ONESECURITY

NUESTRA SOLUCION

Con ONESECURITY eliminamos las brechas de seguridad en cualquier actividad del usuario y en los endpoints, utilizando una combinación de técnicas avanzadas de protección contra amenazas, detección y respuesta. Todo esto se gestiona a través de una única plataforma con un solo agente, garantizando una defensa integral y eficiente.

ESPECIFICACIONES TÉCNICAS DE LA SOLUCIÓN DE PROTECCIÓN ENDPOINT

PROTECCIÓN AVANZADA CONTRA MALWARE

- Virus, troyanos, gusanos, spyware, ransomware y variantes emergentes.
- Malware avanzado, ataques sin archivos (fileless), cryptomining y ransomware.
- Prevención contra ataques de día cero y vulnerabilidades conocidas y desconocidas.
- Mecanismos proactivos basados en: Firmas actualizadas automáticamente.
- Análisis de comportamiento, heurística, reputación de archivos y web, con tecnología en la nube.

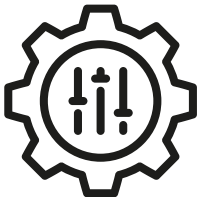
CARACTERÍSTICAS DE ENDPOINT PROTECTION PLATFORM (EPP) Y ENDPOINT DETECTION AND RESPONSE (EDR)

- Un solo agente para EPP y EDR.
- Detección, análisis y eliminación de:Virus, spyware, troyanos, keyloggers, rootkits, phishing, y más.
- Prevención de ataques explotando vulnerabilidades aún sin parches disponibles.
- Protección específica para navegadores contra scripts maliciosos.

MANEJO DE POLÍTICAS Y CONTROLES

CONSOLA CENTRALIZADA PARA:

Administración de reglas de acceso/bloqueo para aplicaciones y dispositivos.



Configuración de políticas de listas blancas y negras.

CAPACIDAD PARA:

Restringir dispositivos de almacenamiento USB, CD/DVD, y carpetas compartidas.

Asignar permisos como control total, solo lectura o bloqueo completo.

GESTIÓN CENTRALIZADA E INTEGRACIÓN

COMPATIBLE CON:

- Soluciones SIEM vía Syslog.
- Directorio Activo, con configuración e implementación incluidas.
- Integración con plataformas de terceros mediante API.

SEGURIDAD DE RED Y COMUNICACIÓN

MÓDULOS DE FIREWALL Y IDS/IPS INTEGRADOS, CON:

- Prevención de intrusiones basada en host (HIPS).
- Reglas de bloqueo para puertos, accesos indebidos y protocolos específicos.
- Protección contra desbordamiento de búfer (buffer overflow).
- Bloqueo de paquetes de tipo exploit dirigidos a sistemas operativos, aplicaciones y bases de datos.

PREVENCIÓN DE PÉRDIDA DE DATOS (DLP)

- Nativamente integrada en la suite de seguridad para Endpoint y servidores.
- Detección basada en expresiones regulares y escaneos de contenido.
- Capacidad de creación y administración de políticas centralizadas.

CIFRADO DE DATOS

MÓDULO INTEGRADO PARA CIFRADO DE DISCOS, ARCHIVOS Y CARPETAS:

- Compatible con AES-256 y el estándar de seguridad FIPS 140-2

OPCIONES DE CIFRADO CON:

- Llaves locales o de grupo.
- Contraseñas fijas para compartir con usuarios externos.

COMPATIBILIDAD DEL SISTEMA OPERATIVO

- Windows 11, Windows 10 (32/64-bit), Windows 7 (32/64-bit).
- Servidores Windows Server 2019, 2016, 2012 R2, 2008 R2 (32/64-bit).
- MacOS.

ACTUALIZACIÓN Y ESCALABILIDAD

- Distribución incremental de actualizaciones desde la consola a clientes y servidores.
- Tecnología basada en cloud computing para optimizar reputación de archivos y sitios web.

REPORTES Y ALERTAS

- Reportes predefinidos y personalizados.
- Programación de alertas y notificaciones en tiempo real.

FLAMMAS

INTEGRACIÓN

ADAPTACIÓN CON ECOSISTEMAS DE FLAMMAS

- Comunicación en tiempo real: One Security envía eventos y alertas directamente a Marcus para su análisis y gestión.
- Soporte de protocolos estándar: Integración mediante Syslog, API RESTful y SNMP.
- Administración centralizada: Marcus gestiona políticas de seguridad sincronizadas con One Security.
- Detección y respuesta mejorada: Datos y análisis avanzados de amenazas compartidos entre ambos sistemas.