ONESECURITY

NUESTRA SOLUCIÓN

ONESECURITY es nuestra solución integral que combina técnicas avanzadas de protección contra amenazas en una arquitectura de agente único, diseñada para cerrar cualquier brecha de seguridad en las actividades de los usuarios y en cualquier dispositivo endpoint.

SEGURIDAD INTEGRAL PARA ENDPOINT

PROTECCIÓN AVANZADA ANTI-MALWARE

- Protección contra virus, troyanos, gusanos, spyware y variantes emergentes
- Ataques sin archivos (fileless), ransomware, cryptomining, etc
- 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 cloud computing
- Inteligencia de amenazas global y local para C&C, Botnet (IP, DNS, Malicious Networks)
- Evitar descargar componentes maliciosos
- Bloqueo de ejecución sin autorización o maliciosos (IP, User, Unknown/Known Application, Etc)

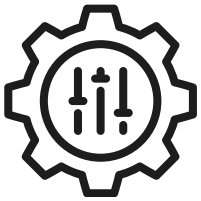
ENDPOINT PROTECTION PLATFORM (EPP) Y ENDPOINT DETECTION AND RESPONSE (EDR)

- Detección, análisis y eliminación de: Virus, Programas Publicitarios, spyware, troyanos, keyloggers, rootkits, phishing, etc
- Un solo agente para EPP y EDR
- Parches virtuales
- Capacidad de prevenir y detener ataques de malware que exploten vulnerabilidades sin parches disponibles
- Protección específica para navegadores contra scripts maliciosos

MANEJO DE POLÍTICAS Y CONTROLES

CONSOLA CENTRALIZADA

- Capacidad de configurar políticas de seguridad (IP, User, Application, Reputation (web, archivos), Etc)
- Consola On-Premise



- Capacidad de crear Whitelist/Blacklist (IP, User, Unknown/Known Application, Etc)
- Gestionar la configuración de todos los módulos de seguridad

CAPACIDAD

- Políticas de denegación de escritura
- Provisión y restricción de acceso a dispositivos de almacenamiento USB, CD/DVD y carpetas compartidas
- Creación de Whitelists para dispositivos USB, CD/DVD y carpetas compartidas autorizados.

- Asignación de permisos (full control, modification, read-only, read-only and execute, blocking access to content)
- Capacidad de configurar diferentes acciones como acceso, monitoreo y bloqueo (IP, User, Unknown/Known Application, Etc)

GESTIÓN CENTRALIZADA E INTEGRACIÓN

- Soluciones SIEM vía Syslog
- Disponible como servicio
- Directorio Activo
- Integración con plataformas de terceros mediante API
- Capacidad de integrarse en el ecosistema de soluciones Flammas (MARCUS, FLAMMAS SIEM, ONE SOAR)

SEGURIDAD DE RED Y COMUNICACIÓN

MÓDULOS DE FIREWALL Y IDS/IPS INTEGRADOS

- Prevención de intrusiones basada en host (HIPS)
- Reglas de bloqueo y acceso (unauthorized access, ports, protocols, application)
- 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
- Capacidad para extraer textos de distintos tipos de documentos ejecutando 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
- Cifrado local

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 programados y personalizados
- Programación de alertas y notificaciones en tiempo real

FLAMMAS

INTEGRACIÓN

ADAPTACIÓN CON ECOSISTEMAS DE FLAMMAS