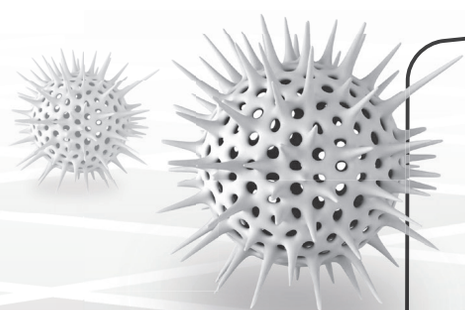
安全检查

基于 Check Point 软件定义防护架构的网络威胁分析报告

客　　户：ABC 公司
撰　　写：Check Point 解决方案中心
日　　期：2014 年 1 月 20 日
文件版本：2.0



Check Point
SOFTWARE TECHNOLOGIES LTD.
We Secure the Internet.

TOC

目录

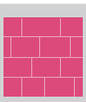
摘要

本文件提供了近期对您基础设施安全分析的事件。文件概述了这些事件，并针对发现的事件，提出了一套建议。

分析基于利用下列特征收集的数据：

安全分析日期：	12/01/2014	**分析持续时间：**	2 周
行业：	保险公司	**国家**	美国
公司规模：	2,500 名员工	**分析的网络：**	内部局域网
安全网关版本：	R77	**分析模式：**	镜像端口
安全网关软件刀片：	应用程序控制、URL 过滤、反僵尸、反病毒、IPS、DLP、身份识别、威胁仿真、合规性		
安全设备：	Check Point 4800 安全网关		

下面概述了发现的主要高风险和重大风险安全事件：



访问控制和数据保护

30,670	高风险应用程序事件
22	数据泄密事件

威胁防御

9	僵尸事件
5	病毒事件
16	零日事件
18	入侵和攻击事件

终端

893	涉及高风险事件的终端

合规性

65%	符合 Check Point 最佳实践
58%	符合法规要求

01 访问控制和数据保护发现

网络安全事件

主要高风险应用程序和网站

在网络应用程序和网站中，下列项目具有最高风险水平 [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] 风险水平 5 表示可绕过安全或隐藏身份的应用程序（如 Tor、VTunnel）。风险水平 4 表示可在用户不知情情况下造成数据泄露或恶意软件感染的应用程序（如文件共享、P2P uTorrent 或 P2P Kazaa）。当管理员和帮助台使用时，远程管理应用程序可能是合法的。

符合企业安全策略的高风险应用程序

高风险应用程序是那些可绕过安全、隐藏身份、在用户不知情情况下造成数据泄露或甚至恶意软件感染的应用程序。在大多数情况下，使用这些应用程序是违反企业安全策略的。然而，在某些情况下，可使特定应用程序符合企业策略。下列高风险应用程序在安全分析中被发现，但它们符合企业安全策略。

应用程序	组织安全策略
TeamViewer	允许支持小组用于远程帮助客户
LogMeIn	允许帮助台用于远程帮助员工

主要高风险应用程序描述

下表简要解释了发现的主要事件及其关联的安全或业务风险：

应用程序及描述	类别	应用程序风险	事件
Tor Tor 是一个旨在实现在线匿名的应用程序。Tor 客户端软件引导互联网流量通过一个全球自愿服务器网络，以向进行网络监控或流量分析的任何人隐藏用户的位置或使用情况。使用 Tor 使得跟踪用户的互联网活动更加困难，如网站访问、在线发帖、即时消息和其它通信形式。	匿名程序	重大	228
Ultrasurf Ultrasurf 是一个免费的代理工具，使用户能够避开防火墙和互联网内容拦截软件。	匿名程序	重大	51
VTunnel VTunnel 是一个免费的匿名通用网关接口（CGI）代理程序，它隐藏 IP 地址，使用户能够匿名连接和查看网站，绕过网络安全策略。	匿名程序	重大	18
BitTorrent BitTorrent 是一种对等网络文件共享 P2P 通信协议。它是一种广泛分发大量数据的方法。目前有许多以各种编程语言编写并在各种计算平台上运行的兼容 BitTorrent 客户端。P2P 应用程序可在用户不知情情况下造成数据泄露或恶意软件感染。	P2P 文件共享	高	464
ZumoDrive ZumoDrive 是一个混合云存储应用程序。它允许用户从计算机和移动电话访问其音乐、照片和文件。通过公共云共享数据可能造成敏感数据泄露。	文件存储和共享	高	148

高风险应用程序主要用户

下列用户涉及的高风险应用程序和网络使用事件最多：

用户	事件
Ginger Cash	12
Ivan Whitewash	9
Jim Josh	7
Bob Bash	5
Damien Dash	2

*** 备注：**只有在启用并配置 Check Point 身份识别软件刀片后，用户名才显示在上表中。

数据泄密事件

您的公司数据是您组织最宝贵的资产之一。任何故意或无意泄密会损害您的组织。下面描述了在分析过程中确定的数据泄密事件的特点。

主要数据泄密事件

下表总结了确定的数据泄密活动及具体事件发生的次数。

严重程度	数据	类别	事件
重大	信用卡号	合规	5
高	商业计划	商业信息	6
	财务报告	财务信息	3
	源代码	知识产权	2
	Outlook 消息 - 机密	机密信息	1
中	工资单文件	人力资源	4
	U.S. 社会保障号	可确认的个人信息	1

通过 HTTP 发送到组织外部的主要文件

下表给出了被发送到组织外部且可能包含敏感数据的文件：

主机	数据类型	文件名	URL
192.168.75.26	信用卡号	customer orders.xlsx	www.ccvalidator.com
192.168.75.48	财务报告	Q4 Report - draft2.docx	www.dropbox.com
192.168.125.28	源代码	new_feature.C	www.java-help.com
192.168.125.10	客户名称	Customer List.xlsx	www.linkedin.com
192.168.125.78	HIPAA- 受保护的健康信息	Medical File - Rachel Smith.pdf	www.healthforum.com

通过 SMTP 发送到组织外部的主要文件

下表给出了被发送到组织外部且可能包含敏感数据的文件：

收件人	数据类型	文件名	电子邮件主题
bella@otherBiz.com	信用卡号	Customer Invoices.xlsx	FW：发票
betty@otherBiz.com	商业计划	Q1 2015 Goals.pdf	RE：2015 年计划
doreen@otherBiz.com	员工姓名	employees.xls	公司员工
zoe@otherBiz.com	Salesforce 报告	Q4 sales summary.doc	RE：Q4 销售。机密！
jordana@otherBiz.com	公司新闻稿	New Release - draft2.docx	FW：新闻稿PR 草稿 - 请勿转发！！

按邮件发件人的主要数据泄密事件

下表显示了您网络中按邮件发件人的数据泄露事件。

发件人	事件
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 访问控制和数据保护发现

僵尸事件

僵尸是入侵您计算机的恶意软件。僵尸允许犯罪分子在用户不知情的情况下远程控制计算机系统，并执行非法活动。这些活动包括：窃取数据、扩散垃圾邮件、分发恶意软件、参与拒绝服务攻击等。僵尸经常在被称为高级持续威胁（APTs）的针对性攻击中被用作工具。僵尸网络是这些受控计算机系统的集合。

下表总结了感染僵尸的主机数量及在您的网络中发现的活动。

感染僵尸的主机	8
安装广告软件的主机	1
发生 SMTP 和 DNS 恶意软件相关事件的主机	2

僵尸恶意活动

描述	发现
与 C&C 站点通信的僵尸	4
测试连接的僵尸	2
僵尸感染造成的其它恶意活动	1
安装广告软件造成的不受欢迎的网络活动	1
事件总计	**8**

发生高风险和重大风险僵尸事件的主机

在 3D 安全分析中，Check Point 解决方案发现了许多表明僵尸活动的恶意软件相关事件。下表显示了发生高风险事件的主机样本。

主机	活动	威胁名称	资源
192.168.75.7	与 C&C 通信	Operator.Virus.Win32. Sality.d.dm	yavuztuncil.ya.funpic.de/images/ logos.gif?f58891=16091281
10.10.2.32	解析 C&C 站点的 DNS 客户端查询或 DNS 服务端	Operator.Conficker.bhvl	zsgnmngn.net
192.168.75.22	解析 C&C 站点的 DNS 客户端查询或 DNS 服务端	Operator.Zeus.bt	zsxwd.com
172.23.25.35	解析 C&C 站点的 DNS 客户端查询或 DNS 服务端	Operator. BelittledCardigan.u	zwoppfqnjj.com
10.100.2.33	解析 C&C 站点的 DNS 客户端查询或 DNS 服务端	Operator.APT1.cji	zychpupeydq.biz
10.1.1.22	解析 C&C 站点的 DNS 客户端查询或 DNS 服务端	Operator.Virus.Win32. Sality.f.h	zykehk.com

关于本报告发现的恶意软件的更多详细信息，请搜索 Check Point ThreatWiki - Check Point 公开恶意软件数据库，threatwiki.checkpoint.com

病毒事件

网络犯罪分子利用许多渠道来分发恶意软件。大多数常见方法引诱用户打开电子邮件附件中的被感染文件，下载被感染文件，或点击指向一个恶意网站的链接。

下表总结了在您的网络中发现的恶意软件下载及对感染恶意软件网站的访问事件。

恶意软件下载

描述	发现
下载恶意软件的主机	8
发生的事件数量	9

访问恶意网站

描述	发现
访问已知包含恶意软件的网站的主机	5
发生的事件数量	8

发生高风险和重大风险病毒事件的主机

在安全分析中，Check Point 解决方案发现了许多表明下载恶意文件或连接感染恶意软件网站的恶意软件相关事件。下表显示了发生高风险事件的主机样本。

主机	活动	资源
192.168.75.78	恶意文件 / 漏洞下载	r.openx.net/set?pid=619cb264-acb9-5a18-89ed-c1503429c217&rtb=3105223559/basic.pdf
192.168.125.76	恶意文件 / 漏洞下载	lavilla.de/links.jpg
192.168.125.10	访问已知包含恶意软件的网站	zzoygsulaeli.com/img_cache.php
192.168.125.48	为其背后客户端解析已知包含恶意软件的网站的 DNS 服务端	zzoygsulaeli.com

关于本报告发现的恶意软件的更多详细信息，请搜索 Check Point ThreatWiki - Check Point 公开恶意软件数据库，**threatwiki.checkpoint.com**

零日威胁

随着网络威胁变得越来越高级，高级威胁经常包括几乎天天扩散的新漏洞，对它们没有现成的防护。这些漏洞利用包括对新漏洞的零日攻击以及无数新恶意软件变种。

本节总结了在您的网络中发现的零日威胁。欲了解具体事件的详细恶意软件分析，请联系本地 Check Point 代表。

扫描的文件总数	169

事件	发现	涉及的主机
从网络下载的零日恶意软件	7	6
通过电子邮件（SMTP）发送的零日恶意软件	9	9

从网络下载的主要零日恶意软件

文件	恶意软件活动	主机	资源
0dd730ed4.pdf	意外进程崩溃	192.87.2.7	www.lostartofbeingadame.com/wpcontent/plugins/www.fotosupload.php
guide04d88.pdf	恶意文件系统活动 恶意网络活动 恶意注册表活动 意外进程创建 意外进程终止	10.23.33.24	silurian.cn/modules/mod_cmsfix/fix.php

通过电子邮件（SMTP）发送的主要零日恶意软件

下表总结了在基于 SMTP 流量的电子邮件中发现的主要零日恶意软件：

文件	发件人	收件人	主题	恶意软件活动
Notice231488.doc	asia@shippingoods.com	logistics@mybiz.biz	包裹详细信息	恶意软件创建另一个进程 恶意软件生成可疑文件 恶意软件检索模块名称 恶意软件创建另一个自己的实例 恶意软件篡改浏览器历史
invoiceBQW8OY.doc	No-Replay@shop. sip	jhon@mybiz. biz	您的发票	恶意软件影响系统其它进程 恶意软件创建另一个进程 恶意软件生成可疑文件 恶意软件创建一个挂起状态的进程（用于逃避进程） 恶意软件删除自己 恶意软件检索模块名称 恶意软件运行在一个不同进程的环境中 恶意软件创建一个子进程 恶意软件篡改浏览器历史
Summit_Agenda.doc	events@conferences.org	marketing@mybiz.biz	即将举行的活动日程	恶意软件创建另一个进程 恶意软件生成可疑文件 恶意软件创建一个挂起状态的进程（用于逃避进程） 恶意软件删除自己 恶意软件检索模块名称 恶意软件篡改重要系统文件

入侵和攻击事件

主要入侵和攻击事件

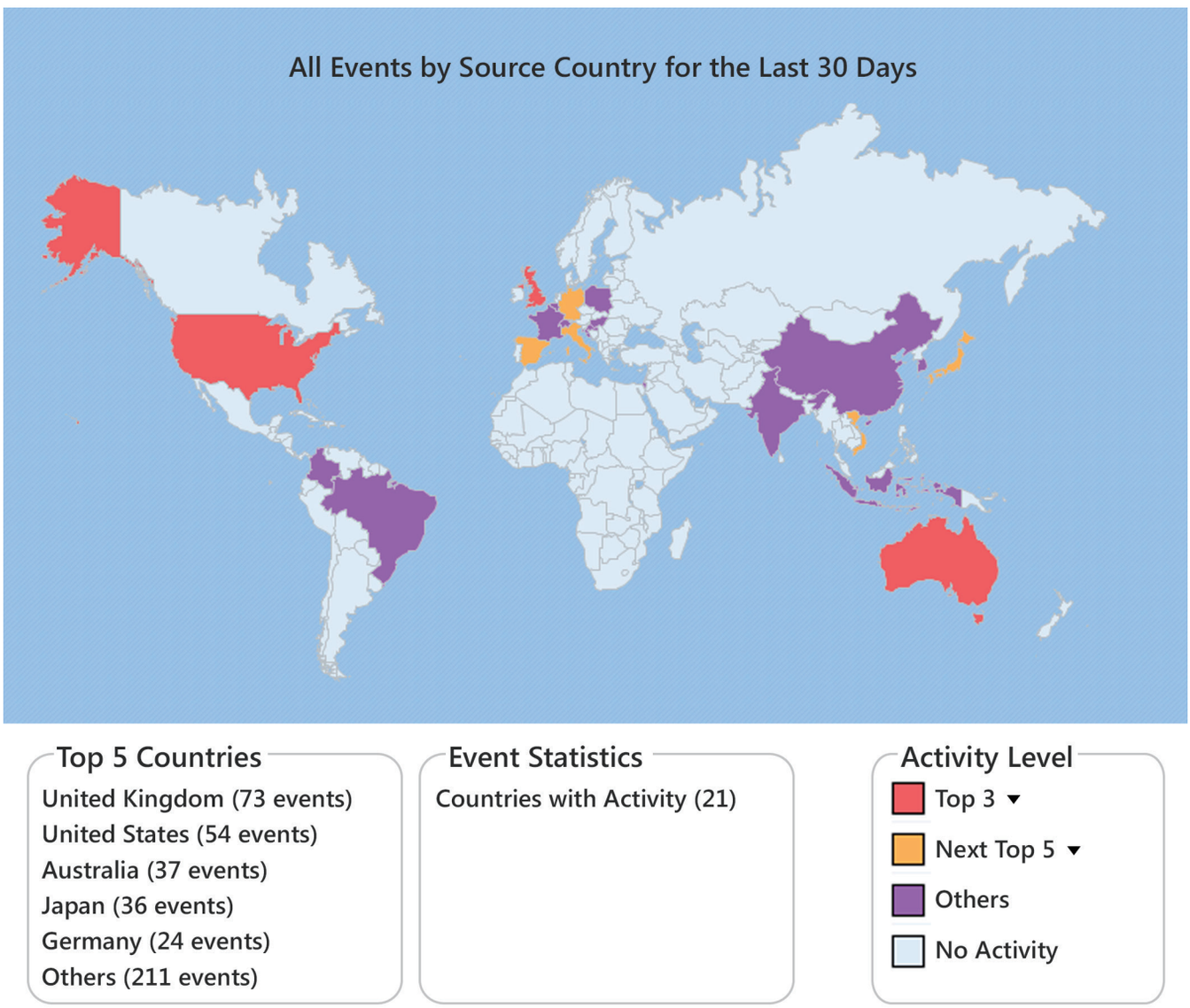
在安全分析中，Check Point 解决方案发现了许多入侵防御相关事件。某些事件分类为高风险。下表显示了按严重程度的事件分布。

严重程度	事件名称	CVE 清单 *	事件
重大	Microsoft SCCM 反射型跨站脚本 (MS12-062)	CVE-2012-2536	5
	Joomla 非授权文件上传远程代码执行	-	2
	Web 服务器恶意 HTTP 头文件目录遍历	-	1
	ImageMagick GIF 备注处理 Off-by-one 缓冲区溢出 (CVE-2013-4298)	CVE-2013-4298	3
	Adobe Flash Player SWF 文件缓冲区溢出 (APSB13-04)	CVE-2013-0633	2
高	PHP php-cgi 查询字符串参数代码执行	CVE-2012-1823	1
	Oracle 数据库服务器 CREATE_TABLES SQL 注入	CVE-2007-3890	4

*CVE（常见漏洞和披露）是一个已知的安全漏洞字典。欲了解具体 IPS 事件的更多信息，请利用国家漏洞数据库搜索网页搜索 CVE ID。

按国家的 IPS 事件

下图显示了按其来源国家的 IPS 事件分布。



03 终端安全发现

本节提供了关于您基础设施主机的安全发现。它概述了这些发现，并按安全向量提供了详细信息。本报告补救措施部分针对发现的事件提供了一套建议。

终端安全事件摘要

运行高风险网络应用程序的终端总数	**6**
涉及数据泄密事件的终端总数	19
涉及入侵和攻击事件的终端总数	20
涉及恶意软件事件的终端总数	848

运行高风险应用程序的主要终端

下表显示了运行高风险应用程序或访问高风险网站的主要终端主机：

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

主要终端入侵和攻击事件

下表显示了发生入侵防御相关事件的主要终端主机。

源地址	目的地址	严重程度	事件名称	CVE 清单
192.87.2.47	192.168.75.27	重大	Microsoft SCCM 反射型跨站脚本 (MS12-062)	CVE-2012-2536
192.78.2.214	192.168.75.58	重大	Joomla 非授权文件上传远程代码执行	-
192.84.2.220	192.168.75.58	重大	Web 服务器恶意 HTTP 头文件目录遍历	-
192.85.2.133	192.168.75.58	重大	ImageMagick GIF 备注处理 Off-by-one 缓冲区溢出 (CVE-2013-4298)	CVE-2013-4298
192.116.2.151	192.168.75.58	重大	Adobe Flash Player SWF 文件缓冲区溢出 (APSB13-04)	CVE-2013-0633
192.195.2.88	192.168.75.60	高	PHP php-cgi 查询字符串参数代码执行	CVE-2012-1823
192.87.2.211	192.168.86.3	高	Oracle 数据库服务器 CREATE_TABLES SQL 注入	CVE-2007-3890

涉及数据泄密事件的主要终端

下表显示了发生数据泄密相关事件的主要终端主机。

终端	事件	发送的数据
192.168.125.36	4	信用卡号
	1	商业计划
192.168.75.0	5	财务报告
192.168.125.0	4	源代码
192.168.86.47	4	Outlook 消息 - 机密
192.168.86.38	2	美国社会保障号

涉及恶意软件事件的主要终端

下表显示了发生恶意软件相关安全事件的主要终端主机。

主机	威胁名称	恶意软件活动
192.168.86.8	Operator.Virus.Win32.Sality.f.h	解析 C&C 站点的 DNS 客户端查询或 DNS 服务端
192.168.75.0	Operator.APT1.cji	解析 C&C 站点的 DNS 客户端查询或 DNS 服务端
192.168.75.3	Operator.Virus.Win32. Sality. d.dm	与 C&C 通信
192.168.75.7	REP.yjjde	访问已知包含恶意软件的网站
192.168.75.10	RogueSoftware.Hack_Style_ RAT.pbco	与 C&C 通信
192.168.75.13	Trojan.Win32.Agent.aaeyr.cj	恶意文件 / 漏洞下载

合规性安全分析

本节详细分析了您当前 Check Point 网络安全部署的安全策略。

分析通过 Check Point 合规性软件刀片来进行，该软件刀片利用一个包含数百安全最佳实践和建议的广泛库来提高您组织的网络安全。

安全策略合规性

合规性软件刀片扫描您的安全管理、网关和安装的软件刀片的配置。结果与我们的安全最佳实践样本进行比较。根据我们的 102 个推荐最佳实践，我们发现，67 个完全符合，而 35 个缺失或不符合。这使得总体合规性水平为 65%。

	**65%**	符合 Check Point 推荐的安全最佳实践
	**102**	分析安全配置
	**67**	发现配置合规
	**35**	发现配置不合规或缺失
	**12**	监控的安全网关

合规摘要

下表显示了您的网络安全合规水平。这种状态通过分析各种 Check Point 安全网关配置和软件刀片设置并与法规要求比较而确定。

法规	要求数量	安全最佳实践数量	符合性状态
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%
英国数据保护法	1	29	49%
防火墙 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%

按安全软件刀片的最佳实践合规性

下表显示了每种软件刀片的总体安全状况。

对于每种软件刀片，Check Point 推荐了一套最佳实践。100% 分数意味着该刀片的所有最佳实践均安全配置。不到 100% 的分数表明配置不符合最佳实践，因此会给您的环境带来潜在安全缺陷。

安全软件刀片	安全最佳实践数量	安全状况
数据泄密防护	2	7%
IPS	4	29%
应用程序控制	13	54%
移动接入	3	66%
IPSec VPN	16	73%
URL 过滤	5	87%
防火墙	35	88%
反病毒	13	91%
反垃圾邮件和邮件	3	100%
反僵尸	8	100%

合规摘要

下表显示了您的网络安全合规水平。这种状态通过分析各种 Check Point 安全网关配置和软件刀片设置并与法规要求比较而确定。

刀片	ID	名称	状态
防火墙	FW101	检查在防火墙规则库中定义了“Clear Rule”	0%
防火墙	FW102	检查每个网关都启用了防地址欺骗	0%
防火墙	FW103	检查每个网关都将防地址欺骗设置为“Prevent”	0%
防火墙	FW105	检查每条防火墙规则都定义了“记录日志”设置	0%
防火墙	FW130	检查在防火墙规则库中定义了“Stealth Rule”	0%
防火墙	FW152	检查每条防火墙规则都定义了“名称”	0%
防火墙	FW153	检查每条防火墙规则都定义了“备注”	0%
防火墙	FW107	检查为每个网关定义了一个额外的日志服务器，用于存储防火墙日志	0%
防火墙	FW116	检查在防火墙设置中启用了 NAT/PAT	87%
防火墙	FW146	检查在防火墙规则库中未定义“Any Any Accept”规则	0%
防火墙	FW159	检查选择了“之后锁定管理员账户”	0%
防火墙	FW160	检查在 3 次登录失败后锁定管理员	0%
防火墙	FW161	检查选择了“之后解锁管理员账户”	0%
防火墙	FW162	检查在 30 分钟后解锁管理员账户	0%
防火墙	FW163	检查显示锁定管理员的详细消息	0%

05 带宽分析

下面部分总结了分析时您组织的带宽使用及网络浏览情况。

按应用程序和网站的主要带宽使用

下表显示了按消耗带宽发现的主要网络应用程序和网站。

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

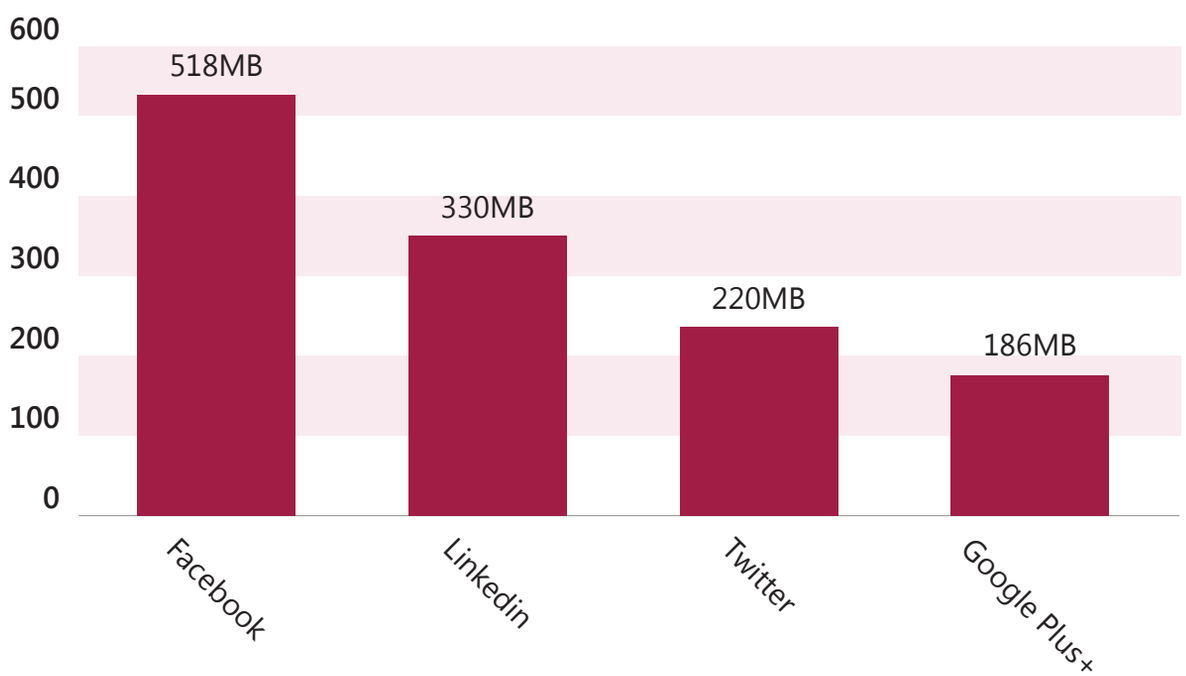
主要网络类别

下表显示了与员工互联网浏览相关的主要 10 种类别及点击数量。

类别	点击数量	占点击总数的 %
社交网络	113	31.65%
Webmail	42	11.76%
视频流	36	10.08%
搜索引擎 / 门户网站	35	9.80%
多媒体	29	8.12%
浏览器插件	25	7.00%
商业应用程序	15	4.20%
介质共享	13	3.64%
网络应用程序	9	2.52%
其它	40	11.20%
总计	**357**	**100%**

社交网络带宽 (MB)

在工作场所和家中使用社交网络已变得常见起来。许多企业利用社交网络技术来开展营销和招聘计划。在分析中，下列社交网络消耗的网络带宽最多，这与总体市场趋势是一致的：



06 补救措施建议

访问控制和数据保护建议

本报告涉及在多个安全领域发现的不同严重程度的安全事件。下表显示了最严重的事件，并提出了缓解风险的方法。Check Point 提供多种方法来应对这些威胁及担忧。对每个事件，注明了相关防护以及纳入防御的软件刀片。

网络安全事件补救措施建议

应用程序 / 网站	应用风险	事件	补救措施
Tor	重大	228	在应用程序控制和 URL 过滤软件刀片中，您可以激活、跟踪和阻止使用所有提到的应用程序和网站。您可以定义一条高粒度策略，以只允许特定小组使用某些应用程序。 利用 UserCheck： • 教育用户组织的网络浏览和应用程序使用策略。 • 当其行为违反安全策略时，向用户提供即时反馈。
Ultrasurf	重大	51	
Vtunnel	重大	18	
BitTorrent	高	464	
ZumoDrive	高	148	

点击以了解关于 Check Point **应用程序控制**和 **URL 过滤**安全网关软件刀片的更多信息。

数据泄密事件补救措施建议

严重程度	数据	事件	补救措施
重大	信用卡号	14	为补救发现的事件，激活 DLP 软件刀片。根据探测的 DLP 数据类型，配置 DLP 策略，选择一种动作（探测 / 阻止 / 询问用户等）。如果您认为探测的数据类型是敏感信息，则推荐动作为“阻止”。 利用 UserCheck： • 教育用户组织的数据使用策略。 • 当其行为违反数据使用安全策略时，向用户提供即时反馈。
高	商业计划	1	
	财务报告	3	
	源代码	12	
	Outlook 消息 - 机密	147	
中	工资单文件	25	
	美国社会保障号	15	

点击以了解关于 Check Point **DLP** 安全网关软件刀片的更多信息。

威胁防御建议

恶意软件威胁补救措施建议

应用程序 / 网站	应用风险	事件	补救措施
REP.yjjde	重大	36	启用 Check Point 反僵尸软件刀片，以检测僵尸感染主机，并防止僵尸破坏。 启用 Check Point 反病毒软件刀片，以防止下载恶意软件。 启用 Check Point 威胁仿真软件刀片，以阻止新的未被发现恶意软件威胁。 为补救感染的主机，首先在 Check Point ThreatWiKi 中搜索发现的恶意软件，以找到相关信息。然后，遵循恶意软件补救措施网页中显示的补救措施说明。
Operator.Virus.Win32. Sality.d.dm	重大	28	
Operator.Conficker.bhvl	高	27	
Operator.Zeus.bt	高	11	
Operator.BelittledCardigan.u	高	8	

点击以了解关于 Check Point **反僵尸**、**反病毒**和**威胁仿真**安全网关软件刀片的更多信息。

入侵和攻击事件补救措施建议

威胁	严重程度	事件	事件
Microsoft SCCM 反射型跨站脚本 (MS12-062)	重大	15	在 Check Point IPS 软件刀片中，启用下列防护：**Microsoft SCCM 反射型跨站脚本 (MS12-062)**
Joomla 非授权文件上传远程代码执行	重大	13	在 Check Point IPS 软件刀片中，启用下列防护：**Joomla 非授权文件上传远程代码执行**
Microsoft 活动目录 LSASS 递归栈溢出 [MS09-066]	高	4	在 Check Point IPS 软件刀片中，启用下列防护：**Microsoft 活动目录 LSASS 递归栈溢出 [MS09-066]**

点击以了解关于 Check Point **IPS** 安全网关软件刀片的更多信息。

终端安全补救措施建议

本节涉及在多个安全领域发现的不同严重程度的终端安全事件。下表显示了最严重的事件，并提出了缓解风险的方法。Check Point 提供多种方法来应对这些威胁及担忧。对每个事件，注明了相关防护以及纳入防御的终端软件刀片。

网络安全事件 - 终端补救措施建议

主机	应用程序 / 网站	风险	补救措施
192.168.75.36	Tor	重大	**Check Point 终端安全**控制高风险应用程序和网站的使用，即使终端与公司网络断开且没有网络安全解决方案。 利用 **Check Point 程序控制软件刀片**，只允许批准的程序在终端上运行，终止未批准或非信任程序。 利用 **WebCheck 终端软件刀片**，保护企业免遭网络威胁攻击，如被控式下载、钓鱼网站和零日攻击。 利用 **Check Point 符合性检查软件刀片**，验证某个程序是否在终端设备上运行，在必要时限制其网络访问。 通过**终端防火墙软件刀片**，控制进出流量，限制对特定端口和网络服务的访问。 利用 UserCheck： • 教育用户组织的网络浏览和应用程序使用策略。 • 当其行为违反安全策略时，向用户提供即时反馈。
192.168.75.71	Ultrasurf	重大	
192.168.86.0	VTunnel	重大	
192.168.86.19	BitTorrent	高	
192.168.86.30	ZumoDrive	高	

点击以了解关于下列 Check Point 终端安全软件刀片的更多信息：

- **程序控制**终端安全软件刀片
- **WebCheck** 终端安全软件刀片
- **合规性检查**终端安全软件刀片
- **防火墙**终端安全软件刀片

入侵和攻击事件 - 终端补救措施建议

源地址	目的地址	事件名称	补救措施
192.87.2.47	192.168.75.27	Microsoft SCCM 反射型跨站脚本 (MS12-062)	**利用终端符合性软件刀片**，确保您组织的终端安装了最新安全补丁和更新。 **终端符合性软件刀片**将确保终端是安全的，即使与组织网络断开且没有网络安全防护。例如，在家中或路上办公。
192.78.2.214	192.168.75.58	Joomla 非授权文件上传远程代码执行	
192.84.2.220	192.168.75.58	Web 服务器恶意 HTTP 头文件目录遍历	
192.85.2.133	192.168.75.58	ImageMagick GIF 备注处理 Off-by-one 缓冲区溢出 (CVE-2013-4298)	
192.116.2.151	192.168.75.58	Adobe Flash Player SWF 文件缓冲区溢出 (APSB13-04)	
192.195.2.88	192.168.75.60	PHP php-cgi 查询字符串参数代码执行	
192.87.2.211	192.168.86.3	Oracle 数据库服务器 CREATE_TABLES SQL 注入	

点击以了解关于下列 **Check Point 终端安全软件刀片**的更多信息：

- **防火墙**终端安全软件刀片
- **符合性检查**终端安全软件刀片

数据泄密事件 - 终端补救措施建议

主机	类型	补救措施
192.168.75.0	信用卡号	利用 **Check Point 全磁盘加密软件刀片**，确保安装在终端硬盘驱动器上的敏感信息安全，包括用户数据、操作系统文件以及临时和删除的文件，防止在笔记本电脑丢失或被盗时发生非授权访问。 利用 **Check Point 介质加密软件刀片**，加密存储在移动设备上的敏感数据，分别跟踪和管理移动设备。 利用 **Check Point 文件安全软件刀片**，您可以仅允许授权个人访问敏感文件。 利用 UserCheck： • 教育用户组织的数据使用策略。 • 当其行为违反数据使用安全策略时，向用户提供即时反馈。
192.168.86.47	商业计划	
192.168.125.0	源代码	
192.168.125.36	工资单文件	

点击以了解关于下列 **Check Point 终端安全软件刀片**的更多信息：

- **全磁盘加密**终端安全软件刀片
- **介质加密**终端安全软件刀片
- **文件安全**终端安全软件刀片

恶意软件事件 - 终端补救措施建议

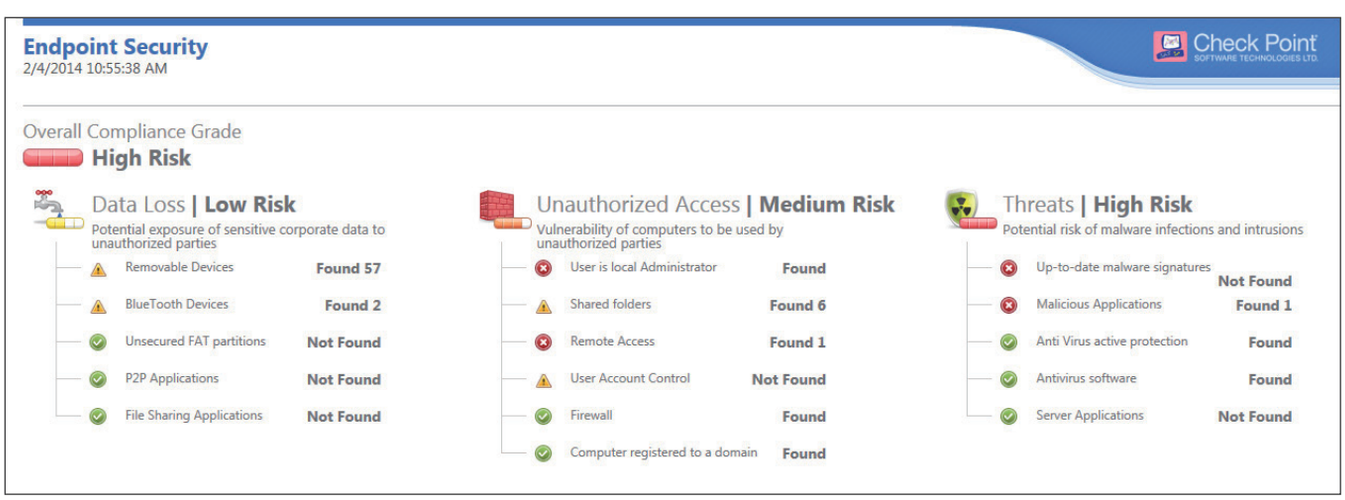
主机	严重程度	补救措施
192.53.2.161	重大	利用 **Check Point 终端反恶意软件软件刀片**，检测并防止恶意软件、病毒、键盘记录程序、木马和 root kits（根工具）等威胁感染企业终端。 **Check Point 终端反恶意软件软件刀片**将使您的企业终端受到保护，即使与组织网络断开且没有网络安全防护。例如，在家中或路上办公。 利用**终端合规性软件刀片**，确保终端安装了最新安全更新，且符合企业安全策略。 要在感染主机上开始补救过程，**在 Check Point ThreatWiki** 中搜索发现的恶意软件，以找到关于恶意软件的附加补救帮助信息。该信息可帮助你更好地了解感染情况及其潜在风险。 利用 **UserCheck**，教育用户组织网络浏览和网络应用程序使用策略。
192.57.2.32	重大	
192.57.2.209	重大	
192.59.2.27	重大	
192.59.2.79	重大	

点击以了解关于下列 **Check Point 终端安全软件刀片**的更多信息：

- **反恶意软件**终端安全软件刀片
- **防火墙和合规性**检查终端安全软件刀片

运行综合终端安全分析报告

要对您的终端进行更全面的分析，以了解安全状况和潜在风险，运行终端安全分析报告或联系您的本地 Check Point 代表。



合规性刀片补救措施建议

本报告涉及 Check Point 软件刀片发现的需要关注的安全配置。下表显示了根据如何提高安全水平的指导需处理的一些项目。

风险	补救措施	相关对象
高	根据下列定义，在相关策略包中创建一条新“Stealth Rule”，或修改现有“Stealth Rule”：Source = Any ; Destination = GW’s ; Service = Any ; Action = Drop ;Install On = Policy Target ; Time = Any。	策略包 A
高	根据下列定义，在相关策略包中创建一条新“Stealth Rule”，或修改现有“Stealth Rule”：Source = Any ; Destination = Any; VPN = Any Traffic ; Service = Any ; Action = Drop ; Track = Log; Install On = Policy Targets ; Time = Any；注意，“Clear Rule”必须位于防火墙规则库最后一行。	策略包 B
高	在 IPS 刀片中激活自动更新防护	IPS 网关 公司网关
高	在应用程序控制刀片中，创建一条新策略，或修改现有策略，使得重大风险应用程序和网站被拦截。	策略包 A
高	在“Global Properties”中，修改“Authentication Timeout ”设置，使其介于 20 - 120 分钟。	全局属性
高	为所有策略包的所有防火墙规则定义“跟踪”设置。	策略包 A - 规则号 18 - 规则号 35 - 规则号 64 策略包 B - 规则号 11 - 规则号 23 - 规则号 88

软件定义防护

在一个需求爆发的 IT 基础架构和网络的世界中，边界不再清晰，威胁变得越来越智能，我们需要找到正确的方式来保护不断变化的环境中企业。

目前，各种安全产品广泛发展；然而，这些单打独斗的产品本质上是被动的，而非面向架构的。今天企业需要一个综合高性能网络安全设备和主动实时防护的统一架构。

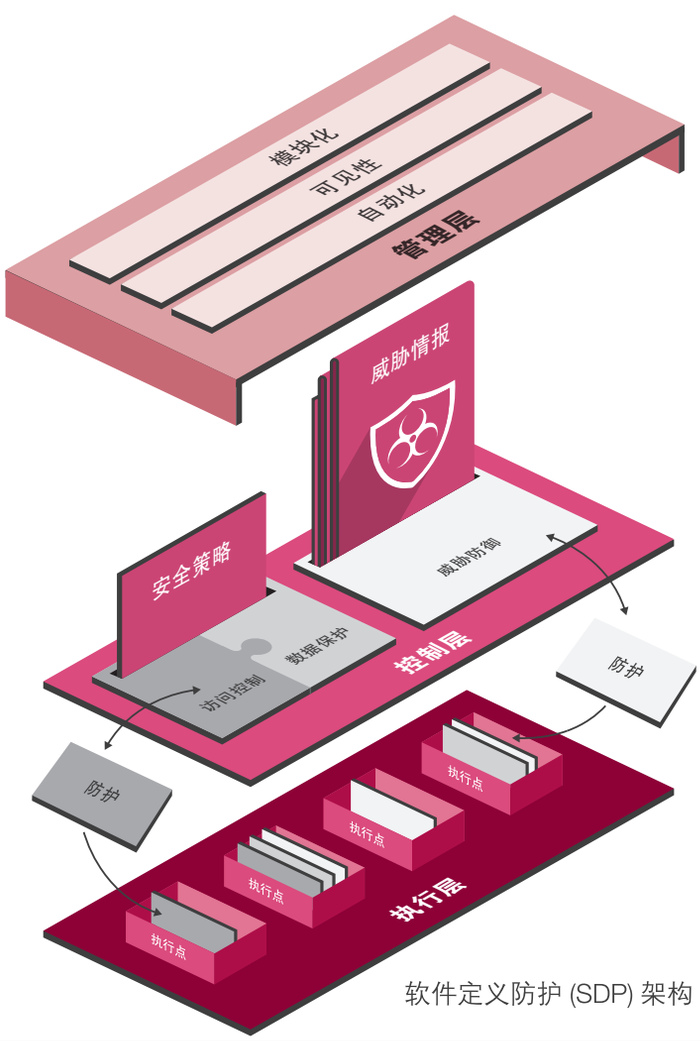
一种新的模式来前瞻性地保护公司和企业。

软件定义防护 (SDP) 是一种新型实用的安全架构和方法。它提供一种模块化、敏捷和最重要的一点，安全的基础架构。

不论公司规模大小，这种基础架构必须对公司的各个位置提供保护：总部网络、分支机构、智能手机、移动设备漫游或在使用云环境时。

防护可以根据安全边界自动调整，而无需安全管理员手动跟踪数千条策略和告警。这些防护可以无缝集成到更大的 IT 环境中，该架构必须综合利用内部和外部的最新安全威胁信息进行防护。
软件定义防护（SDP）架构将安全基础设施分成三个互联层：

- **执行层**，基于物理主机、虚拟主机和网络分段，并在高扩展需求环境中实现防护。
- **控制层**，分析不同的威胁信息源，为执行层提供防护策略。
- **管理层**，协调基础架构，为整个架构带来最高程度的敏捷性。



软件定义防护 (SDP) 架构

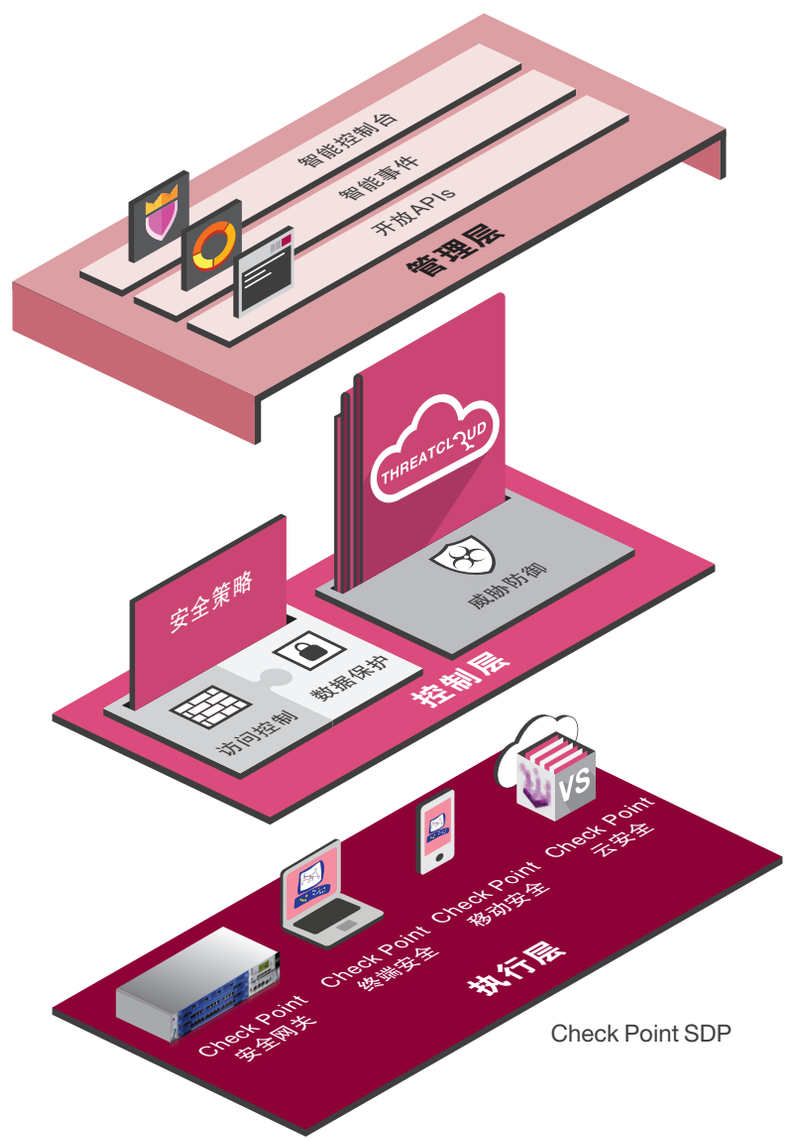
通过整合高性能的执行层与快速发展、动态的控制层，SDP 架构不仅提供了操作的灵活性，而且还针对不断变化的安全威胁提供了前瞻性的防御。

先进的 SDP 架构不仅支持传统的网络安全和访问控制策略，而且为应用了 SDN 等最新网络技术的现代企业提供了必需的威胁防御技术。

CHECK POINT 软件定义防护

Check Point 提供实现一个具有最佳管理和最佳安全的完整 SDP 架构需要的所有正确组件。

Check Point 软件定义防护提供应对新威胁和新技术所需的灵活性。我们的解决方案针对已知和未知威胁生成不断更新的防护，并通过威胁云前瞻性地分发这些内容。Check Point 安全解决方案使企业能够自信地应用各种先进的 IT 系统解决方案。



Check Point SDP

CHECK POINT SDP 执行层

为确保每个网段边界的安全，Check Point 提供一系列广泛的执行点。这些包括高性能网络安全设备、虚拟网关以及终端主机软件和移动设备应用程序。Check Point 为企业提供分区域管理、合并和确保系统与网络安全需要的所有模块。

CHECK POINT SDP 控制层

Check Point SDP 控制层基于 Check Point 软件刀片架构，向客户提供灵活、高效的安全解决方案，以满足其具体需求。软件刀片架构提供 20 多种软件刀片选择，其模块性允许客户按执行点创建相关安全解决方案，并随着时间扩展其安全基础设施。

下一代威胁防御

Check Point 高效地提供控件，以应对许多已知和未知威胁。Check Point 威胁防御解决方案包括：综合入侵防御系统（IPS）、基于网络的反病毒、威胁仿真和反僵尸。Check Point 构建了一个独特的基于云的威胁情报大数据和防护生成器 Check Point ThreatCloud ™。Check Point ThreatCloud 采用一种协作的方式打击网络犯罪，提供实时安全威胁情报，并转换成控制层的安全指标。

下一代防火墙和数据保护

Check Point 访问控制基于我们综合了多种软件刀片的下一代防火墙，启用了一条统一的基于上下文的安全策略：下一代防火墙和 VPN、用户身份识别、应用程序控制、数据和内容识别。

下一代数据保护

Check Point 下一代数据保护增加了数据识别。它包括我们的数据泄密防护（DLP）软件刀片，该刀片执行内容检测，将文件内容与存储在企业库中的文件匹配。另外，Check Point 为静态和以加密技术存储的数据提供数据保护。这些技术可在所有执行点采用，以防止敏感文件和机密数据被非授权用户访问或传输到移动介质上。

CHECK POINT SDP 管理层

所有 Check Point 防护和执行点从一个统一的安全管理控制台管理。Check Point 安全管理高度可升级，能够管理数千万对象，同时保持超快的用户界面响应时间。

Check Point 模块化 / 分层策略管理

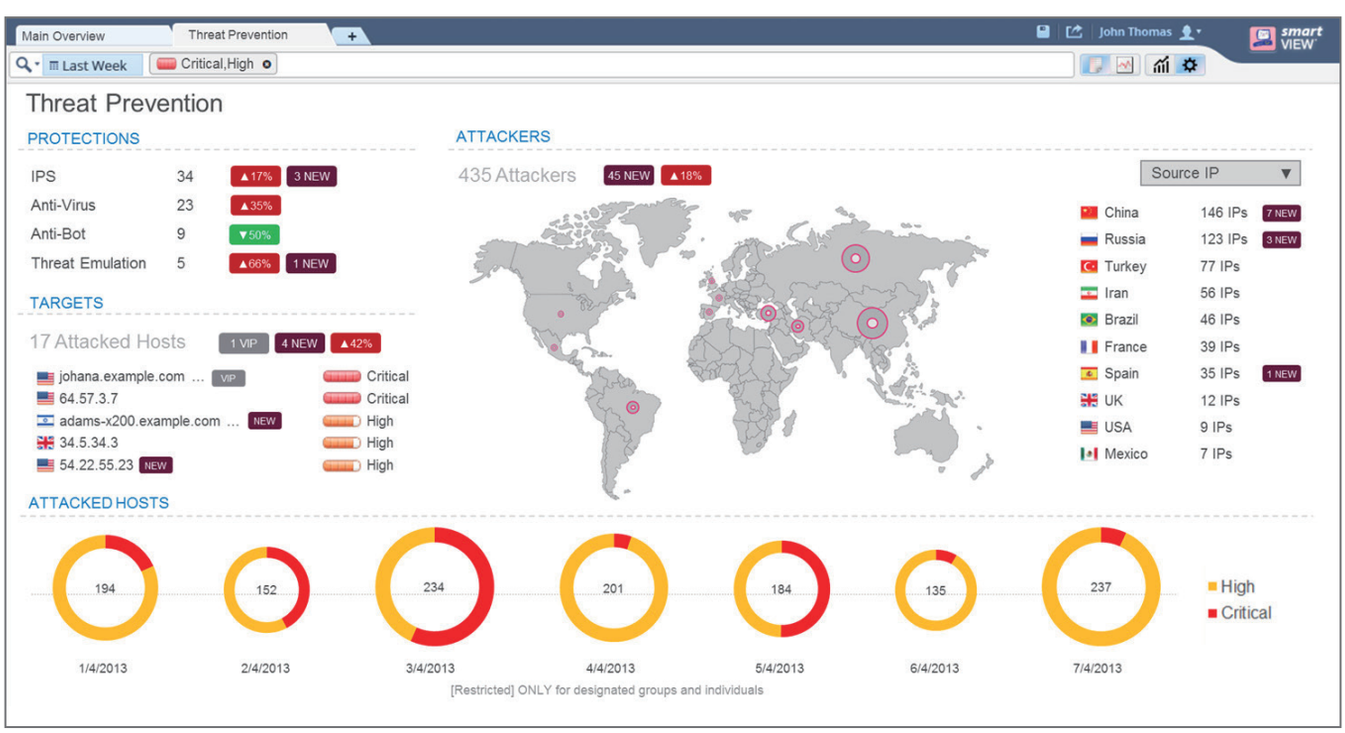
Check Point 安全管理支持企业网络分段，允许管理员为每个网段定义安全策略，同时以层和子层的新理念划分职责。可为每个网段定义策略。访问控制策略可利用各层进行定义，它们可分配给不同管理员。然后，多个管理员可同时使用相同策略。

自动化和协调

Check Point 安全管理提供 CLIs 和网络服务 APIs，允许组织集成网络管理、CRM、故障通知单、身份管理和云协调器等其它系统。

通过 Check Point SmartEvent 的可见性

Check Point SmartEvent 进行大数据分析和实时安全事件关联。它能够根据多种信息源提供一个合并的关联事件视图。安全事件分析以威胁指标的形式生成可行情报，并通过 ThreatCloud 分发，以实时阻止威胁。



通过 Check Point SmartEvent 的事件管理

了解关于 Check Point 软件定义防护及其如何帮助您的安全基础设施与今天快速变化的威胁情况同步的更多信息。访问 **www.checkpoint.com/securitycheckup**

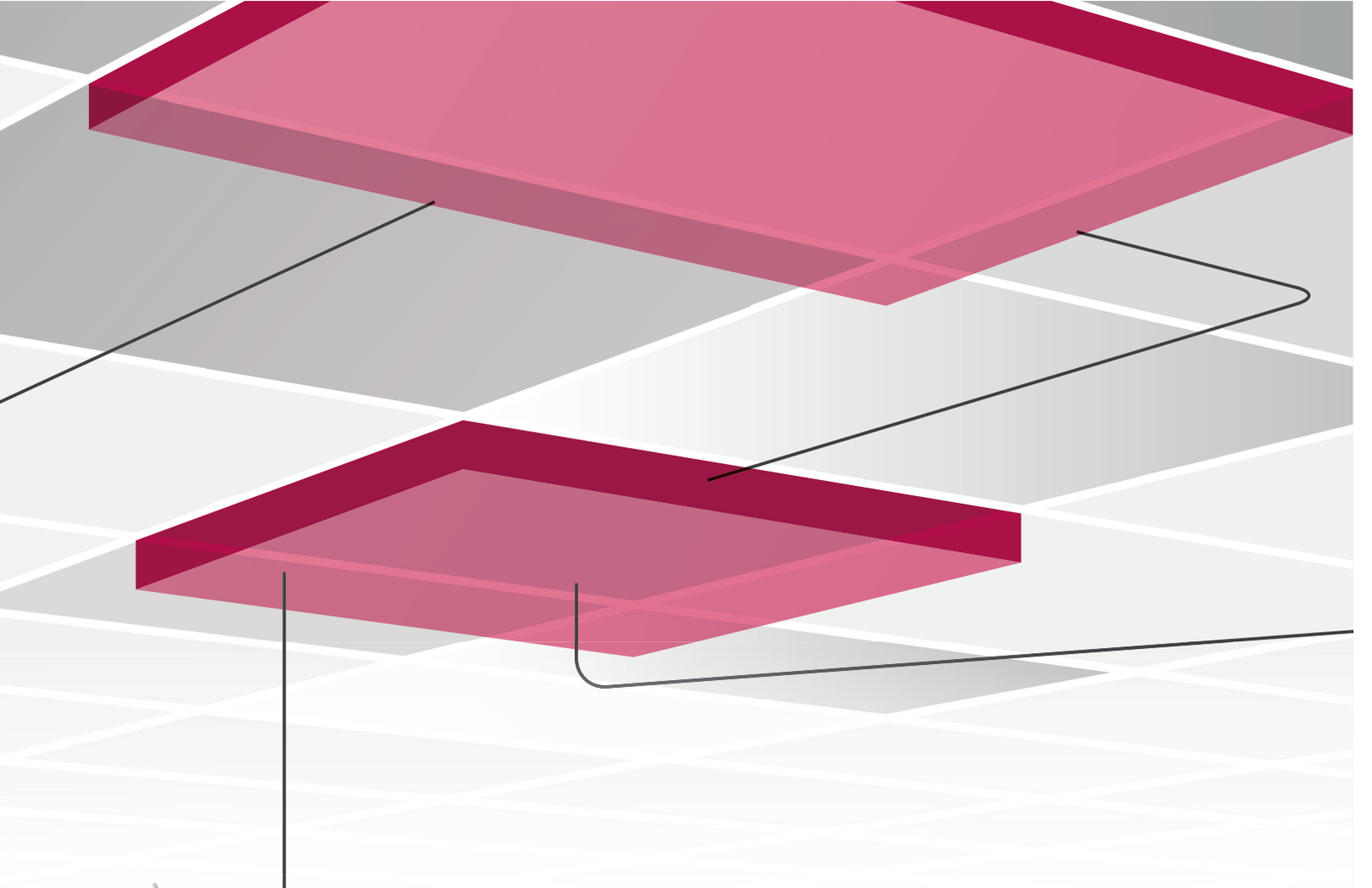
关于 CHECK POINT 软件技术有限公司

Check Point 软件技术有限公司 (**www.checkpoint.com**) 的任务是确保互联网安全。Check Point 成立于 1993 年，已开发了多种技术来确保企业和消费者互联网通信与交易的安全。

Check Point 以我们的 FireWall-1 和专利状态检测技术而成为行业先驱。Check Point 通过开发软件刀片架构而扩展了其 IT 安全创新。动态的软件刀片架构提供可定制的安全、灵活和简单解决方案，以满足任何组织或环境的安全需求。

Check Point 开发了市场，支持一系列广泛的 IT 安全软件以及综合硬件和软件产品与服务。我们向客户提供广泛的网络与网关安全解决方案、数据与终端安全解决方案和管理解决方案产品组合。我们的解决方案在一个统一的安全架构下操作，通过一系列统一安全网关实现端到端安全，允许所有终端安全采用一个代理，并可从一个统一的管理控制台进行管理。这种统一管理便于部署和集中控制，支持实时安全更新，并得到增强。

我们的产品和服务出售给企业、服务提供商、中小型企业和消费者。我们的开放安全平台(OPSEC) 框架允许客户通过第三方硬件和安全软件应用程序扩展我们产品与服务的能力。我们的产品通过一个全球合作伙伴网络出售、集成和维护。Check Point 客户包括成千上万各种规模的企业和组织，包括所有财富百强公司。Check Point 获奖的 ZoneAlarm 解决方案保护数百万消费者免遭黑客、间谍软件和身份盗用攻击。



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

Check Point 北京代表处
地址：北京市朝阳区东三环中路7号
财富中心写字楼A座615室（100020）
电话：(86) 10 6590 7630
传真：(86) 10 6590 7631

Check Point上海代表处
地址：上海市淮海中路93号
大上海时代广场26楼（200021）
电话：21-5117 6332/33
传真：21-5117 9300

Check Point 广州代表处
地址：广州天河区天河路385号
太古汇一座702 – 11（510620）
电话：020-2886 1546/47/48/49/50
传真：020-2886 1555