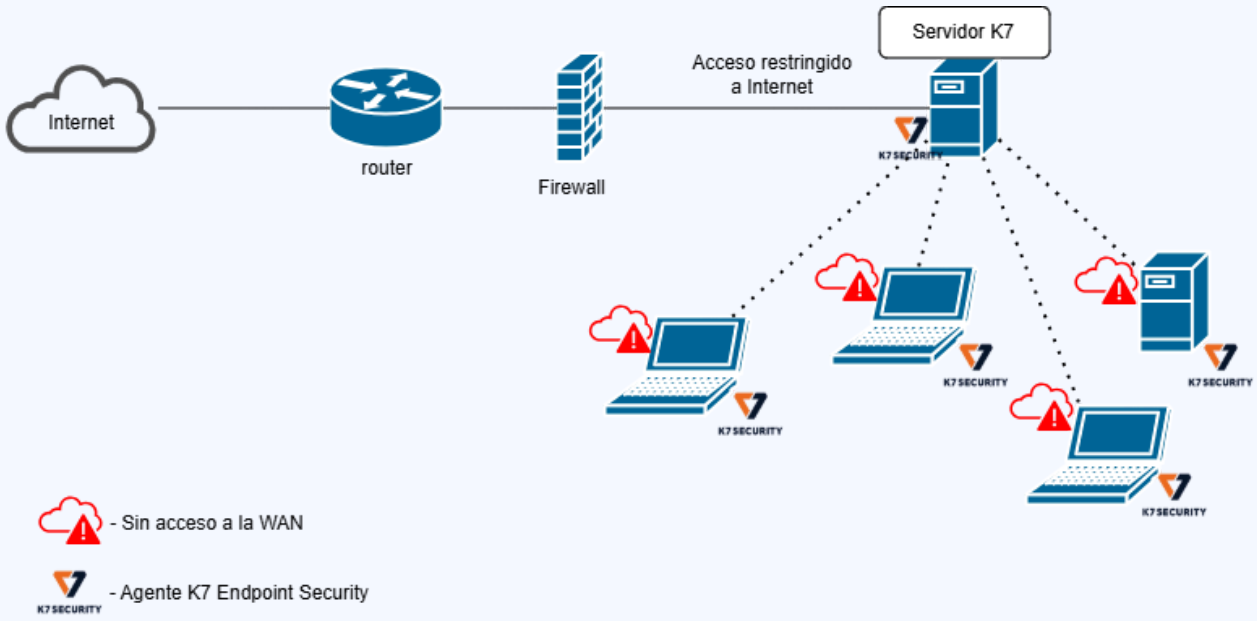
Protección de Ordenadores y Servidores

Una empresa de ingeniería y automatización con operaciones repartidas por múltiples ubicaciones se enfrentaba al reto de reforzar la seguridad de sus ordenadores y servidores en un entorno altamente restringido, sin acceso directo a Internet. Era necesario implementar una solución sólida de protección contra el malware, el ransomware y las amenazas avanzadas, garantizando al mismo tiempo un control centralizado y el cumplimiento de las políticas internas de seguridad.

Para hacer frente a este reto, se implementó una solución de protección de terminales y servidores, on-premises, distribuida en dos emplazamientos distintos. La arquitectura se diseñó para funcionar en una red aislada, permitiendo únicamente las comunicaciones con la WAN estrictamente necesarias para las actualizaciones de seguridad, mediante configuraciones específicas a nivel del cortafuegos y de la gestión de certificados.



La implementación incluyó:

- Instalación de consolas de gestión K7 en cada ubicación
- Definición de políticas para dispositivos finales y servidores
- Creación de grupos lógicos para facilitar la administración
- Distribución automatizada del agente de seguridad K7
- Control detallado de los accesos y permisos a la consola

En cuanto a la protección, se han mantenido los mecanismos incluidos en la configuración predeterminada de la solución, que incluyen funciones como:

Detección de malware basada en firmas

Cortafuegos con sistemas HIDS/HIPS integrados

Protección contra el ransomware con análisis de comportamiento

Filtrado web y control de aplicaciones

Durante el proyecto surgieron importantes retos técnicos, en particular en lo que respecta a la actualización de los sistemas en un entorno sin conexión a Internet y a la compatibilidad con los procesos de automatización interna. Estos obstáculos se superaron mediante ajustes específicos, como la instalación de los certificados necesarios para una comunicación segura y la parametrización de la configuración del sistema para evitar conflictos con aplicaciones críticas.

Como resultado de la implementación, se observó un refuerzo significativo de la postura de seguridad de la organización, acompañado de una mayor visibilidad centralizada de todos los activos protegidos. Además, se logró reducir el riesgo de ataques de malware y ransomware, garantizando al mismo tiempo la continuidad operativa, incluso en un entorno restringido. La infraestructura quedó, asimismo, preparada para cumplir con los requisitos de auditoría y conformidad.

El proyecto demuestra que es posible implementar una solución de ciberseguridad eficaz en entornos complejos y con recursos limitados, garantizando altos niveles de protección sin comprometer los requisitos operativos específicos de la empresa.

C/ Marqués de Urquijo nº 34 3º izq 28008 Madrid

(+351) 937 204 492

comercial@dssi.es