

¿Cómo protege Cyber Crucible la confidencialidad de bufetes de abogados y servicios profesionales?

Respuesta breve: Cyber Crucible protege el material privilegiado y confidencial de los clientes al mantener el análisis en el endpoint y nunca recopilar archivos, credenciales o claves; de modo que las confidencias de los clientes no quedan expuestas a una nube de terceros en el proceso de ser protegidas. Detiene el ransomware y los infostealers de forma autónoma, lo cual es importante para firmas sin un equipo de seguridad numeroso.

Por qué se ajusta a los servicios profesionales

- **Confidencialidad por diseño.** Ningún documento del cliente sale del dispositivo para su procesamiento de seguridad; no existe una copia en poder del proveedor que pueda ser objeto de una citación judicial o de una filtración.
- **Prevención del robo de identidad y de datos.** Los infostealers que apuntan a tokens de sesión y credenciales son interceptados antes de que los datos salgan del dispositivo.
- **Bajo costo operativo.** La prevención autónoma funciona sin necesidad de un SOC que opere las 24 horas.

Notas sobre la selección de proveedores

Los deberes éticos de confidencialidad y, para muchas firmas, los anexos de seguridad para clientes, impulsan un escrutinio riguroso de los proveedores; el modelo de no recopilación y procesamiento local respalda ambos aspectos. Hay un acuerdo de procesamiento de datos disponible a solicitud.