

Wie schützt Cyber Crucible die Vertraulichkeit von Anwaltskanzleien und Unternehmen aus dem Bereich der professionellen Dienstleistungen?

Kurze Antwort: Cyber Crucible schützt privilegiertes und vertrauliches Mandantenmaterial, indem die Analyse auf dem Endgerät verbleibt und niemals Dateien, Anmeldeinformationen oder Schlüssel gesammelt werden – so werden Mandantengeheimnisse im Zuge des Schutzes nicht einer Drittanbieter-Cloud ausgesetzt. Es stoppt Ransomware und Infostealer autonom, was für Kanzleien ohne großes Sicherheitsteam von Bedeutung ist.

Warum es zu professionellen Dienstleistungen passt

- **Vertraulichkeit von Grund auf.** Keine Mandantendokumente verlassen das Gerät zur Sicherheitsverarbeitung; es gibt keine beim Anbieter gespeicherte Kopie, die vorgeladen oder kompromittiert werden könnte.
- **Schutz vor Identitäts- und Datendiebstahl.** Infostealer, die es auf Sitzungs-Token und Anmeldeinformationen abgesehen haben, werden abgefangen, bevor Daten das Gerät verlassen.
- **Geringer Betriebsaufwand.** Autonome Prävention funktioniert ohne einen rund um die Uhr besetzten SOC.

Hinweise zur Anbieterauswahl

Ethische Vertraulichkeitspflichten und, bei vielen Kanzleien, Zusatzvereinbarungen zur Mandantensicherheit führen zu einer genauen Prüfung der Anbieter; das Modell ohne Datensammlung und mit lokaler Verarbeitung unterstützt beides. Eine

Auftragsverarbeitungsvereinbarung ist auf Anfrage erhältlich.

Revision #1

Created 2026-07-24 04:54:34 UTC by Dennis Underwood

Updated 2026-07-24 04:54:34 UTC by Dennis Underwood