Gobernanza y Soberanía de Datos

Qué recopila y qué nunca recopila Cyber Crucible, cómo se protegen los datos en tránsito, dónde se procesan, qué puede divulgarse bajo proceso legal, y cómo se controlan el riesgo de la cadena de suministro y el riesgo interno.

¿Qué datos recopila Cyber Crucible — y qué datos nunca recopila?

Respuesta breve: Cyber Crucible opera bajo una directiva de Cero Recopilación de Contenido (Zero-Content Harvesting). Procesa telemetría operativa del sistema — rutas de ejecución de procesos, cadenas de procesos padre-hijo, indicadores de ejecución de hardware y estados de integridad de memoria — analizada localmente en el endpoint. No recopila, transmite, almacena ni procesa claves de cifrado, credenciales, tokens de sesión ni sus archivos.

Categorías estrictamente excluidas

El software de Cyber Crucible no recopila, transmite, almacena ni procesa:

- **Variables criptográficas** — claves privadas, claves de descifrado y claves de cifrado de aplicaciones.
- **Credenciales de usuario** — contraseñas de usuario, secretos de Active Directory y claves privadas de API.
- **Identificadores de sesión** — tokens OAuth, tokens de acceso, tokens de actualización y cookies de sesión.
- **Datos de contenido del cliente** — archivos propietarios, documentos, contenidos de bases de datos, cuerpos de correos electrónicos y comunicaciones de usuarios.

Por qué la protección completa no requiere recopilar contenido

La capacidad completa del software de prevención de amenazas se logra sin recopilar ni exfiltrar contenido privado del cliente. El motor de comportamiento evalúa *lo que un programa está haciendo* — a qué procesos está accediendo, habiendo hecho qué anteriormente — y nada de eso requiere abrir el archivo o leer el secreto.

Este es el mismo principio detrás de la protección de identidad: el acceso se rastrea y analiza sin que se acceda a la credencial en sí.

Dónde ocurre el análisis

Las rutas de ejecución de procesos, el linaje de procesos, los indicadores de ejecución de hardware y los estados de integridad de memoria se analizan **localmente en el endpoint**. Cuando la gestión asistida por la nube o centralizada está habilitada, la telemetría administrativa saliente se limita estrictamente a los indicadores operativos necesarios para el monitoreo de la salud del sistema y la generación de informes de seguridad.

¿Cuál es la diferencia entre la telemetría del sistema y los datos del cliente?

Respuesta breve: La telemetría del sistema describe cómo se comporta el software: qué proceso inició a cuál, cómo se ve la memoria, si los patrones de ejecución son anómalos. Los datos del cliente son el contenido que su empresa crea y conserva: archivos, correos electrónicos, registros de bases de datos, credenciales. Cyber Crucible analiza lo primero y nunca recopila lo segundo.

Una manera útil de entenderlo

La telemetría son metadatos sobre el *comportamiento de la máquina*. El contenido es la *información misma*.

Saber que el `proceso A` generó el `proceso B`, el cual luego intentó leer un almacén de credenciales del navegador mostrando indicios de modificación en memoria, es suficiente para identificar un ataque. No es necesario leer lo que contenía ese almacén de credenciales, y Cyber Crucible no lo hace.

Qué significa esto en la práctica

- El análisis de comportamiento se realiza sobre el acceso a la identidad **sin procesar la información de identidad en sí**.
- La telemetría que sale del endpoint en implementaciones asistidas por la nube se limita a indicadores operativos para el monitoreo de estado y los informes de seguridad.
- Los metadatos técnicos y de comportamiento se tratan como datos personales únicamente cuando pueden identificar directa o indirectamente a una persona, y en esos casos los identificadores se seudonimizan o enmascaran.

Control del cliente

Las fuentes de telemetría son configurables. Las organizaciones pueden ajustar qué fuentes se recopilan, de modo que no se adquiera información innecesaria. Los campos que no son esenciales para la detección de amenazas se excluyen o descartan.

¿Cyber Crucible vende o comparte los datos de los clientes con terceros?

Respuesta breve: No. Cyber Crucible no comparte, licencia, comercializa ni divulga información de clientes o telemetría a ningún tercero, y los datos de los clientes no están, bajo ninguna circunstancia, a la venta.

Los compromisos

- **Cero intercambio con terceros** — sin compartir, licenciar, comercializar ni divulgar información de clientes o telemetría a ningún tercero.
- **Prohibición de monetización comercial** — los datos de los clientes no están a la venta, bajo ninguna circunstancia.
- **Sin corretaje de datos de identidad o telemetría** — no se comercializan, licencian ni monetizan con ninguna parte.

Por qué esto es arquitectónicamente creíble

Muchos proveedores hacen la promesa de no vender datos. Lo que hace diferente a este compromiso es que gran parte del material sensible simplemente no se recopila en primer lugar. Una empresa que nunca tiene en su poder sus claves de descifrado, credenciales o archivos no tiene nada en esas categorías para vender, compartir o perder, sin importar la política.

Las políticas pueden cambiar. La arquitectura es más difícil de revertir.

> Consulte también: "*¿Qué puede divulgar Cyber Crucible si un gobierno o un tribunal lo obliga a hacerlo?*"

¿Qué puede divulgar Cyber Crucible si es obligado por un gobierno o un tribunal?

Respuesta breve: Nada en las categorías que más importan, porque nunca las posee. Cyber Crucible no recopila, almacena ni conserva claves de descifrado, credenciales de usuario ni archivos de clientes; por lo tanto, no hay nada de ese tipo que entregar a ninguna parte privada, gobierno o potencia extranjera. Como cualquier empresa estadounidense, sigue sujeta a la legislación aplicable, pero no puede entregar datos que nunca posee.

"Nada que divulgar por diseño"

Se trata de una postura arquitectónica deliberada y no de una promesa legal. Un proceso legal puede obligar a una empresa a entregar lo que posee. No puede obligar a una empresa a producir lo que nunca se recopiló.

Dado que Cyber Crucible no recopila ni conserva claves de cifrado, credenciales ni contenido privado, esas categorías están vacías por diseño.

Por qué esto importa más que antes

Las arquitecturas de seguridad centralizadas crean un punto de agregación de alto valor. Un proveedor que posee las claves y los tokens de sesión de miles de clientes es un objetivo tanto para atacantes criminales como para actores patrocinados por estados, y puede ser accedido mediante compulsión legal, en ocasiones sin que el cliente lo sepa.

La postura de Cyber Crucible respecto al depósito de claves (key escrow) sigue el mismo razonamiento: deliberadamente no mantiene un almacén central de claves, de modo que no existe un único punto de falla que pueda ser vulnerado o citado judicialmente.

Un límite honesto

Cyber Crucible es una empresa estadounidense y está sujeta a la legislación de los Estados Unidos. La afirmación aquí es acotada y específica: no puede divulgar datos que no posee. Esto es una declaración sobre la arquitectura, no una afirmación de inmunidad frente a procesos legales.

¿Cómo se protegen los datos de Cyber Crucible en tránsito?

Respuesta breve: Todas las comunicaciones entre el agente y el servidor exigen TLS 1.3. Los payloads de datos operativos utilizan además JSON Web Encryption (JWE) con pares de claves criptográficas únicos por agente, de modo que los payloads no pueden interceptarse ni manipularse en tránsito. El acceso administrativo requiere autenticación basada en claves además de validación de tokens OAuth 2.0.

Las capas

- **Canales cifrados** — toda comunicación entre el agente y el servidor exige TLS 1.3.
- **Cifrado de payload por agente** — los payloads operativos utilizan JWE con pares de claves únicos por agente. Como cada agente tiene su propio par de claves, comprometer un circuito de tránsito no expone a los demás, y se impide la interceptación o manipulación en línea.
- **Administración autenticada** — el acceso al sistema requiere autenticación individual de usuario basada en claves y validación de tokens OAuth 2.0, restringiendo las acciones administrativas al personal autorizado.

Por qué son importantes las claves por agente

El cifrado de transporte por sí solo protege el canal. El cifrado de payload por agente protege el *contenido del mensaje* de forma independiente del canal, de modo que un atacante posicionado en línea, o un intermediario comprometido, aun así no puede leer ni alterar lo que envió el agente.

Infraestructura compartida

Cuando se utilizan entornos de nube pública o nube privada virtual para la administración del backend, Cyber Crucible aplica un estricto aislamiento lógico de inquilinos junto con cifrado de extremo a extremo de los payloads. Los proveedores de nube y los operadores de infraestructura tienen **visibilidad cero** sobre los payloads de datos operativos o los estados de los sistemas de los clientes.

¿Dónde se procesan mis datos y pueden permanecer dentro de mi país?

Respuesta breve: Sí. La infraestructura de Cyber Crucible puede configurarse de modo que el procesamiento se realice geográficamente cerca de su jurisdicción legal o dentro de ella, y una implementación totalmente local con air-gap mantiene todo dentro del límite de su propia red, sin telemetría saliente.

Configuración soberana

La infraestructura puede posicionarse para mantener el procesamiento dentro de la jurisdicción legal del cliente, o geográficamente cerca de ella. Esto está diseñado para respaldar el cumplimiento de los mandatos de residencia de datos, incluidos el Reglamento General de Protección de Datos de la UE (GDPR), la Ley de Protección de Datos Personales de Arabia Saudita (PDPL), el Decreto-Ley Federal N.º 45/2021 de los EAU y la Ley de Protección de Datos de Kenia.

La opción más sólida

Para las organizaciones que requieren un aislamiento total, el modelo local ejecuta todo el software de gestión backend dentro de sus propios racks de servidores físicamente protegidos. Cero telemetría y cero datos salen del límite de su red soberana.

Dado que la evaluación de amenazas y la interdicción de procesos ocurren localmente en el endpoint, típicamente en menos de 200 milisegundos, la protección no depende de ninguna conexión externa. La soberanía no tiene ningún costo en capacidad defensiva.

> Vea también: "*¿Qué modelos de implementación están disponibles para la soberanía de datos?*"

¿Qué modelos de implementación están disponibles para la soberanía de datos?

Respuesta breve: Dos. Un modelo local totalmente aislado (air-gapped), en el que nada sale de su red, y un modelo alojado o híbrido asistido por la nube, con comunicaciones TLS cifradas mediante JWE hacia servidores organizados regionalmente. Ambos ofrecen la misma prevención local en menos de 200 milisegundos.

Comparación

	Soberano en las instalaciones (Air-Gapped)	**Alojado / Híbrido asistido por la nube**
Límite de tránsito de datos	100% contenido dentro de los racks de servidores físicamente asegurados del cliente	Comunicaciones TLS cifradas mediante JWE hacia servidores de aplicaciones regionales
Flujo transfronterizo	Ningún flujo de red externo; cero telemetría saliente	Organización geográficamente localizada para cumplir con los límites regionales
Alineación normativa	Compatible con requisitos estrictos de residencia y soberanía de datos nacionales	Diseñado para alinearse con directivas globales de privacidad (GDPR, PDPL, entre otras)

Cómo elegir entre ellos

El modelo air-gapped es adecuado para el gobierno, la defensa, la infraestructura crítica y cualquier organización sujeta a mandatos estrictos de residencia nacional o que opere en entornos desconectados.

El modelo híbrido es adecuado para organizaciones que desean una gestión centralizada y generación de informes en toda la flota, manteniendo al mismo tiempo los datos dentro de un límite regional.

La prevención es idéntica en ambos casos. El ciclo local Detect–Decide–Respond se ejecuta en el kernel del endpoint independientemente del modelo de implementación; la diferencia radica únicamente en dónde reside la infraestructura de gestión e informes.

¿Cómo gestiona Cyber Crucible el riesgo de la cadena de suministro y el riesgo interno?

Respuesta breve: Mediante acuerdos de confidencialidad mutuos y vinculantes para todo el personal con acceso potencial, un acceso administrativo estrictamente limitado según la necesidad de saber, restringido a personal verificado, y un mandato de tolerancia cero para aislar o desvincular de inmediato a cualquier proveedor, vendedor, contratista o empleado que represente un riesgo para los clientes o su propiedad intelectual.

Los controles

- **Acuerdos de confidencialidad obligatorios** — todo el personal con acceso potencial a los datos operativos de los clientes o a los sistemas de gestión está legalmente obligado por un acuerdo de confidencialidad mutuo antes de su incorporación.
- **Acceso estricto según la necesidad de saber** — el acceso administrativo a las instancias de gestión de clientes está restringido exclusivamente a personal verificado, y únicamente cuando sea necesario para llevar a cabo una operación comercial o de soporte validada.
- **Mandato de desvinculación de proveedores y recursos** — si algún proveedor, vendedor de software, contratista o empleado representa un riesgo de seguridad, privacidad o propiedad intelectual para los clientes, Cyber Crucible gestiona y aísla activamente ese riesgo o desvincula el recurso de inmediato.

Por qué el riesgo interno y el riesgo de la cadena de suministro van de la mano

Ambos son el mismo problema visto desde ángulos diferentes: alguien con acceso legítimo que se convierte en el vector. Controlarlo requiere limitar quién tiene acceso, vincularlo contractualmente y estar dispuesto a cortar una relación rápidamente cuando surge el riesgo, incluida una relación comercial.

El mandato de desvinculación es la parte que las organizaciones suelen no tener. Los contratos y los acuerdos de confidencialidad establecen obligaciones; la disposición a rescindir un proveedor de inmediato es lo que les da sentido.

¿Cyber Crucible integra bibliotecas de terceros o código extranjero?

Respuesta breve: No. Los sensores de kernel, los controladores y los modelos de comportamiento de Genetic AI se diseñan internamente. No se integra en el software ningún SDK patrocinado por estados extranjeros, biblioteca de terceros no verificada ni mecanismo de telemetría oculto. Los controladores de kernel de Windows se presentan para su certificación en el marco del Windows Hardware Compatibility Program (WHCP) de Microsoft.

La ventaja de la ingeniería propia

Desarrollar sensores de kernel y modelos de comportamiento de manera interna es costoso y lento. La mayoría de los proveedores ensamblan componentes en su lugar. Ese ensamblaje es precisamente el punto por el que el riesgo de la cadena de suministro se introduce en un producto de seguridad: la herramienta con los privilegios de sistema más profundos es también aquella en la que una dependencia no verificada puede causar el mayor daño.

Los componentes de Cyber Crucible son propietarios y se mantienen de forma interna, lo que elimina esa categoría de exposición en lugar de simplemente gestionarla.

Validación externa

Todos los controladores de kernel de Windows se someten a pruebas internas de control de calidad y se presentan para su certificación en el marco del Windows Hardware Compatibility Program (WHCP) de Microsoft, una validación independiente de la calidad y la resistencia a manipulaciones del código que se ejecuta a nivel de kernel.

Sin telemetría oculta

No existen mecanismos de telemetría ocultos. Lo que el software recopila está documentado, y las categorías que nunca recopila se enumeran de forma explícita.

¿Qué significa la neutralidad geopolítica en el software de seguridad?

Respuesta breve: Significa que el software está diseñado para proteger a su organización sin incorporar puertas traseras estratégicas extranjeras, asociaciones de inteligencia con estados extranjeros o dependencias obligatorias de la nube, de modo que su uso no importe los intereses estratégicos de otro país a su infraestructura.

El problema que aborda

Las herramientas de seguridad heredadas suelen depender de modelos centralizados de recolección en la nube que exfiltran continuamente la telemetría de los endpoints, los detalles de las cuentas y los artefactos del sistema de archivos a través de fronteras nacionales y geopolíticas. Eso resulta lento frente a ataques a velocidad de máquina, y genera exposición en materia de cumplimiento y seguridad conforme al GDPR, la PDPL de Arabia Saudita, la Ley Federal de Decreto-Ley N.º 45/2021 de los EAU y la Ley de Protección de Datos de Kenia.

También plantea una pregunta que la mayoría de los procesos de adquisición nunca formula: *¿en qué jurisdicción termina mi telemetría, y quién más puede acceder a ella allí?*

Los tres componentes

1. **Sin puertas traseras estratégicas extranjeras** — sin componentes de código patrocinados por estados ni SDK extranjeros no verificados.
2. **Sin asociaciones de inteligencia con estados extranjeros** — la telemetría del cliente no se comparte con ningún tercero, incluidos gobiernos.
3. **Sin dependencia obligatoria de la nube** — el software funciona completamente sin conexión, por lo que ningún dato tiene que cruzar una frontera para que el producto funcione.

El tercer punto es lo que hace exigibles a los dos primeros. Un producto que *requiere* una conexión a la nube no puede prometer de manera creíble que sus datos permanecerán en su lugar.