD			1x 480GB SSD	2x 480GB SSD
AC Power Supplies	2x redundant power supplies				
LOM	✓				

[1] Measured with the Enterprise testing conditions

For more information: checkpoint.com/quantum/next-generation-firewall/

QUANTUM 3000

ENTERPRISE SECURITY FOR BRANCH OFFICES

Quantum 3600

Quantum 3800

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 Quantum 3600 and 3800 Security Gateways are an ideal solution for delivering security to small and branch offices.

The Quantum 3600 and 3800 Security Gateways 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 Gateways provide up to 3 Gbps of Next Generation Firewall throughput and up to 1.5 Gbps of threat prevention throughput.

ALL-INCLUSIVE SECURITY PACKAGES

NEXT-GEN FIREWALL

Check Point SandBlast™

ZERO-DAY THREAT PREVENTION

HIGH LEVEL OVERVIEW

The compact design, multi-core technology and SandBlast Zero-Day Protection available in the Quantum 3600 and 3800 Security Gatewayss make these gateways ideally suited for deployment in small offices and remote branch offices.

Maximum Capacities	3600	3800
Threat prevention (Gbps)[1]	780 Mbps	1.5
NGFW with IPS (Gbps)[1]	1.5	3
VPN throughput (Gbps)	2.71	2.75
RAM	8 GB	16 GB
1 GbE ports (Copper)	6	
Storage	1x 240GB SSD	
Enclosure	Desktop	
Power Consumption (Max)	24.2W	

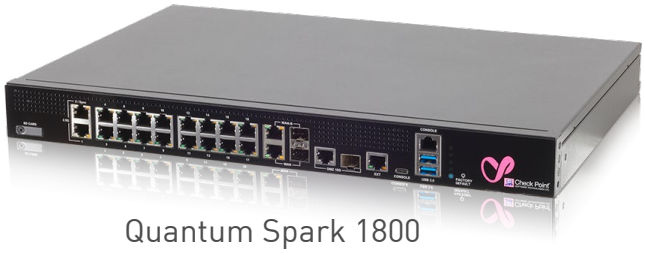
[1] Measured with the Enterprise testing conditions

For more information: checkpoint.com/quantum/next-generation-firewall/

QUANTUM SPARK™ 1600, 1800

SMB NETWORK SECURITY

Quantum Spark 1600



Quantum Spark 1800

OVERVIEW

Enforcing consistent network security is challenging for small to mid-size businesses where there are few users with little to no IT expertise. Small to mid-size business offices require the same level of protection from sophisticated cyber-attacks and zero-day threats that is available in larger enterprise offices.

The Check Point Quantum Spark 1600 and 1800 security gateways deliver enterprise-grade security in simple, affordable, all-in-one security solutions in a 1 Rack Unit (RU) form factor to protect small to mid-size business employees, networks and data from cyber-theft. High threat prevention throughput and high port capacity with 2.5 and 10 GbE network interfaces in the 1800 make these NGFWs ideal for larger branch and SMB networks.

ALL-INCLUSIVE SECURITY

NEXT-GEN FIREWALL

Check Point SandBlast™

ZERO-DAY THREAT PREVENTION

HIGH LEVEL OVERVIEW

The 1600 and 1800 gateways come standard with sixteen (16) 1-Gigabit Ethernet LAN switch ports and a 1-GbE WAN port configuration that supports copper or fiber connections. The DMZ port is a combination copper/fiber 1 GbE port in the 1600 and 10 GbE in the 1800. The 1800 has an additional two (2) 2.5 GbE LAN ports and two (2) power supplies for redundancy.

Maximum Capacities	1600	1800
Threat prevention[1]	1.5 Gbps	2 Gbps
Next-Gen Firewall + IPS	3.2 Gbps	5 Gbps
LAN ports	16x 1GbE copper ports	16x 1GbE copper plus 2x 2.5GbE copper ports
WAN ports	1x 1GbE copper/fiber port	2x 1GbE copper/fiber port
DMZ ports	1x 1GbE copper/fiber port	1x 10GbE copper/fiber port
Power supplies	1	2 redundant
Storage	32 GB eMMC plus a 64 GB micro-SD card option	32 GB eMMC plus a 256 GB SSD

For more information: checkpoint.com/quantum/next-generation-firewall/

QUANTUM SPARK™ 1500

SMALL OFFICE SECURITY

Quantum Spark 1530/1550 Wi-Fi

Quantum Spark 1570/1590 Wi-Fi

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 Quantum Spark 1500 security gateways 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 Quantum Spark 1500 security gateways 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 on-premises or cloud-hosted security management to remotely manage and apply a consistent security policy to thousands of devices across the field offices.

ALL-INCLUSIVE SECURITY

NEXT-GEN FIREWALL

Check Point SandBlast™

ZERO-DAY THREAT PREVENTION

HIGH LEVEL OVERVIEW

Available in four appliances, the 1530/1550 and the 1570/1590, these gateways come standard with sixt (6) or ten (10) 1-Gigabit Ethernet ports respectively. Connect securely from any device directly or through secure authenticated Wi-Fi.

Maximum Capacities	1530	1550	1570	1590
Threat prevention	340 Mbps	450 Mbps	500 Mbps	660 Mbps
NGFW + IPS	600 Mbps	800 Mbps	970 Mbps	1,300 Mbps
1 GbE ports	1x WAN, 5x LAN switch		1x WAN, 1x DMZ, 8x LAN switch	
1 GbE fiber DMZ port	-		1x 1000BaseF SFP port	
Wi-Fi option	802.11 b/g/n/ac, one band 2.4 or 5GHz		802.11 n/ac, dual band 2.4 and 5GHz	
DSL option	✖		✓	
LTE option	✖		✓	
Mobile Access Users (default)	100		200	

For more information: checkpoint.com/quantum/next-generation-firewall/

QUANTUM RUGGED

SECURITY FOR HARSH ENVIRONMENTS

Quantum Rugged 1570R

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 Quantum Rugged 1570R security gateway complements our extensive appliance family to support a diverse range of deployment environments and meet specialized requirements. For instance, the 1570R 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 security gateways would fail, this appliance keeps you secure.

ALL-INCLUSIVE SECURITY PACKAGES

NEXT-GEN FIREWALL

Check Point SandBlast™

ZERO-DAY THREAT PREVENTION

HIGH LEVEL OVERVIEW

Copper and fiber 1GbE Ethernet ports are included as is a Wi-Fi and a 3G/4G/LTE wireless embedded modem option.

Maximum Capacities	1570R
Threat Prevention throughput	400 Mbps
NGFW throughput	700 Mbps
WAN	1x 10/100/1000BaseT RJ45 or 1x 1000BaseF port
DMZ	1x 10/100/1000BaseT RJ45 or 1x 1000BaseF port
LAN	8x 10/100/1000BaseT RJ45 ports
Mount Options	DIN rail or wall mount
Certifications	Industrial, Maritime, Rugged (shock and vibration), IP30 IP rating
Operating Temperature Range	40ºC ~ 75ºC (-40ºF ~ +167ºF)

For more information: checkpoint.com/quantum/next-generation-firewall/

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.

CloudGuard Network

Amazon Web Services

CloudGuard Network

Microsoft Azure

CloudGuard Network

VMware Cloud on AWS

CloudGuard Network

Google Cloud Platform

CloudGuard Network

Alibaba Cloud

CloudGuard Network

Oracle Cloud

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.

CloudGuard Network

Cisco ACI

CloudGuard Network

VMware NSX

CloudGuard Network

OpenStack

CloudGuard Network

Virtual Edition NGFW

For more information: checkpoint.com/cloudguard/cloud-network-security/

QUANTUM SMART-1

SECURITY MANAGEMENT IN THE ERA OF BIG DATA


600-S


600-M


6000-L


6000-XL

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 Quantum 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 Quantum 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 addtion Smart-1 Appliances provide up to 48 TB of built-in storage and up to 384 GB of Random Access Memory (RAM).

Maximum Capacities	600-S	600-M	6000-L	6000-XL
Managed Gateways	10	50	150	400+
Maximum Domains (Multi-Domain Management)	×	×	50	200
Peak Logs/Sec	70,000	90,000	150,000	300,000
Sustained Indexed Logs/Sec	8,000/2,000[1]	13,000/4,000[1]	23,000/23,000[1]	40,000/40,000[1]
Log Size/Day (GB)	200/50[1]	295/105[1]	616/38[1]	999/65[1]
Storage	1x 2TB HDD	2x 4TB HDD	12x 4TB HDD	12x 4TB SSD
RAM	32 GB	64 GB	192 GB	384 GB
Hot Swappable Power Supplies	×	✓	✓	✓

[1]600-S and 600-M tested with SmartLog and SmartEvent configuration, 6000-L/6000-XL tested with dedicated SmartEvent configuration

For more information: checkpoint.com/quantum/unified-cyber-security-platform/

DDOS PROTECTOR

STOP DENIAL OF SERVICE IN SECONDS

6

20 / 60

110 / 220

200 / 400

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 400 Gbps of performance. DDoS Protectors extend company's security perimeters to block destructive DDoS attacks before they cause damage.

Maximum Capacities	6	20	60	110	200	220	400
Mitigation Bandwidth (Gbps)	6	20	60	110	200	220	400
Max DDoS Flood Attack Rate	5.8M	25M	25M	50M	330M	146M	330M
SSL/TLS CPS (RSA 2K)	20 K	95 K	95K	150K	-	150K	-
Latency	< 60 micro seconds						
Network Operation	Transparent L2 Forwarding/IP Forwarding						
Deployment Modes	Inline, SPAN port, copy port, Hybrid (cloud scrubbing center option)						
Ports	8x RJ45, 2x 1/10 GbE	24x 1/10 GbE	24x 10, 8x 40, 4x 100 GbE	20x 10, 4x 40, 4x 100 GbE		24x 10, 8x 40, 4x 100 GbE	20x 10, 4x 40, 4x 100 GbE
Enclosure	1U	2U	2U	2U	2U	2U	2U

For more information: checkpoint.com/quantum/ddos-protector/

SANDBLAST APPLIANCES

PRIVATE CLOUD ZERO DAY THREAT PREVENTION

TE2000XN-28VM

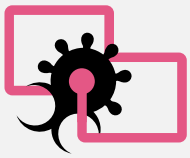
TE2000XN-56VM

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 SandBlast Threat Emulation security appliances for customers who have regulatory or privacy concerns preventing them from using the SandBlast Threat Emulation cloud-based services.

Maximum Capacities	TE2000XN-28VM	TE2000XN-56VM
Unique Files/Hour	5,000	8,000
Number of Virtual Machines	28	56
100G QSFP28	2	2
10/100/1000BaseT RJ45	2	2
Memory	128 GB	128 GB
Lights-out Management	✓	✓
Enclosure	1U	1U
Storage	1x 2TB SSD	1x 2TB SSD
Power Supplies	Dual, hot-swappable	Dual, hot-swappable

For more information: checkpoint.com/quantum/advanvced-network-threat-prevention/

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 LEADER 2020 NETWORK FIREWALL MAGIC QUADRANT

22x

Check Point Software Technologies is proud to be named a Leader in the 2021 Magic Quadrant for Network Firewalls (NFW). This marks the 22nd time in the company's history to be named a Leader by Gartner. Gartner's annual report analyzes, rigorously tests and places key performers in the "Leader" Quadrant. Our robust Infinity architecture and focus on cloud security solidified our position in the 2021 report receiving high regards for performance, prevention and product integration. We are recognized for our pioneering centralized security management capabilities, efficient policy management, and the advanced Threat Prevention technology.

NSS LABS RECOMMENDED

Check Point actively participated in NSS Labs tests since 2011 and achieved NSS Labs Recommended status in firewall, Next Generation Firewall, Intrusion Prevention System (IPS) and Breach Prevention Systems (BPS) group tests. The NSS Labs 2019 BPS Highest Security Effectiveness Score is significant because it incorporates multiple solutions that enable a vendor to provide a breach prevention posture to its customers. Involving multiple solutions provides synergy between various security components that when combined effectively block attacks throughout the cyber kill chain. In Check Point's case, the solution involved myriad technologies such as SandBlast Network, SandBlast Agent, threat extraction, anti-bot and more.

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.

Gartner, Magic Quadrant for Network Firewalls, By Rajpreet Kaur, Jeremy D'Hoinne, Nat Smith, Adam Hils, 1 November 2021.

Contact Us

www.checkpoint.com/about-us/contact-us

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