ENDPOINT SECURITY

EVOLUTION

Aumente el nivel de protección de sus puestos de trabajo con una solución EDR proactiva

Instalación

ON-PREM Y SAAS

API REST

INTEGRACIÓN EN EL ECOSISTEMA

Ultra personalizable

PARÁMETROS DE SEGURIDAD AJUSTABLES

Autónomo

POLÍTICA DE SEGURIDAD ADAPTADA

Máxima protección con nuestra solución EDR

La solución de protección de puestos de trabajo y servidores de nueva generación. Basada en una tecnología de análisis sin firmas, el agente detecta ataques y amenazas y responde de manera adecuada.

Seguridad proactiva

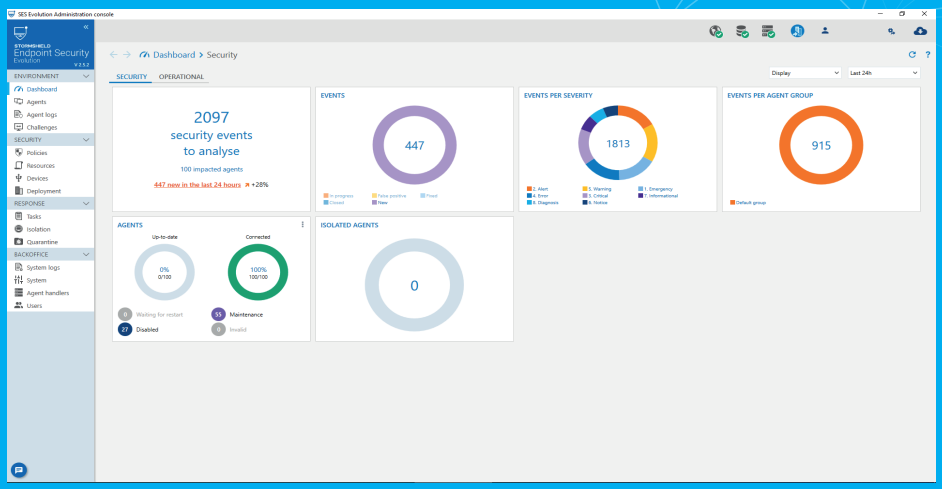
- Ataque bloqueado en tiempo real
- Análisis y reparación predefinidos y personalizables
- Gráfico de ataques y Threat Hunting (reglas IoC, Yara, etc.)

Análisis conductual

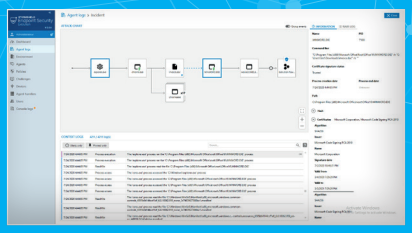
- Protección contra ataques de día cero
- Combate las técnicas de explotación de vulnerabilidades
- Protección antiransomware

Protección contextual

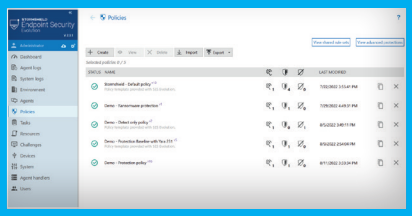
- La política de seguridad se adapta dinámicamente al entorno, incluso sin conexión
- Políticas personalizables por grupo de usuarios
- Políticas de seguridad predeterminadas actualizadas por los equipos del Stormshield Customer Security Lab



Cuadro de mando



Vista detallada de un incidente



Política de seguridad

FUNCIONES

Protección día cero contra las amenazas conocidas y desconocidas

Técnicas de análisis conductual

- Corrupción de memoria (buffer overflow, heap spray)
- Elevación de privilegios (token stealing)
- Robo de información sensible (keylogging, acceso a procesos)
- Process hollowing y sus variantes
- Inyección de código (application hooking)
- Protección contra los ataques sin archivo

Protección contra ransomware

- Identificación de procesos de cifrado dañinos
- Restauración de archivos cifrados por ransomware
- Windows Shadow Copy
- Política de copias de seguridad

Protección sin firma

Remediación personalizada

- Eliminar un proceso
- Eliminar un archivo
- Eliminar o modificar una clave del registro o su valor
- Uso de scripts PowerShell para acciones personalizadas (detención y eliminación de un servicio, etc.)
- Cuarentena automática de malware
- Aislamiento de los puestos de trabajo comprometidos

Identificación de indicadores de compromiso (IoC)

- Texto sospechoso (nombre de archivo, nombre de host, nombre de objeto, etc.)
- Información de red (direcciones IP, URL sospechosas, DNS)
- Hash SHA1, SHA256, MD5 y SSDEEP
- Búsqueda manual, programada o por detección
- Protección contra la evasión de los sistemas de detección de EDR

Control de periféricos

- Redes wifi
- Memorias USB
- Bluetooth
- Acceso a los volúmenes de disco
- Conexiones de red
- Control de ejecución

Agente optimizado

- Consumo de memoria
- Consumo de CPU

Política de seguridad

- Adaptación dinámica en función del contexto
- Conjunto de reglas de análisis conductual y de control de periféricos proporcionado y mantenido por Stormshield
- Soporte de las reglas Yara

Administración centralizada

- Gestión de la política por grupos de agentes
- Gestión de los administradores por función
- Activación/desactivación de los módulos por grupos de agentes
- API REST para la integración con productos de terceros
- Informe de actividad con indicadores MCS y MCO en formato HTML
- Notificación automática por correo electrónico de las alertas de seguridad

COMPATIBILIDAD

AGENTE

Recursos

CPU:
1 core 1 GHz (mín.) - 2 cores 2 GHz (recomendado)

RAM:
1 GB (mín.) - 2 GB (recomendado)

Espacio en el disco:
100 MB (instalación) - 200 MB (datos)

Sistema operativo

Cliente:
Windows 7 SP1, 8.1, 10 y 11

Servidor:
Windows Server 2008 R2, 2012 R2, 2016, 2019 y 2022 (incluida la versión Core)

ADMINISTRACIÓN

Posibilidad de gestión SaaS u on-premise

PARA LA ADMINISTRACIÓN ON- PREMISE

Backend

CPU:
1 core 1 GHz (mín.) - 2 cores 2 GHz (recomendado)

RAM:
1 GB (mín.) - 2 GB (recomendado)

Espacio en el disco:
100 MB (instalación) - 200 MB (datos)

Servidor:
Windows Server 2012 R2, 2016, 2019 y 2022 (incluida la versión Core)

Gestor de agente

CPU:
2 cores 2 GHz (mín.)

RAM:
2 GB (mín.)

Espacio en el disco:
200 MB (instalación) - 1 GB (datos/mín.)

Cliente:
Windows 10 y 11

Servidor:
Windows Server 2008 R2, 2012 R2, 2016, 2019 y 2022 (incluida la versión Core)

Base de datos:
SQL Server 2017 y posterior