УСТРОЙСТВА CHECK POINT SANDBLAST

CHECK POINT SANDBLAST УСТРОЙСТВА

Остановят новые и неизвестные атаки

Преимущества продукта

- Предотвращает новые и неизвестные атаки в документах и исполняемых файлах
- Снижает стоимость, используя существующую инфраструктуру
- Максимизирует безопасность вместе с унифицированным управлением, мониторингом, отчетностью
- Усиливает защиту, автоматически взаимодействуя с ThreatCloud™

Возможности продукта

- Обнаруживает вредоносный код в более 40 форматах файлов, включая: Adobe PDF, Microsoft Office, Java, Flash, исполняемых архивах
- Защищает разные версии Windows от таргетированных атак
- Устройства с разной производительностью - от 100 тыс. до 2 млн проверяемых файлов в месяц
- Threat Extraction удаляет опасное содержимое для мгновенной доставки очищенных файлов
- Уникальная технология проверки на уровне ЦП останавливает вредоносный код до его выпонения, не давая ему возможности скрыться

ВНЕЗАПНО

С увеличением сложности киберугроз многие таргетированные атаки начинаются с использования уязвимостей в загружаемых файлах и вложениях email. Эти угрозы включают как новые эксплойты, так и модификации известных, отличающихся контрольными суммами, что крайне затрудняет их обнаружение традиционными решениями.

Новые и не обнаруживаемые опасности требуют новых подходов, не полагающихся на сигнатуры известных угроз.

РЕШЕНИЕ

Check Point SandBlast устойчив к попыткам вредоносного ПО избежать обнаружения. Решение обеспечивает исчерпывающую защиту даже от наиболее опасных атак, сохраняя при этом быструю доставку пользователям безопасного содержимого. В основе лежат две уникальные технологии – Threat Emulation и Threat Extraction, которые поднимают защиту на следующий уровень. Являясь частью решения Check Point SandBlast, движок Threat Emulation перехватывает вредоносное ПО уже на стадии эксплойта, до попытки применения техник, препятствующих обнаружению в песочнице. Файлы инспектируются в виртуальной песочнице для обнаружения опасного внедренного кода и помещаются в карантин, предотвращая их распространение в сети. Инновационная технология совмещает инспекцию в песочнице на уровне операционных систем и на уровне центрального процессора (CPU-level inspection), обнаруживая и останавливая самые опасные эксплойты, таргетированные атаки и атаки нулевого дня.

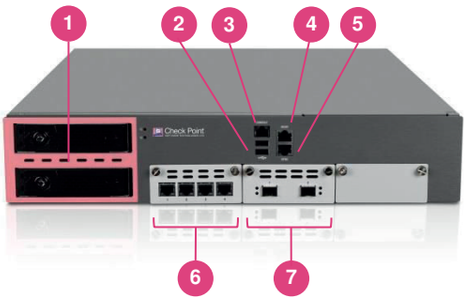
Кроме того, компонента SandBlast Threat Extraction создает для пользователей безопасную версию потенциально опасного содержимого. Содержимое, включающее макросы и внедренные объекты, удаляется, а документ реконструируется для исключения потенциальных угроз. Доступ к оригинальному документу блокируется до тех пор, пока он не будет полностью проанализирован. Пользователи получают моментальный доступ к безопасному содержимому документа и могут быть полностью уверены в своей защите даже от самых продвинутых атак и вредоносного ПО.

УСТРОЙСТВА SANDBLAST

Мы предлагаем большой выбор устройств SandBlast**.** Они отлично подходят компаниям, которые не могут использовать облачный сервис эмуляции SandBlast Threat Emulation вследствие принятых политик, требований регуляторов или иных причин.

Пример: TE1000X SandBlast Appliance

1. 2 x 2 TB жесткий диск
2. 2 x USB порта
3. Консольный порт
4. 10/100/1000Base-T порт управления
5. 10/100/1000Base-T порт синхронизации
6. 4 x 10/100/1000Base-T порты
7. 2 x 10GBase-F SFP+ порты



ВАРИАНТЫ ВНЕДРЕНИЯ

Эмуляция угроз на ваш выбор:

1. Частное облако: Шлюзы Check Point отправляют файлы на проверку на устройство SandBlast
2. Inline: Устройство SandBlast подключается в разрыв или на SPAN порт, задействуя блейды Threat Emulation, Threat Extraction, Anti-Virus и Anti-Bot для обеспечения безопасности трафика.

ИСЧЕРПЫВАЮЩАЯ ЗАЩИТА ОТ УГРОЗ

Устройство SandBlast защищает вас как от известных, так и неизвестных угроз с помощью компонент Antivirus, Anti-Bot, Threat Emulation и Threat Extraction.

SANDBLAST - ЗАЩИТА НУЛЕВОГО ДНЯ

Технология SandBlast Threat Emulation представляет собой наиболее быструю и точную песочницу для анализа поведения файлов и защиты вашей организации от угроз до того, как они попадут в вашу сеть.

ОБНАРУЖЕНИЕ ИЗВЕСТНЫХ УГРОЗ

Программный блейд Antivirus использует сигнатуры вирусов, получаемые в реальном времени из ThreatCloud™ для обнаружения и блокирования вредоносного кода непосредственно на шлюзе, предотвращая заражение пользователей. Блейд Anti-Bot обнаруживает ПК, инфицированные ботами, предотвращая ущерб, блокируя их взаимодействие с командными центрами.

СКРЫТЬСЯ НЕВОЗМОЖНО

Традиционные песочницы обнаруживают вредоносное ПО по поведению на уровне операционной системы, после того, как заражение состоялось и вредоносный код запустился. Как следствие, их можно обмануть.

SandBlast Threat Emulation использует уникальную технологию CPU-level inspection, которая отслеживает ход выполнения программы на уровне инструкций ЦП. Таким образом обнаруживает уже саму попытку внедрения вредоносного кода, а не последствия этого. Это позволяет противостоять самым изощренным попыткам обмануть песочницу и остаться незамеченным.

ПРОАКТИВНОЕ ПРЕДОТВРАЩЕНИЕ С МОМЕНТАЛЬНОЙ ДОСТАВКОЙ БЕЗОПАСНОГО СОДЕРЖИМОГО

Когда дело доходит до предотвращения угроз, не обязательно идти на компромисс между скоростью, полнотой и точностью проверок. В отличие от многих других решений Check Point Zero-Day Protection может работать в режиме предотвращения, обеспечивая при этом непрерывность бизнес-процессов.

SandBlast Threat Extraction удаляет опасное содержимое, включая макросы, внедренные объекты, реконструирует файлы для исключения потенциальных угроз и моментально доставляет очищенную информацию пользователям.

Threat Extraction можно настроить как для моментальной доставки реконструированного содержимого пользователю, так и с ожиданием подтверждения от SandBlast Threat Emulation о безопасности исходного документа с последующей его доставкой.

ПРОВЕРЯЕТ ЗАШИФРОВАННЫЙ ТРАФИК

Файлы, приходящие в организацию по протоколам SSL и TLS, представляют вектор атаки, способный обойти многие стандартные внедрения систем защиты. Check Point Threat Prevention просматривает в том числе SSL, TLS для извлечения файлов и их проверки на скрытые угрозы.

ДЕТАЛЬНЫЙ ОТЧЕТ THREAT EMULATION

При эмуляции каждого файла создается детальный отчет. Для простоты понимания отчеты включают информацию о потенциальных угрозах, возникающих при открытии файла. Они так же включают актуальные скриншоты, появляющиеся в виртуальной среде в процессе эмуляции.

ЭКОСИСТЕМА THREATCLOUD

Для каждой новой угрозы, выявленной Threat Emulation, создается новая сигнатура и отсылается в Check Point ThreatCloud. Оттуда впоследствии распространяется на подключенные к нему шлюзы Check Point. Threat Emulation конвертирует ранее неизвестные и только что идентифицированные угрозы в известные сигнатуры, давая возможность блокировать эти угрозы до того, как они получат шанс широко распространиться. Такое постоянное взаимодействие делает экосистему ThreatCloud наиболее продвинутой и актуальной из имеющихся.

СПЕЦИФИКАЦИЯ

	TE100X	TE250X	TE1000X	TE2000X / TE2000X HPP
				
Производительность				
Рекомендуется, файлов в месяц	100 тыс	250 тыс	1 млн	1.5 млн / 2 млн
Рекомендуется, пользователей	До 1,000	До 3,000	До 10,000	До 20,000
Производительность	150 Mbps	700 Mbps	2 Gbps	4 Gbps
Количество виртуальных машин	4	8	28	40 / 56
Аппаратное обеспечение				
Хранилище	1 TB HDD		Резервированные, горячей замены 2 TB HDD, RAID1	
LOM	Не включено			
Рельсы (22” to 32”)	Включено			
Сеть				
10/100/1000Base-T RJ45	5	9	6	6
10GBase-F SFP+	-	-	2	4
Слоты расширения	Не используются			
Размеры				
Форм-фактор	1U	1U	2U	2U
Ширина, глубина, высота	435 x 448 x 44 мм	438 x 621 x 44 мм	438 x 561 x 88 мм	
В люймах (W x D x H)	17.13 x 17.64 x 1.63	17.25 x 24.45 x 1.73	17.24 x 22.1 x 3.46	
Вес	7.7 кг (16.9 lbs.)	9.8 кг (21.6 lbs.)	17.05 кг (37.6 lbs.)	
Окружение				
Рабочее	32º ~ 104ºF / 0º ~ 40ºC, (20~90%, без конденсации)			
При хранении	-14° to 158°F / -10° to 70°, (20% - 90% без конденсации)			
Питание				
Два БП горячей замены	-	Возможно	Включено	
Переменный ток	100-240V			
Частота	47-63 Hz			
Мощность блока питания	250W	400W	400W	400W
Максимальное потребление	50.4W	104W	225.6W	
Максимальная теплоотдача	172.2 BTU/h	355.7 BTU/h	771.5 BTU/h	
Сертификации				
Безопасность	CB, UL, Multiple Listing, LVD, TUV			
Излучение	FCC, CE, VCCI, RCM			
Среда	RoHS			

ВАРИАНТЫ КОМПЛЕКТАЦИИ

БАЗОВАЯ КОНФИГУРАЦИЯ [1]	
TE100X SandBlast Appliance with 1 year Threat Emulation, Threat Extraction, Antivirus and Anti-Bot annual service (includes Microsoft Windows and Office license for 4 Virtual Machines)	**CPAP-TE100X-4VM**
TE250X SandBlast Appliance with 1 year Threat Emulation, Threat Extraction, Antivirus and Anti-Bot annual service (includes Microsoft Windows and Office license for 8 Virtual Machines)	**CPAP-TE250X-8VM**
TE1000X SandBlast Appliance with 1 year Threat Emulation, Threat Extraction, Antivirus and Anti-Bot annual service (includes Microsoft Windows and Office license for 28 Virtual Machines)	**CPAP-TE1000X-28VM**
TE2000X SandBlast Appliance with 1 year Threat Emulation, Threat Extraction, Antivirus and Anti-Bot annual service (includes Microsoft Windows and Office license for 40 Virtual Machines)	**CPAP-TE2000X-40VM**
TE2000X High Performance Pack SandBlast Appliance with 1 year Threat Emulation, Threat Extraction, Antivirus and Anti-Bot annual service (includes Microsoft Windows and Office license for 56 Virtual Machines)	**CPAP-TE2000X-56VM-HPP**
НАБОРЫ ПРОГРАММНЫХ БЛЕЙДОВ [1]	
Threat Emulation, Threat Extraction, Antivirus and Anti-Bot annual service for the TE100X Appliance	**CPSB-TE-100-1Y**
Threat Emulation, Threat Extraction, Antivirus and Anti-Bot annual service for the TE250X Appliance	**CPSB-TE-250-1Y**
Threat Emulation, Threat Extraction, Antivirus and Anti-Bot annual service for the TE1000X Appliance	**CPSB-TE-1000-1Y**
Threat Emulation, Threat Extraction, Antivirus and Anti-Bot annual service for the TE2000X and TE2000X HPP Appliance	**CPSB-TE-2000-1Y**

[1] SKUs for 2 and 3 years are available, see the online Product Catalog

АКСЕССУАРЫ

СЕТЕВЫЕ КАРТЫ И ТРАНСИВЕРЫ	
SFP+ transceiver module for 10G fiber ports - long range (10GBase-LR)	**CPAC-TR-10LR**
SFP+ transceiver module for 10G fiber ports - short range (10GBase-SR)	**CPAC-TR-10SR**
ЗАПАСНЫЕ ЧАСТИ	
AC Power Supply for TE250X	**CPAC-PSU-TE250X**
Replacement parts kit (including 1 Hard Disk Drive and one Power Supply) for TE1000X and TE2000X appliances	**CPAC-SPARES-TE1000X/2000X**

КОНТАКТЫ

Международная штаб-квартира
5 Ha'Solelim Street, Tel Aviv 67897, Israel | Телефон: 972-3-753-4555 | Факс: 972-3-575-9256 | Эл. почта: info@checkpoint.com | http://checkpoint.com

Представительство в России и СНГ
Check Point Software Technologies (Russia) | 109240, Москва, ул. Николоямская, д. 13, стр. 17 | Тел./факс: +7 495 967 7444