Check Point vs. Symantec (Broadcom) Battle Card

About Symantec:

(1982-2019)

Enterprise Security division was acquired by Broadcom in 2019.

Consumer division rebranded as NortonLifeLock Inc

Sold business security service division to Accenture.

Symantec
A Division of Broadcom

ENDPOINT SECURITY
- Endpoint Security Complete (includes mobile endpoints)
- Threat Hunting Center
- Managed EDR
- Endpoint Management

WEB & EMAIL SECURITY
- Secure Web Gateway
- Web Isolation
- Email & Email.Cloud
- Content Analysis with Sandboxing
- Security Analytics/SSLV

INFORMATION SECURITY
- Data Loss Prevention
- CloudSOC CASB
- Secure Access Cloud

IDENTITY SECURITY
- Authentication
- Access Management
- Privileged Access Management
- Identity Management

Approaching Symantec Customers

Uncertainty
After Broadcom acquisition, **Symantec has negatively changed**. The future of which products and customers they will continue to support is currently unclear

The struggle is real
Symantec is struggling to renew contracts with customers in all of their offerings, including SWG, Content Analysis, Cloud&CASB, Endpoint and Mobile

Symantec's current offerings
Given the high customer abandon rate, Symantec are currently offering some of their products (such as SEP), with a default discount of 70%. Don't be misled with the pricing on expense of unstable security

Not everyone is equal
Only Symantec's highly-rated customers are currently being supported, leaving thousands of customer in doubt with unanswered tickets, in addition to End-of-support and End-of-sale notices for some of their products

The Check Point Alternative
Every Symantec customer is an opportunity for Check Point. Check Point is the market leading vendor in security, with **a long time track record** amongst the security market, with a broad security portfolio that allows you **to replace any existing Symantec products,** with a better preventive security approach and a more cost effective alternative

Industry	Check Point *INFINITY* Architecture		Check Point SOFTWARE TECHNOLOGIES LTD.	Symantec		
NGFW/SWG	SandBlast	NGTP	Firewall	✗	SWG	ProxySG (BlueCoat)
			Application Control & URLF	Application Control & URLF		
			IPS	✗		
Sandbox			Anti-bot	✗		
			Anti Virus	Anti Malware	Content Analysis	
		SandBlast	Threat Emulation	Sandbox		
CDR			Threat Extraction	✗		
DLP	DLP		DLP	DLP	DLP	
CSPM	CloudGuard		Dome9 & Log.ic	Workload Assurance	Cloud / Server Security	
CWPP			Workload	Workload Protection		
CASB			SaaS	CloudSOC CASB (Elastica)		
vGW			IaaS	✗		
FWaaS			Connect & Edge	WSS Web Security Services		
Endpoint & Mobile Security	Mobility & Endpoint		SandBlast Agent	SEP Endpoint Protection	SEP	
			SandBlast Mobile	SEP Mobile (Skycure)		

Top Competitive Differentiators

	Check Point	Symantec
Endpoint Security		
A Leading Endpoint security solution named by 3rd party analysis SandBlast Agent received the highest security block rate by NSS AEP 2020 test	✓	✗
Cost effective Endpoint security SandBlast Agent 3 year TCO (2500 user price) is 60% less than Symantec Endpoint solution	$15.7 U/Y SBA Adv.	$50 U/Y EPP + EDR
Autonomous EDR and Threat Remediation SandBlast Agent automatically analyzes, reports and remediates the full attack chain of the threat	✓	Manual EDR & Remediation
A complete Endpoint Security solution in a single product subscription While Symantec's requires additional subscriptions, SandBlast Agent protects from all attack vectors	SBA Complete	SEP + EDR + Encryption
Industry-leading automated Forensics reports While Symantec requires manual EDR investigation, SandBlast Agent produces intuitive fully-detailed Incident reports automatically with simple IoC search, saving time and costs of analysts	✓ Automated	✗ Manual
Threat Prevention / SWG		
Business continuity by delivering instant clean documents while analyzing new files SandBlast Threat Extraction sanitizes documents from any potential risk both in mail and web, allowing quick access to risk-free documents (while keeping original)	Built in for Web and Mail	3rd Party Solution
Supports HTTP/2 protocol Check Point support of HTTP/2 allows efficient communication and higher security in modern web	✓	✗
Support both in-line and proxy traffic flow modes SandBlast can be configured as proxy, NGFW or both at the same time, ProxySG is only a proxy	Flow / Proxy / Hybrid	Proxy
Clustering and failover Easily handle High Availability deployments, while ProxySG causes redundancy issues in HA deployment	Easy	Complicated
Pay as you grow – replace your legacy Secure Web Gateway Maestro Hyperscale can grow as performance requirement grows	✓	✗
Dynamic appliance configuration for flexible network / cloud deployments (available as IaaS) Integrated Sandboxing, IPS, Firewall, Anti-bot, Anti Malware and URL Filtering	✓	SWG Only (URLF/DLP/APCL)
Mobile Security		
Reliable solution with a low false positive rate SandBlast Mobile blocks malicious networks accurately, while SEP Mobile reports every captive network (such as hotels) as a false positive, leading to disruption of business and admin overhead	✓ Minimal	✗ High F/P
Ease of deployment: Install Mobile Threat Defense via MDM with minimal user interaction SandBlast Mobile allows deployment via leading MDMs requires minimal user action for protection	Minimal	Manual
Protecting data from C&C Communication SandBlast Mobile On-Device Network Protection prevents remote C&C and data exfiltration	✓	Requires WSS (Separated)
A Leading Mobile security solution named by 3rd party analysis SandBlast Mobile for the highest security score by Miercom 2019	Top Solution	4th
The solution is stable and will continue to be supported Symantec is currently not focusing on mobile security at all, and their solution might be dropped in the short term – Read More	✓	✗ Uncertain

SandBlast Agent & Mobile – Symantec equivalent

Endpoint	Sub-Category	SBA Complete	SBA Advanced	SBA Basic	SEP	SEP EDR	SEP Encryption
Endpoint Protection (EPP)	Ransomware Rollback	✓	✓	✓	✗	✗	✗
	Anti-bot (blocking C&C connections)	✓	✓	✓	WSS	✗	✗
	Exploit prevention	✓	✓	✓	✓	✗	✗
	Unknown malware (Behaviour Guard / AI)	✓	✓	✓	✓	✗	✗
Endpoint Forensics & Mitigation (EDR)	Automated incident analysis	✓	✓	✓	✗	✓	✗
	Malware Entry Point	✓	✓	✓	✗	✓	✗
	Auto-remediation	✓	✓	✓	✗	✗	✗
	Search for IoC	✓	✓	✓	✓	✓	✗
	MITRE ATT&CK Integration	✓	✓	✓	✗	✓	✗
	Attack chain sterilization (only relevant info)	✓	✓	✓	✗	✗	✗
Endpoint Encryption & Control	At-Rest (FDE / Media)	✓	✗	✗	✗	✗	✓
	In-Motion (VPN)	✓	✓	✓	✓	✗	✗
	Port Control	✓	✓	✓	✓	✗	✗
	Application Control	✓	✓	✓	✓	✗	✗
	Endpoint Firewall	✓	✓	✓	✓	✗	✗
	Endpoint Compliance	✓	✓	✓	✓	✗	✗
	Category-Based URL Filtering	✓	✓	✓	WSS	✗	✗
Prevention	Threat Emulation (Sandboxing)	✓	✓	✗	✗	✓	✗
	Threat Extraction	✓	✓	✗	✗	✗	✗
	Zero-Day Phishing Protection	✓	✓	✓	✗	✗	✗
	Anti-Exploit	✓	✓	✓	✓	✗	✗
	Browser Extension	✓	✓	✓	✗	✗	✗
	Threat Intelligence	✓	✓	✓	✓	✓	✗
Management	Cloud	✓	✓	✓	✓	✓	✓
	On-Prem	✓	✓	✓	✓	✓	✓
Solution Price	Price Per user + Support (1 / 3 Year)	$55 / $165	$35 / $105	$20 / $60	$33 / $80	$67 / $159	$40 / $147
Total Price - Price Per user + Support (1 / 3 Year)		$55 / $165	$35 / $105	$20 / $60	$140 / $386		

Mobile	Sub-Category	SandBlast Mobile	SEP Mobile (Skycure)
Network Attack Vector	Malware download prevention	✓	✗
	Anti-bot (blocking C&C connections)	✓	✗
	Zero-day anti-phishing	✓	✗
	Network detection (MiTM)	✓	Yes -High False Positive
Device Risk Detection & Control	URL Filtering	✓	WSS (separate cloud solution)
	Conditional corporate resource access	✓	✓
	Risk Assessment (Vulnerability, OS, Network, Profile)	✓	✓
	Block Unknown malware	✓	✗
Integration and Threat Intelligence	MDM flexible MTD deployment	Simple & Rapid	Cumbersome
	Threat Cloud	Network, endpoint & mobile	Mobile only
Total Price - Price Per user + Support (1 / 3 Year)		$48 / $144	$57 / $172

Top Competitive Differentiators

Check Point SOFTWARE TECHNOLOGIES LTD. | Symantec

		Check Point	Symantec
Cloud Security	**Cloud security posture visualization** Dome9 & Log.ic provide at a glance views of cloud security posture & exposure	Visualized	Text-Based
	Cloud traffic & user security events remediation Auto remediation can take actions based on Log.ic context event	✓	✗
	Out-of-the-box cloud compliance and governance polices CloudGuard Dome9 gives the best coverage for compliance standards	20+	5
	Protocol and port coverage in cloud-delivered security services CloudGuard Connect supports all traffic and not just web traffic (such as Symantec WSS)	Full Traffic	Only Web
	Content Disarm & Reconstruction is integrated within the O365 security solution Symantec CloudSoC requires also their Email Gateway for enforcement, and still lacks CDR	✓	✗
	Preventing account takeover in SaaS Applications CloudGuard SaaS prevents account takeover, blocking sophisticated multilayer phishing attacks	✓	✗
Management & License	**Pricing and licensing model – the hidden costs** Check Point allows you to subscribe to the tailored security you need, without charging for every add-on	✓	Many add-ons
	Network and endpoint event analysis Correlating network & endpoint logs, allowing cross-organization IoC search and detailed forensics	✓	✗
	Consolidated cloud security management with Infinity Portal Infinity Portal allows management of all of Check Point's cloud solutions in a single portal	✓	✗
	Same management server for network and endpoint with centralized logging Both management policies and logs write to the same management console in a unified format	R80 MGMT	SEP + WSS

"How to replace Symantec" / Objection Handling

Endpoint

Claim: "We are comfortable with Symantec Endpoint Protection and we do not see the need of a new solution"

Response: **SandBlast Agent replaces all of Symantec Endpoint Protection components for a lower cost, and has a more certain future as a product and company. You can follow the AV replacement guide for more details on the replacement process**

SWG

Claim: "We already use BlueCoat/ProxySG services and it provides the security we need for our perimeter"

Response: **SandBlast appliances provide world-class scalable prevention solution, managed by the leading R80 MGMT**

WSS

Claim: "Symantec Web Services help us secure roaming/mobile users"

Response: **WSS only protects web traffic. With CloudGuard Connect, you can secure roaming users from all threat, and not just the web. If web security for roaming users is what you need, SandBlast Web is your way to go.**

Mobile

Claim: "We use SEP Mobile to secure the mobile devices of the company, both BYOD and fully managed devices"

Response: **With SandBlast Mobile, not only you provide better protection to mobile devices, but also provide enhanced filtering capabilities, corporate resource protection, zero-day anti phishing and an easier solution to deploy and manage.**

Competitive Assets

Winning against Symantec | SEP Cheatsheet | SEP 14.2 elevation of privileges vulnerability | SEP Mobile Cheatsheet