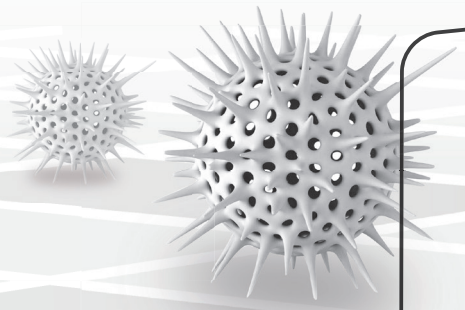
SECURITY CHECKUP

THREAT ANALYSIS REPORT

Prepared for:	ABC Corp.
Prepared by:	Check Point Solution Center
Date:	January 20, 2014
Document Version:	2.0



Check Point
SOFTWARE TECHNOLOGIES LTD.
We Secure the Internet.

TABLE OF CONTENTS

EXECUTIVE SUMMARY

This document provides the findings of a recent security analysis of your infrastructure. The document represents a summary of these findings and presents a set of recommendations for addressing the detected events.

The analysis is based on data collected using the characteristics below:

Security Analysis Date:	12/01/2014	**Analysis duration:**	2 weeks
Industry:	Insurance	**Country**	USA
Company size:	2,500 Employees	**Network analyzed:**	Internal LAN
Security Gateway version:	R77	**Analysis mode:**	Mirror Port
Security Gateway Software Blades:	Application Control, URL Filtering, Anti-Bot, Anti-Virus, IPS, DLP, Identity Awareness , Threat Emulation, Compliance		
Security device:	Check Point 4800 Security Gateway		

The following is a summary of the main high and critical risk security events detected:

ACCESS CONTROL & DATA PROTECTION

30,670	High risk application events
22	Data loss events

THREAT PREVENTION

9	Bot events
5	Virus events
16	Advanced threats events
18	Intrusions & attack events

ENDPOINT

893	Endpoints involved in high risk events

COMPLIANCE

65%	Compliant with Check Point best practices
58%	Compliant with regulatory requirements

01 ACCESS CONTROL & DATA PROTECTION FINDINGS

WEB SECURITY EVENTS

Top High Risk Applications & Sites

Within the areas of web applications and websites, the following items are of the highest risk levels[1]

Application / Site	Category	App Risk	Number of Users	Traffic	Number of Events
Tor	Anonymizer	5 Critical	35	149 MB	228
Ultrasurf	Anonymizer	5 Critical	33	1 GB	51
Coralcdn	Anonymizer	5 Critical	2	2 MB	45
VTunnel	Anonymizer	5 Critical	1	24 MB	18
Kugou	P2P File Sharing	5 Critical	2	7 MB	15
Suresome	Anonymizer	5 Critical	7	1 MB	9
Hola	Anonymizer	5 Critical	3	98 KB	4
PacketiX VPN	Anonymizer	5 Critical	2	300 KB	2
Kproxy	Anonymizer	5 Critical	1	400 KB	2
Sopcast	P2P File Sharing	5 Critical	1	350 KB	1
DarkComet-RAT	Remote Administration	5 Critical	1	260 KB	1
Dropbox	File Storage and Sharing	4 Critical	3573	37 GB	19,443
GoToAssist-RemoteSupport	Remote Administration	4 Critical	1573	4 GB	5,733
Lync	Instant Messaging	4 Critical	118	937 MB	1,144
TeamViewer	Remote Administration	4 Critical	182	831 MB	768
BitTorrent Protocol	P2P File Sharing	4 Critical	113	168 MB	464
Lync-sharing	Instant Messaging	4 Critical	93	70 MB	443
uTorrent	P2P File Sharing	4 Critical	2	21 MB	327
QQ IM	Instant Messaging	4 Critical	30	26 MB	294
Free Download Manager	Download Manager	4 Critical	6	373 MB	257
AOL Desktop	Anonymizer	4 Critical	47	2 MB	233
ad.adlegent.com/iframe	Spam	4 Critical	3	32 MB	228
linkuryjs.info	Spam	4 Critical	2	85 MB	227
Dropbox-web download	File Storage and Sharing	4 Critical	2	3 MB	193
LogMeIn	Remote Administration	4 Critical	39	30 MB	179
digsby	Instant Messaging	4 Critical	36	5 MB	166
ZumoDrive	File Storage and Sharing	4 Critical	17	3 MB	148
AliWangWang	File Storage and Sharing	4 Critical	2	3 MB	140

[1] Risk level 5 indicates an application that can bypass security or hide identities (for example: Tor, VTunnel). Risk level 4 indicates an application that can cause data leakage or malware infection without user knowledge (for example: File Sharing, P2P uTorrent or P2P Kazaa). Remote Administration applications might be legitimate when used by admins and helpdesk.

High Risk Applications Compliant with Organizational Security Policy

High risk applications are applications that can bypass security, hide identities, cause data leakage or even malware infection without user knowledge. In most cases, use of such applications is against organizational security policy. However, in some cases specific applications can be made compliant with organizational policy. The following high risk applications were detected during the security analysis, but comply with organizational security policy.

Application	Organizational Security Policy
TeamViewer	Allowed to be used by Support team for remote assisting customers
LogMeIn	Allowed to be used by Helpdesk for remote assisting employees

Top High Risk Applications Description

The following tables provide summary explanations of the top events found and their associated security or business risks:

Application and Description	Category	App. Risk	Events
Tor Tor is an application intended to enable online anonymity. Tor client software directs internet traffic through a worldwide volunteer network of servers to conceal a user's location or usage from anyone conducting network monitoring or traffic analysis. Using Tor makes it more difficult to trace Internet activity such as website visits, online posts, instant messages and other communication forms, back to the user.	Anonymizer	Critical	228
Ultrasurf Ultrasurf is a free proxy tool that enables users to circumvent firewalls and Internet content blocking software.	Anonymizer	Critical	51
VTunnel VTunnel is a free anonymous common gateway interface (CGI) proxy that masks IP addresses enabling users to connect to and view websites anonymously and bypass network security enforcement.	Anonymizer	Critical	18
BitTorrent BitTorrent is a peer-to-peer file sharing P2P communication protocol. It is a method of distributing large amounts of data widely. There are numerous compatible BitTorrent clients, written in a variety of programming languages, and running on a variety of computing platforms. P2P Applications can cause data leakage or malware infection without user knowledge.	P2P File Sharing	High	464
ZumoDrive ZumoDrive is a hybrid cloud storage application. It allows users to access their music, photos, and documents from computers and mobile phones. Sharing data on a public cloud might cause leakage of sensitive data.	File Storage and Sharing	High	148

Top Users of High Risk Applications

The following users were involved in the highest number of risky application and web usage events:

Users	Events
Ginger Cash	12
Ivan Whitewash	9
Jim Josh	7
Bob Bash	5
Damien Dash	2

***Note:** User names will be displayed in the above table only when Check Point Identity Awareness Software Blade is enabled and configured.

DATA LOSS EVENTS

Your company data is one of the most valuable assets of your organization. Any intentional or unintentional loss can cause damage to your organization. The following represents the characteristics of the data loss events that were identified during the course of the analysis.

Top Data Loss Events

The following list summarizes the identified data loss activity and the number of times that the specific type of event occurred.

Severity	Data	Category	Events
Critical	Credit Card Numbers	Compliance Regulation	5
High	Business Plan	Business Information	6
	Financial Reports	Finance Information	3
	Source Code	Intellectual Property	2
	Outlook Message - Confidential	Confidential Information	1
Medium	Pay Slip File	Human Resources	4
	U.S. Social Security Numbers	Personally Identifiable Information	1

Top Files Sent Outside of the Organization over HTTP

The following table presents files sent outside of the organization that may contain sensitive data.

Host	Data Type	File Name	URL
192.168.75.26	Credit Card Numbers	customer orders.xlsx	www.ccvalidator.com
192.168.75.48	Financial Reports	Q4 Report - draft2.docx	www.dropbox.com
192.168.125.28	Source Code	new_feature.C	www.java-help.com
192.168.125.10	Customer Names	Customer List.xlsx	www.linkedin.com
192.168.125.78	HIPAA - Protected Health Information	Medical File - Rachel Smith.pdf	www.healthforum.com

Top Files Sent Outside of the Organization over SMTP

The following table presents files sent outside of the organization that may contain sensitive data.

Recipients	Data Type	File Name	Email Subject
bella@otherBiz.com	Credit Card Numbers	Customer Invoices.xlsx	FW: Invoices
betty@otherBiz.com	Business Plan	Q1 2015 Goals.pdf	RE: 2015 Plan
doreen@otherBiz.com	Employee Names	employees.xls	company employees
zoe@otherBiz.com	Salesforce Reports	Q4 sales summary.doc	RE: Q4 Sales. Confidential!
jordana@otherBiz.com	Corporate Press Release	New Release - draft2. docx	FW: new release PR draft - do not forward!!

Top Data Loss Events by Mail Sender

This chart shows data leakage by mail sender on your network.

Sender	Events
tommythrash@myBiz.com	4
susansash@myBiz.com	4
joejosh@myBiz.com	4
ikewhitewash@myBiz.com	3
johnjosh@myBiz.com	3
ebenezereyelash@myBiz.com	2
jeffjosh@myBiz.com	2
claudecash@myBiz.com	1
bradbash@myBiz.com	1
chloecash@myBiz.com	1

02 THREAT PREVENTION FINDINGS

BOT EVENTS

A bot is malicious software that invades your computer. Bots allow criminals to remotely control computer systems and execute illegal activities without user's awareness. These activities can include: stealing data, spreading spam, distributing malware, participating in Denial of Service attacks and more. Bots are often used as tools in targeted attacks known as Advanced Persistent Threats (APTs). A botnet is a collection of such compromised computer systems.

The following table summarizes the number of hosts infected with bots and their activities detected in your network.

Hosts infected with Bots	8
Hosts with Installed Adware	1
Hosts with SMTP and DNS malware-related events	2

Bot Malicious Activities

Description	Findings
Bot communicating with C&C site	4
Bot testing connectivity	2
Other malicious activity due to Bot infection	1
Unwanted network activity due to installed Adware	1
Total Events	**8**

Hosts with High and Critical Bot Events

During the security analysis, the Check Point solution identified a number of Malware-related events that indicate bot activity. This table shows a sample of hosts that experienced high risk events.

Host	Activity	Threat Name	Resource
192.168.75.7	Communication with C&C	Operator.Virus.Win32.Sality.d.dm	yavuztuncil.ya.funpic.de/images/logos.gif?f58891=16091281
10.10.2.32	DNS client query or DNS server resolving a C&C site	Operator.Conficker.bhvl	zsgnmngn.net
192.168.75.22	DNS client query or DNS server resolving a C&C site	Operator.Zeus.bt	zsxwd.com
172.23.25.35	DNS client query or DNS server resolving a C&C site	Operator.BelittledCardigan.u	zwoppfqnjj.com
10.100.2.33	DNS client query or DNS server resolving a C&C site	Operator.APT1.cji	zychpupeydq.biz
10.1.1.22	DNS client query or DNS server resolving a C&C site	Operator.Virus.Win32.Sality.f.h	zykehk.com

More details about malware identified in this report can be found by searching Check Point ThreatWiki, Check Point's public malware database at **threatwiki.checkpoint.com**

VIRUS EVENTS

There are numerous channels that cybercriminals use to distribute malware. Most common methods motivate users to open an infected file in an email attachment, download an infected file, or click on a link leading to a malicious site.

The following tables summarize malware downloads and access to malware-infested sites events, detected in your network.

Malware Downloads

Description	Findings
Hosts downloaded a malware	8
Number of events detected	9

Access to Malicious Sites

Description	Findings
Hosts accessed a site known to contain malware	5
Number of events detected	8

Hosts with High and Critical Virus Events

During the security analysis, the Check Point solution identified a number of Malware-related events which indicate malicious file downloads or connections to malware-infested sites. This table shows a sample of hosts that experienced high risk events.

Host	Activity	Resource
192.168.75.78	Malicious file/exploit download	r.openx.net/set?pid=619cb264-acb9-5a18-89ed-c1503429c217&rtb=3105223559/basic.pdf
192.168.125.76	Malicious file/exploit download	lavilla.de/links.jpg
192.168.125.10	Access to site known to contain malware	zzoygsulaeli.com/img_cache.php
192.168.125.48	DNS server resolving a site known to contain malware for a client behind it	zzoygsulaeli.com

More details about malware identified in this report can be found by searching Check Point ThreatWiki, Check Point's public malware database at **threatwiki.checkpoint.com**

ADVANCED THREATS

With cyber-threats becoming increasingly sophisticated, advanced threats often include new exploits that are spread almost daily and there are no existing protections. These exploits include zero-day attacks of new vulnerabilities and countless new malware variants.

This section summarizes advanced threats detected in your network. To receive a detailed malware analysis on specific event, please contact the local Check Point representative who conducted this report.

Total files scanned	**169**

Event	**Findings**	**Hosts involved**
Advanced threats downloaded from web	7	6
Advanced threats sent via email (SMTP)	9	9

Top Advanced Threats Downloaded from Web

The following table summarizes the top advanced threats downloaded from the web:

File	Malware Activity	Host	Resource
0dd730ed4.pdf	Unexpected Process Crash	192.87.2.7	www.lostartofbeingadame.com/wpcontent/plugins/www.fotosupload.php
guide04d88.pdf	Malicious Filesystem Activity Malicious Network Activity Malicious Registry Activity Unexpected Process Creation Unexpected Process Termination	10.23.33.24	silurian.cn/modules/mod_cmsfix/fix.php

Top Advanced Threats Sent via Email (SMTP)

The following table summarizes the top advanced threats detected in emails based on SMTP traffic:

File	Sender	Recipient	Subject	Malware Activity
Notice231488.doc	asia@shippingoods.com	logistics@mybiz.biz	Parcel details	Malware create another process Malware create suspicious files Malware retrieve module name Malware spawns another instance of self Malware tampers browser history
invoiceBQW8OY.doc	No-Replay@shop.sip	jhon@mybiz.biz	Your invoice	Malware affects other process on the system Malware create another process Malware create suspicious files Malware creates a process in suspended state (used to escape process) Malware delete itself Malware retrieve module name Malware runs on a context of a different process Malware spawns a child process Malware tampers browser history
Summit_Agenda.doc	events@conferences.org	marketing@mybiz.biz	The agenda for the upcoming event	Malware create another process Malware create suspicious files Malware creates a process in suspended state (used to escape process Malware delete itself Malware retrieve module name Malware tampers important system files

INTRUSION & ATTACK EVENTS

Top Intrusion & Attack Events

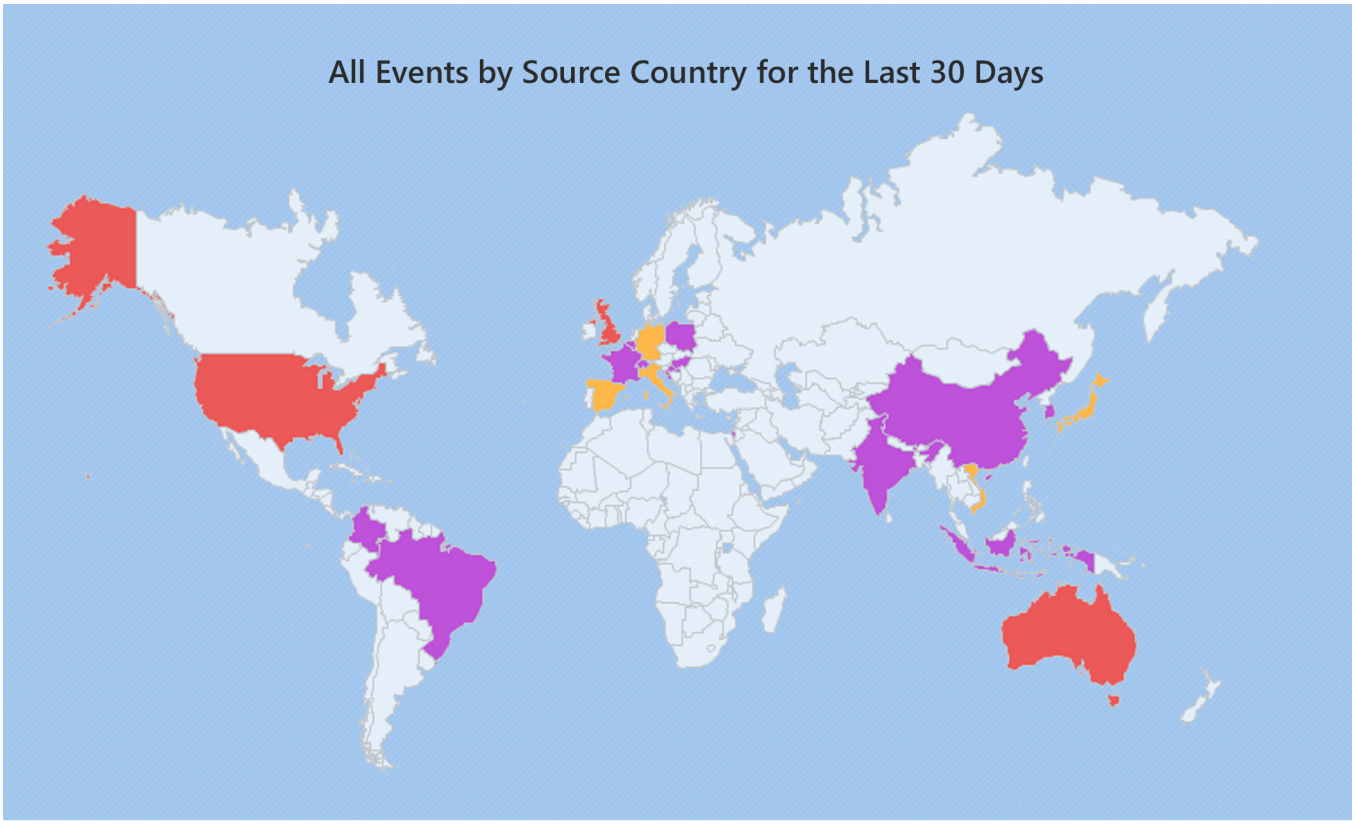
During the security analysis, the Check Point solution identified a number of intrusion prevention-related events. Some of these events were categorized as high risk. The following chart shows the distribution of events according to severity:

Severity	Event Name	CVE List*	Events
Critical	Microsoft SCCM Reflected Cross-site Scripting (MS12-062)	CVE-2012-2536	5
	Joomla Unauthorized File Upload Remote Code Execution	-	2
	Web Servers Malicious HTTP Header Directory Traversal	-	1
	ImageMagick GIF Comment Processing Off-by-one Buffer Overflow (CVE-2013-4298)	CVE-2013-4298	3
	Adobe Flash Player SWF File Buffer Overflow (APSB13-04)	CVE-2013-0633	2
High	PHP php-cgi query string parameter code execution	CVE-2012-1823	1
	Oracle database server CREATE_TABLES SQL injection	CVE-2007-3890	4

*CVE (Common Vulnerabilities and Exposures) is a dictionary for publicly known security vulnerabilities. To find more information about a specific IPS event, search the CVE ID using National Vulnerability Database CVE search web page.

IPS Events by Country

The following map shows the distribution of IPS events according to their countries of origin.



03 ENDPOINT SECURITY FINDINGS

This section of the report provides the security findings related to the hosts of your infrastructure. The section represents a summary of these findings and detailed information per security vector. The remediation section of this report presents a set of recommendations for addressing the detected events.

Endpoint Security Events Summary

Total endpoints running high risk web applications	6
Total endpoints involved in data loss Incidents	19
Total endpoints involved in intrusion and attack events	20
Total endpoints involved in malware incidents	848

Top Endpoints Running High Risk Applications

The following table presents top endpoint machines running high risk applications or that have accessed a high risk website:

Source	Application / Site	Category	App Risk
192.168.2.13	Tor	Anonymizer	5 Critical
10.10.10.235	Ultrasurf	Anonymizer	5 Critical
192.168.2.33	Coralcdn	Anonymizer	5 Critical
192.168.5.66	VTunnel	Anonymizer	5 Critical
192.168.5.33	Kugou	P2P File Sharing	5 Critical
10.10.23.235	Suresome	Anonymizer	5 Critical
172.26.25.11	Hola	Anonymizer	5 Critical
10.10.22.31	PacketiX VPN	Anonymizer	5 Critical
10.10.1.235	Kproxy	Anonymizer	5 Critical
192.168.5.39	Sopcast	P2P File Sharing	5 Critical
192.168.5.37	DarkComet-RAT	Remote Administration	5 Critical
10.23.55.33	Dropbox	File Storage and Sharing	4 Critical
10.23.55.34	GoToAssist-RemoteSupport	Remote Administration	4 Critical

Top Endpoints Intrusion & Attack Events

The following table presents top endpoint machines with intrusion prevention-related events.

Source	Destination	Severity	Event Name	CVE List
192.87.2.47	192.168.75.27	Critical	Microsoft SCCM Reflected Cross-site Scripting (MS12-062)	CVE-2012-2536
192.78.2.214	192.168.75.58	Critical	Joomla Unauthorized File Upload Remote Code Execution	-
192.84.2.220	192.168.75.58	Critical	Web Servers Malicious HTTP Header Directory Traversal	-
192.85.2.133	192.168.75.58	Critical	ImageMagick GIF Comment Processing Off-by-one Buffer Overflow (CVE-2013-4298)	CVE-2013-4298
192.116.2.151	192.168.75.58	Critical	Adobe Flash Player SWF File Buffer Overflow (APSB13-04)	CVE-2013-0633
192.195.2.88	192.168.75.60	High	PHP php-cgi query string parameter code execution	CVE-2012-1823
192.87.2.211	192.168.86.3	High	Oracle database server CREATE_ TABLES SQL injection	CVE-2007-3890

Top Endpoints Involved in Data Loss Incidents

The following table present top endpoint machines with data loss related events

Endpoint	Events	Data Sent
192.168.125.36	4	Credit Card Numbers
	1	Business Plan
192.168.75.0	5	Financial Reports
192.168.125.0	4	Source Code
192.168.86.47	4	Outlook Message - Confidential
192.168.86.38	2	U.S. Social Security Numbers

Top Endpoints Involved in a Malware Incident

The following table presents top endpoint machines with Malware-related security events

Host	Threat Name	Malware Activity
192.168.86.8	Operator.Virus.Win32.Sality.f.h	DNS client query or DNS server resolving a C&C site
192.168.75.0	Operator.APT1.cji	DNS client query or DNS server resolving a C&C site
192.168.75.3	Operator.Virus.Win32.Sality.d.dm	Communication with C&C
192.168.75.7	REP.yjjde	Access to site known to contain malware
192.168.75.10	RogueSoftware.Hack_Style_RAT.pbco	Communication with C&C
192.168.75.13	Trojan.Win32.Agent.aaeyr.cj	Malicious file/exploit download

COMPLIANCE SECURITY ANALYSIS

This section presents a detailed analysis of the security policies of your existing Check Point Network Security deployment.

The analysis was performed using Check Point Compliance Software Blade which utilizes an extensive library of hundreds of security best practices and recommendations for improving your organization's network security

Security Policy Compliance

The Compliance Software Blade scanned the configuration of your Security Management, Gateways and installed Software Blades. The results have been compared with a sample of our security best practices. From our 102 recommended best practices, we found that 67 were fully compliant, while 35 were missing or not compliant. This results in an overall compliance level of 65%.

	**65%**	Compliant with Check Point recommended security best practices
	**102**	Analyzed security configurations
	**67**	Configurations found compliant
	**35**	Configurations found not compliant or missing
	**12**	Security gateways monitored

Security Best Practices Compliance Top Findings

The table below presents the most important security best practices that were detected to be missing or not fully configured.

Blade	ID	Name	Status
Firewall	FW101	Check that "Clean up Rule" is Defined in Firewall Rule Base	0%
Firewall	FW102	Check that Anti-Spoofing has been activated on each Gateway	0%
Firewall	FW103	Check that Anti-Spoofing is set to Prevent on each Gateway	0%
Firewall	FW105	Check that each Firewall rule has defined Track settings	0%
Firewall	FW130	Check that "Stealth Rule" is Defined in Firewall Rule Base	0%
Firewall	FW152	Check that each Firewall rule has a Name defined	0%
Firewall	FW153	Check that each Firewall rule has a Comment defined	0%
Firewall	FW107	Check that there is an additional log server defined for each Gateway for the storage of Firewall logs	0%
Firewall	FW116	Check that NAT/PAT is enabled in the Firewall settings	87%
Firewall	FW146	Check that an "Any Any Accept" rule is not defined in the Firewall Rule Base	0%
Firewall	FW159	Check that "Lockout Administrator\'s account after" is selected	0%
Firewall	FW160	Check that Administrators are locked out after 3 login failures	0%
Firewall	FW161	Check that "Unlock Administrator\'s account after" is selected	0%
Firewall	FW162	Check that Administrators\' accounts are unlocked after 30 minutes	0%
Firewall	FW163	Check that a detailed message is displayed to locked out Administrators	0%

Best Practices Compliance by Security Software Blade

The table below shows the overall security status for each Software Blade.

For each Software Blade Check Point recommends a set of best practices. A score of 100% means that all best practices for that blade were found to be securely configured. A score less than 100% indicates configurations not according to the best practices and therefore pose potential security weaknesses in your environment.

Security Software Blade	Number of Security Best Practices	Security Status
Data Loss Prevention	2	7%
IPS	4	29%
Application Control	13	54%
Mobile Access	3	66%
IPSec VPN	16	73%
URL Filtering	5	87%
Firewall	35	88%
Anti-Virus	13	91%
Anti-Spam & Mail	3	100%
Anti-Bot	8	100%

Regulatory Compliance Summary

The following table shows your network security regulatory compliance level. The status is determined by analysing various Check Point Security Gateway configurations and Software Blade settings and comparing them with regulations requirements.

Regulation	Number of Requirements	Number of Security Best Practices	Compliance Status*
ISO 27001	27	102	78%
PCI DSS	55	102	86%
HIPAA	16	102	78%
DSD	14	68	67%
GLBA	5	102	45%
NIST 800-41	22	25	85%
ISO 27002	198	102	77%
NIST 800-53	25	71	86%
CobiT 4.1	15	102	66%
UK Data Protection Act	1	29	49%
Firewall STIG	30	54	87%
GPG 13	9	31	87%
NERC CIP	8	56	74%
MAS TRM	25	102	77%
SOX	15	102	66%
FIPS 200	25	71	87%

* The Compliance Status is based on the set of Security Best Practices linked to each regulation

05 BANDWIDTH ANALYSIS

The following section summarizes the bandwidth usage and web browsing profile of your organization during the time of analysis.

Top Bandwidth Utilization by Applications & Websites

The following table presents the top detected web applications and websites sorted by consumed bandwidth.

Application / Site	Matched Category	App Risk	Sources	Traffic	Number of Events
YouTube	Media Sharing	2 Low	2339	413 GB	5550
Google Services	Web Services Provider	2 Low	19866	301 GB	213165
Pandora Radio	Media Sharing	2 Low	737	203 GB	4402
FTP Protocol	Network Protocols	3 Medium	399	186 GB	6439
Netflix-streaming	IPTV	2 Low	2	179 GB	303
Instagram	Mobile Software	2 Low	171	158 GB	1269
downloading_garmin.com	Computers/Internet	- Unknown	2	129 GB	224
App Store	Mobile Software	1 Very Low	4	113 GB	459
Google Search	Search Engines/Portals	2 Low	128	112 GB	2401
SSH Protocol	Network Protocols	3 Medium	414	96 GB	10846
Windows Update	Software Update	1 Very Low	3784	84 GB	47284
akamaihd.net	Business/Economy	- Unknown	13	74 GB	477
OpenSSH	Network Utilities	3 Medium	248	61 GB	2197
Web Browsing	Web Browsing	- Unknown	3420	61 GB	11345
macromedia.com	Computers/Internet	- Unknown	25	50 GB	508
bloomingdales.com	Fashion	- Unknown	117	48 GB	1586
macys.com	Fashion	- Unknown	296	45 GB	3453
Netflix	IPTV	2 Low	1849	44 GB	5600
update.nai.com	Computers/Internet	- Unknown	827	44 GB	8330
iTunes	Media Sharing	2 Low	4	44 GB	418
apple.com	Computers/Internet	- Unknown	16	43 GB	628
Yahoo! Services	Web Services Provider	2 Low	7118	39 GB	26999
Syslog Protocol	Network Protocols	1 Very Low	11	38 GB	1757
Dropbox	File Storage and Sharing	4 High	3573	37 GB	19443
Facebook	Social Networking	2 Low	16512	35 GB	150378
SMTP Protocol	Network Protocols	3 Medium	5471	32 GB	87960
download.micosoft.com	Computers/Internet	- Unknown	12	30 GB	434
grooveshark	Media Sharing	2 Low	2	29 GB	176
iTunes-podcasts	Media Sharing	2 Low	55	27 GB	594
Gmail	Email	3 Medium	4313	26 GB	24286
IAX2 Protocol	Network Protocols	2 Low	85	25 GB	149
Adobe Update	Software Update	1 Very Low	6326	24 GB	27764
c.2mdn.net	Web Advertisements	- Unknown	6	24 GB	438
cloudfront.net	Computers/Internet	- Unknown	54	24 GB	702

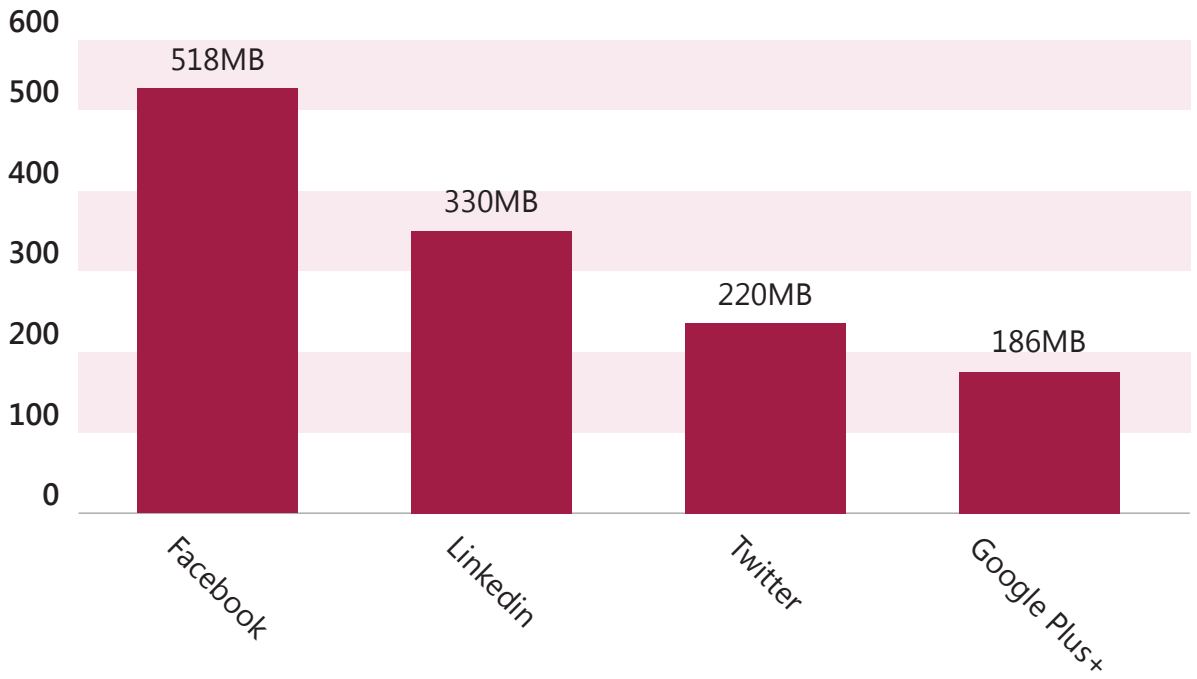
Top Web Categories

The following table shows the top 10 categories and number of hits associated with employee Internet browsing.

Category	Number of Hits	% of Total Hits
Social Networking	113	31.65%
Webmail	42	11.76%
Video Streaming	36	10.08%
Search Engines / Portals	35	9.80%
Multimedia	29	8.12%
Browser Plugin	25	7.00%
Business Applications	15	4.20%
Media Sharing	13	3.64%
Network Utilities	9	2.52%
Other	40	11.20%
Total	**357**	**100%**

Social networking bandwidth (MB)

The use of social networking sites has become common at the workplace and at home. Many businesses leverage social networking technologies for their marketing and sales efforts, and their recruiting programs. During the course of this analysis, and consistent with over-all market trends, the following social networking sites consumed the most network bandwidth:



06 REMEDIATION RECOMMENDATIONS

ACCESS CONTROL & DATA PROTECTION RECOMMENDATIONS

This report addresses identified security events across multiple security areas and at varying levels of criticality. The table below reviews the most critical of these incidents and presents methods to mitigate their risks. Check Point provides multiple methods for addressing these threats and concerns. Relevant protections are noted for each event, with the software blades into which the defenses are incorporated.

Web Security Events Remediation Recommendations

Application/Site	App. Risk	Events	Remediation Steps
Tor	Critical	228	In Application Control and URL Filtering Software Blades, you can activate, track and prevent the use of all the mentioned applications & web sites. You can define a granular policy to allow certain applications to specific groups only. Use UserCheck to: • Educate users about the organization's web browsing and application usage policy. • Provide users with instant feedback when their actions violate the security policy.
Ultrasurf	Critical	51	
Vtunnel	Critical	18	
BitTorrent	High	464	
ZumoDrive	High	148	

Click for more information about Check Point **Application Control** and **URL Filtering** Security Gateway Software Blades.

Data Loss Events Remediation Recommendations

Severity	Data	Events	Remediation Steps
Critical	Credit Card Numbers	14	To remediate the detected events activate DLP Software Blade. Configure DLP policy based on the detected DLP data type and choose an action (Detect/ Prevent/Ask User/etc.). If you consider the detected data type as sensitive information the recommended action is prevent. Use UserCheck to: • Educate users about the organization's data usage policy. • Provide users with instant feedback when their actions violate the data usage security policy.
High	Business Plan	1	
	Financial Reports	3	
	Source Code	12	
	Outlook Message - Confidential	147	
Medium	Pay Slip File	25	
	U.S. Social Security Numbers	15	

Click for more information about Check Point **DLP** security gateway software blade.

THREAT PREVENTION RECOMMENDATIONS

Malware Threats Remediation Recommendations

Malware	Severity	Events	Remediation Steps
REP.yjjde	Critical	36	Enable Check Point Anti-Bot Software Blade to detect bot infected machines and prevent bot damages. Enable Check Point Anti-Virus Software Blade to prevent malware downloads. Enable Check Point Threat Emulation Software Blade to protect from new and undiscovered malware threats. To remediate an infected machine, first search for the detected malware in Check Point ThreatWiKi to find information about it. Next, follow the remediation instructions appears in the Malware Remediation Steps web page.
Operator.Virus.Win32.Sality.d.dm	Critical	28	
Operator.Conficker.bhvl	High	27	
Operator.Zeus.bt	High	11	
Operator.BelittledCardigan.u	High	8	

Click for more information about Check Point **Anti-Bot**, **Anti-Virus** and **Threat Emulation** Security Gateway Software Blades.

Intrusions & Attacks Events Remediation Recommendations

Threat	Severity	Events	Remediation Steps
Microsoft SCCM Reflected Cross-site Scripting (MS12-062)	Critical	15	In Check Point IPS Software Blade, enable the following protection: **Microsoft SCCM Reflected Cross-site Scripting (MS12-062)**
Joomla Unauthorized File Upload Remote Code Execution	Critical	13	In Check Point IPS Software Blade, enable the following protection: **Joomla Unauthorized File Upload Remote Code Execution**
Microsoft Active Directory LSASS Recursive Stack Overflow [MS09-066]	High	4	In Check Point IPS Software Blade, enable the following protection: **Microsoft Active Directory LSASS Recursive Stack Overflow [MS09-066]**

Click for more information about Check Point **IPS** Security Gateway Software Blade.

ENDPOINT SECURITY REMEDIATION RECOMMENDATIONS

This section addresses identified endpoint security events across multiple security areas and at varying levels of criticality. The tables below review the most critical of these incidents and presents methods to mitigate their risks. Check Point provides multiple methods for addressing these threats and concerns. Relevant protections are noted for each event, with the Endpoint Software Blades into which the defenses are incorporated.

Web Security Events - Endpoint Remediation Recommendations

Host	App/Site	Risk	Remediation Steps
192.168.75.36	Tor	Critical	**Check Point Endpoint Security** controls the usage of high risk applications and websites even when the endpoint is off-the corporate network and without network security solution. Use **Check Point Program Control Software Blade** to allow only approved programs to run on the endpoint and terminate not approved or untrusted programs. Use **Check Point Compliance Check Software Blade** to verify if a certain program is running on the endpoint device and restrict its network access if needed. Control inbound and outbound traffic with **Endpoint Firewall Software Blade** to restrict access to specific ports and network services. Use **UserCheck** to: • Educate users about the organization's web browsing and application usage policy. • Provide users with instant feedback when their actions violate the security policy.
192.168.75.71	Ultrasurf	Critical	
192.168.86.0	VTunnel	Critical	
192.168.86.19	BitTorrent	High	
192.168.86.30	ZumoDrive	High	

Click for more information about the following Check Point Endpoint Security Software Blades:

- **Program Control** Endpoint Security Software Blade
- **Compliance Check** Endpoint Security Software Blade
- **Firewall** Endpoint Security Software Blade

Intrusion & Attack Events - Endpoint Remediation Recommendations

Source	Destination	Event Name	Remediation Steps
192.87.2.47	192.168.75.27	Microsoft SCCM Reflected Cross-site Scripting (MS12-062)	Use **Endpoint Compliance Software Blade** to verify the endpoints in your organization are up to date with the latest security patches and updates. The **Endpoint Compliance Software Blade** will ensure the endpoints are secured even when off the organizational network and without network security protection. For example working from home or on the road.
192.78.2.214	192.168.75.58	Joomla Unauthorized File Upload Remote Code Execution	
192.84.2.220	192.168.75.58	Web Servers Malicious HTTP Header Directory Traversal	
192.85.2.133	192.168.75.58	ImageMagick GIF Comment Processing Off-by-one Buffer Overflow (CVE-2013-4298)	
192.116.2.151	192.168.75.58	Adobe Flash Player SWF File Buffer Overflow (APSB13-04)	
192.195.2.88	192.168.75.60	PHP php-cgi query string parameter code execution	
192.87.2.211	192.168.86.3	Oracle database server CREATE_TABLES SQL injection	

Click for more information about the following **Check Point Endpoint Security Software Blades**:

- **Firewall** Endpoint Security Software Blade
- **Compliance Check** Endpoint Security Software Blade

Data Loss Events - Endpoint Remediation Recommendations

Host	Type	Remediation Steps
192.168.75.0	Credit Card Numbers	Use **Check Point Full Disk Encryption Software Blade** to secure sensitive information installed on endpoint hard drives, including user data, operating system files and temporary and erased files, from unauthorized access when laptops are lost or stolen. Use **Check Point Media Encryption Software Blade** to encrypt sensitive data stored on removable devices and to track and manage removable devices individually. By using **Check Point Document Security Software Blade** you can grant access to sensitive documents only to authorized individuals. Use **UserCheck** to: • Educate users about the organization's data usage policy. • Provide users with instant feedback when their actions violate the data usage security policy.
192.168.86.47	Business Plan	
192.168.125.0	Source Code	
192.168.125.36	Pay Slip File	

Click for more information about the following **Check Point Endpoint Security Software Blades**:

- **Full Disk Encryption** Endpoint Security Software Blade
- **Media Encryption** Endpoint Security Software Blade
- **Document Security** Endpoint Security Software Blade

Malware Events - Endpoint Remediation Recommendations

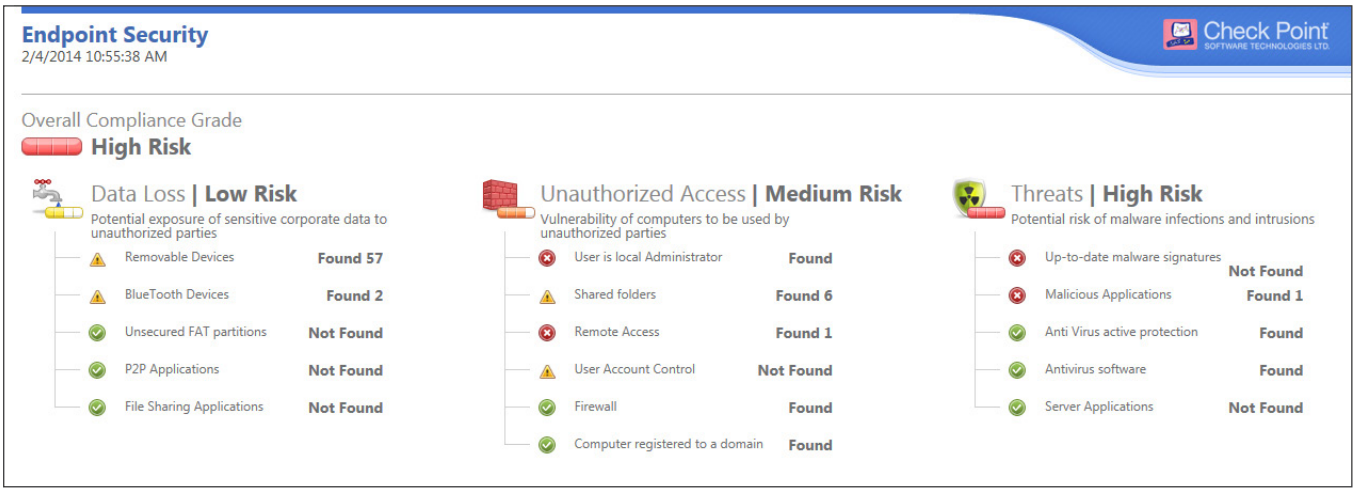
Host	Severity	Remediation Steps
192.53.2.161	Critical	Use **Check Point Endpoint Anti-Malware Software Blade** to detect and prevent threats such as malware, viruses, keystroke loggers, Trojans, and root kits from infecting enterprise endpoints. **Check Point Endpoint Anti-Malware Software Blade** will keep your enterprise endpoints are protected even when off the organizational network and without network security protection. For example working from home or on the road. Use the **Endpoint Compliance Software Blade** to ensure the endpoints are updated with the latest security updates and compliant with the organization security policy. To start the remediation process on an infected machine, search the detected Malware in **Check Point ThreatWiki** to find additional remediation supporting information about the Malware. This information can help you better understand the infection and its potential risks. Use **UserCheck** to educate users about the organization web browsing and web applications usage policy.
192.57.2.32	Critical	
192.57.2.209	Critical	
192.59.2.27	Critical	
192.59.2.79	Critical	

Click for more information about the following **Check Point Endpoint Security Software Blades**:

- **Anti-Malware** Endpoint Security Software Blade
- **Firewall & Compliance** Check Endpoint Security Software Blade

Running Comprehensive Endpoint Security Analysis Report

To perform a more comprehensive analysis on your endpoints for the security posture and potential risks, run the Endpoint Security analysis report or contact your local Check Point representative.



COMPLIANCE BLADE REMEDIATION RECOMMENDATIONS

This report addresses identified security configuration requires attention across Check Point Software Blades. The table below reviews some items to address with guidance on how to improve security level.

Risk	Remediation Steps	Relevant Objects
High	Create a new Stealth Rule or modify the existing Stealth Rule in the relevant Policy Packages in accordance with the following definition: Source = Any ; Destination = GW's ; Service = Any ; Action = Drop ; Install On = Policy Target ; Time = Any.	Policy Package A
High	Create a new Clean-up-Rule or modify the existing Clean-up-Rule in the relevant Policy Packages in accordance with the following definition: Source = Any ; Destination = Any; VPN = Any Traffic ; Service = Any ; Action = Drop ; Track = Log ; Install On = Policy Targets ; Time = Any; Note that the Clean-up-Rule must be the last row listed in the Firewall Rule Base.	Policy Package B
High	Activate automatic update protections in the IPS Blade	IPS Gateway Corporate Gateway
High	Create a new policy or modify the existing policy in the Application Control Blade so that critical risk applications and websites will be blocked.	Policy Package A
High	Modify the Authentication Timeout settings in the Global Properties so that it is between 20 and 120 minutes.	Global Properties
High	Define a Track settings for all Firewall rules across all policy packages.	Policy Package A — Rule number 18 — Rule number 35 — Rule number 64 Policy Package B — Rule number 11 — Rule number 23 — Rule number 88

SOFTWARE-DEFINED PROTECTION

In a world with high-demanding IT infrastructures and networks, where perimeters are no longer well defined, and where threats grow more intelligent every day, we need to define the right way to protect enterprises in the ever changing threat landscape.

There is a wide proliferation of point security products; however these products tend to be reactive and tactical in nature rather than architecturally oriented. Today's corporations need a single architecture that combines high performance network security devices with real-time proactive protections.

A new paradigm is needed to protect organizations proactively.

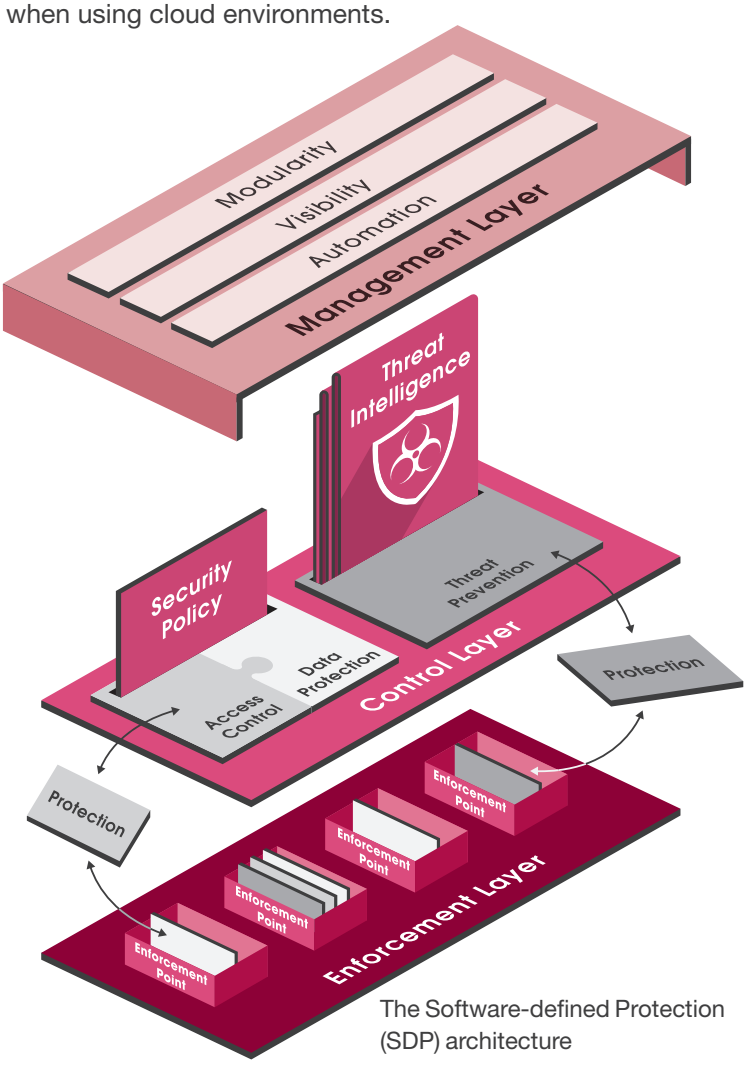
Software-defined Protection is a new, pragmatic security architecture and methodology. It offers an infrastructure that is modular, agile and most importantly, SECURE.

Such architecture must protect organizations of all sizes at any location: headquarters networks, branch offices, roaming through smartphones or mobile devices, or when using cloud environments.

Protections should automatically adapt to the threat landscape without the need for security administrators to follow up manually on thousands of advisories and recommendations. These protections must integrate seamlessly into the larger IT environment, and the architecture must provide a defensive posture that collaboratively leverages both internal and external intelligent sources.

The Software Defined Protection (SDP) architecture partitions the security infrastructure into three interconnected layers:

- An **Enforcement Layer** that is based on physical, virtual and host-based security enforcement points and that segments the network as well as executes the protection logic in high-demand environments.
- A **Control Layer** that analyzes different sources of threat information and generates protections and policies to be executed by the Enforcement Layer.
- A **Management Layer** that orchestrates the infrastructure and brings the highest degree of agility to the entire architecture.



The Software-defined Protection (SDP) architecture

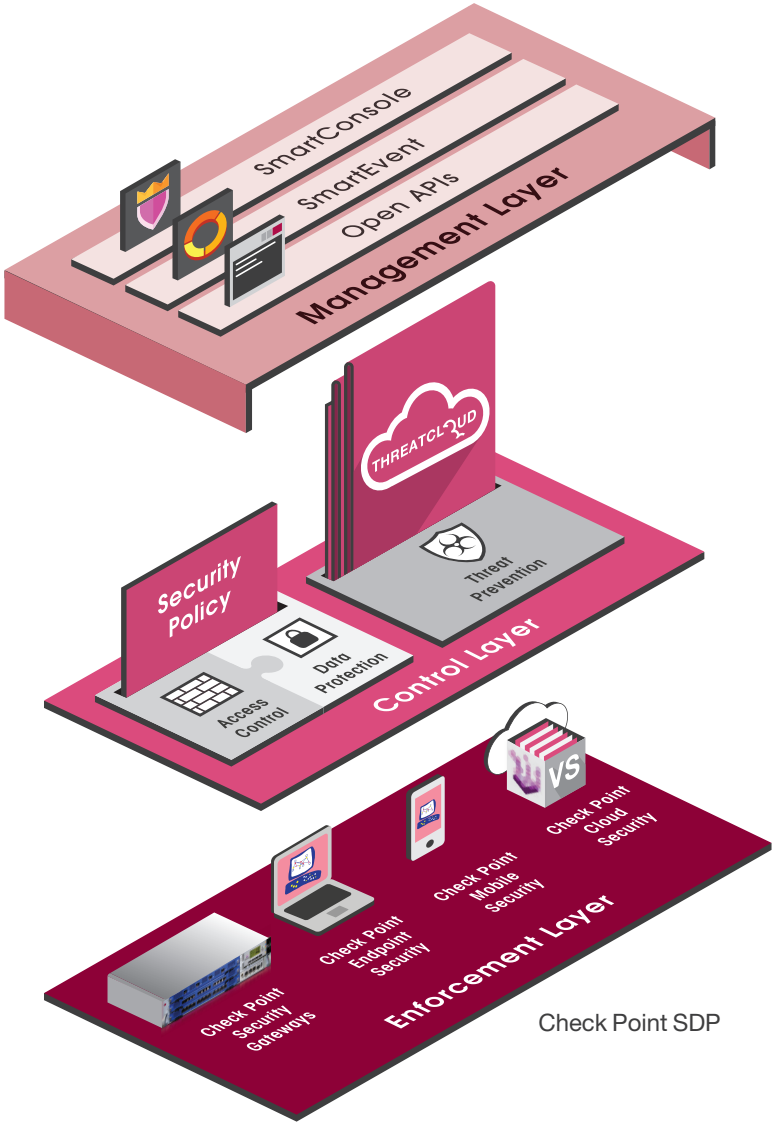
By combining the high performance Enforcement Layer with the fast-evolving and dynamic software-based Control Layer, the SDP architecture provides not only operational resilience, but also proactive incident prevention for an ever-changing threat landscape.

Designed to be forward-looking, the SDP architecture supports traditional network security and access control policies requirements as well as the threat prevention needed by modern enterprises that embrace new technologies such as mobile computing and Software-defined Networks (SDN).

CHECK POINT SOFTWARE-DEFINED PROTECTION

Check Point provides all the right components needed to implement a complete SDP architecture with the best management and the best security.

Check Point software-defined protections provide the flexibility needed to cope with new threats and embrace new technologies. Our solutions generate new and updated protections for known and unknown threats and proactively distribute this knowledge through the cloud. Implementing Check Point security solutions based on sound architectural security design empowers enterprises to embrace leading-edge information system solutions with confidence.



Check Point SDP

CHECK POINT SDP ENFORCEMENT LAYER

To secure the boundaries of each segment, Check Point offers a wide range of enforcement points. These include high-performance network security appliances, virtual gateways, and endpoint host software and mobile device applications. Check Point provides enterprises with all the building blocks needed to engineer segmented, consolidated and secure systems and networks.

CHECK POINT SDP CONTROL LAYER

Check Point SDP control layer is based on Check Point Software Blade Architecture that provides customers with flexible and effective security solutions to match their exact needs. With a choice of over 20 Software Blades, the modular nature of the Software Blade Architecture allows customers to build a relevant security solution per enforcement point and to expand their security infrastructure over time.

Next Generation Threat Prevention

Check Point efficiently delivers controls to counter many of the known and unknown threats. The Check Point Threat prevention solution includes: Integrated Intrusion Prevention System (IPS), Network based Anti-Virus, Threat Emulation and Anti-Bot. Check Point built a unique cloud-based threat intelligence big data and protection generator, Check Point ThreatCloud™. Check Point ThreatCloud enables a collaborative way to fight cybercrime, delivering real-time security threat intelligence converted into security indicators to the control layer.

Next Generation Firewall and Data Protection

Check Point access control is based on our next generation firewall combined with multiple software blades and enables a unified context-based security policy: Next Generation Firewall and VPN, User identity Awareness, Application Control, Data and Content Awareness

Next Generation Data Protection

Check Point Next Generation Data Protection adds data awareness. It includes our Data Loss Prevention (DLP) software blade which performs content inspection and matches file contents with files stored in enterprise repositories. In addition, Check Point provides Data Protection for data at rest and in storage with encryption technologies. These technologies can be implemented on all enforcement points protecting sensitive documents and confidential data from being accessed or transferred to removable media or by unauthorized users.

CHECK POINT SDP MANAGEMENT LAYER

All Check Point protections and enforcement points are managed from a single unified security management console. Check Point security management is highly scalable, providing the ability to manage tens of millions of objects while maintaining super-fast user interface response times.

Check Point Modular / Layered Policy Management

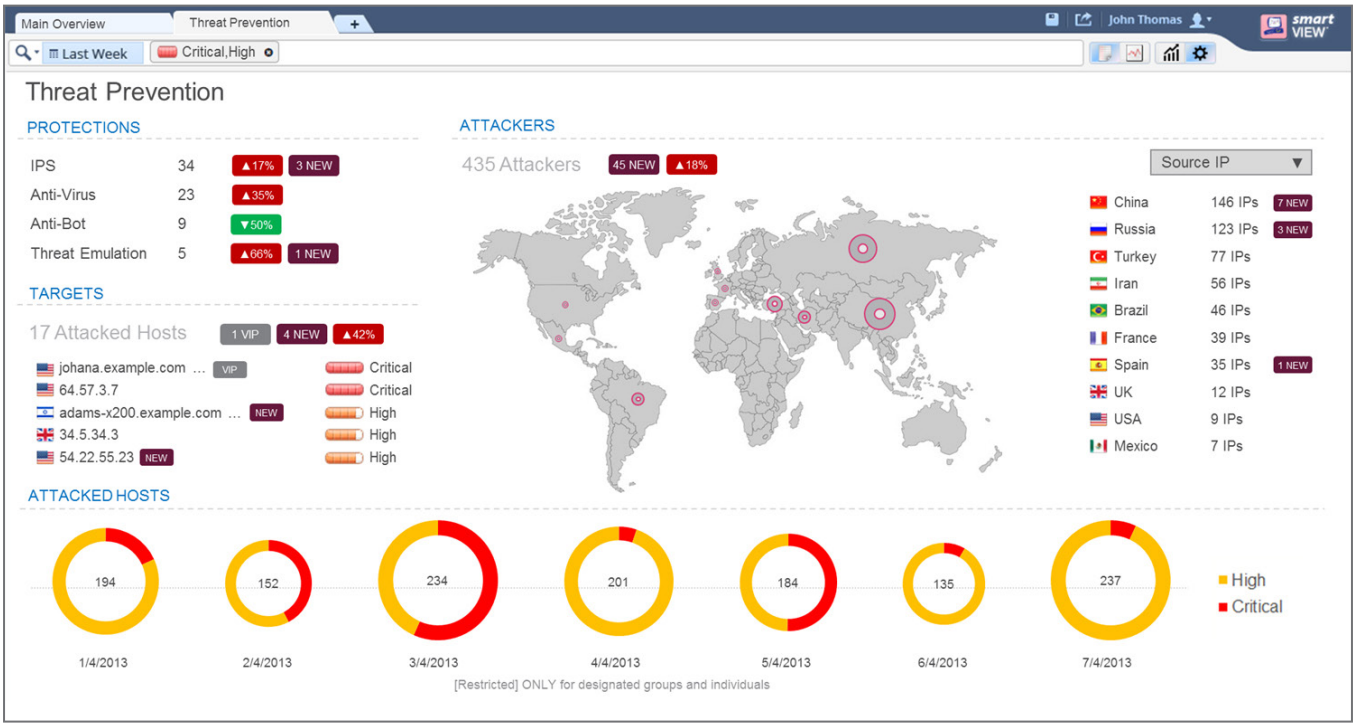
Check Point Security Management support the enterprise segmentation, allowing administrators to define security policy for each segment while enforcing segregation of duties with a new concept called Layers and Sub Layers. Policies can be defined for each segment. Access control policies can be defined using separate layers, which can be assigned to different administrators. Multiple administrators can then work on the same policy simultaneously.

Automation and Orchestration

Check Point Security Management provides CLIs and Web Services APIs that allow organizations to integrate with other systems such as network management, CRM, trouble ticketing, identity management and cloud orchestrators.

Visibility with Check Point SmartEvent

Check Point SmartEvent performs big data analysis and real-time security event correlation. It offers the ability to provide a consolidated and correlated view of an incident based on multiple sources of information. Security event analysis creates actionable intelligence in the form of threat indicators that can be distributed via ThreatCloud to block threats in real-time.



Event Management with Check Point SmartEvent

Learn more about Check Point Software-defined Protection and how it can help your security infrastructure keep pace with today's rapidly changing threat landscape. Visit **www.checkpoint.com/securitycheckup**

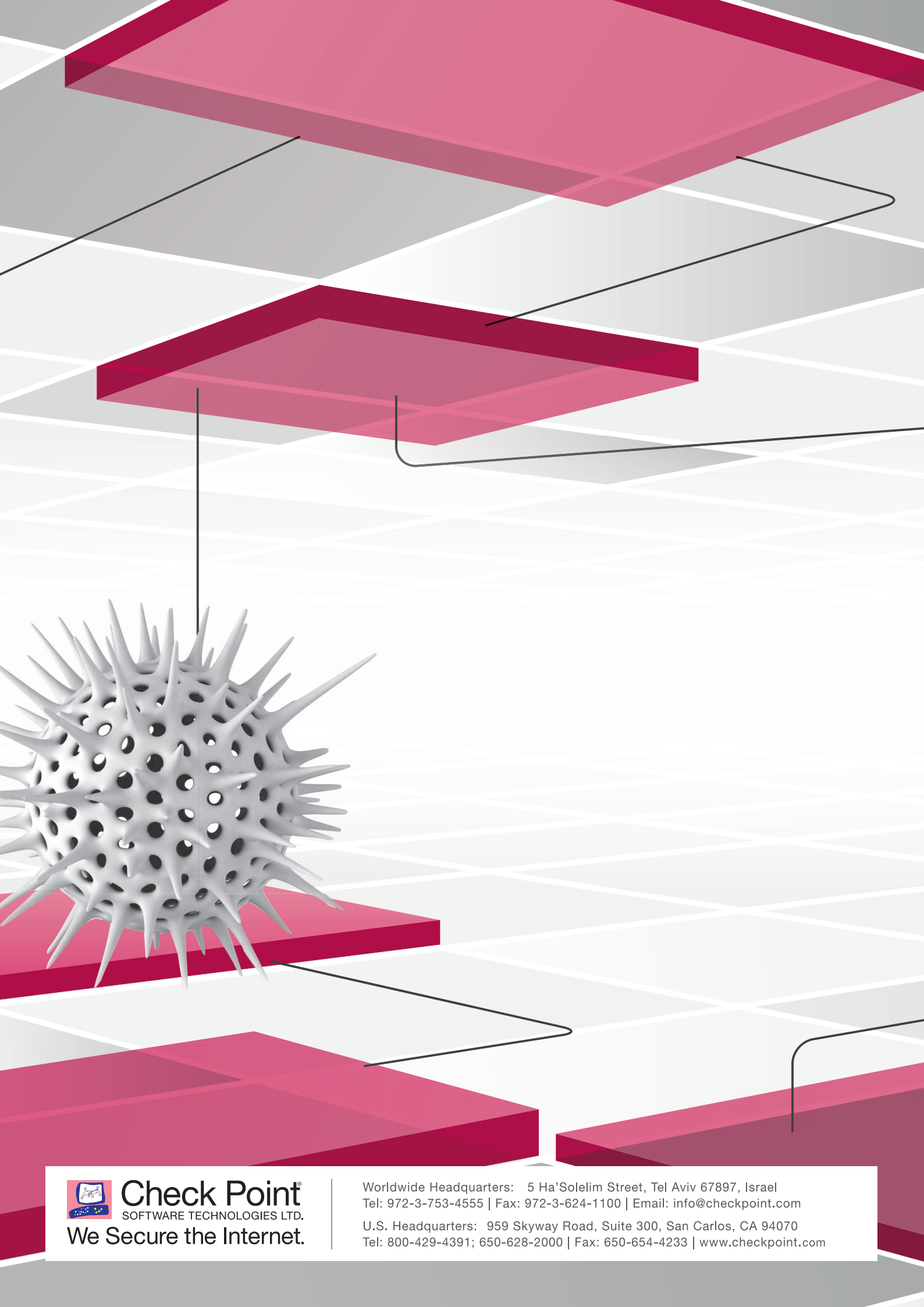
ABOUT CHECK POINT SOFTWARE TECHNOLOGIES

Check Point Software Technologies' **(www.checkpoint.com)** mission is to secure the Internet. Check Point was founded in 1993, and has since developed technologies to secure communications and transactions over the Internet by enterprises and consumers.

Check Point was an industry pioneer with our FireWall-1 and our patented Stateful Inspection technology. Check Point has extended its IT security innovation with the development of our Software Blade architecture. The dynamic Software Blade architecture delivers secure, flexible and simple solutions that can be customized to meet the security needs of any organization or environment.

Check Point develops markets and supports a wide range of software, as well as combined hardware and software products and services for IT security. We offer our customers an extensive portfolio of network and gateway security solutions, data and endpoint security solutions and management solutions. Our solutions operate under a unified security architecture that enables end-to-end security with a single line of unified security gateways, and allow a single agent for all endpoint security that can be managed from a single unified management console. This unified management allows for ease of deployment and centralized control and is supported by, and reinforced with, real-time security updates.

Our products and services are sold to enterprises, service providers, small and medium sized businesses and consumers. Our Open Platform for Security (OPSEC) framework allows customers to extend the capabilities of our products and services with third-party hardware and security software applications. Our products are sold, integrated and serviced by a network of partners worldwide. Check Point customers include tens of thousands of businesses and organizations of all sizes including all Fortune 100 companies. Check Point's award-winning ZoneAlarm solutions protect millions of consumers from hackers, spyware and identity theft.



Check Point®
SOFTWARE TECHNOLOGIES LTD.
We Secure the Internet.

Worldwide Headquarters: 5 Ha'Solelim Street, Tel Aviv 67897, Israel
Tel: 972-3-753-4555 | Fax: 972-3-624-1100 | Email: 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