CHECK POINT SANDBLAST AGENT

CHECK POINT SANDBLAST AGENT

CON ***ANTI-RANSOMWARE***

El Poder de Proteger.
La Visión para Entender.

Beneficios

- Solución EDR* completa con capacidades avanzadas de prevención
- Previene y neutraliza ataques de ransomware evasivos
- Bloquea de forma proactiva malware desconocido y de día cero
- Proporciona al instante información de utilidad para comprender los ataques
- Remedia infecciones automáticamente
- Protege las credenciales de los usuarios

Funcionalidades

- **Threat Emulation:** Tecnología sandbox resistente a evasiones
- **Threat Extraction:** Proporciona a los usuarios archivos desinfectados y libres de riesgos en tiempo real
- **Anti-ransomware:** Previene y neutraliza el ransomware evasivo
- **Zero-Phishing:** Bloquea sitios de phishing y alerta sobre la reutilización de contraseñas
- **Anti-Bot:** Identifica y aísla los servidores y hosts infectados
- **Forensics:** registra y analiza todos los eventos en los end-points aportando informes forenses procesables.

** EDR: Detección y Respuesta para end-points*

LA SITUACIÓN

El aumento en las brechas causadas por el malware, el ransomware y los sofisticados ataques de ingeniería social ha convertido a los end-points en un punto de entrada frecuente para las ciberamenazas. Esos ataques pueden estar ocultos en contenido descargado de Internet, archivos adjuntos en emails, dispositivos de almacenamiento extraíbles o recursos compartidos de red. Los empleados pueden, sin saberlo, convertirse en víctimas de este tipo de ataques, que dan lugar a grandes pérdidas financieras, fugas de datos y pérdidas de productividad. Incluso la simple acción de reutilizar contraseñas y credenciales corporativas para servicios web fuera del negocio puede poner en peligro la organización. Al mismo tiempo, los usuarios demandan protección en tiempo real que puedan dar soporte a su necesidad de acceso sin restricciones y de entrega inmediata de información crítica y correos electrónicos.

Además, cada vez más empleados que utilizan dispositivos de empresa para trabajar de forma remota, y a medida que y más personal subcontratado o contratistas externos incorporan sus propios sistemas a la empresa, los cibercriminales atacan las debilidades de la seguridad "tradicional" para infiltrarse e infectar estos sistemas. Una vez dentro, los hackers aprovechan las comunicaciones "laterales" a través de la red para infectar otros dispositivos adicionales. A medida que las amenazas evolucionan, las organizaciones deben encontrar nuevas formas de detectar, prevenir y responder con rapidez ante los ataques contra los end-points a fin de limitar y reparar los daños.

Por tanto ¿cómo mantener a los empleados a salvo de estas amenazas emergentes, permitiéndoles al mismo tiempo trabajar al ritmo que el negocio exige?

LA SOLUCIÓN

Check Point SandBlast Agent ofrece funciones avanzadas de protección de día cero especialmente diseñadas para navegadores web y dispositivos end-point, aprovechando la tecnología líder de protección de redes de Check Point. SandBlast Agent asegura una cobertura completa y en tiempo real para todos los vectores de amenaza, permitiendo que los empleados trabajen de forma segura con independencia de dónde se encuentren y sin comprometer la productividad. *Threat Emulation* permite emular archivos desconocidos en un entorno aislado para detectar comportamientos maliciosos y prevenir infecciones, en tanto que *Threat Extraction* proporciona archivos desinfectados a los usuarios al instante.

Check Point SandBlast Agent incluye *Anti-Ransomware*, una protección construida específicamente para proteger contra este tipo de amenazas, y que detiene el ransomware cuando está de camino y neutraliza el daño automáticamente, asegurando que las organizaciones están protegidas contra esta forma de extorsión que cifra datos de negocio para posteriormente demandar el pago de un rescate por su recuperación.

Mediante la tecnología *Zero Phishing*, SandBlast Agent bloquea de forma proactiva el acceso a sitios web nuevos y desconocidos, y protege las credenciales de los usuarios al impedir el uso de contraseñas corporativas en sitios web externos.

SandBlast Agent captura datos forenses a través de una recopilación continua de todos los eventos de sistema relevantes, para luego proporcionar análisis procesables que servirán para entender rápidamente el ciclo de vida completo de los ataques. A través de una total visibilidad sobre el alcance, el daño y los vectores de ataque, los equipos de respuesta maximizarán su productividad y minimizarán la exposición.

PREVENCIÓN DE ATAQUES DE DÍA CERO

Check Point SandBlast Agent amplía las soluciones de protección SandBlast Zero-Day Protection a los dispositivos *end-point* y a los navegadores web. Threat Extraction reconstruye en pocos segundos los archivos descargados, eliminando posibles amenazas, para entregar al instante una versión segura al usuario. Al mismo tiempo, Threat Emulation detecta comportamientos maliciosos e impide infecciones de nuevo malware y ataques dirigidos inspeccionando rápidamente los archivos en un entorno virtual.

PROTECCIÓN CONTRA RANSOMWARE

La protección anti-ransomware de SandBlast Agent evita los ciberataques evasivos de extorsión que pueden sortear los antivirus convencionales y otras soluciones de protección contra malware. El ransomware impacta en la empresa mediante el cifrado de archivos y la posterior petición de un rescate para su recuperación. Anti-Ransomware utiliza un motor de análisis de conducta especialmente diseñado para este propósito, capaz de detectar y remediar infecciones de ransomware en el end-point. Su tecnología sin firma evita depender de actualizaciones continuas y puede funcionar tanto *online* como *offline*. Las infecciones de Ransomware son automáticamente aisladas y puestas en cuarentena en función del análisis forense de SandBlast Agent. Finalmente, Anti-Ransomware restaura automáticamente los archivos que fueron cifrados antes de la contención del ataque.

BLOQUEO DE ATAQUES DE PHISHING DE DÍA CERO

La capacidad *Zero Phishing* incluida en SandBlast Agent utiliza análisis dinámico y heurística avanzada para identificar y prevenir el acceso a sitios de *phishing* nuevos y desconocidos contra las credenciales de los usuarios en tiempo real a través del navegador.

Además, esta capacidad evita el robo de credenciales corporativas a partir de brechas de contraseñas en sitios de terceros alertando al usuario cuando éste viola las políticas de utilización de contraseñas corporativas.

IDENTIFICACIÓN Y CONTENCIÓN DE INFECCIONES

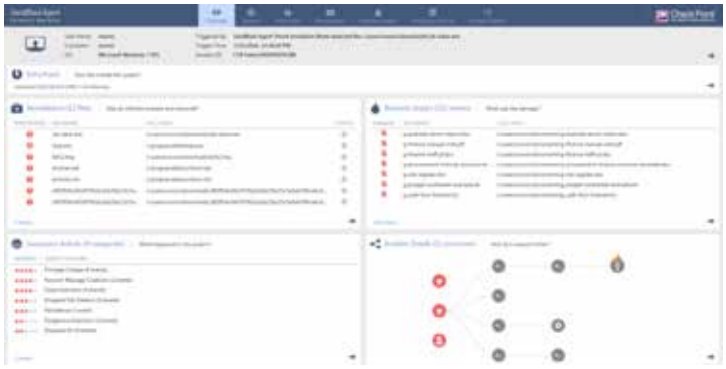
Con una versión local de la protección de seguridad Anti-Bot, actualizada continuamente con los últimos datos de *Threat Intelligence* a través de ThreatCloud, SandBlast Agent identifica y bloquea las comunicaciones entre las redes *bot* y los servidores *Command & Control* de la organización para aislar y poner en cuarentena los servidores infectados.

COBERTURA COMPLETA A LO LARGO DE LOS IFERENTES VECTORES DE AMENAZA

El Agente SandBlast protege a los usuarios ante amenazas que se introducen a través de descargas web, mediante técnicas como *phishing*, contenido malicioso copiado de unidades extraíbles, infecciones causadas por el movimiento "lateral" de datos y malware entre sistemas en un segmento de red, así como infecciones transmitidas a través de contenido cifrado.

VISIBILIDAD TOTAL DE EVENTOS DE SEGURIDAD

Check Point SandBlast Agent proporciona una visibilidad completa a través sus capacidades forenses, monitorizando y registrando todos los eventos de seguridad en los dispositivos *end-point*: archivos afectados, procesos iniciados, cambios en el registro del sistema y actividad de la red. SandBlast Agent puede rastrear y reportar los pasos seguidos por el malware, incluyendo amenazas de día cero. La monitorización de SandBlast Agent asegura que los datos estarán disponibles una vez completado el ataque, incluso aunque se hayan eliminado archivos, y también otros indicadores de peligro hallados en el sistema.



ANÁLISIS DE INCIDENTES PARA LA TOMA DE ACCIONES

Cada vez que se produce un evento de malware, SandBlast Agent inicia automáticamente un proceso de análisis forense. A través de una combinación de algoritmos avanzados y un profundo análisis de los datos forenses brutos, se construye un informe completo sobre la incidencia. Este informe proporciona información clave sobre el ataque, incluyendo:

Eventos maliciosos. ¿Qué pruebas de comportamiento sospechoso fueron detectadas durante el ciclo de vida del ataque?

Puntos de entrada. ¿Cómo penetró el ataque en la red? ¿Cuáles fueron los elementos principales utilizados? ¿Cómo se inició?

Alcance de los daños. ¿Qué hizo el malware, una vez activado, que pueda afectar al negocio? ¿Qué datos fueron comprometidos y/o filtrados al exterior?

Servidores infectados. ¿Quién o qué más ha sido afectado?

Este completo diagnóstico y visibilidad sobre los ataques complementa los esfuerzos de mitigación. Los administradores de sistemas y los equipos de respuesta ante incidentes pueden manejar y resolver los ataques de forma rápida y eficiente, haciendo que la organización retorne a su operativa habitual lo más rápido posible.

INFORMES DE INCIDENCIAS DETALLADOS

Las capacidades de análisis forense de SandBlast Agent permiten ver desde un punto central todos los informes de eventos, lanzados por el *gateway* o por el propio *end-point*, mediante la herramienta *SmartEvent*. Por su parte, los administradores podrán generar sus propios informes sobre eventos conocidos a través de análisis de tipo *kill chain*. Estos informes proporcionan una analítica procesable, acelerando la comprensión del ciclo de vida del ataque, los daños y los diferentes vectores de amenaza.

INTEGRACIÓN CON ENTORNOS DE TERCEROS

SandBlast Agent trabaja en conjunto con la tecnología antivirus y otras soluciones de seguridad, tanto de Check Point como de otros proveedores, mejorando las capacidades de detección de los productos antivirus existentes, aportando protección contra amenazas avanzadas y proporcionando análisis de incidentes accionables.

Cuando son activados como consecuencia de un evento o por una solicitud de investigación desde otro componente de Check Point o desde una solución de terceros, estos registros forenses sobre *end-points* son analizados para generar informes accesibles desde SmartEvent y SmartLog.

LA FAMILIA DE SOLUCIONES SANDBLAST

La *suite* de soluciones SandBlast Zero-Day Protection también incluye otros productos que proporcionan protección avanzada para redes corporativas (SandBlast Network) y para aplicaciones en la nube (SandBlast Cloud).

FLEXIBILIDAD EN EL DESPLIEGUE, SENCILLEZ EN LA GESTIÓN

SandBlast Agent ofrece flexibles opciones de implementación para atender a las necesidades de seguridad de cada organización. Hay tres paquetes disponibles:

SandBlast Agent for Browsers

SandBlast Agent for Browsers es una extensión para navegadores diseñada para la prevención de ataques que utilizan estos programas como punto de entrada. Incluye *Threat Emulation, Threat Extraction, Zero Phishing* y protección de credenciales.

Esta solución *stand-alone* se puede implementar utilizando un sencillo *plugin* de navegador simple y encaja a la perfección en organizaciones que buscan un despliegue rápido con un impacto mínimo. SandBlast Agent for Browsers utiliza herramientas estándar para administración de *end-points*, como GPO (*Group Policy Object*), que ayuda a implementar las políticas en los dispositivos de los usuarios.

SandBlast Agent

SandBlast Agent previene las amenazas contra dispositivos *end-point*. Incluye *Threat Emulation, Threat Extraction, Zero Phishing*, Anti-Ransomware, *Anti-Bot* y análisis forense.

SandBlast Agent se despliega rápidamente, y todas las políticas se administran de forma centralizada a través de SmartCenter. A través de SmartEvent y SmartLog, el administrador puede acceder a los registros de eventos e informes sobre incidentes que le aportarán una visión más profunda y una mejor compresión de los ataques, incluso de los más avanzados.

Endpoint Complete Protección

La suite Endpoint Complete Protection de Check Point añade a SandBlast Agent cifrado completo de disco, antivirus y firewall

Con independencia del paquete que seleccione, el despliegue no intrusivo y de bajo nivel utiliza un entorno *sandbox* aislado del sistema que funciona como servicio, ya sea dentro del propio servicio de SandBlast o en los dispositivos privados del cliente, con un impacto mínimo en el rendimiento local y una total compatibilidad con las aplicaciones existentes.

ESPECIFICACIONES TÉCNICAS

SANDBLAST AGENT - PAQUETES	
Paquetes disponibles	• **SandBlast Agent for Browsers**. Incluye Threat Emulation, Threat Extraction, Zero Phishing y Credential Protection • **SandBlast Agent**. Incluye Threat Emulation, Threat Extraction, Anti-Ransomware, Zero Phishing, protección de credenciales, Anti-Bot, análisis forense y análisis automático de incidentes • **Endpoint Complete Protection**. Protección completa para *end-points* que añade a SandBlast Agent cifrado completo de disco, antivirus y firewall
ENDPOINT SECURITY – SANDBLAST AGENT	
Sistemas operativos	• Windows 7, 8 y 10 • Windows Server 2008 R2, 2012 y 2012 R2
BROWSER PROTECTION – SANDBLAST AGENT FOR BROWSERS	
Navegadores soportados	• Google Chrome • *Próximamente: Internet Explorer, Firefox*
DOWNLOAD PROTECTION - THREAT EMULATION AND THREAT EXTRACTION	
Threat Extraction – Tipos de archivo soportados	• Adobe PDF • Microsoft Word, Excel, PowerPoint
Threat Emulation – Tipos de archivo soportados	• Más de 40 tipos de archive, incluyendo: Adobe PDF, Microsoft Word, Excel y PowerPoint, ejecutables (EXE, COM, SCR), Shockwave Flash (.SWF), texto enriquecido (.RTF) y "Archivos"
Opciones de despliegue	• SandBlast Service (alojado en la nube de Check Point) • SandBlast Appliance (alojado en las instalaciones del cliente)
ANTI-RANSOMWARE	
Anti-Ransomware	• Detección de ransomware sin firma, a través de análisis de conducta. No requiere conexión a Internet • Detección de actividades maliciosas de cifrado de archivos • Cuarentena automática de ransomware • Restauración automatizada de datos encriptados (si el cifrado comenzó antes de la cuarentena)
ZERO PHISHING AND CREDENTIAL PROTECTION	
Zero Phishing	• Protección en tiempo real de sitios de *phishing* desconocidos • Detección estática y heurística de elementos sospechosos en sitios que solicitan credenciales de usuario
Protección de credenciales corporativas	• Detección de reutilización de credenciales corporativas en sitios externos
MONITORIZACIÓN DEL SISTEMA DE FICHEROS	
Threat Emulation	• Contenidos copiados desde unidades de almacenamiento extraíbles • Movimiento "lateral" de datos y malware entre sistemas en un segmento de red
Modos de aplicación	• Detección y notificación • Bloqueo (modo "*Background*" / modo "*Hold*")
ANTI-BOT	
Modos de aplicación	• Detección y notificación • Bloqueo (modo "*Background*" / modo "*Hold*")
FORENSICS	
Activadores de análisis	• Detección Anti-ransomware en el end-point • Detección Anti-Bot en la red o en el end-point • Detección Threat Emulation en la red • Detección Antivirus en el end-point • Detección Antivirus de terceros en el end-point • Indicadores manuales de elementos comprometidos (IoCs)
Detección de daños	• Identificación automática de exfiltración, manipulación o encriptación de datos. Registro de contraseñas
Análisis de causa raíz	• Rastreo e identificación de causas raíz in real-time a lo largo de múltiples reinicios del sistema
Análisis de flujos de malware	• Generación automática de modelos gráficos de los flujos de ataque
Detección de conductas maliciosas	• Más de 40 categorías de conductas maliciosas • Cientos de indicadores maliciosos
GESTIÓN	
Gestión de políticas	• Gestión de políticas para end-points (EPM)
Monitorización de eventos	• SmartLog • SmartEvent
Gestión de *end-points* (version)	• R77.30.03/E80.65 y superior
Gestión de *end-points* (paquetes disponibles)	• Incluido de serie con los *appliances* SmartCenter y Smart-1 • Disponible como licencia de software

CONTACTE CON NOSOTROS

Worldwide Headquarters | 5 Ha'Solelim Street, Tel Aviv 67897, Israel | Tel: 972-3-753-4555 | Fax: 972-3-624-1100 | Email: info@checkpoint.com
U.S. Headquarters | 959 Skyway Road, Suite 300, San Carlos, CA 94070 | Tel: 800-429-4391; 650-628-2000 | Fax: 650-654-4233 | **www.checkpoint.com**