

Seguridad en Redes y Datos



Endpoint Security

Tormenta de Ideas



- * ¿Qué necesitamos proteger en el PC del usuario?
 - 🜟 Escritorio, Documentos, imágenes, videos, ... (Archivos de Usaurio)
 - Evitar fuga (DLP)
 - Respaldar
 - * Cifrar la información (disco) por si pierde el equipo (o lo roban o lo prenden de noche) Veracrypt
 - Detectar la integridad de los archivos
 - * Emparchado al día
 - Lista blanca de aplicaciones
 - Política de instalación
 - 💥 Firewall local
 - Control de dispositivos extraíbles
 - * Que no se ejecuten ejecutables cuya ejecución ejecute maldades
 - Capacitación de Usaurios

Tormenta de ideas



- * ¿Qué tecnologías para proteger equipos de usuario conocen?
 - * Cifrador de disco
 - AV (AV, AS, AM, A*)
 - * Linga de seguridad
 - * Agente de respaldo
 - **⋇** GP
 - * Add-ons de navegador
 - **★** 2FA

¿Qué es Endpoint Protection?



- Desde la perspectiva de producto:
 - * Software que detecta, contiene y controla las amenazas de malware
 - AV con esteroides
 - ... y algunos add-ons:
 - ★ Cifrado de disco
 - Llavero de contraseñas
 - Manejo de parches
 - ⋆ Inventario?
- * Desde la perspectiva de Seguridad de la Información:
 - 💥 🛮 Todo lo anterior, más...
 - Gestión de políticas
 - * Control y administración remotas
 - * Gestión de amenazas y actualización de software
 - * Reportería + métricas
 - * Automatización de tareas
 - * Respaldos
 - **★** DLP?

Detección de amenazas



- El tradicional Antivirus + antispyware + anti<cualquiercosa>
- * La estrategia de patrones ya no es efectiva por si sola
- * Sandboxing
- Behavior analysis
- Listados de reputación
- Integración con navegadores (filtro de navegación/proxy)
- * ¿Host IDS? ¿Honeypot?
- Consola de gestión centralizada (Enterprise)
- Integración con SIEM
- * ¿Ejemplos de mercado?

Nuestro ranking (Corporate)

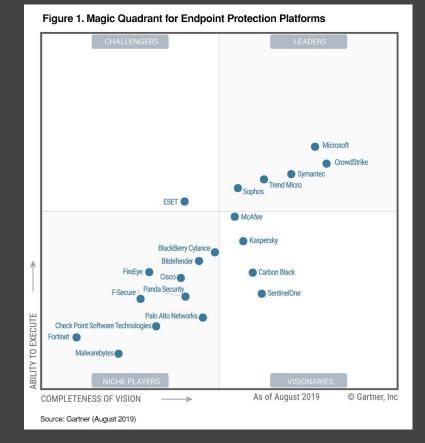


- * Hagamos nuestro propio ranking:
 - * Trend Micro
 - * Symantec
 - ★ McAfee (Intel sec)
 - Kaspersky
 - *
 - Panda AV
 - Windows Defender
 - * SentinelOne
 - ★ Avast
 - **☀** AVG
 - * Avira
 - ★ Nod32

Endpoint protection market



- * Según Gartner
- * ¿Qué jugadores conocen?
- ¿Quienes aparecieron/no esperaban?
- ¿Quienes juegan en la Empresa?



Desafíos y consideraciones



- * Herramientas de despliegue
- * Compatibilidad con otras soluciones
- * Laboratorios del fabricante
 - Extrusión de datos / telemetría