CHECK POINT SANDBLAST 设备



CHECK POINT SANDBLAST 设备

防御新的未知威胁

产品优点

- 防御文档和可执行文件中新的未知攻击
- 使黑客无法逃逸检测
- 利用现有安全基础设施，以降低成本
- 通过统一管理、监控和报告，最大化防护
- 通过与 ThreatCloud™ 自动共享新攻击信息，提高安全性

产品特点

- 识别 40 多种文件类型中隐藏的新恶意软件，包括 Adobe PDF、Microsoft Office、Java、Flash、可执行文件和压缩文件
- 防御针对多种 Windows 操作系统环境的攻击
- 提供一系列设备，每月文件扫描速率 100K - 2M
- 威胁净化清除可利用内容，无延迟提供干净的文件
- 在可能部署和逃逸检测前，独特的 CPU 层技术捕捉恶意软件

洞察

随着网络威胁越来越高级，许多针对性攻击都是从下载的文件和电子邮件附件中的软件漏洞利用开始的。

这些威胁包括新漏洞或甚至是已知漏洞的变种，它们几乎每天都在发布，没有现成签名，因此就没有检测这些变种的标准解决方案。新的未发现威胁需要超越已知威胁签名的新解决方案。

解决方案

Check Point SandBlast 零日防护具有抗逃逸恶意软件检测能力，可对最危险攻击提供全面防护，同时保证向用户快速交付安全内容。我们解决方案的核心是两种独特能力，即威胁仿真和威胁净化，它们将威胁防御推向更高层次。

作为 Check Point SandBlast 解决方案的一部分，威胁仿真引擎在漏洞利用阶段识别恶意软件，甚至在黑客应用逃逸技术企图绕过沙盒之前。文件被快速隔离和检测，在虚拟沙盒中运行，以在其进入网络前发现恶意行为。这种创新解决方案将 CPU 层检测与 OS 层沙盒结合起来，防止最危险漏洞利用及零日和针对性攻击造成的感染。

此外，SandBlast 威胁净化能力向用户即时提供潜在恶意内容的安全版本。可利用内容，包括活动内容和各种形式的嵌入式对象，被从重构的文件中提取出来，以消除潜在威胁。对原始可疑版本的访问被阻止，直到被 SandBlast 零日防护完全分析。用户可即时访问内容，确信他们受到保护，免遭最高级恶意软件和零日威胁的攻击。

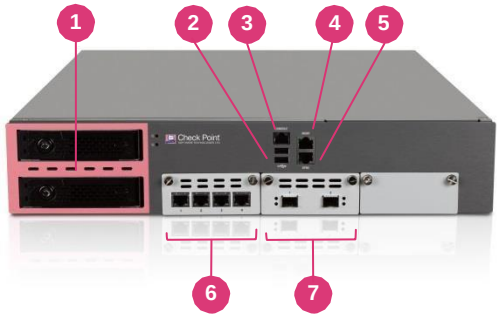
SANDBLAST 设备

我们提供一系列 SandBlast 设备。这些设备是有法规或隐私担忧的客户的完美选择，使他们可利用 SandBlast 威胁仿真基于云的服务。

©2015 Check Point Software Technologies Ltd. All rights reserved. [Protected] Non-confidential content | August 25, 2015

TE1000X SandBlast 设备

1. 2 x 2 TB 硬盘
2. 2 x USB 端口
3. 控制台端口
4. 10/100/1000Base-T 管理端口
5. 10/100/1000Base-T 同步端口
6. 4 x 10/100/1000Base-T 端口
7. 2 x 10GBase-F SFP+端口



部署选项

在下列部署选项之一中仿真威胁：

1. 私有云：Check Point 安全网关将文件发送到 SandBlast 设备进行仿真
2. 内联：这是一种独立选项，内联或通过 SPAN 端口部署 SandBlast 设备，利用威胁仿真、威胁净化、反病毒和反僵尸软件刀片来确保流量安全。

全面威胁防护

SandBlast 设备通过反病毒、反僵尸、威胁仿真（沙盒）和威胁净化技术保护你免遭已知和未知威胁攻击。

SANDBLAST 零日防护

SandBlast 威胁仿真技术利用最快速、最准确的沙盒引擎来预筛选文件，在攻击者进入你的网络前，保护你的组织免遭其攻击。

已知威胁检测

反病毒软件刀片利用 ThreatCloud™的实时病毒签名，在用户受到影响前，在网关处检测和拦截已知恶意软件。反僵尸软件刀片检测感染僵尸的计算机，通过拦截僵尸的指挥与控制通信而防止破坏。

抗逃逸检测

传统沙盒解决方案在 OS 层检测恶意软件行为，往往在漏洞利用发生及黑客代码运行之后。因此，它们易被逃逸。

SandBlast 威胁仿真能力利用独特的 CPU 层检测引擎，监控 CPU 层指令流，以检测企图绕过 OS 安全控制的漏洞利用，在攻击发起前有效阻止攻击。

前瞻性防御迅速交付安全内容

对于威胁防御，不一定要在速度、覆盖和准确性之间寻求平衡。与其它解决方案不同，Check Point 零日防护可以防御模式部署，同时仍能保持业务流不中断。

SandBlast 威胁净化清除可利用内容，包括活动内容和嵌入式对象，重构文件，消除潜在威胁，并向用户迅速交付净化内容，保持业务流不中断。

以下列方式之一配置威胁净化：向用户快速提供重构的文件，或在决定是否重构文件前，等待 SandBlast 威胁仿真的响应。

检测加密通信

通过 SSL 和 TLS 交付给组织的文件代表一种可绕过许多行业标准实施的安全攻击向量。Check Point 威胁防御查看这些受保护 SSL 和 TLS 隧道内部，以提取和运行文件，发现隐藏的威胁。

威胁仿真详细报告

每次文件仿真生成一份详细报告。报告易于理解，包括关于运行该文件所发起的任何恶意企图的详细取证信息。报告提供了运行文件的仿真环境的实际屏幕截图。

威胁云生态系统

对威胁仿真发现的每个新威胁，创建新签名，并发送给 Check Point ThreatCloud，以分发给其它 Check Point 联网网关。威胁仿真将新识别的未知攻击变成已知签名，以在其扩散前拦截这些威胁。这种持续协作使 ThreatCloud 生态系统成为最高级、最新的威胁网络。

©2015 Check Point Software Technologies Ltd. All rights reserved. [Protected] Non-confidential content | August 25, 2015

技术规格

	TE100X	TE250X	TE1000X	TE2000X / TE2000X HPP
				
性能				
推荐文件数/月	100K	250K	1M	1.5M / 2M
推荐用户数	高达 1,000	高达 3,000	高达 10,000	高达 20,000
吞吐量	150 Mbps	700 Mbps	2 Gbps	4 Gbps
虚拟机数量	4	8	28	40 / 56
硬件				
存储	1 TB HDD		冗余双热插拔 2 TB HDD, RAID1	
LOM	不包括			
滑轨 (22” - 32”)	包括			
网络				
10/100/1000Base-T RJ45	5	9	6	6
10GBase-F SFP+	-	-	2	4
扩展槽	未使用			
尺寸				
机箱	1U	1U	2U	2U
公制 (W x D x H)	435 x 448 x 44 mm	438 x 621 x 44 mm	438 x 561 x 88 mm	
标准 (W x D x H)	17.13 x 17.64 x 1.63 in.	17.25 x 24.45 x 1.73 in.	17.24 x 22.1 x 3.46 in	
重量	7.7 kg (16.9 lbs.)	9.8 kg (21.6 lbs.)	17.05 kg (37.6 lbs.)	
环境				
工作	32º ~ 104ºF / 0º ~ 40ºC, (20~90%, 无冷凝)			
贮藏	-14° - 158°F / -10° - 70°, (20% - 90%，无冷凝)			
电源				
双热插拔	-	可选	包括	
AC 输入	100-240V			
频率	47-63 Hz			
单电源额定功率	250W	400W	400W	400W
最高功耗	50.4W	104W	225.6W	
最高热功率	172.2 BTU/h	355.7 BTU/h	771.5 BTU/h	
认证				
安全	CB, UL, 多列表, LVD, TUV			
排放	FCC, CE, VCCI, RCM			
环境	RoHS			

©2015 Check Point Software Technologies Ltd. All rights reserved. [Protected] Non-confidential content | August 25, 2015

设备包

基本配置 [1]	
TE100X SandBlast 设备，1 年期威胁仿真、威胁净化、反病毒和反僵尸服务（包括 4 台虚拟机的 Microsoft Windows 和 Office 许可证）	CPAP-TE100X-4VM
TE250X SandBlast 设备，1 年期威胁仿真、威胁净化、反病毒和反僵尸服务（包括 8 台虚拟机的 Microsoft Windows 和 Office 许可证）	CPAP-TE250X-8VM
TE1000X SandBlast 设备，1 年期威胁仿真、威胁净化、反病毒和反僵尸服务（包括 28 台虚拟机的 Microsoft Windows 和 Office 许可证）	CPAP-TE1000X-28VM
TE2000X SandBlast 设备，1 年期威胁仿真、威胁净化、反病毒和反僵尸服务（包括 40 台虚拟机的 Microsoft Windows 和 Office 许可证）	CPAP-TE2000X-40VM
TE2000X 高性能包 SandBlast 设备，1 年期威胁仿真、威胁净化、反病毒和反僵尸服务（包括 56 台虚拟机的 Microsoft Windows 和 Office 许可证）	CPAP-TE2000X-56VM-HPP
软件刀片包 [1]	
TE100X 设备的威胁仿真、威胁净化、反病毒和反僵尸年度服务	CPSB-TE-100-1Y
TE250X 设备的威胁仿真、威胁净化、反病毒和反僵尸年度服务	CPSB-TE-250-1Y
TE1000X 设备的威胁仿真、威胁净化、反病毒和反僵尸年度服务	CPSB-TE-1000-1Y
TE2000X 和 TE2000X HPP 设备的威胁仿真、威胁净化、反病毒和反僵尸年度服务	CPSB-TE-2000-1Y

[1] 2 年和 3 年 SKUs 可用，见在线产品目录

附件

接口卡和收发器	
10G 光纤端口 SFP+收发器模块 – 远程 (10GBase-LR)	CPAC-TR-10LR
10G 光纤端口 SFP+收发器模块 – 短程 (10GBase-SR)	CPAC-TR-10SR
备件和其它	
TE250X AC 电源	CPAC-PSU-TE250X
TE1000X 和 TE2000X 设备更换部件套装（包括 1 个硬盘驱动器和 1 个电源）	CPAC-SPARES-TE1000X/2000X

联系我们

全球总部 | 以色列特拉维夫市 Ha'Solelim 街 5 号，67897 | 电话: 972-3-753-4555 | 传真: 972-3-624-1100 | 电邮: info@checkpoint.com

美国总部 | 加利福尼亚州圣卡洛斯市 Skyway 路 959 号 300 室，94070 | 电话: 800-429-4391; 650-628-2000 | 传真: 650-654-4233 | www.checkpoint.com

©2015 Check Point Software Technologies Ltd. All rights reserved. [Protected] Non-confidential content | August 25, 2015