Caso de éxito

# Infraestructuras de TI protegidas

Al ser un agente fundamental del sector farmacéutico, Kohlpharma exige tener la mejor seguridad de la información del mercado. Para garantizar que los medicamentos estén disponibles para los pacientes en forma oportuna y a un precio razonable, las operaciones de Kohlpharma dependen de una logística perfecta y una protección de datos sólida suministrada por las soluciones de seguridad de ESET.

kohlpharma

**INDUSTRIA**
Distribución farmacéutica

**SITIO WEB**
www.kohlpharma.com

**PAÍS**
Alemania

**ENDPOINTS**
1250 equipos

**EL ACUERDO COMERCIAL INCLUYE**

- ESET Enterprise Inspector
- ESET Dynamic Threat Defense
- ESET Endpoint Protection Advanced
- Servicio de implementación y actualización
- Servicio de evaluación inicial y optimización
- Soporte Premium

**Caso de éxito / Kohlpharma**

## ACERCA DE KOHLPHARMA

Kohlpharma se fundó en 1979 y actualmente es uno de los principales importadores farmacéuticos en Europa. Ubicado en Merzig, Saarland, Kohlpharma compra medicamentos de marcas originales a fabricantes farmacéuticos reconocidos de otros países de la UE a precios favorables y los importa a Alemania. Tanto los pacientes como las aseguradoras de salud obtienen grandes beneficios en precio y comodidad, y los médicos también ahorran en sus presupuestos. Kohlpharma tiene 800 empleados y suministra medicamentos de calidad a farmacias, así como a mayoristas farmacéuticos alemanes. Efectividad de la detección de ESET.

## REQUISITOS EXHAUSTIVOS

Kohlpharma también es una empresa líder por haber implementado la automatización completa y la industria 4.0 en Alemania. Muchos de sus procesos laborales principales ya han sido parcial o totalmente automatizados. Dichos sistemas son objetivos potenciales de ataques cibernéticos y requieren una protección compleja. Por lo tanto, Kohlpharma buscaba una solución innovadora de seguridad de TI que incluyera no solo protección antimalware sino también un sistema de detección y respuesta para endpoints (EDR). Johannes Zenner, Gerente de Proyecto de Kohlpharma, elaboró una ambiciosa matriz de requisitos que contempla las perspectivas económicas, funcionales y administrativas. Solo tres proveedores de soluciones de seguridad llegaron a la lista final de candidatos. *"Nuestra empresa de ingeniería de sistemas ttt-it AG nos recomendó las soluciones de ESET. Con sus excelentes tasas de detección, su tecnología de última generación y las recomendaciones de Gartner y AV-Comparatives, ESET parecía cumplir nuestras condiciones a la perfección"*, recuerda Johannes Zenner.

Kohlpharma examinó detenidamente todas las posibles soluciones. ESET se desempeñó de manera convincente en varios entornos de prueba para los que se habían clonado servidores y endpoints del entorno de producción. *"La relación costo-beneficio de ESET fue significativamente mejor que la de otros competidores. Sin embargo, lo que nos convenció fueron dos factores humanos: el alto nivel de compromiso y la comunicación abierta sin promesas vacías son lo que selló el trato"*, dice Stefan Pistorius, Gerente de Administración y Procesamiento Electrónico de Datos de Kohlpharma.

## DESPLIEGUE EN TIEMPO RÉCORD

Solo tomó seis semanas implementar completamente la solución **ESET Endpoint Protection Advanced**, que comprende **ESET Endpoint Security, ESET File Security, ESET Shared Local Cache y ESET Security Management Center**. En dos pasos adicionales, se implementaron las herramientas de detección y respuesta para endpoints (EDR) **ESET Dynamic Threat Defense y ESET Enterprise Inspector**. *"La migración completa de 1250 equipos a ESET se caracterizó por la más alta profesionalidad y la cooperación armoniosa de todas las partes involucradas. Fue ejemplar"*, cuenta Stephan Kapetanios de la empresa de ingeniería de sistemas ttt-it AG. A lo largo de todo el proceso de migración, ttt-it AG, ESET y Kohlpharma trabajaron en estrecha colaboración y lograron implementar incluso las configuraciones más específicas en un plazo muy corto.

*"Una solución de seguridad de TI compleja debe funcionar correctamente y, sin embargo, ser fácil de usar. ESET domina este equilibrio de manera ejemplar."*

Stefan Pistorius
Gerente de Administración y Procesamiento Electrónico de Datos, Kohlpharma

### BENEFICIOS PRINCIPALES

- Alto nivel de protección
- Facilidad de implementación
- Informes detallados
- Servicio y soporte continuos
- Rentabilidad

## HERRAMIENTAS DE SEGURIDAD DE TI PARA INFRAESTRUCTURAS CRÍTICAS

*"Las empresas como la nuestra, clasificadas como de Infraestructura Crítica (o CRITIS, del inglés), deben dedicar mucha más atención a la seguridad de TI. Con ese fin, hemos integrado una herramienta de detección y respuesta para endpoints (EDR) a nuestra arquitectura de seguridad"*, explica Johannes Zenner. Esto significa que no puede filtrarse ningún malware y que no puede permanecer ninguna vulnerabilidad en la red sin ser detectada. Si la logística se paralizara debido a un ataque, sin duda causaría pérdidas financieras de millones de dólares diarios. Sin embargo, mucho peor sería la pérdida de confianza de los pacientes y clientes comerciales que Kohlpharma ha conseguido con tanto sacrificio. Un daño así es muy difícil de reparar. Por eso, Kohlpharma confía en dos soluciones de ESET: *ESET Dynamic Threat Defense y ESET Enterprise Inspector.*

## DETECCIÓN DE AMENAZAS DESCONOCIDAS Y PROTECCIÓN ADICIONAL PARA LOS ARCHIVOS

Las redes están expuestas a cientos de archivos desconocidos todos los días. Los documentos más simples y otros archivos no ejecutables generalmente no representan un problema para las soluciones de seguridad con cierta trayectoria. No obstante, la automatización completa de los procesos en Kohlpharma implica que hay muchos archivos ejecutables que se reciben desde el exterior. Por supuesto, esto puede ser extremadamente peligroso, ya que los archivos .exe pueden contener malware oculto. Además, la ejecución de los archivos es esencial para el funcionamiento sin problemas de la empresa. La solución es ejecutar archivos en modo sandbox para evaluar su comportamiento. Desafortunadamente, esto requiere una gran cantidad de recursos informáticos y una variedad de plantillas para sandbox y, por lo tanto, no es factible de hacer en las instalaciones.

**ESET Dynamic Threat Defense** (EDTD) ofrece un modo sandbox basado en la nube capaz de identificar amenazas desconocidas. Las muestras sospechosas se envían a la nube para que ESET las analice. Sus sensores profundizan el análisis de código estático e incluyen el aprendizaje automático, la exploración de la memoria y el análisis del comportamiento. En comparación con las soluciones de seguridad para endpoints, EDTD utiliza una gama mucho más amplia de tecnologías para detectar muestras potencialmente peligrosas. Los resultados del análisis en la nube se devuelven al sistema y los archivos infectados se desinfectan o eliminan de inmediato. Además, EDTD les proporciona a los administradores de Kohlpharma informes detallados.

## ESET ENTERPRISE INSPECTOR DETECTA LAS VULNERABILIDADES INTERNAS

Los requisitos de seguridad de TI que elaboró Stefan Pistorius eran aún más amplios: *"Para nosotros no es suficiente responder a los ataques con soluciones antimalware clásicas. Queremos tener la opción de detectar vulnerabilidades en forma independiente y eliminarlas."* Por eso, Kohlpharma decidió utilizar **ESET Enterprise Inspector.** Esta herramienta de detección y respuesta para endpoints (EDR) recopila datos en tiempo real sobre las acciones y los eventos en las endpoints conectadas y verifica automáticamente si los datos coinciden con los criterios de actividad sospechosa. La información recopilada se procesa y almacena en un formato que luego permite realizar búsquedas. La compilación resultante de las actividades anómalas y sospechosas les permite a los usuarios investigarlas profundizando su nivel de detalle.

Asimismo, **ESET Enterprise Inspector** proporciona datos forenses sobre incidentes pasados y ofrece orientación sobre posibles medidas de seguridad para contrarrestar las amenazas. Incluso las amenazas persistentes avanzadas (APT) presentes en la red pueden eliminarse con éxito. **ESET Enterprise Inspector** recopila y combina información completa de todas las tecnologías de detección de ESET, incluyendo el aprendizaje automático.

## OPERACIÓN SENCILLA DESDE CONSOLAS WEB

A primera vista, la combinación de muchos productos y tecnologías diferentes puede parecer complicada. Sin embargo, Johannes Zenner tiene todo bajo control gracias a las consolas web proporcionadas por ESET. El elemento clave es **ESET Security Management Center**, que le permite administrar de manera centralizada todas las endpoints y los servidores. También usa una consola de administración adicional para **ESET Enterprise Inspector**. *"Ambas herramientas hacen que mi trabajo diario sea mucho más fácil. Son intuitivas, estructuradas, funcionan bien y ofrecen una amplia gama de posibilidades"*, explica el gerente del proyecto. *"La sincronización de datos entre ambas consolas se lleva a cabo en forma automática, por lo que siempre recibo información actualizada. Y si encuentro algún problema, puedo usar la documentación detallada que se actualiza periódicamente."*

Al implementar las soluciones de seguridad de ESET, Kohlpharma ha llevado la protección de sus sistemas a un nivel completamente nuevo. Esto no solo se debe a los aspectos técnicos de la solución. Hay algunos factores humanos que son igualmente importantes, como la estrecha cooperación entre el cliente, el proveedor y la empresa de ingeniería de sistemas, así como el servicio y el soporte, que deben ser integrales y confiables. Kohlpharma sabe que ahora cuenta con un partner fuerte a su lado, incluso en casos de crisis.

## CASO

Kohlpharma buscaba una nueva solución de seguridad de TI que cumpliera con los requisitos de CRITIS. Además de la protección antimalware, necesitaba herramientas de detección y respuesta para endpoints para fortalecer la arquitectura de seguridad de la empresa.

## SOLUCIÓN

La combinación de las soluciones profesionales de ESET, en este caso, ESET Endpoint Protection Advanced (que incluye ESET Endpoint Security, ESET File Security, ESET Shared Local Cache y ESET Security Management Center) junto con ESET Dynamic Threat Defense y ESET Enterprise Inspector, protege efectivamente la compleja arquitectura de seguridad de Kohlpharma ante hackers y ciberdelincuentes.

## BENEFICIO

ESET proporciona un sistema armonioso de soluciones holísticas para la seguridad de TI. Defiende de manera confiable contra ataques externos e identifica eventos internos sospechosos. La excelente usabilidad de las consolas de ESET simplifica el trabajo de los administradores.