Battle Card – Check Point Quantum Spark

OVERVIEW

Check Point Quantum Spark security gateways are high-performance, integrated devices offering firewall, VPN, antivirus, application visibility and control, URL filtering, email security and SandBlast Zero-Day Protection, all in compact form factors that are simple to configure and manage.

- Most advanced threat prevention; including firewall, Application Control, URL Filtering, IPS, Antivirus, Anti-Bot and Anti-Spam
- Full security without compromising on performance
- Integrated 802.11ax 4x4 MIMO **WiFi 6** wireless security with a guest access option
- Diverse WAN connectivity including DSL and **5G** WAN
- Set up within minutes, with out-of-the-box configuration, providing instant protection for what may be the weakest link in your organization

ENTERPRISE-GRADE SMALL OFFICE SECURITY

THE CHECK POINT ADVANTAGE

Defense from Most Common Attacks

- Next Generation Firewall
- IPSec VPN & SSL-VPN
- Application Control & Web Filtering
- Intrusion Prevention
- Antivirus
- Anti-Bot
- Anti-SPAM
- SandBlast Threat Emulation

Easy Deployment

- Full Protection in 60 Seconds
- No Need for an On-Site Technician – Plug it in, Turn it on, and You're Done

Mobile App for Management On-the-Go

- A Security Operations Center in the Palm of Your Hand
- Get Real-time Network Status
- Immediately Remediate Threats

Manage Your Security from a Single Screen

- Simple Web UI
- Threat Prevention Managed Automatically

MARKET LEADERSHIP

Large Scale Distributed Management

According to Gartner:

- The **Check Point** management console is consistently ranked highest by customers…and it remains the de facto "gold standard" against which other consoles are measured.
- Management capability compared with the competition was often the reason why **Fortinet** was shortlisted by, but not selected in enterprises.
- Panorama (**Palo Alto Networks**) scores well in selections seen by Gartner, except for Check Point.

Third Party Tests

- Only vendor to get 17th consecutive NSS Labs Security Value Map "Recommended" rating since 2011 in FW, NGFW, IPS, BDS
- NSS LABS best management Labor TCO for NGFW and NGIPS

Gartner Magic Quadrants

Named a leader for:

- Enterprise Network Firewalls Since 1997
- Unified Threat Management 7 years in a row

SALES RESOURCES

- Branch Office (1600,1800) Page
- SMB Quantum Spark Page
- Appliance Comparison Chart

- Customer Presentation (PartnerMap)
- Spark Content Page (PartnerMap)

CHECK POINT

Comparison Matrix	CHECK POINT		paloalto NETWORKS		FORTINET		CISCO Meraki	
	1555W Pro	**1595W Pro**	**PA-410**	**PA-440**	**FW-40F**	**FW-81F***	**MX67W**	**MX-95**
Threat Prevention Performance (Mbps)[1]	600	900	685	1000	600	900	300	1000
Interface 1GbE	5	8	8	8	4	8	4	4
Wifi (MIMO) / LTE Models	3x3 WiFi 6	4x4 WiFi 6	None		3x3	3x3 + LTE	2x2	No
Application control	~10,200 Apps		~4,000 Apps		~4,400 Apps		~500 Apps	
Cloud MGMT & Zero Touch Deployment	Included		N/A & Add'l Costs[1]		Included		Included	
HW + Sup + SNBT 1-year price	$1,697	$4,703	$1,140[2]	$1,960[2]	$1,330[3]	$4,369[3]	$2,095	$11,393
HW + Sup + SNBT 3-year price	$3,351	$9,285	$1,725[2]	$2,965[2]	$2,370[3]	$7,782[3]	$2,920	$16,893
	1600	**1800**	**PA-450**	**PA-460**	**FG-100F**	**FG-200F**	**MX-105**	**MX-250**
Threat Prevention Performance (Mbps)[1]	2000	2600	1600	2400	1000	3000	1500	2000
Interface 1GbE	18		8	8	18	24	4	16
Interface 10G	No	1	None		2	4	2	10
Application control	~10,200 Apps		~4000 Apps		~4400 Apps		~500 Apps	
Cloud MGMT & Zero Touch Deployment	Included		N/A & Add'l Costs[1]		Included		Included	
HW + Sup + SNBT 1-year price	$5,545	$7,300	$4,580[2]	$6,940[2]	$5,444[3]	$11,179[3]	$17,092	$24,090
HW + Sup + SNBT 3-years price	$10,945	$14,410	$6,920[2]	$10,480[2]	$9,697[3]	$21,452[3]	$25,342	$35,090

*FortiWifi-40F, FortiWIFI-81F-2R-3G4G-DSL
1) PAN lacks cloud MGMT, ZTP requires Panorama = additional Cost
2) Price includes HW + support + PRO bundle
3) Price includes HW + FortiCare Premium and FortiGuard Enterprise

Competitive Benefits of Check Point Quantum Spark

CHECK POINT

A. **Prevention, not just detection** – can prevent patient zero
B. **Best security track record** – Highest security effectiveness score in NSS
C. **Easy Deployment** – Full Protection in 60 Seconds
D. **Application control granularity – over 10,200 applications**
E. **Integrated Wi-Fi 6 and 5G Support** (1595 PRO model).

How to Compete Against…

paloalto NETWORKS

A. **Significant performance degradation with features enabled** - Activating NAT and Logging show additional ~20-30% performance degradation
B. **Skips inspecting for threats and forwards traffic inside the network** – By Default, when a certain queue fills during high load. Watch Here
C. **No integrated Wifi/LTE appliance**
D. **Lacks cloud based managment**
E. **High Limited application visibility & control** – Only ~4,000 apps

FORTINET

A. **Additional hardware required for LTE support**
B. **IPS Skipping** – "Intelligent mode" **only scans first 200KB** of stream
C. **Up to 90% degradation using full UTM security** – Fortigates have high throughput in FW but using threat prevention slows them down considerably
D. **No real time 0-day prevention** – Fortinet sandboxing solution can't block threats in real time, hence **it can't prevent patient-zero**

CISCO Meraki

A. **Nearly 2-3 times the price for similar performing appliance compared to rest of market**
B. **Sacrifices security to gain better performance** – Default IPS configuration creates security holes by performing IPS skipping
C. **Lack of Unified Console** for Efficient Management
D. Cisco appliances affected by endless severe vulnerabilities – Read more
E. **No real time 0-day prevention** – Cisco sandboxing solution can't block threats in real time, hence **it can't prevent patient-zero**
F. **Meraki has a very limited policy granularity** on user/group security policies

CHECK POINT

Comparison Matrix	CHECK POINT		SOPHOS		SONICWALL		WatchGuard	
	1555W Pro	**1595W Pro**	**XGS 107W**	**XGS 116W**	**TZ270W**	**TZ370W**	**Firebox T25W**	**Firebox T45W**
Threat Prevention Performance (Mbps)[1]	600	900	370	720	750[1]	1000[1]	216	301
Interface 1GbE	5	8	8	8	4	8	5	5
Wifi (MIMO) / LTE Models	3x3 WiFi 6	4x4 WiFi 6	2 x 2:2 Wi-Fi 5	2 x 2:2 Wi-Fi 5	2x2 Wave 2	2x2 Wave 2	Wi-Fi 6[3]	Wi-Fi 6
Application control	~10,200 Apps		~3,400 Apps		~3,530 Apps		~1300 Apps	
Cloud MGMT & Zero Touch Deployment	Included		Included		Included		Included	
HW + Sup + SNBT 1-year price	$1,697	$4,703	$1,367	$1,935	$1,040[2]	$1,470[2]	$1,125	$2,125
HW + Sup + SNBT 3-year price	$3,351	$9,285	$2,451	$3,755	$1,825[2]	$2,740[2]	$2,055	$3,880

Comparison Matrix	CHECK POINT		SOPHOS		SONICWALL		WatchGuard	
	1600	**1800**	**XGS 136W**	**XGS 2100**	**TZ470W**	**TZ570W**	**Firebox T85**	**Firebox M290**
Threat Prevention Performance (Mbps)	2000	2600	1000	1250	1500[1]	2000[1]	576	696
Interface 1GbE	18		8	8	18	24	8	8
Interface 10G	No	1	N/A	4	2	4	-	-
Application control	~10,200 Apps		~3,400 Apps		~3500 Apps		~1300 Apps	
Cloud MGMT & Zero Touch Deployment	Included		Included		Included		Included	
HW + Sup + SNBT 1-year price	$5,545	$7,300	$3,852	$6,197	$2,215[2]	$3,025[2]	$3,760	$3,020
HW + Sup + SNBT 3-years price	$10,945	$14,410	$7,867	$13,636	$3,960[2]	$5,445[2]	$6,865	$5,500

1) No URL filtering
2) Threat Protection Service Suite (TPSS) – with additional cost.
3) Optional integrated Wi-Fi 6 wireless module.

Competitive Benefits of Check Point Quantum Spark

CHECK POINT

A. **Prevention, not just detection** – can prevent patient zero
B. **Best security track record** – Highest security effectiveness score in NSS
C. **Easy Deployment** – Full Protection in 60 Seconds
D. **Application control granularity** – over 10,200 applications
E. **Integrated Wi-Fi 6 and 5G Support** (1595 PRO model).

How to Compete Against...

SOPHOS

A. **Sophos relies solely on reputation to recognize known threats**, whereas **Check Point** ML/AI proactively protects **both known and unknown threats.**
B. **Sophos IPS can be easily bypassed. By default, Sophos inspects only the first 8 packets, the 9th packet and onwards are left unscanned. Sophos is prone to blocking legitimate traffic,** as indicated by **VirusTotal** where it ranks **high in terms of false positives.**
C. **Sophos lacks a mobile application to manage and monitor SMB firewalls.**
D. **Limited application visibility & control** – Only ~**3,500** apps

SONICWALL

A. **SonicWall** only provides support for the older **WiFi 5** standard, **whereas Check Point is the pioneer among security vendors, offering WiFi 6 support for SMB appliances in the Pro Series,** resulting in enhanced bandwidth.
B. **SonicWall** has **restricted URL Filtering capabilities,** while Check Point surpasses it by **supporting 115 categories compared to SonicWall's 57.**
C. **SonicWall's Sandbox is limited to supporting only 20 file types, while Check Point,** specifically with X3.5, **accommodates over 70 file types.**

WatchGuard

A. **The performance of the WatchGuard Firebox series is subpar**
B. Insufficient and very basic reporting
C. WatchGuard IPS engine scans only a portion of the session by default, exposing the network to potential threats. When set up to comprehensively safeguard the traffic, it results in over a 60% performance decline.
D. Reporting is both **inadequate** and overly **basic**.
E. The absence of pre-configured security policies adds complexity to security setup.

CHECK POINT™

TARGET AUDIENCE AND QUESTIONS TO ASK

CIO or CISO	DIRECTOR of IT / INFOSEC	SECURITY MANAGERS
Would you consider a single, Advanced Threat Prevention security solution from the world's most trusted security vendor if you could significantly reduce your IT administration tasks?	How do you protect against unknown malware or zero-day attacks?	When you test Advanced Threat Prevention throughput, do you test it with NAT, Logging, real world rule base and a representative traffic blend?
What level of application and threat visibility do you have across your organization?	If you have multiple sites, are you able to centrally manage your firewalls?	How much time in the day do you dedicate to monitor and maintain your current firewall security solution?
How prepared is your organization for malware, APTs, zero-day threats and application and user awareness?	How much encrypted traffic does your network support now and will it need to support in the future?	How does your current Advanced Threat Prevention solution handle advanced evasion techniques?

OBJECTION HANDLING

Other vendors have an easy-to-use Web-based UI management platform.	Check Point Quantum Spark gateways are setup in less than five minutes. The gateway comes preconfigured out of the box leaving only minimal configuration work. Quantum Spark also provides zero touch capability where a partner can mass provision multiple devices before they are installed at the end customers.
Check Point is only a firewall company. PAN claims they are the leaders in network security & you are an old technology.	This is not the opinion of security analysts: Gartner publishes their annual NGFW Magic Quadrant and Check Point has been in the leader's quadrant for over 10 years. In addition, NSS ranks Check Point at the top of their tests for FW, IPS & Application Control. We have over 20 years of security innovation.
Check Point is too expensive.	If you compare similar capabilities of the 1500 Appliances to other competing products Check Point is in most cases less expensive and offers considerably better security effectiveness.

SUMMARY – ENSURING THE WIN

Small businesses and branch offices need the same protections from sophisticated cyber attacks and zero-day threats as main corporate offices. The Check Point 1500/1600/1800 appliances are ideal for small and branch office deployments, delivering all-in-one advanced threat prevention, flexible network connectivity, and maximum port density — all in a compact, high-performance desktop form factor.

TOP POSITIONING TIPS FROM THE FIELD

1. Highlight the ability to enable the most advanced threat prevention security available for Check Point' large enterprises firewalls on an SMB firewall;
2. Highlight the ability to turn on all advanced security features without compromising performance.
3. Emphasize the ease of management; the 1500 Appliances are designed to be easy to deploy and use — even for non-technical staff.
   MSPs and partners can be managed multiple devices via from cloud-based management portal (SMP).
4. Branch deployments can also be centrally managed with Check Point enterprise security management or Multi-Domain Management products, enabling organizations to define a consistent security policy and device profile for thousands of 1500 appliances.