

Daten-Governance & Souveränität

Was Cyber Crucible erfasst und niemals erfasst, wie Daten bei der Übertragung geschützt werden, wo sie verarbeitet werden, was im Rahmen eines gerichtlichen Verfahrens offengelegt werden kann und wie Lieferketten- und Insiderrisiken kontrolliert werden.

- [Welche Daten erfasst Cyber Crucible – und welche niemals?](#)
- [Was ist der Unterschied zwischen Systemtelemetrie und Kundendaten?](#)
- [Verkauft oder teilt Cyber Crucible Kundendaten mit Dritten?](#)
- [Was kann Cyber Crucible offenlegen, wenn es von einer Regierung oder einem Gericht dazu verpflichtet wird?](#)
- [Wie werden die Daten von Cyber Crucible bei der Übertragung geschützt?](#)
- [Wo werden meine Daten verarbeitet, und können sie innerhalb meines Landes verbleiben?](#)
- [Welche Bereitstellungsmodelle stehen für die Datensouveränität zur Verfügung?](#)
- [Wie steuert Cyber Crucible Lieferketten- und Insider-Risiken?](#)
- [Bettet Cyber Crucible Bibliotheken oder Fremdcode von Drittanbietern ein?](#)
- [Was bedeutet geopolitische Neutralität bei Sicherheitssoftware?](#)

Welche Daten erfasst Cyber Crucible – und welche niemals?

Kurzantwort: Cyber Crucible arbeitet nach der Zero-Content-Harvesting-Direktive. Es verarbeitet operative Systemtelemetrie – Prozessausführungspfade, Eltern-Kind-Prozessketten, Hardware-Ausführungsindikatoren und Speicherintegritätszustände –, die lokal auf dem Endgerät analysiert werden. Es erfasst, überträgt, speichert oder verarbeitet keine Verschlüsselungsschlüssel, Zugangsdaten, Sitzungstoken oder Ihre Dateien.

Strikt ausgeschlossene Kategorien

Die Cyber-Crucible-Software erfasst, überträgt, speichert oder verarbeitet nicht:

- **Kryptografische Variablen** — private Schlüssel, Entschlüsselungsschlüssel und Anwendungsverschlüsselungsschlüssel.
- **Benutzeranmeldedaten** — Benutzerpasswörter, Active-Directory-Geheimnisse und private API-Schlüssel.
- **Sitzungskennungen** — OAuth-Token, Zugriffstoken, Refresh-Token und Sitzungscookies.
- **Kundeninhaltsdaten** — vertrauliche Dateien, Dokumente, Datenbankinhalte, E-Mail-Texte und Benutzerkommunikation.

Warum vollständiger Schutz kein Erfassen von Inhalten erfordert

Die volle Leistungsfähigkeit der Bedrohungspräventionssoftware wird erreicht, ohne private Kundeninhalte zu erfassen oder zu exfiltrieren. Die Verhaltens-Engine bewertet, *was ein Programm tut* – welche Prozesse wohin gelangen und was zuvor geschehen ist –, und nichts davon erfordert das Öffnen der Datei oder das Lesen des Geheimnisses.

Dies ist dasselbe Prinzip, das dem Identitätsschutz zugrunde liegt: Zugriffe werden nachverfolgt und analysiert, ohne dass auf die Zugangsdaten selbst zugegriffen wird.

Wo die Analyse stattfindet

Prozessausführungspfade, Prozessabstammung, Hardware-Ausführungsindikatoren und Speicherintegritätszustände werden **lokal auf dem Endgerät** analysiert. Wenn Cloud-unterstütztes oder zentralisiertes Management aktiviert ist, beschränkt sich die ausgehende administrative Telemetrie strikt auf die operativen Indikatoren, die für die Systemzustandsüberwachung und Sicherheitsberichterstattung erforderlich sind.

Was ist der Unterschied zwischen Systemtelemetrie und Kundendaten?

Kurze Antwort: Systemtelemetrie beschreibt, wie sich Software verhält — welcher Prozess welchen anderen gestartet hat, wie der Speicher aussieht, ob Ausführungsmuster anomal sind. Kundendaten sind die Inhalte, die Ihr Unternehmen erstellt und vorhält — Dateien, E-Mails, Datenbankeinträge, Zugangsdaten. Cyber Crucible analysiert Ersteres und erfasst niemals Letzteres.

Eine nützliche Betrachtungsweise

Telemetrie sind Metadaten über *Maschinenverhalten*. Inhalte sind die *Information selbst*.

Zu wissen, dass Prozess A Prozess B gestartet hat, der wiederum versucht hat, einen Browser-Zugangsdatenspeicher zu lesen und dabei Anzeichen einer In-Memory-Modifikation zeigte, genügt, um einen Angriff zu identifizieren. Zu lesen, was sich in diesem Zugangsdatenspeicher befand, ist nicht erforderlich — und Cyber Crucible tut dies nicht.

Was das praktisch bedeutet

- Die Verhaltensanalyse erfolgt beim Zugriff auf Identitäten, **ohne die Identitätsinformationen selbst zu verarbeiten**.
- Telemetrie, die bei Cloud-unterstützten Bereitstellungen den Endpunkt tatsächlich verlässt, beschränkt sich auf betriebliche Indikatoren für Health-Monitoring und Sicherheitsberichterstattung.
- Technische und verhaltensbezogene Metadaten werden nur dann als personenbezogene Daten behandelt, wenn sie eine Person direkt oder indirekt identifizieren können — in diesen Fällen werden Kennungen pseudonymisiert oder maskiert.

Kundenkontrolle

Telemetriequellen sind konfigurierbar. Organisationen können festlegen, welche Quellen erfasst werden, sodass keine unnötigen Informationen erhoben werden. Felder, die für die Bedrohungserkennung nicht essenziell sind, werden ausgeschlossen oder verworfen.

Verkauft oder teilt Cyber Crucible Kundendaten mit Dritten?

Kurze Antwort: Nein. Cyber Crucible teilt, lizenziert, handelt oder offenbart keine Kundeninformationen oder Telemetriedaten an Dritte, und Kundendaten stehen unter keinen Umständen zum Verkauf.

Die Verpflichtungen

- **Keine Weitergabe an Dritte** — keine Weitergabe, Lizenzierung, Handel oder Offenlegung von Kundeninformationen oder Telemetriedaten an Dritte.
- **Verbot der kommerziellen Verwertung** — Kundendaten stehen unter keinen Umständen zum Verkauf.
- **Kein Datenhandel mit Identitäts- oder Telemetriedaten** — keine Weitergabe, Lizenzierung oder Monetarisierung mit Dritten.

Warum dies architektonisch glaubwürdig ist

Viele Anbieter geben das Versprechen ab, keine Daten zu verkaufen. Was dieses Versprechen anders macht, ist die Tatsache, dass ein Großteil der sensiblen Informationen von vornherein gar nicht erfasst wird. Ein Unternehmen, das niemals Ihre Entschlüsselungscodes, Zugangsdaten oder Dateien besitzt, hat in diesen Kategorien nichts zu verkaufen, weiterzugeben oder zu verlieren — unabhängig von der jeweiligen Richtlinie.

Richtlinien können sich ändern. Architektur lässt sich schwerer umkehren.

“ Siehe auch: "Was kann Cyber Crucible offenlegen, wenn es von einer Regierung oder einem Gericht dazu verpflichtet wird?"

Was kann Cyber Crucible offenlegen, wenn es von einer Regierung oder einem Gericht dazu verpflichtet wird?

Kurze Antwort: Nichts in den Kategorien, die am meisten zählen, da diese Daten niemals vorgehalten werden. Cyber Crucible sammelt, speichert oder behält keine Entschlüsselungsschlüssel, Benutzeranmeldedaten oder Kundendateien – es gibt also nichts dergleichen, das an eine Privatpartei, Regierung oder ausländische Macht übergeben werden könnte. Wie jedes US-Unternehmen unterliegt es dem geltenden Recht, kann jedoch keine Daten herausgeben, die es nie besessen hat.

„Nichts offenzulegen – by design“

Dies ist eine bewusste architektonische Haltung und kein bloßes Rechtsversprechen. Ein Gerichtsverfahren kann ein Unternehmen dazu zwingen, das herauszugeben, was es besitzt. Es kann ein Unternehmen jedoch nicht dazu zwingen, etwas vorzulegen, das nie erhoben wurde.

Da Cyber Crucible keine Verschlüsselungsschlüssel, Anmeldedaten oder privaten Inhalte sammelt oder speichert, sind diese Kategorien von vornherein leer.

Warum das heute wichtiger ist als früher

Zentralisierte Sicherheitsarchitekturen schaffen einen hochwertigen Sammelpunkt. Ein Anbieter, der die Schlüssel und Sitzungstoken Tausender Kunden verwahrt, ist ein Ziel sowohl für kriminelle als auch für staatlich unterstützte Angreifer – und kann auch durch rechtlichen Zwang erreicht werden, mitunter ohne Wissen des Kunden.

Die Haltung von Cyber Crucible zur Schlüssel hinterlegung folgt derselben Logik: Es wird bewusst kein zentraler Schlüsselspeicher unterhalten, sodass es keinen einzelnen Angriffs- oder Zustellungspunkt (Single Point of Failure) gibt, der kompromittiert oder per Vorladung erzwungen werden könnte.

Eine ehrliche Grenze

Cyber Crucible ist ein US-Unternehmen und unterliegt US-amerikanischem Recht. Die hier getroffene Aussage ist eng gefasst und spezifisch: Das Unternehmen kann keine Daten offenlegen, die es nicht besitzt. Dies ist eine Aussage über die Architektur, keine Behauptung einer Immunität gegenüber rechtlichen Verfahren.

Wie werden die Daten von Cyber Crucible bei der Übertragung geschützt?

Kurzantwort: Sämtliche Kommunikation zwischen Agent und Server erzwingt TLS 1.3. Operative Datenpayloads verwenden zusätzlich JSON Web Encryption (JWE) mit eindeutigen kryptografischen Schlüsselpaaren pro Agent, sodass Payloads während der Übertragung weder abgefangen noch manipuliert werden können. Der administrative Zugriff erfordert eine schlüsselbasierte Authentifizierung sowie eine OAuth-2.0-Token-Validierung.

Die Schutzebenen

- **Verschlüsselte Kanäle** — die gesamte Kommunikation zwischen Agent und Server erzwingt TLS 1.3.
- **Payload-Verschlüsselung pro Agent** — operative Payloads verwenden JWE mit eindeutigen Schlüsselpaaren pro Agent. Da jeder Agent über sein eigenes Schlüsselpaar verfügt, führt die Kompromittierung eines Übertragungswegs nicht zur Offenlegung anderer, und ein Abfangen oder Manipulieren während der Übertragung wird verhindert.
- **Authentifizierte Administration** — der Systemzugriff erfordert eine individuelle, schlüsselbasierte Benutzerauthentifizierung sowie eine OAuth-2.0-Token-Validierung, wodurch administrative Handlungen auf autorisiertes Personal beschränkt bleiben.

Warum agentenspezifische Schlüssel wichtig sind

Transportverschlüsselung allein schützt nur den Kanal. Die Payload-Verschlüsselung pro Agent schützt den *Inhalt der Nachricht* unabhängig vom Kanal — sodass ein Angreifer, der sich zwischen den Kommunikationswegen befindet, oder ein kompromittierter Vermittler dennoch nicht lesen oder verändern kann, was der Agent gesendet hat.

Gemeinsam genutzte Infrastruktur

Sofern öffentliche oder virtuelle private Cloud-Umgebungen für die Backend-Administration genutzt werden, wendet Cyber Crucible eine strikte logische Mandantentrennung in Kombination mit durchgängiger Payload-Verschlüsselung an. Cloud-Anbieter und Infrastrukturbetreiber haben **keinerlei Einblick** in operative Datenpayloads oder Kundensystemzustände.

Wo werden meine Daten verarbeitet, und können sie innerhalb meines Landes verbleiben?

Kurze Antwort: Ja. Die Infrastruktur von Cyber Crucible kann so bereitgestellt werden, dass die Verarbeitung geografisch nahe an oder innerhalb Ihrer Rechtsordnung erfolgt, und eine vollständig lokale, air-gapped Bereitstellung hält alles innerhalb Ihrer eigenen Netzwerkgrenze — ohne ausgehende Telemetriedaten.

Souveräne Bereitstellung

Die Infrastruktur kann so positioniert werden, dass die Verarbeitung innerhalb — oder geografisch nahe — der Rechtsordnung des Kunden erfolgt. Dies ist darauf ausgelegt, die Einhaltung von Vorgaben zur Datenresidenz zu unterstützen, einschließlich der EU-Datenschutz-Grundverordnung (GDPR), des saudi-arabischen Personal Data Protection Law (PDPL), des VAE-Bundesdekretgesetzes Nr. 45/2021 sowie des kenianischen Data Protection Act.

Die stärkste Option

Für Organisationen, die eine vollständige Isolierung benötigen, betreibt das On-Premises-Modell die gesamte Backend-Verwaltungssoftware innerhalb Ihrer eigenen, physisch gesicherten Serverracks. Es verlassen keinerlei Telemetriedaten und keine Daten Ihre souveräne Netzwerkgrenze.

Da die Bedrohungsbewertung und die Prozessunterbindung lokal auf dem Endpunkt erfolgen — typischerweise in unter 200 Millisekunden —, ist der Schutz nicht auf eine externe Verbindung angewiesen. Souveränität kostet keinerlei Abstriche bei der Schutzwirkung.

“ Siehe auch: *"Welche Bereitstellungsmodelle stehen für Datensouveränität zur Verfügung?"*

Welche Bereitstellungsmodelle stehen für die Datensouveränität zur Verfügung?

Kurze Antwort: Zwei. Ein vollständig air-gapped On-Premises-Modell, bei dem keine Daten Ihr Netzwerk verlassen, und ein gehostetes oder hybrides Cloud-unterstütztes Modell mit JWE-verschlüsselter TLS-Kommunikation zu regional bereitgestellten Servern. Beide bieten dieselbe lokale Prävention in unter 200 Millisekunden.

Vergleich

	Souveräne On-Premises-Lösung (Air-Gapped)	Gehostet / Hybrid Cloud-unterstützt
Grenze der Datenübertragung	100 % innerhalb der physisch gesicherten Serracks des Kunden enthalten	JWE-verschlüsselte TLS-Kommunikation zu regionalen Anwendungsservern
Grenzüberschreitender Datenfluss	Kein externer Netzwerkverkehr; keine ausgehende Telemetrie	Geografisch lokalisiertes Staging zur Einhaltung regionaler Grenzen
Regulatorische Ausrichtung	Unterstützt strenge nationale Anforderungen an Datenresidenz und -souveränität	Ausgelegt auf die Übereinstimmung mit globalen Datenschutzrichtlinien (GDPR, PDPL und andere)

Die richtige Wahl treffen

Das air-gapped Modell eignet sich für Behörden, Verteidigung, kritische Infrastrukturen und jede Organisation, die strengen nationalen Residenzvorgaben unterliegt oder in getrennten (disconnected) Umgebungen arbeitet.

Das Hybridmodell eignet sich für Organisationen, die eine zentrale Verwaltung und ein flottenübergreifendes Reporting wünschen, während die Daten dennoch innerhalb einer regionalen Grenze verbleiben.

Die Prävention ist in beiden Fällen identisch. Die lokale Detect-Decide-Respond-Schleife läuft unabhängig vom Bereitstellungsmodell im Kernel auf dem Endpunkt — der einzige Unterschied besteht darin, wo die Management- und Reporting-Infrastruktur angesiedelt ist.

Wie steuert Cyber Crucible Lieferketten- und Insider-Risiken?

Kurze Antwort: Durch verbindliche gegenseitige Vertraulichkeitsvereinbarungen (NDAs) für alle Mitarbeitenden mit potenziellem Zugriff, streng auf das Need-to-know-Prinzip beschränkten administrativen Zugriff für überprüftes Personal sowie eine Null-Toleranz-Vorgabe, jeden Lieferanten, Anbieter, Auftragnehmer oder Mitarbeitenden, der ein Risiko für Kunden oder deren geistiges Eigentum darstellt, zu isolieren oder unverzüglich von der Zusammenarbeit auszuschließen.

Die Kontrollen

- **Verpflichtende Vertraulichkeitsvereinbarungen (NDAs)** — Alle Mitarbeitenden mit potenziellem Zugriff auf operative Kundendaten oder Managementsysteme sind vor dem Onboarding rechtlich durch eine gegenseitige NDA gebunden.
- **Strikter Need-to-know-Zugriff** — Der administrative Zugriff auf Kunden-Management-Instanzen ist ausschließlich auf überprüftes Personal beschränkt, und dies nur, wenn dies zur Durchführung eines validierten Geschäfts- oder Supportvorgangs erforderlich ist.
- **Vorgabe zur Trennung von Anbietern und Ressourcen** — Stellt ein Lieferant, Softwareanbieter, Auftragnehmer oder Mitarbeitender ein Sicherheits-, Datenschutz- oder Risiko für das geistige Eigentum der Kunden dar, steuert und isoliert Cyber Crucible dieses Risiko aktiv oder trennt sich unverzüglich von der betreffenden Ressource.

Warum Insider- und Lieferkettenrisiken zusammengehören

Beide sind im Grunde dasselbe Problem, nur aus unterschiedlichen Blickwinkeln betrachtet: Jemand mit legitimem Zugriff wird zum Angriffsvektor. Um dies zu kontrollieren, muss man einschränken, wer Zugriff hat, diese Personen vertraglich binden und bereit sein, eine Beziehung schnell zu beenden, sobald ein Risiko erkennbar wird — auch eine geschäftliche Beziehung.

Die Vorgabe zur Trennung ist der Teil, der Organisationen am häufigsten fehlt. Verträge und NDAs begründen Pflichten; erst die Bereitschaft, einen Lieferanten sofort zu kündigen, macht sie wirksam.

Bettet Cyber Crucible Bibliotheken oder Fremdcode von Drittanbietern ein?

Kurze Antwort: Nein. Kernel-Sensoren, Treiber und Genetic-AI-Verhaltensmodelle werden intern entwickelt. In die Software sind keine SDKs staatlich gesteuerter ausländischer Akteure, keine ungeprüften Bibliotheken von Drittanbietern und keine versteckten Telemetrie-Hooks eingebettet. Windows-Kernel-Treiber werden zur Zertifizierung im Rahmen des Windows Hardware Compatibility Program (WHCP) von Microsoft eingereicht.

Der technologische Wettbewerbsvorteil

Der interne Aufbau von Kernel-Sensoren und Verhaltensmodellen ist aufwendig und zeitintensiv. Die meisten Anbieter setzen stattdessen auf die Zusammenstellung vorhandener Komponenten. Genau an dieser Stelle entsteht in einem Sicherheitsprodukt das Risiko in der Lieferkette — und ausgerechnet das Tool mit den weitreichendsten Systemrechten ist dasjenige, bei dem eine ungeprüfte Abhängigkeit den größten Schaden anrichten kann.

Die Komponenten von Cyber Crucible sind proprietär und werden intern gepflegt, wodurch diese Art der Gefährdung von vornherein ausgeschlossen wird, anstatt sie lediglich zu verwalten.

Externe Validierung

Alle Windows-Kernel-Treiber durchlaufen interne Qualitätssicherungstests und werden zur Zertifizierung im Rahmen des Windows Hardware Compatibility Program (WHCP) von Microsoft eingereicht — eine unabhängige Validierung der Qualität und Manipulationssicherheit von Code, der auf Kernel-Ebene ausgeführt wird.

Keine versteckte Telemetrie

Es gibt keine versteckten Telemetrie-Hooks. Welche Daten die Software erfasst, ist dokumentiert, und die Kategorien, die niemals erfasst werden, sind ausdrücklich aufgeführt.

Was bedeutet geopolitische Neutralität bei Sicherheitssoftware?

Kurze Antwort: Es bedeutet, dass die Software so entwickelt wurde, dass sie Ihr Unternehmen schützt, ohne ausländische strategische Hintertüren, ausländische Partnerschaften mit staatlichen Nachrichtendiensten oder verpflichtende Cloud-Abhängigkeiten einzubetten – sodass ihre Nutzung nicht die strategischen Interessen eines anderen Landes in Ihre Infrastruktur einbringt.

Das Problem, das dies adressiert

Herkömmliche Sicherheitstools verlassen sich häufig auf zentralisierte Cloud-Erfassungsmodelle, die kontinuierlich Endpunkt-Telemetriedaten, Kontodetails und Dateisystemartefakte über nationale und geopolitische Grenzen hinweg übertragen. Das ist gegenüber Angriffen in Maschinengeschwindigkeit zu langsam und schafft zudem Compliance- und Sicherheitsrisiken im Hinblick auf GDPR, das saudi-arabische PDPL, das Bundesdekretgesetz Nr. 45/2021 der VAE und das kenianische Datenschutzgesetz (Kenya Data Protection Act).

Es wirft zudem eine Frage auf, die in den meisten Beschaffungsprozessen nie gestellt wird: *In wessen Rechtshoheit landen meine Telemetriedaten letztlich, und wer kann dort sonst noch darauf zugreifen?*

Die drei Komponenten

1. **Keine ausländischen strategischen Hintertüren** – keine staatlich geförderten Codekomponenten oder ungeprüften ausländischen SDKs.
2. **Keine Partnerschaften mit ausländischen staatlichen Nachrichtendiensten** – Kunden-Telemetriedaten werden mit keinem Dritten geteilt, einschließlich Regierungen.
3. **Keine verpflichtende Cloud-Abhängigkeit** – die Software funktioniert vollständig offline, sodass keine Daten jemals eine Grenze überschreiten müssen, damit das Produkt funktioniert.

Der dritte Punkt ist das, was die ersten beiden erst durchsetzbar macht. Ein Produkt, das *zwingend* eine Cloud-Verbindung benötigt, kann nicht glaubwürdig versprechen, dass Ihre Daten an ihrem Ort verbleiben.