



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

**CLOUD • MOBILE  
THREAT PREVENTION**

**WELCOME TO THE FUTURE  
OF CYBER SECURITY**



# Welcome to The Future of Cyber Security

The future is here, today. Everything is interconnected, generating more business opportunities and almost infinite possibilities. However, this also creates more opportunities for cyber criminals to exploit this hyperconnected world for their own purposes.

Every vector is a potential target: **enterprise networks, cloud, and mobile.**

Our next-generation networks need protecting against the ever-growing threat of sophisticated, known and unknown cyber attacks: we can no longer afford to be exposed.

But deploying security which is based on detection is costly and inefficient, because it allows attackers to get into the network and cause damage before remediation is done. The connectivity between separate IT environments often drives businesses to apply different solutions to protect each of these environments separately. This complicates security operations, and creates inherent gaps in security posture. Enterprises need a complete architecture that scales with dynamic business demands, and focuses on prevention to ensure all IT environments are completely protected.

## **Check Point Infinity is the Cyber Security architecture of the future.**

It is the first consolidated security architecture to provide pre-emptive threat prevention across networks, cloud and mobile. This future-state architecture provides unified threat intelligence, open interfaces and single-console management to pre-emptively block even the most sophisticated attacks, across all environments.



# Check Point Infinity: The Future of Cyber Security



## The Future of Cyber Security:

- The first consolidated security across networks, cloud and mobile, providing the highest level of threat prevention.
- One security platform – leveraging unified threat intelligence and open interfaces.
- Pre-emptive threat prevention – blocking the most sophisticated attacks before they happen.
- One consolidated system including single-console management with modular policy and integrated threat visibility.

Check Point Infinity is the only fully unified cyber security architecture that future-proofs your business and IT infrastructure across all networks, cloud and mobile.

The architecture resolves the complexities of growing connectivity and inefficient security based on individual, point solutions. Check Point's threat prevention strategy blocks the most sophisticated attacks before they occur.

It provides complete threat prevention which seals security gaps, enables automatic, immediate threat intelligence sharing across all security environments, and a consolidated security management for efficient security operations. Check Point Infinity delivers unprecedented protection against known and unknown attacks – now and in the future.

## Unified security across all networks, cloud and mobile

Check Point Infinity leverages unified threat intelligence and open interfaces to block attacks on all platforms before they can infiltrate the network. The interconnectivity between all Check Point's components delivers consistent security through advanced threat prevention, data protections, web security and more, across all enterprise networks, in the cloud and on mobile devices.

## Pre-emptive cyber security

Check Point continually creates new cyber security protections with a multi-layered set of capabilities, to pre-emptively protect against the most sophisticated known and unknown threats. This approach prevents cyber attacks from penetrating the network, saving time and the costs associated with remediating the damages.

Check Point's advanced set of protections, led by the SandBlast product family, blocks both known and zero-day, unknown threats. With over 30 different innovative technologies, the SandBlast family of solutions adds additional prevention capabilities across all environments: on the network, on users' endpoints, on mobile devices, and in the cloud.

## Consolidated security management

The entire security network is unified and efficiently managed through a single console, based on modular policy management and rich integrations with 3rd party solutions through flexible APIs. This consolidation brings all security protections and functions under one umbrella, with a unified policy for users, data, applications and networks that introduces unparalleled granular control and consistent security.

Check Point Infinity unifies your entire IT security architecture, providing real-time shared threat intelligence and pre-emptive protection—all managed by a single, consolidated console. It future-proofs your business and ensures business continuity.



Scan me to  
view website

# The Future of Threat Prevention: Check Point SandBlast

## The Future of Cyber Security:

- CPU-level analysis and OS-level sandboxing – in one integrated solution.
- The industry's highest catch rate for malware, giving you ultimate protection.
- Accelerated delivery of safe content to your employees.
- Exploits detected and neutralised before they occur.



Scan me to view website

Malware and ransomware is increasingly sophisticated, evasive and disruptive. In 2016, 53% of enterprise gateways downloaded unknown malware; and 36% of organisations were impacted by ransomware. Conventional antivirus tools are no longer enough to protect against this barrage of attacks.

Check Point SandBlast is the most comprehensive zero-day threat prevention suite, protecting networks, clouds, endpoints and mobile devices. The suite of technologies ensures immediate and safe delivery of content to your users whilst preventing advanced cyber attacks.



SandBlast detects malware before it can even infect your network, stopping the most dangerous exploits, zero-day and targeted attacks from harming your network. Unlike point technologies such as O/S Level only sandboxes or machine learning engines, SandBlast utilises over 28 different engines to detect every form of malware; from the simplest to the most advanced and evasive attacks.

### SandBlast Suite of Technologies:

**Threat Extraction:** providing end users with real-time access to documents and images whilst preventing embedded malicious payloads from detonating

**Zero Phishing:** protecting the end user web experience by ensuring that corporate credentials are not leaked to phishing sites in a transparent manner

**Anti-Bot:** preventing malware from spreading laterally or calling home

**Threat Emulation:** immediately preventing unknown, evasive or zero-day malware from entering the business

**Forensics:** providing automated analysis and visualisation within minutes of an attempted attack

**Anti-Ransomware:** automatically kills ransomware processes in seconds and restores any encrypted files to their original state without the loss of data

The Sandblast suite of technologies is deployed using a flexible architecture that protects the network perimeter, end points, cloud environments and custom applications. All threat protection is managed from a single pane of glass for maximum visibility and sharing of intelligence across your business.



# The Future of Mobile Security: SandBlast Mobile

## The Future of Cyber Security:

- The industry's highest mobile threat catch rate – for both iOS and Android.
- Advanced threat protection on mobile devices, in applications and in your network.
- Real-time threat intelligence and visibility.
- End-user privacy is protected, with files and browser histories kept private.



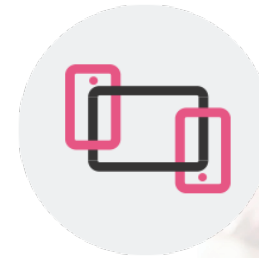
Scan me to view website

The latest extension of the SandBlast family of advanced threat prevention solutions, SandBlast Mobile is the market's leading mobile threat defense solution, providing protection against advanced mobile threats to more than 900 businesses worldwide, an 800% growth in customer deployments year over year.

SandBlast Mobile detects and mitigates mobile threats before they start, on both iOS and Android devices. Whether your data's at rest on a device or in the cloud, SandBlast Mobile protection is from advanced mobile cyber-attacks. It provides a complete mobile security solution that protects devices from threats on the device (OS), in apps, in the network, and in SMS messages, delivering the industry's highest threat catch rate for iOS and Android.

Only SandBlast Mobile provides a complete mobile security solution that protects employees' devices from: malware attacks via infected apps, Man-in-the-Middle attacks on compromised Wi-Fi networks and hotspot logins, exploitation of operating systems for rooting and jailbreaking, malicious links sent on SMS messages, and cellular-based attacks ('SS7').

SandBlast Mobile uses malicious app detection to find known and unknown threats by applying threat emulation, advanced static code analysis, app reputation, and machine learning. Its dynamic threat response prevents compromised devices from accessing your organisation's network, while allowing your business to set adaptive policy controls. Check Point SandBlast Mobile protects your organisation from the next security breach: mobile devices.



# Complete protection for public and private clouds: Check Point vSEC

## The Future of Cyber Security:

- The most advanced protection for modern data centres.
- Consistently manage and enforce security across virtual and physical environments.
- vSEC products provide integrated security and expertise to help you build your cloud infrastructure today and protect your future deployments.
- Protection designed for the scale and elasticity of private cloud data centres.

Check Point vSEC Cloud Security integrates with the largest number of private and public cloud platforms such as Amazon Web Services, Microsoft Azure and Google Cloud, ensuring cloud environments are instantly and easily protected against even the most sophisticated malware and zero-day attacks. **Check Point Cloud Security protects any cloud and any service, anywhere.**

### SDN and private clouds

Network virtualisation has created a shift in traffic behavior, as more and more traffic goes East-West in the data centre creating new security challenges. With few controls to secure this east-west traffic, threats can travel unimpeded once inside the data centre.

Check Point vSEC seamlessly delivers advanced threat protections to prevent threats spreading laterally within software-defined data centres, as well as the visibility and control to effectively manage security in both physical and virtual environments – all from a single unified management solution. It seamlessly supports Cisco ACI, VMware NSX and OpenStack.

### Public cloud protection

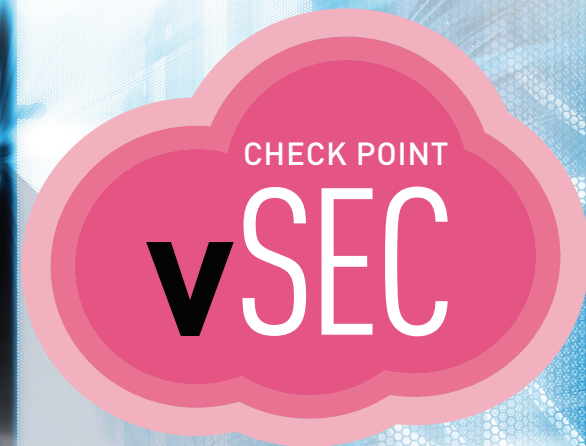
While infrastructure protection is delivered by the public cloud provider, businesses still want the ability to control their own data and keep it private, while maintaining compliance with regulatory mandates. Check Point vSEC enables reliable connectivity to public cloud assets while protecting applications and data with advanced threat prevention across public and hybrid cloud environments. vSEC supports Amazon Web Services, Google Cloud, Microsoft Azure, and VMware vCloud Air.

### Data centre virtualisation and NFV

Check Point vSEC delivers advanced, multi-layered security for virtual data centre and Network Function Virtualisation (NFV) environments and is designed to equip service providers with comprehensive threat prevention security, zero-day protection, agile delivery, management, and automation across core network function, software-defined WAN and vCPE deployments.



Scan me to  
view website



# The Future of Incident Response – Today



## The Future of Cyber Security:

- Lightning fast, 24/7 response to any security incident.
- Information capture and analysis so the attack is fully understood and responded to appropriately.
- Return to business as usual quickly and in confidence.
- Mitigate future risk with post-incident advisement.

Even with the most advanced cyber security, it's dangerous to assume that your organisation will never fall victim to a cyber attack.

**So what will you do if the worst should happen? If you fail to plan for this, you're planning for failure.**

From distributed-denial-of-service (DDoS) attacks that simply aim to clog and shut down your systems, to highly sophisticated data thefts incorporating social engineering and other exploits, the range of security incidents your organisation could be subject to is huge. But the same incident response principles apply every time.

Check Point's Incident Response services deliver a comprehensive, lightning-fast response to any security incident.

Our dedicated infosecurity experts are on hand 24/7, ready to deploy real-time log capture and data analysis to understand exactly what has happened – and may still be happening. We identify and counteract botnets, mitigate DDoS attacks, and neutralise malware, virus and data loss incidents. Our aim, always, is to minimise any damage and disruption, and get you back to normal operations as quickly as possible.

Suffering one cyber attack is unlucky, but suffering the same kind of attack later is careless. Intelligent incident response is also about analysing and learning from what has happened, and putting measures in place to ensure it can't happen again. In the incident's aftermath, we will help you apply the latest industry best practice to strengthen your security controls.

Our Incident Response portal offers everything you need to prepare for and respond to a security attack, and also allows you to view actionable attack remediation data so you are always on the front foot – giving you the future of incident response today, when you need it most.



**Scan me to view website**



**Are you under attack?**

0800-088-5471  
emergency-response@checkpoint.com



# Facts at a glance

Check Point Software Technologies Ltd., the largest pure-play security vendor globally, provides industry-leading solutions, and protects customers from cyber attacks with an unmatched catch rate of malware and other types of attacks. Check Point offers a complete security architecture defending enterprises' networks to mobile devices, in addition to the most comprehensive and intuitive security management. Check Point first pioneered the industry with FireWall-1 and its patented stateful inspection technology.

## Company

Check Point Software Technologies Ltd.

## Stock Ticker Symbol

NASDAQ: CHKP

## Founded

1993

## Mission

Check Point Software Technologies is the worldwide leader in securing the Internet. Making Internet communications and critical data secure, reliable and available everywhere has been and continues to be our ongoing vision. We are committed to staying focused on real customer needs and to developing new and innovative security solutions that redefine the security landscape.

## U.S. Headquarters

San Carlos, California

## International Headquarters

Tel Aviv, Israel

## Employees

Approximately 4,300

## Market Leadership

- A leader in Gartner's "Enterprise Network Firewall Magic Quadrant" (1999-2002, 2004-2016)
- A leader in Gartner's "Mobile Data Protection Magic Quadrant" (2001-2015)
- A leader in Gartner's "Unified Threat Management (UTM) Magic Quadrant" (2010-2016)
- Market share leader in worldwide combined Firewall and UTM appliance revenue (IIDC FY 2015 Security Appliance Tracker)
- NSS Labs "Recommend" Rating for Breach Detection Systems (BDS) (NSS Labs 2015-2016)
- NSS Labs "Recommend" Rating for Next Generation Firewall (NSS Labs 2011 - 2016)
- NSS Labs "Recommend" Rating for Network Firewall (NSS Labs 2011, 2013)
- NSS Labs "Recommend" Rating for IPS (NSS Labs 2011 - 2013)

## Patents

Check Point's products contain the world's most advanced security technology. The Company currently holds 70 United States patents, more than 60 U.S. patents pending, and additional patents issued and patent applications pending worldwide.

## Our Customers

Check Point's products and services are sold to enterprises, service providers, small- and medium-sized businesses and consumers. We secure more than 100,000 businesses and millions of users worldwide.

## Awards / Industry Honours

As an industry leader, Check Point has received recognition from around the globe.

## Acquisition Highlights

- April 2015: **Lacoon Mobile Security**
- February 2015: **Hyperwise CPU-Level Threat Prevention**
- October 2011: **Dynasec**
- June 2010: **Liquid Machines**
- December 2009: **FaceTime Communications' application database**
- March 2009: **Nokia Security Appliance Business**
- January 2007: **Protect Data**
- January 2007: **NFR Security**
- March 2004: **Zone Alarm**

## Distribution

**Check Point products are distributed worldwide via:**

- Distributors, OEMs, Resellers, OPSEC Partners, MSPs
- Check Point solutions are sold, integrated and serviced by a network of thousands of certified partners

Check Point headquarters are located internationally in Tel Aviv, Israel, and in the United States in San Carlos, California. The Company has offices in the U.S. in Alabama, Arizona, Northern and Southern California, Colorado, Florida, Georgia, Illinois, Massachusetts, Michigan, Minnesota, New York, New Jersey, Ohio, Pennsylvania, Texas, Virginia, Washington and Wisconsin; as well as in Canada, in the Ontario area.

The Company also has international subsidiaries located in Austria, Belarus, Belgium, Czech Republic, Denmark, Finland, France, Germany, Greece, Hungary, Italy, the Netherlands, Norway, Poland, Portugal, Romania, Russia, Spain, Sweden, Switzerland, Turkey, the United Kingdom, Australia, New Zealand, India, Japan, Hong Kong, P.R. China, Philippines, Singapore, South Korea, Taiwan, Thailand, Argentina, Brazil, Colombia, Mexico and Canada.





# 2016

## SECURITY REPORT

DOWNLOAD HERE:



Expose potential  
risks by  
scheduling a

**SECURITY CHECKUP**



**SIGN UP FOR A FREE Security Checkup TODAY**

### FOLLOW US



@check\_point\_uk



+checkpoint



Check Point Software Technologies



CPGlobal



checkpoint.com/rss



Check Point Software Technologies



blog.checkpoint.com

### CONTACT US



0207 628 4211



uksales@checkpoint.com



checkpoint.com

