

SECURITY CHECKUP

ПРОВЕРКА БЕЗОПАСНОСТИ

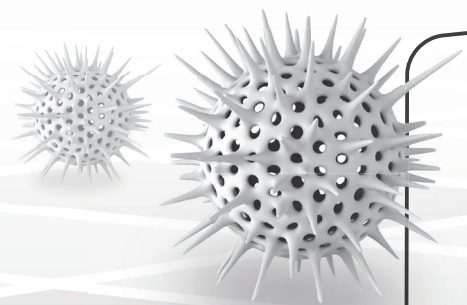
ОТЧЕТ ПО АНАЛИЗУ УГРОЗ

Подготовлен для: ABC Corp.

Подготовлен: Центр решений компании Check Point

Дата: 20 января 2014 г.

Версия документа: 2.0



Check Point
SOFTWARE TECHNOLOGIES LTD.

We Secure the Internet.



СОДЕРЖАНИЕ

SUMMARY	КРАТКИЙ ОБЗОР	3
01	УПРАВЛЕНИЕ ДОСТУПОМ И ЗАЩИТА ДАННЫХ	4
	БЕЗОПАСНОСТЬ WEB	4
	ПОТЕРЯ ДАННЫХ	7
02	ПРЕДОТВРАЩЕНИЕ УГРОЗ	10
	БОТЫ	10
	ВИРУСЫ	12
	УГРОЗЫ «НУЛЕВОГО ДНЯ»	13
	ВТОРЖЕНИЯ И АТАКИ	15
03	БЕЗОПАСНОСТЬ КОНЕЧНЫХ СТАНЦИЙ	17
04	АНАЛИЗ СООТВЕТСТВИЯ ТРЕБОВАНИЯМ БЕЗОПАСНОСТИ	20
05	АНАЛИЗ ПОЛОСЫ ПРОПУСКАНИЯ	24
06	РЕКОМЕНДАЦИИ ПО КОРРЕКТИРУЮЩИМ ДЕЙСТВИЯМ	26
SDP	SOFTWARE-DEFINED PROTECTION	35
ABOUT	О КОМПАНИИ CHECK POINT SOFTWARE TECHNOLOGIES	39



КРАТКИЙ ОБЗОР

Документ содержит данные, полученные в результате анализа безопасности Вашей инфраструктуры. В документе представлены краткий обзор этих данных, а также рекомендации по ответным действиям на обнаруженные события.

Анализ основан на данных, собранных при следующих условиях:

Дата проведения анализа безопасности:	12/01/2014	Длительность анализа:	2 недели
Отрасль экономики:	Страхование	Страна:	США
Размер компании:	2,500 сотрудников	Анализируемая сеть:	Внутренняя ЛВС
Версия шлюза безопасности:	R77	Режим анализа:	Зеркальный порт
Модули шлюза безопасности:	Контроль приложений (Application Control), Фильтрация URL (URL Filtering), Анти-бот (Anti-Bot), Анти-вирус (Anti-Virus), Предотвращение вторжений (IPS), Предотвращение утечки данных (DLP), Контроль идентификации (Identity Awareness), Эмуляция угроз (Threat Emulation), Контроль соответствия требованиям (Compliance).		
Устройство безопасности:	Шлюз безопасности Check Point 4800 Security Gateway		

Ниже приведена сводка полученных данных по обнаруженным событиям, относящимся к высокой и критической степеней риска безопасности:



УПРАВЛЕНИЕ ДОСТУПОМ И ЗАЩИТА ДАННЫХ:

- 30,670 событий с приложениями высокой степени риска
- 22 события потери данных



ПРЕДОТВРАЩЕНИЕ ВТОРЖЕНИЙ

- 9 событий, связанных с ботами
- 5 событий, связанных с вирусами
- 16 событий «нулевого дня»
- 18 Intrusions & Attacks Events



КОНЕЧНЫЕ УСТРОЙСТВА

- 893 конечных устройства были вовлечены в события высокого уровня риска



СООТВЕТСТВИЕ ТРЕБОВАНИЯМ

- 65% соответствия лучшим практикам Check Point
- 58% соответствия требованиям регуляторов



УПРАВЛЕНИЕ ДОСТУПОМ И ЗАЩИТА ДАННЫХ

БЕЗОПАСНОСТЬ WEB

Приложения и сайты высокой степени риска

На высших уровнях риска находились следующие веб-приложения и веб-сайты¹

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 Уровень риска 5 обозначает приложение, которое может обойти средства безопасности или скрыть идентификационные признаки (например, Tor, VTunnel). Уровень риска 4 обозначает приложение, которое может привести к утечке данных или к заражению вредоносным ПО незаметно для пользователя (например, File Sharing, P2P uTorrent или P2P Kazaa). Приложения удаленного администрирования могут быть легитимными в случаях, если они используются службой техподдержки или администраторами.

Приложения высокой степени риска, соответствующие политике безопасности организации

Приложения высокой степени риска – это приложения, которые могут обходить средства обеспечения безопасности, скрывать идентификационную информацию, быть причиной утечки данных или даже заражения вредоносным ПО незаметно для пользователя. В большинстве случаев использование таких приложений запрещено политикой безопасности организации. Однако, некоторые специальные приложения могут быть разрешены к использованию политикой безопасности. Ниже приведены приложения, обнаруженные в период проведения анализа, которые принадлежат к категории высокой степени риска, но разрешены в рамках политики безопасности организации.

Приложение	Политика безопасности организации
TeamViewer	Разрешено для использования группой поддержки для удаленной помощи заказчикам.
LogMeln	Разрешено для использования службой техподдержки для удаленной помощи сотрудникам

Описание приложений высокой степени риска

Следующая таблица содержит краткое описание обнаруженных событий и соответствующих им рисков безопасности или ведения бизнеса:

Приложение и его описание	Категория	Риск Приложения	События
Tor Приложение, разработанное для анонимизации онлайн активности. Клиентское ПО Tor посылает интернет-трафик через всемирную сеть серверов, предоставленных волонтерами для сокрытия местонахождения пользователя или факта использования Интернета от любых средств мониторинга сети или анализа трафика. Использование Tor существенно затрудняет отслеживание Интернет-активности пользователя, - такой, как: посещение веб-сайтов, записи онлайн, мгновенных сообщений и других форм коммуникации.	Анонимайзер	Критический	228
Ultrasurf Свободно распространяемый инструмент проксирования, предоставляющий пользователям возможность обходить МСЭ и ПО блокировки Интернет-контента.	Анонимайзер	Критический	51
VTunnel Свободно распространяемый CGI (Common Gateway Interface) прокси, маскирующий IP адрес, что позволяет пользователям анонимно устанавливать соединения и просматривать веб-сайты, а также обходить средства сетевой безопасности.	Анонимайзер	Критический	18
BitTorrent Протокол пирингового (P2P, peer-to-peer) обмена файлами. Является инструментом широкого распространения больших объемов данных. Существуют многочисленные варианты ПО, поддерживающие протокол BitTorrent, написанные на различных языках программирования и исполняемые на широком спектре вычислительных платформ. Приложения P2P могут приводить к утечке данных или заражению вредоносным ПО незаметно для пользователя.	P2P Обмен Файлами	Высокий	464
ZumoDrive Приложения для гибридного облачного хранения данных. Позволяет пользователю получать доступ к его музыкальным файлам, фотографиям и документам с компьютеров и мобильных телефонов. Предоставление разделяемого доступа в общедоступном облаке может приводить к утечке важной информации.	Хранение и обмен файлами	Высокий	148

Наиболее активные пользователи приложений высокой степени риска

Следующие пользователи были наиболее часто ассоциированы с событиями применения приложений высокого риска и использования Web:

Пользователи	События
Ginger Cash	12
Ivan Whitewash	9
Jim Josh	7
Bob Bash	5
Damien Dash	2

***Примечание:** Имена пользователей будут показываться в вышеприведенной таблице в случае, если активирован и настроен программный модуль Контроля идентификации Check Point Identity Awareness Software Blade.

ПОТЕРЯ ДАННЫХ

Данные Вашей компании являются одним из наиболее важных активов Вашей организации. Любая потеря данных, намеренная или ненамеренная, может нанести Вашей организации существенный ущерб. Ниже приведена информация, характеризующая события потери данных, которые наблюдались в течение анализируемого периода времени.

Наиболее частые события потери данных

Следующий список обобщает установленные события потери данных и показывает количество событий каждого типа.

Уровень важности	Данные	Категория	Число событий
Критический	Данные кредитных карт	Соответствие требованиям	5
Высокий	Бизнес-план	Бизнес-информация	6
	Финансовые отчеты	Финансовая информация	3
	Исходный код	Интеллектуальная собственность	2
	Сообщения из Outlook – конфиденциальные	Конфиденциальная информация	1
Средний	Файл с квитанцией заработной платы	Отдел кадров	4
	Номера социального страхования США	Персональная идентификационная информация	1

Файлы, наиболее часто пересылаемые вовне организации по протоколу HTTP

В следующей таблице приведены пересланные вовне организации файлы, которые могли содержать важные данные.

Хост	Тип данных	Имя файла	URL
192.168.75.26	Номера кредитных карт	customer orders.xlsx	www.ccvalidator.com
192.168.75.48	Финансовые отчеты	Q4 Report - draft2.docx	www.dropbox.com
192.168.125.28	Исходный код	new_feature.C	www.java-help.com
192.168.125.10	Имена заказчиков	Customer List.xlsx	www.linkedin.com
192.168.125.78	Медицинская информация, защищаемая согласно HIPAA	Medical File - Rachel Smith.pdf	www.healthforum.com

Файлы, наиболее часто пересылаемые вовне организации по протоколу SMTP

В следующей таблице приведены пересланные вовне организации файлы, которые могли содержать важные данные:

Получатель	Тип данных	Имя файла	Email Subject
bella@otherBiz.com	Номера кредитных карт	Customer Invoices.xlsx	FW: Invoices
betty@otherBiz.com	Бизнес-план	Q1 2015 Goals.pdf	RE: 2015 Plan
doreen@otherBiz.com	Имена сотрудников	employees.xls	company employees
zoe@otherBiz.com	Отчеты по продажам	Q4 sales summary.doc	RE: Q4 Sales. Confidential!
jordana@otherBiz.com	Корпоративные пресс-релизы	New Release - draft2.docx	FW: new release PR draft - do not forward!!

Наиболее частые события потери данных: распределение по отправителям

Эта таблица показывает распределение событий утечки данных в Вашей сети по отправителям сообщений электронной почты:

Отправитель	Количество событий
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

ПРЕДОТВРАЩЕНИЕ УГРОЗ

БОТЫ

Бот представляет из себя вредоносное ПО, вторгающееся в Ваш компьютер. Боты позволяют преступникам удаленно управлять компьютерными системами и исполнять неразрешенные действия незаметно для пользователей. Такие действия могут включать: кражу данных, распространение нежелательных сообщений электронной почты (спам), распространение вредоносного ПО, участие в атаках класса «отказ в обслуживании» и многое другое. Боты часто используются в качестве инструментов в направленных атаках, известных как Advanced Persistent Threat (APT). Ботнетом называется совокупность скомпрометированных (зараженных) таким образом компьютерных систем.

Следующая таблица показывает количество хостов, зараженных ботами, и их активность, обнаруженную в Вашей сети.

Хосты, зараженные ботами	8
Хосты с установленным ПО нежелательной рекламы (adware)	1
Хосты с обнаруженными событиями активности вредоносного ПО по протоколам SMTP и DNS	2

Вредоносная активность ботов

Описание	Количество обнаружений
Бот, связывающийся с центром управления	4
Бот, проверяющий соединение	2
Другие вредоносные действия, связанные с заражением ботом	1
Нежелательная активность, связанная с установленным рекламным ПО adware	1
Всего событий	8

Хосты, где наблюдались события высокого и критического уровней, связанные с бот-активностью

В ходе 3D анализа безопасности решение Check Point идентифицировало определенное число событий, связанных с вредоносным ПО, что указывало на активность ботов. Данная таблица содержит список хостов, подверженных событиям высокой степени риска:

Хост	Активность	Наименование угрозы	Ресурс
192.168.75.7	Связь с центром управления	Operator.Virus.Win32.Sality.d.dm	yavuztuncil.ya.funpic.de/images/logos.gif?f58891=16091281
10.10.2.32	Клиентский запрос DNS или DNS сервер, разрешающий имя сайта центра управления	Operator.Conficker.bhvl	zsgnmngn.net
192.168.75.22	Клиентский запрос DNS или DNS сервер, разрешающий имя сайта центра управления	Operator.Zeus.bt	zsexwd.com
172.23.25.35	Клиентский запрос DNS или DNS сервер, разрешающий имя сайта центра управления	Operator.BelittledCardigan.u	zwoppfqnj.com
10.100.2.33	Клиентский запрос DNS или DNS сервер, разрешающий имя сайта центра управления	Operator.APT1.cji	zychpupeydaq.biz
10.1.1.22	Клиентский запрос DNS или DNS сервер, разрешающий имя сайта центра управления	Operator.Virus.Win32.Sality.f.h	zykehk.com

Дополнительную информацию о вредоносном ПО, указанном в данном отчете, можно получить на сайте Check Point ThreatWiki, содержащем общедоступную базу данных компании Check Point по вредоносному ПО, по адресу: threatwiki.checkpoint.com.

ВИРУСЫ

Существуют различные каналы, по которым киберпреступники распространяют вредоносное ПО. Наиболее распространенным методом является мотивация пользователя открыть приложенный к сообщению электронной почты зараженный файл, загрузить зараженный файл или перейти по ссылке, ведущей на вредоносный сайт.

Следующие таблицы показывают обобщенную статистику Вашей сети по загрузкам вредоносного ПО и доступа к зараженным сайтам.

Загрузка вредоносного ПО

Описание	Количество
Количество хостов, загружавших вредоносное ПО	8
Число наблюдавшихся событий	9

Доступ к вредоносным сайтам

Описание	Количество
Количество хостов, осуществлявших доступ к сайтам, заведомо содержащим вредоносное ПО	5
Число наблюдавшихся событий	8

Хосты, где наблюдались события высокого и критического уровней, связанные с вирусной активностью

В ходе анализа безопасности, решение Check Point идентифицировало определенное число событий, связанных с вредоносным ПО, указывающих на загрузку вредоносных файлов или соединения с зараженными сайтами. Данная таблица содержит список хостов, подверженных событиям высокой степени риска:

Хост	Активность	Ресурс
192.168.75.78	Загрузка вредоносного файла/эксплоита	r.openx.net/set?pid=619cb264-acb9-5a18-89ed-c1503429c217&rtb=3105223559/basic.pdf
192.168.125.76	Загрузка вредоносного файла/эксплоита	lavilla.de/links.jpg
192.168.125.10	Доступ к сайту, заведомо содержащему вредоносное ПО	zoygsulaeli.com/img_cache.php
192.168.125.48	DNS сервер разрешает для клиента имя сайта, заведомо содержащего вредоносное ПО	zoygsulaeli.com

Дополнительную информацию о вредоносном ПО, указанном в данном отчете, можно получить на сайте Check Point ThreatWiki, содержащем общедоступную базу данных компании Check Point по вредоносному ПО, по адресу: threatwiki.checkpoint.com.

УГРОЗЫ «НУЛЕВОГО ДНЯ»

Киберугрозы становятся все более изощренными, перспективные угрозы часто включают в себя новые эксплоиты, распространяемые ежедневно, для которых нет существующей защиты. К таким эксплоитам относятся атаки «нулевого дня» на новые уязвимости и большое количество новых вариантов вредоносного ПО.

Этот раздел содержит статистику угроз «нулевого дня», обнаруженных в Вашей сети. Для получения детального отчета по отдельным событиям, связанным с вредоносным ПО, пожалуйста, свяжитесь с представителем Check Point, подготовившим данный отчет.

Всего сканировано файлов	169
---------------------------------	------------

События	Обнаружения	Вовлеченные Хосты
3 агрузка вредоносного ПО «нулевого дня» из Web	7	6
Вредоносное ПО «нулевого дня» послано электронной почтой (SMTP)	9	9

Наиболее часто загружаемое из Web вредоносное ПО «нулевого дня»

Файл	Вредоносная активность	Хост	Ресурс
0dd730ed4.pdf	Внезапный краш процесса	192.87.2.7	www.lostartofbeingadame.com/wpcontent/plugins/www.fotosupload.php
guide04d88.pdf	Вредоносная активность в файловой системе, вредоносная сетевая активность, вредоносная активность в Реестре (Registry), внезапное создание процесса, внезапное прекращение процесса	10.23.33.24	silurian.cn/modules/mod_cmsfix/fix.php

Вредоносное ПО «нулевого дня», наиболее часто посылаемое электронной почтой (SMTP)

Следующая таблица содержит статистику вредоносного ПО «нулевого дня», наиболее часто обнаруживаемого в сообщениях электронной почты, переданных по протоколу SMTP:

Файл	Отправитель	Получатель	Тема сообщения	Вредоносная активность
Notice231488.doc	asia@shippinggoods.com	logistics@mybiz.biz	Детали посылки	Вредоносное ПО создает другой процесс, вредоносное ПО создает подозрительные файлы Вредоносное ПО получает имя модуля Вредоносное ПО запускает себя в дополнительном процессе, вредоносное ПО подделывает историю браузера
invoiceBQW8OY.doc	No-Replay@shop.sip	jhon@mybiz.biz	Ваш счет	Вредоносное ПО влияет на другой процесс в системе, вредоносное ПО создает другой процесс Вредоносное ПО создает подозрительные файлы Вредоносное ПО создает процесс в подвешенном состоянии (используется для процесса выхода (escape)) Вредоносное ПО удаляет себя Вредоносное ПО получает имя модуля Вредоносное ПО исполняется в контексте другого процесса, вредоносное ПО порождает дочерний процесс Вредоносное ПО подделывает историю браузера
Summit_Agenda.doc	events@conferences.org	marketing@mybiz.biz	Программа следующего мероприятия	Вредоносное ПО создает другой процесс Вредоносное ПО создает подозрительные файлы Вредоносное ПО создает процесс в подвешенном состоянии (используется для процесса выхода (escape)) Вредоносное ПО удаляет себя Вредоносное ПО получает имя модуля Вредоносное ПО подделывает важные системные файлы

ВТОРЖЕНИЯ И АТАКИ

Наиболее частые события вторжений и атак

В рамках анализа безопасности, решение Check Point идентифицировало ряд событий, относящихся к категории предотвращения вторжений. Некоторые из них были отнесены к категории высокого риска. Следующая таблица показывает распределение этих событий по степени важности:

Уровень важности	Наименование события	Индекс по списку CVE*	Количество событий
Критический	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
Высокий	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) представляет собой каталог общеизвестных уязвимостей безопасности. Для получения дополнительной информации о конкретном событии предотвращения вторжений (IPS), осуществите запрос по индексу CVE ID на поисковой странице Национальной базы данных уязвимостей CVE.



БЕЗОПАСНОСТЬ КОНЕЧНЫХ СТАНЦИЙ














Этот раздел отчета содержит наблюдения, относящиеся к безопасности хостов в Вашей инфраструктуре. В нем приведены статистика наблюдений и подробная информация по каждому направлению безопасности. Раздел «Корректирующие действия» содержит набор рекомендаций по мерам, предпринимаемым в случае тех или иных событий.

Краткая статистика по безопасности конечных станций

Общее количество конечных станций, на которых выполняются приложения высокой степени риска	6
Общее количество конечных станций, вовлеченных в инциденты потери данных	19
Общее количество конечных станций, подвергнутых вторжениям и атакам	20
Общее количество конечных станций, вовлеченных в инциденты с вредоносным ПО	848

Рейтинг конечных станций, на которых выполняются приложения высокой степени риска

Следующая таблица содержит статистику по конечным станциям, на которых выполняются приложения высокой степени риска или имеющие доступ к веб-сайтам высокого риска:

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

Рейтинг конечных станций, подвергавшихся вторжениям и атакам

Следующая таблица содержит информацию о конечных станциях, в наибольшей степени подвергавшихся вторжениям и атакам:

Адрес источника	Адрес назначения	Уровень важности	Наименование события	Индекс по списку CVE
192.87.2.47	192.168.75.27	Критический	Microsoft SCCM Reflected Cross-site Scripting (MS12-062)	CVE-2012-2536
192.78.2.214	192.168.75.58	Критический	Joomla Unauthorized File Upload Remote Code Execution	-
192.84.2.220	192.168.75.58	Критический	Web Servers Malicious HTTP Header Directory Traversal	-
192.85.2.133	192.168.75.58	Критический	ImageMagick GIF Comment Processing Off-by-one Buffer Overflow (CVE-2013-4298)	CVE-2013-4298
192.116.2.151	192.168.75.58	Критический	Adobe Flash Player SWF File Buffer Overflow (APSB13-04)	CVE-2013-0633
192.195.2.88	192.168.75.60	Высокий	PHP php-cgi query string parameter code execution	CVE-2012-1823
192.87.2.211	192.168.86.3	Высокий	Oracle database server CREATE_TABLES SQL injection	CVE-2007-3890

Рейтинг конечных станций, вовлеченных в инциденты потери данных

Следующая таблица содержит информацию о конечных станциях, в наибольшей степени вовлеченных в инциденты потери данных:

Конечная станция	Количество событий	Отправленные данные
192.168.125.36	4	Номера кредитных карт
	1	Бизнес-план
192.168.75.0	5	Финансовые отчеты
192.168.125.0	4	Исходный код
192.168.86.47	4	Сообщения из Outlook –конфиденциальные
192.168.86.38	2	Номера социального страхования США

Рейтинг конечных станций, вовлеченных в инциденты с вредоносным ПО

Следующая таблица содержит информацию о конечных станциях, в наибольшей степени вовлеченных в инциденты, связанные с вредоносным ПО:

Хост	Наименование угрозы	Активность вредоносного ПО
192.168.86.8	Operator.Virus.Win32.Sality.f.h	Клиентский запрос DNS или DNS сервер, разрешающий имя сайта центра управления
192.168.75.0	Operator.APT1.cji	Клиентский запрос DNS или DNS сервер, разрешающий имя сайта центра управления
192.168.75.3	Operator.Virus.Win32.Sality.d.dm	Связь с центром управления
192.168.75.7	REP.yjjde	Доступ к сайту, заведомо содержащему вредоносное ПО
192.168.75.10	RogueSoftware.Hack_Style_RAT.pbco	Связь с центром управления
192.168.75.13	Trojan.Win32.Agent.aeeyr.cj	Загрузка вредоносного файла/эксплоита








АНАЛИЗ СООТВЕТСТВИЯ ТРЕБОВАНИЯМ БЕЗОПАСНОСТИ

Этот раздел содержит детальный анализ политик безопасности Вашего текущего решения сетевой безопасности Check Point.

Анализ проводился с применением модуля Check Point Compliance Software Blade, использующего расширенную библиотеку, включающую сотни примеров лучших практик и рекомендации по улучшению сетевой безопасности Вашей организации.

Соответствие политике безопасности

Модуль Compliance Software Blade сканировал настройки Вашей системы управления безопасностью, шлюза и установленных модулей Software Blades. Результаты затем были сопоставлены с примерами из лучших практик. Из общего количества 102 конфигураций было выявлено полное соответствие рекомендованным лучшим практикам в 67 случаях, в то время как 35 конфигураций не соответствовали практикам или отсутствовали. Таким образом, уровень соответствия составил 65%.

	65%	Соответствие лучшим практикам, рекомендованным Check Point
	102	Конфигурации проанализировано
	67	Конфигураций полностью соответствуют
	35	Конфигураций не соответствуют или отсутствуют
	12	Шлюзов безопасности были включены в мониторинг

Обзор соответствия требованиям регуляторов

Следующая таблица показывает уровень соответствия Вашей сети требованиям регулирующих организаций. Состояние определялось путем анализа конфигураций шлюзов безопасности Check Point и настроек модулей Software Blades, а также их сопоставления с требованиями регуляторов.

Регулирующий стандарт	Количество требований	Количество лучших практик безопасности	Статус соответствия
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%
MASTRM	25	102	77%
SOX	15	102	66%
FIPS 200	25	71	87%

Соответствие лучшим практикам настроек модулей Security Software Blades

Следующая таблица показывает общий уровень безопасности каждого модуля Software Blade.

Для каждого модуля Software Blade компания Check Point рекомендует определенный набор лучших практик. Уровень 100% означает, что для данного модуля были сконфигурированы все лучшие практики. Уровень ниже 100% обозначает конфигурации, не соответствующие лучшим практикам, и, таким образом, представляющие слабые звенья в Вашем сетевом окружении.

Модуль Security Software Blade	Число лучших практик безопасности	Уровень безопасности
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%

Соответствие лучшим практикам безопасности

В следующей таблице собраны наиболее важные примеры лучших практик, которые либо отсутствовали, либо не были полностью сконфигурированы.

Модуль Blade	Идентификатор	Название	Статус
МСЭ (Firewall)	FW101	Проверка, определено ли правило "Очистки" (Clean up Rule) в наборе правил МСЭ	0%
МСЭ (Firewall)	FW102	Проверка активации функции антиспуфинга на каждом Шлюзе	0%
МСЭ (Firewall)	FW103	Проверка установки функции антиспуфинга в режим "Предотвращать" (Prevent) на каждом Шлюзе	0%
МСЭ (Firewall)	FW105	Проверка того, что каждое правило МСЭ имеет определенные настройки отслеживания (Track).	0%
МСЭ (Firewall)	FW130	Проверка, определено ли правило "Скрытого режима" (Stealth Rule) в наборе правил МСЭ	0%
МСЭ (Firewall)	FW152	Проверка, определено ли имя у каждого правила МСЭ	0%
МСЭ (Firewall)	FW153	Проверка, определено ли поле комментария у каждого правила МСЭ	0%
МСЭ (Firewall)	FW107	Проверка наличия определенного дополнительного сервера журналирования (log server) для каждого МСЭ для хранения журналов МСЭ	0%
МСЭ (Firewall)	FW116	Проверка, активна ли настройка NAT/PAT на МСЭ	87%
МСЭ (Firewall)	FW146	Проверка того, что правило "Any Any Асцепт" не определено в наборе правил МСЭ	0%
МСЭ (Firewall)	FW159	Проверка, определена ли опция "Блокировать учетную запись администратора после" ("Lockout Administrator's account after")	0%
МСЭ (Firewall)	FW160	Проверка наличия блокировки учетной записи администратора после трех неудачных попыток входа	0%
МСЭ (Firewall)	FW161	Проверка, выбрана ли опция "Деблокировать учетную запись администратора после" "Unlock Administrator's account after")	0%
МСЭ (Firewall)	FW162	Проверка наличия деблокировки учетных записей администраторов после 30 минут	0%
МСЭ (Firewall)	FW163	Проверка того, выводится ли детальное сообщение для заблокированных администраторов	0%



АНАЛИЗ ПОЛОСЫ ПРОПУСКАНИЯ

Данный раздел содержит краткое описание результатов анализа использования полосы пропускания и профиля использования Web в Вашей организации в период проведения исследования.

Рейтинг использования полосы пропускания по приложениям и вебсайтам

Следующая таблица представляет рейтинг веб-приложений и веб-сайтов относительно использованной ими полосы пропускания:

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

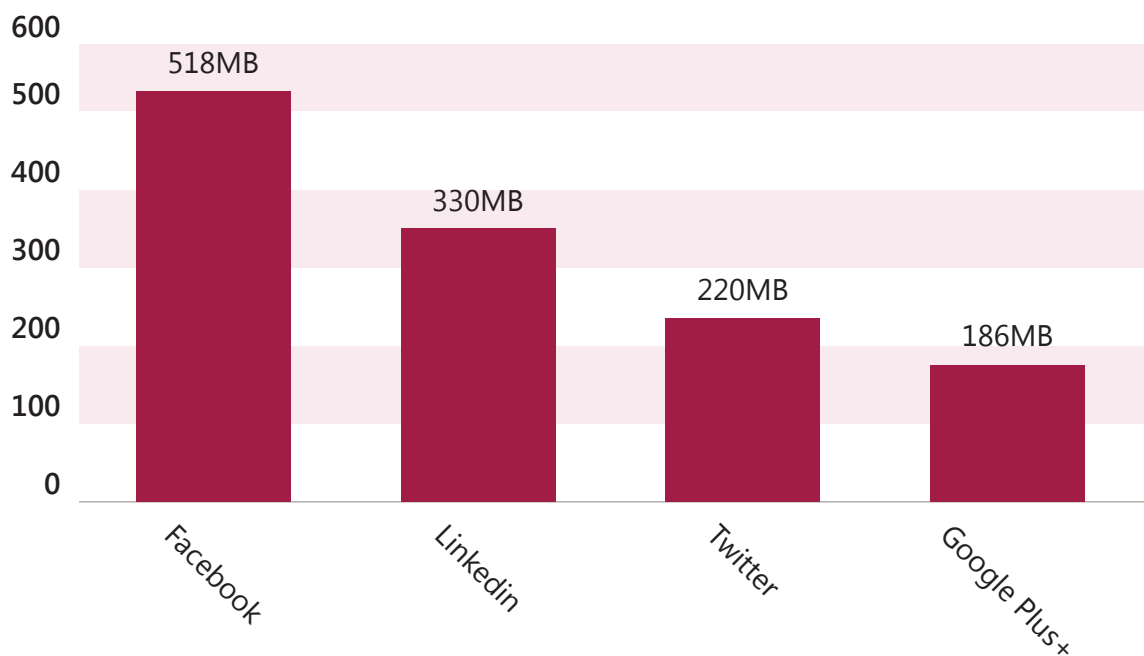
Рейтинг категорий Web

Следующая таблица содержит рейтинг категорий веб-ресурсов по количеству запросов (hit), соответствующих просмотру Интернет сотрудниками компании:

Категория	Количество запросов	% от общего количества запросов
Социальные сети	113	31.65%
Web-почта	42	11.76%
Потоковое видео	36	10.08%
Поисковые системы/Порталы	35	9.80%
Мультимедиа	29	8.12%
Модули (plug-in) браузеров	25	7.00%
Бизнес-приложения	15	4.20%
Разделенный доступ к медиа-файлам (Media Sharing)	13	3.64%
Сетевые утилиты	9	2.52%
Другое	40	11.20%
Total	357	100%

Полоса пропускания для социальных сетей (в Мб)

Использование социальных сетей становится общей практикой как в домашних условиях, так и на работе. Многие компании используют технологии социальных сетей для своей маркетинговой активности, продаж, а также рекрутинговых программ. В ходе анализа была получена представленная ниже статистика использования полосы пропускания социальной сетевой активностью, что полностью соответствует общим тенденциям на рынке:





РЕКОМЕНДАЦИИ ПО КОРРЕКТИРУЮЩИМ ДЕЙСТВИЯМ

РЕКОМЕНДАЦИИ ПО УПРАВЛЕНИЮ ДОСТУПОМ И ЗАЩИТЕ ДАННЫХ

В ходе подготовки данного отчета были выявлены события, происходившие в различных областях информационной безопасности и на различных уровнях критичности. Нижеприведенная таблица представляет обзор наиболее критичных инцидентов и предлагает пути по устранению связанных с ними рисков. Компания Check Point рекомендует различные методы для устранения этих угроз и проблем. Для каждого события указаны соответствующие меры защиты, а также названия модулей Software Blade, где реализованы эти механизмы защиты.

Рекомендации по корректирующим действиям в области Web безопасности

Приложение/Сайт	Риск приложения	Количество событий	Корректирующие действия
Tor	Критический	228	В модулях Software Blades Контроля приложений (Application Control) и Фильтрации URL (URL Filtering) Вы можете активировать, отслеживать и предотвращать использование перечисленных приложений и веб-сайтов. Вы можете также определять детальную политику для разрешения конкретных приложений только для определенных групп пользователей.
Ultrasurf	Критический	51	
Vtunnel	Критический	18	
BitTorrent	Высокий	464	Используйте функцию проверки пользователя UserCheck для:
ZumoDrive	Высокий	148	<ul style="list-style-type: none">• Информирования пользователей о политиках организации в области просмотра Web и использования приложений.• Настройки мгновенного оповещения пользователей при осуществлении ими действий, нарушающих политику безопасности.

Пройдите по ссылкам для получения дополнительной информации о модулях шлюза безопасности Check Point [Application Control](#) и [URL Filtering](#) Software Blades.

Рекомендации по корректирующим действиям в области защиты от потери данных

Severity	Data	Events	Remediation Steps
Критический	Номера кредитных карт	14	<p>Для корректирующих действий в связи с замеченными событиями активируйте модуль Предотвращения потери данных DLP Software Blade. Сконфигурируйте политику предотвращения потери данных на основании обнаруженных типов потери данных и выберите действие «Обнаруживать/Предотвращать/Спрашивать пользователя/и т.д.» (Detect/Prevent/Ask User/etc.). Если Вы считаете, что потерянная информация значима, необходимо выбрать «Предотвращать».</p>
Высокий	Бизнес-план	1	
	Финансовые отчеты	3	
	Исходный код	12	
	Сообщения из Outlook – конфиденциальные	147	
Средний	Файл с квитанцией заработной платы	25	<p>Используйте функцию UserCheck для:</p> <ul style="list-style-type: none"> • Информирования пользователей о политиках организации в области просмотра Web и использования приложений. • Настройки мгновенного оповещения пользователей при осуществлении ими действий, нарушающих политику безопасности.
	Номера социального страхования	15	

Пройдите по ссылке для получения дополнительной информации о модуле шлюза безопасности Check Point [DLP software blade](#).

РЕКОМЕНДАЦИИ ПО ПРЕДОТВРАЩЕНИЮ УГРОЗ

Рекомендации по уменьшению угроз, связанных с вредоносным ПО

Вредоносное ПО	Уровень важности	Количество событий	Корректирующие действия
REP.yjjde	Критический	36	Активируйте модуль Check Point Anti-Bot Software Blade для обнаружения машин, зараженных ботами и предотвращения ущерба от ботов. Активируйте модуль Check Point Anti-Virus Software Blade для предотвращения загрузки вредоносного ПО.
Operator.Virus.Win32.Sality.d.dm	Критический	28	
Operator.Conficker.bhvl	Высокий	27	Активируйте модуль Check Point Threat Emulation Software Blade для защиты от новых и неоткрытых угроз, а также от вредоносного ПО.
Operator.Zeus.bt	Высокий	11	Для корректирующих действий по отношению к зараженной машине сначала осуществите поиск информации об обнаруженном вредоносном ПО в каталоге Check Point ThreatWiki. Затем следуйте рекомендациям, указанным на веб-странице Malware Remediation Steps.
Operator.BelittledCardigan.u	Высокий	8	

Пройдите по ссылкам для получения дополнительной информации о модулях шлюза безопасности Check Point [Anti-Bot](#), [Anti-Virus](#) and [Threat Emulation](#) Software Blades.

Рекомендации по корректирующим действиям, связанным с вторжениями и атаками

Угроза	Уровень важности	Количество событий	Remediation Steps
Microsoft SCCM Reflected Cross-site Scripting (MS12-062)	Критический	15	На модуле Check Point IPS Software Blade активируйте следующую защиту: Microsoft SCCM Reflected Cross-site Scripting (MS12-062)
Joomla Unauthorized File Upload Remote Code Execution	Критический	13	На модуле Check Point IPS Software Blade активируйте следующую защиту: Joomla Unauthorized File Upload Remote Code Execution
Microsoft Active Directory LSASS Recursive Stack Overflow [MS09-066]	Высокий	4	На модуле Check Point IPS Software Blade активируйте следующую защиту: Microsoft Active Directory LSASS Recursive Stack Overflow [MS09-066]

Кликните по ссылке для получения дополнительной информации о модуле Шлюза безопасности Check Point [IPS Software Blade](#).

РЕКОМЕНДАЦИИ ПО КОРРЕКЦИИ БЕЗОПАСНОСТИ КОНЕЧНЫХ СТАНЦИЙ

В этом разделе рассмотрены события, относящиеся к безопасности конечных станций и происходившие в различных областях информационной безопасности и на различных уровнях критичности. Нижеприведенная таблица представляет обзор наиболее критичных инцидентов и предлагает пути по устранению связанных с ними рисков. Компания Check Point рекомендует различные методы для устранения этих угроз и проблем. Для каждого события указаны соответствующие меры защиты, а также название модулей Endpoint Software Blade, где реализованы эти механизмы защиты.

Рекомендации по коррекции безопасности конечных станций при событиях, связанных с безопасностью Web

Хост	Приложение/ Сайт	Риск	Корректирующие действия
192.168.75.36	Tor	Критический	Check Point Endpoint Security контролирует использование приложений и сайтов даже в случаях, когда конечная станция находится вне сети организации и без средств сетевой безопасности. Используйте модуль Check Point Program Control Software Blade чтобы дать возможность только разрешенным программам исполняться на конечных устройствах, а также для принудительного завершения неразрешенных или не доверенных программ.
192.168.75.71	Ultrasurf	Критический	Используйте модуль WebCheck Endpoint Software Blade для защиты предприятия от угроз со стороны Web, таких как загрузки “на проходе” (drive-by), фишинговых сайтов и атак “нулевого дня”.
192.168.86.0	VTunnel	Критический	Используйте модуль Check Point Compliance Check Software Blade для того, чтобы удостовериться, что определенная программа исполняется на конечном устройстве и ограничить, если это необходимо, ее доступ к сети.
192.168.86.19	BitTorrent	Высокий	Контролируйте входящий и исходящий трафик с помощью модуля Endpoint Firewall Software Blade для ограничения доступа только по определенным портам или к определенным сервисам.
192.168.86.30	ZumoDrive	Высокий	Используйте функцию UserCheck для: <ul style="list-style-type: none"> • Информирования пользователей о политиках организации в области просмотра Web и использования приложений. • Настройки мгновенного оповещения пользователей при осуществлении ими действий, нарушающих политику безопасности.

Пройдите по ссылкам для получения дополнительной информации о модулях Check Point Endpoint Security Software Blades:

- [Program Control](#) Endpoint Security Software Blade
- [WebCheck](#) Endpoint Security Software Blade
- [Compliance Check](#) Endpoint Security Software Blade
- [Firewall](#) Endpoint Security Software Blade

Рекомендации по коррекции безопасности конечных станций при событиях, связанных с вторжениями и атаками

Адрес источника	Адрес назначения	Наименование события	Корректирующие действия
192.87.2.47	192.168.75.27	Microsoft SCCM Reflected Cross-site Scripting (MS12-062)	<p>Используйте модуль Endpoint Compliance Software Blade чтобы удостовериться, что все конечные станции в Вашей сети имеют актуальные последние версии обновлений безопасности (security patches and updates).</p> <p>Модуль Endpoint Compliance Software Blade будет обеспечивать безопасность конечных станций при работе вне сети организации или без средств сетевой защиты (например, при работе дома или в командировках).</p>
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	

Пройдите по ссылкам для получения дополнительной информации о следующих модулях **Check Point Endpoint Security Software Blades**:

- [Firewall](#) Endpoint Security Software Blade
- [Compliance Check](#) Endpoint Security Software Blade

Рекомендации по коррекции безопасности конечных станций при событиях, связанных с потерей данных

Хост	Тип данных	Корректирующие действия
192.168.75.0	Номера кредитных карт	Используйте модуль шифрования дисков Check Point Full Disk Encryption Software Blade для защиты важной информации, хранящейся на жестких дисках конечных станций, включая пользовательские данные, файлы операционной системы, временные и удаленные файлы и для защиты от неавторизованного доступа при утере или краже ноутбуков.
192.168.86.47	Бизнес-план	Используйте модуль шифрования дисков Check Point Media Encryption Software Blade для шифрования важной информации, хранящейся на съемных устройствах, а также индивидуального отслеживания и управления съемных устройств.
192.168.125.0	Исходный код	Используя модуль Check Point Document Security Software Blade , Вы можете предоставлять доступ к важной информации только авторизованным сотрудникам.
192.168.125.36	Файл с квитанцией заработной платы	Используйте функцию UserCheck для: <ul style="list-style-type: none"> • Информирования пользователей о политиках организации в области просмотра Web и использования приложений. • Настройки мгновенного оповещения пользователей, при осуществлении ими действий, нарушающих политику безопасности.

Пройдите по ссылкам для получения дополнительной информации о следующих модулях **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

Рекомендации по коррекции безопасности конечных станций при событиях, связанных с вредоносным ПО

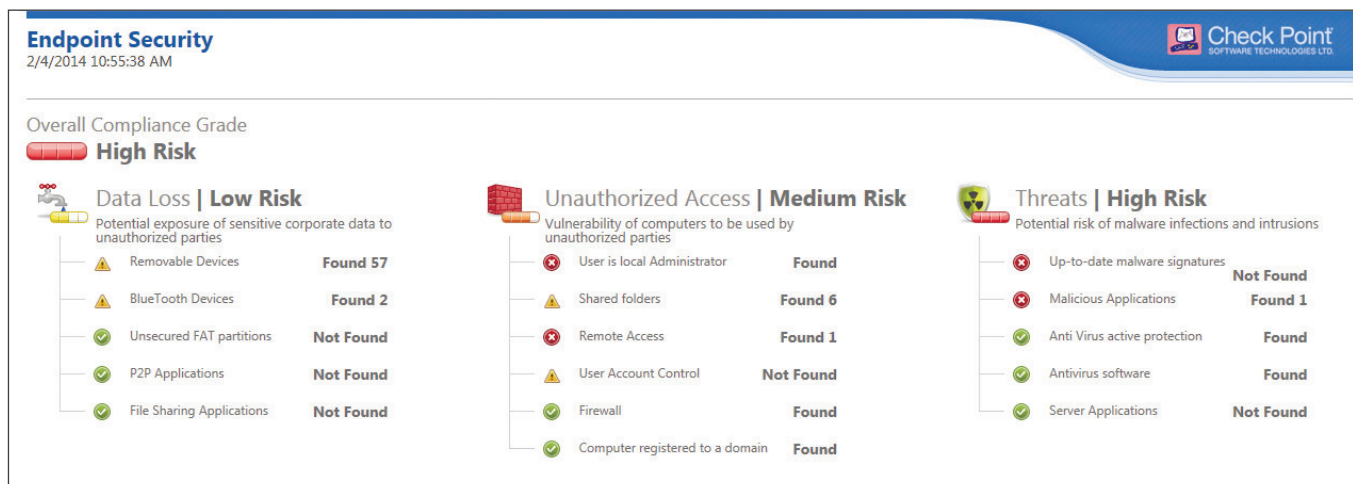
Хост	Уровень важности	Корректирующие действия
192.53.2.161	Критический	Используйте модуль Check Point Endpoint Anti-Malware Software Blade для обнаружения и предотвращения заражения конечных станций вредоносным ПО, вирусами, считывателями клавиатуры, троянскими программами и рут-китами.
192.57.2.32	Критический	Модуль Check Point Endpoint Anti-Malware Software Blade предохраняет конечные устройства предприятия даже в случае их нахождения вне сети организации или без средств обеспечения сетевой безопасности (например, при работе из дома или в командировке).
192.57.2.209	Критический	Используйте модуль Endpoint Compliance Software Blade для обеспечения последних обновлений безопасности на конечных станциях и их соответствия политике безопасности организации. Для начала процесса корректирующих действий на зараженной машине, найдите обнаруженное вредоносное ПО на сайте Check Point ThreatWiki , чтобы получить дополнительную информацию по корректирующим действиям в связи с конкретным вредоносным ПО. Эта информация может помочь Вам лучше понять механизм заражения и сопутствующие риски.
192.59.2.27	Критический	
192.59.2.79	Критический	Используйте функцию UserCheck для информирования пользователей о политиках организации в области просмотра Web и использования приложений.

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

Получение подробного аналитического отчета по безопасности конечных станций

Для получения подробного отчета о состоянии безопасности Ваших конечных станций и потенциальных рисках запустите «Аналитический отчет по безопасности конечных станций» (Endpoint Security analysis report) или обратитесь к Вашему локальному представителю компании Check Point.



РЕКОМЕНДАЦИИ ПО КОРРЕКЦИИ СООТВЕТСТВИЯ ТРЕБОВАНИЯМ

Этот отчет показывает, какие из конфигураций безопасности среди модулей Check Point Software Blades требуют дополнительного внимания. Нижеприведенная таблица показывает некоторые из настроек, требующих внимания, и дает указания по их улучшению.

Risk	Remediation Steps	Relevant Objects
Высокий	Создать новое или модифицировать существующее правило Stealth Rule в соответствующих пакетах политик, согласно следующему определению: Source = Any ; Destination = GW's ; Service = Any ; Action = Drop ; Install On = Policy Target ; Time = Any.	Пакет политик A (Policy Package A)
Высокий	Создать новое или модифицировать существующее правило Clean-up-Rule в соответствующих пакетах политик, согласно следующему определению: Source = Any ; Destination = Any ; VPN = Any Traffic ; Service = Any ; Action = Drop ; Track = Log ; Install On = Policy Targets ; Time = Any ; Обратить внимание, что это правило должно находиться в последней строке Набора Правил МСЭ (Firewall Rule Base).	Пакет политик B (Policy Package B)
Высокий	Активировать автоматическую защиту обновлений на модуле предотвращения вторжений IPS Blade	Система предотвращения вторжений корпоративного шлюза безопасности (IPS Gateway Corporate Gateway)
Высокий	Создать новую или модифицировать существующую политику на модуле контроля приложений Application Control Blade таким образом, чтобы приложения или вебсайты с критическим уровнем риска блокировались.	Пакет политик A (Policy Package A)
Высокий	Изменить таймаут аутентификации (Authentication Timeout) в глобальных настройках так, чтобы его значение было в диапазоне 20-120 минут.	Глобальные настройки (Global Properties)
Высокий	Определить настройки отслеживания (Track) во всех правилах МСЭ по всем пакетам политик.	<ul style="list-style-type: none"> — Пакет политик A (Policy Package A) Правило номер 18 Правило номер 35 Правило номер 64 — Пакет политик B (Policy Package B) Правило номер 11 Правило номер 23 Правило номер 88



SOFTWARE-DEFINED PROTECTION

В современном мире с его высокопроизводительными ИТ-инфраструктурами и сетями, где уже не существует понятия периметра и угрозы становятся все более изощренными, мы должны определить правильное направление защиты предприятий от постоянно меняющегося спектра угроз.

Несмотря на широкое распространение точечных продуктов безопасности, они остаются по своей природе более реактивными и тактическими решениями, нежели архитектурно-ориентированными. Современные корпорации нуждаются в единой архитектуре, сочетающей в себе высокую производительность сетевых устройств безопасности с проактивными средствами защиты в реальном времени.

Для проактивной защиты организаций требуется новая парадигма.

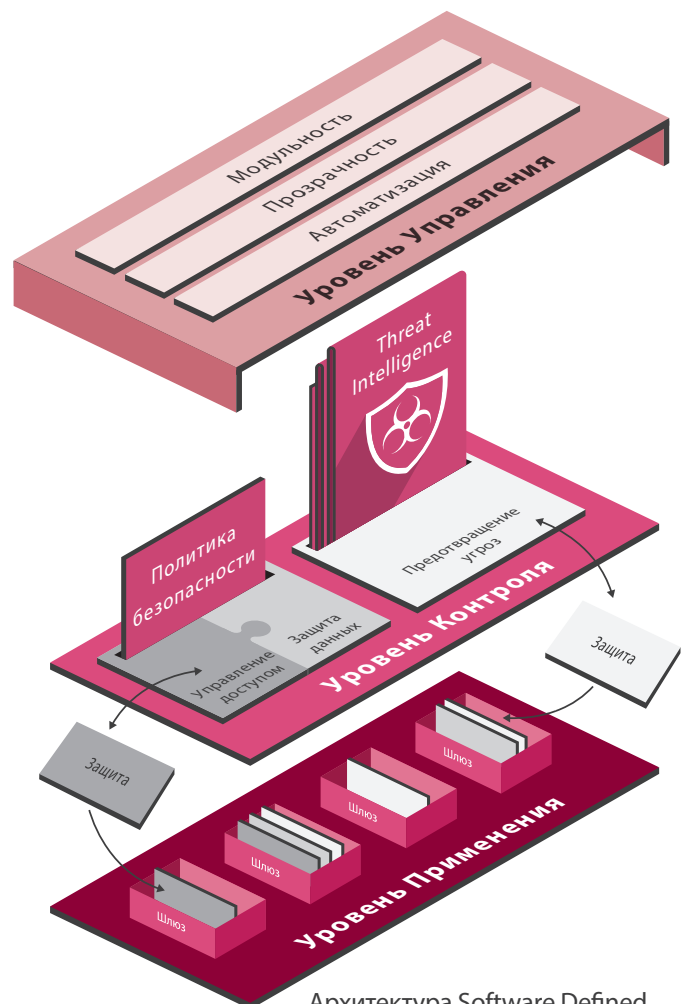
Software Defined Protection¹ представляет собой новую методологию и прагматичную архитектуру безопасности. Она предлагает модульную, гибко реагирующую и, что наиболее важно, – БЕЗОПАСНУЮ инфраструктуру.

Архитектура такого типа призвана обеспечить защиту организации любого масштаба и местоположения: сети головных офисов и филиалов, смартфонов или мобильных устройств путешествующих сотрудников, или при использовании облачных ресурсов.

Средства защиты должны автоматически адаптироваться к любому спектру угроз без необходимости применения администраторами безопасности многочисленных инструкций и рекомендаций в ручном режиме. Эти средства должны органически интегрироваться в большие ИТ-системы, и их архитектура должна предоставлять оборонительный потенциал, использующий внутренние и внешние источники информации.

Архитектура Software Defined Protection (SDP) делит инфраструктуру безопасности на три взаимосвязанных слоя:

- **Уровень Применения (Enforcement Layer)** основан на физических, виртуальных или хостовых точках применения политик безопасности, осуществляет сегментацию сети и исполнение логики защиты в высокопроизводительных средах.
- **Уровень Контроля (Control Layer)** анализирует различные источники информации об угрозах и создает защитные механизмы и политики, которые будут исполняться на Уровне Применения.
- **Уровень Управления (Management Layer)** – управляет инфраструктурой и обеспечивает высокий уровень скорости реагирования для всей архитектуры.



Архитектура Software Defined Protection (SDP)

¹ Программно-определяемая защита

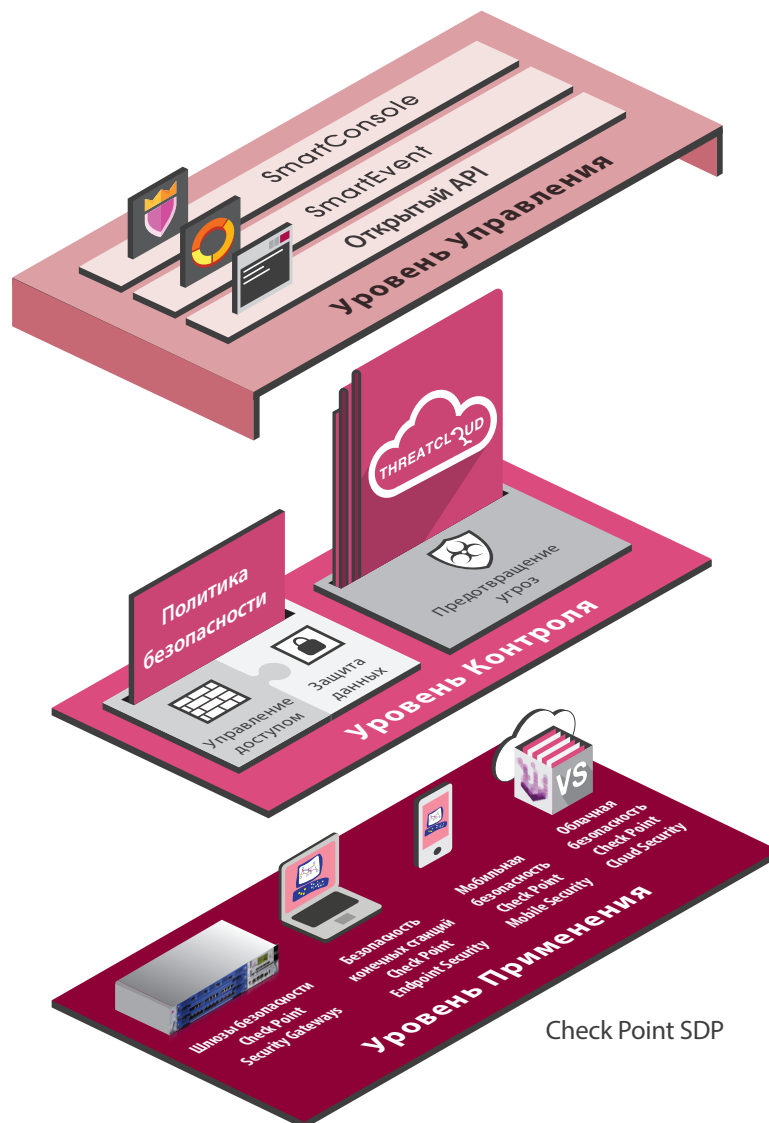
Комбинируя высокопроизводительный Уровень Применения с быстро перестраиваемым динамическим программным Уровнем Контроля, архитектура SDP обеспечивает не только надежность в работе, но и возможность проактивно предотвращать инциденты безопасности при быстро меняющемся спектре угроз.

Созданная на перспективу, архитектура SDP поддерживает традиционные требования сетевой безопасности и контроля доступа, равно как и механизмы защиты от угроз, необходимых для современного предприятия, включая такие новые технологии, как: мобильные вычисления и программно-определяемые сети (SDN, Software-defined Network).

CHECK POINT SOFTWARE-DEFINED PROTECTION

Компания Check Point предлагает полный спектр компонентов для реализации всей архитектуры SDP с наилучшими характеристиками безопасности и управления.

Программно-определяемые средства защиты компании Check Point обеспечивают необходимую гибкость для того, чтобы противостоять новым угрозам и соответствовать требованиям новейших технологий. Наши решения создают новые механизмы защиты от известных и неизвестных угроз, и проактивно распространяют информацию о них в облаке. Применение решений Check Point, основанных на новой архитектуре безопасности, позволяет предприятиям с уверенностью внедрять новейшие информационные системы.





УРОВЕНЬ ПРИМЕНЕНИЯ CHECK POINT SDP

Для обеспечения безопасности каждого сегмента компания Check Point предлагает широкий спектр точек применения политик безопасности. Это и высокопроизводительные устройства сетевой безопасности, и виртуальные шлюзы, программное обеспечение для конечных станций и приложения для мобильных устройств. Компания Check Point предоставляет предприятию все «строительные блоки», необходимые для построения сегментированных, консолидированных и безопасных систем и сетей.



УРОВЕНЬ КОНТРОЛЯ CHECK POINT SDP

Уровень Управления Check Point SDP основан на архитектуре программных модулей Check Point Software Blade Architecture, предоставляющей пользователям гибкие и эффективные решения безопасности, в точности отвечающие их потребностям. Наличие широкого выбора из более 20 программных модулей и модульный характер архитектуры Software Blades дает пользователям возможность выстроить адекватное решение в каждой точке применения политик и расширять инфраструктуру безопасности по мере необходимости.

Предотвращение угроз нового поколения

Компания Check Point позволяет эффективно противостоять широкому спектру известных и неизвестных угроз. Решение Check Point по предотвращению угроз Check Point threat Prevention включает в себя: Интегрированную Систему предотвращения вторжений (IPS), Сетевой Антивирус (Anti-Virus), Эмулятор угроз (Threat Emulation) и систему Анти-бот (Anti-Bot). Компания Check Point также создала уникальную облачную систему анализа большого объема информации в целях выявления угроз и создания методов защиты Check Point ThreatCloud™. Check Point ThreatCloud создает коллаборативную среду для борьбы с киберпреступностью и проводит анализ угроз в реальном времени с целью выработки настроек безопасности для Уровня Управления.

Защита данных и МСЭ нового поколения

Управление доступом компании Check Point базируется на нашем МСЭ нового поколения, комбинированном с многочисленными модулями Software Blades. Это позволяет реализовывать унифицированную контекстуальную политику безопасности, основанную на МСЭ нового поколения и VPN, использовании идентификационной информации пользователей, контроле приложений, использовании информации о данных или контенте.

Защита данных нового поколения

Защита данных нового поколения от компании Check Point отличается от традиционных решений использованием информации о характере данных. Она включает в себя модуль Предотвращения потери данных (Data Loss Prevention, DLP) Software Blade, выполняющий инспекцию контента и сравнение его с содержимым файлов, хранящихся в репозитории компании. Дополнительно компания Check Point предоставляет решение для защиты данных, хранящихся на носителях, с помощью технологии шифрования. Эти технологии могут быть реализованы в любой точке применения политик для защиты важных и конфиденциальных документов от переноса на съемные носители или доступа к ним неавторизованных пользователей.



УРОВЕНЬ УПРАВЛЕНИЯ CHECK POINT SDP

Все средства защиты и точки применения политик Check Point управляются с помощью единой унифицированной консоли управления безопасностью. Система управления безопасностью Check Point имеет высокую степень масштабируемости и дает возможность управлять десятками миллионов объектов, сохраняя сверхбыстрое время отклика пользовательского интерфейса.

Модульная система управления Check Point с многоуровневыми политиками

Система управления безопасностью Check Point поддерживает сегментацию предприятия, позволяя администратору определять политики безопасности для каждого сегмента, сохраняя разделение полномочий в соответствии с новой концепцией уровней и подуровней (Layers and Sub Layers). Политики могут определяться в каждом сегменте. Политики управления доступом могут быть определены с использованием отдельных уровней, которые могут назначаться разным администраторам. Несколько администраторов имеют возможность работать над одной и той же политикой одновременно.

Автоматизация и интеграция

Система управления безопасностью Check Point предоставляет интерфейсы командной строки (CLI) и программный интерфейс веб-сервисов (Web Services API), позволяющие интегрироваться с другими системами, - такими, как: системы управления сетями, CRM, системы сопровождения запросов на поддержку, системы управления идентификационной информацией или системы управления облачными решениями.

Обеспечение прозрачности с помощью системы Check Point SmartEvent

Система Check Point SmartEvent выполняет анализ больших объемов данных и проводит корреляцию событий в реальном времени. Это дает возможность получать консолидированную и коррелированную картину инцидента на основе информации из различных источников. Анализ события безопасности предоставляет результаты в виде индикаторов угроз, которые могут быть переданы в систему ThreatCloud для блокировки угроз в реальном времени.



Управление событиями с помощью системы Check Point SmartView

Дополнительную информацию об архитектуре Check Point Software Defined Protection и о том, как она может помочь Вам поддерживать эффективной инфраструктуру безопасности в современном быстроменяющемся мире угроз, можно получить, посетив сайт www.checkpoint.com/securitycheckup.



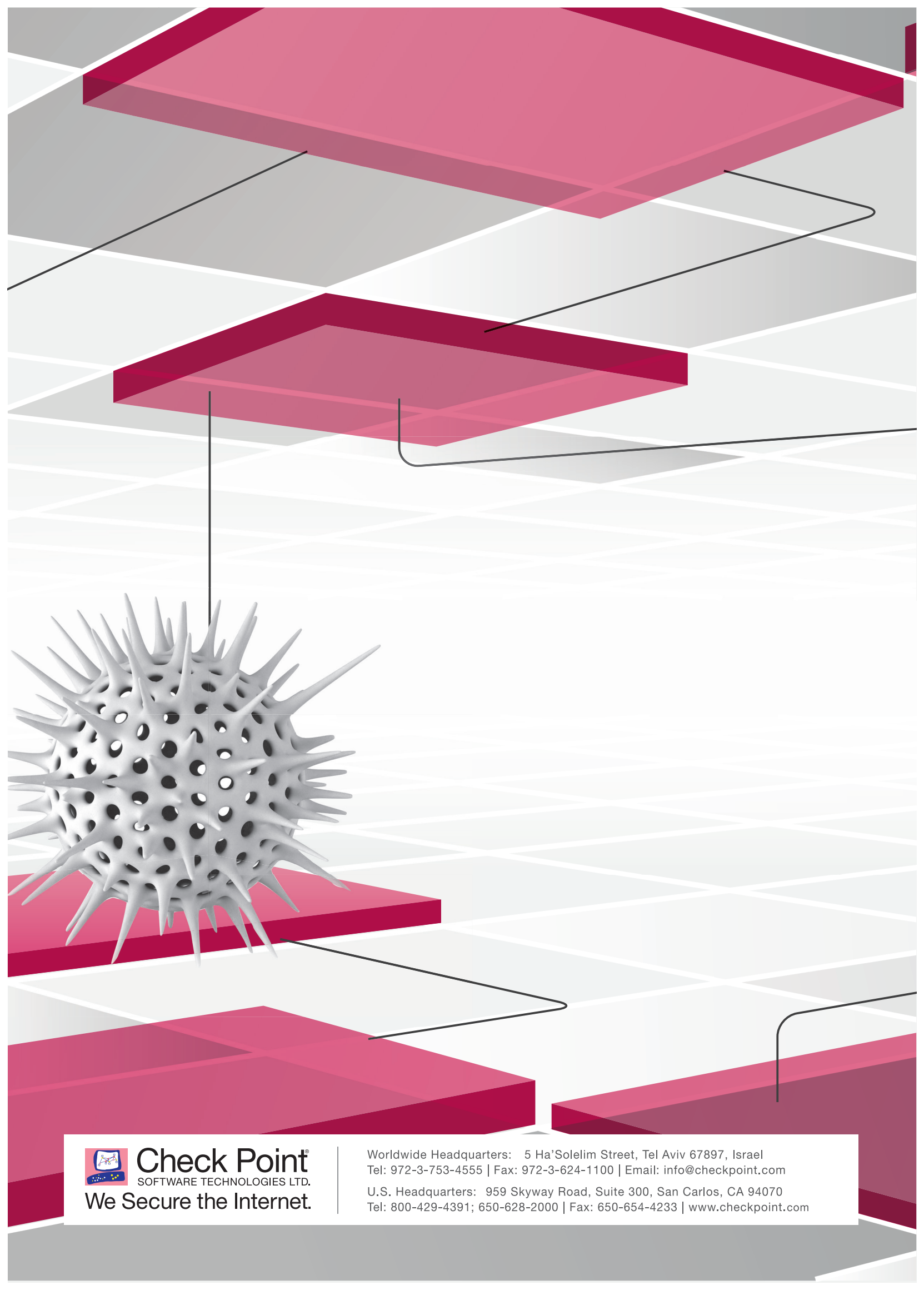
О КОМПАНИИ CHECK POINT SOFTWARE TECHNOLOGIES

Миссией компании Check Point Software Technologies Ltd. (www.checkpoint.com) является обеспечение безопасности в сети Интернет. Компания Check Point была основана в 1993 году и с тех пор разрабатывает технологии для обеспечения безопасности передачи данных и транзакций через сеть Internet для предприятий и частных клиентов.

Check Point был первой компанией, представившей на рынок межсетевой экран FireWall-1 с патентованной технологией Stateful Inspection. Check Point расширила свои ИТ инновации, разработав архитектуру программных модулей Software Blade Architecture. Эта динамическая архитектура предоставляет клиентам безопасные, простые и гибкие решения, которые могут быть полностью адаптированы для соответствия требованиям безопасности любой организации.

Check Point развивает рынок, поддерживая широкий спектр программных и программно-аппаратных продуктов и услуг для ИТ безопасности. Мы предлагаем нашим клиентам широкий портфель решений сетевой безопасности и шлюзов, решения по безопасности данных и конечных устройств, а также системы управления. Наши решения разработаны в соответствии с унифицированной архитектурой безопасности, что обеспечивает сквозную безопасность с единой линией шлюзов безопасности, и позволяет использовать один агент для безопасности конечных станций, который управляется с помощью единой унифицированной консоли управления. Такой подход к управлению позволяет легко развернуть и централизованно управлять решением, дополнительно усиливая его поддержкой и регулярными обновлениями безопасности в реальном времени.

Наши продукты и услуги поставляются промышленным предприятиям, сервис-провайдерам, малому и среднему бизнесу, а также индивидуальным потребителям. Наша Открытая Платформа Безопасности OPSEC (Open Platform for Security) позволяет пользователям расширять возможности наших продуктов и услуг с помощью использования устройств и приложений других производителей. Поставка, интеграция и поддержка наших продуктов осуществляется широкой сетью партнеров по всему миру. Клиентами компании Check Point являются десятки тысяч компаний и организаций различного масштаба, включая все компании из списка Fortune 100. Знаменитое решение ZoneAlarm от Check Point защищает миллионы клиентов от хакеров, шпионского ПО и краж идентификационной информации.



Check Point
SOFTWARE TECHNOLOGIES LTD.

We Secure the Internet.

Worldwide Headquarters: 5 Ha'Soleim 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