

Governança e Soberania de Dados

O que a Cyber Crucible coleta e nunca coleta, como os dados são protegidos em trânsito, onde são processados, o que pode ser divulgado sob processo legal, e como o risco da cadeia de suprimentos e de ameaças internas é controlado.

- [Que dados a Cyber Crucible recolhe — e que dados nunca recolhe?](#)
- [Qual é a diferença entre a telemetria do sistema e os dados do cliente?](#)
- [A Cyber Crucible vende ou compartilha dados de clientes com terceiros?](#)
- [O que a Cyber Crucible pode divulgar se for obrigada por um governo ou tribunal?](#)
- [Como os dados da Cyber Crucible são protegidos em trânsito?](#)
- [Onde os meus dados são processados e podem permanecer dentro do meu país?](#)
- [Quais modelos de implantação estão disponíveis para a soberania de dados?](#)
- [Como a Cyber Crucible gerencia riscos da cadeia de suprimentos e riscos internos?](#)
- [A Cyber Crucible incorpora bibliotecas de terceiros ou código estrangeiro?](#)
- [O que significa neutralidade geopolítica em software de segurança?](#)

Que dados a Cyber Crucible recolhe — e que dados nunca recolhe?

Resposta breve: A Cyber Crucible opera sob uma diretiva de Zero-Content Harvesting (recolha zero de conteúdo). Processa telemetria operacional do sistema — caminhos de execução de processos, cadeias de processos pai-filho, indicadores de execução de hardware e estados de integridade da memória — analisados localmente no endpoint. Não recolhe, transmite, armazena ou processa chaves de encriptação, credenciais, tokens de sessão ou os seus ficheiros.

Categorias estritamente excluídas

O software da Cyber Crucible não recolhe, transmite, armazena ou processa:

- **Variáveis criptográficas** — chaves privadas, chaves de descriptação e chaves de encriptação de aplicações.
- **Credenciais de utilizador** — palavras-passe de utilizador, segredos do Active Directory e chaves privadas de API.
- **Identificadores de sessão** — tokens OAuth, tokens de acesso, tokens de atualização e cookies de sessão.
- **Dados de conteúdo do cliente** — ficheiros proprietários, documentos, conteúdos de bases de dados, corpos de e-mails e comunicações do utilizador.

Por que a proteção total não requer a recolha de conteúdo

A capacidade total do software de prevenção de ameaças é alcançada sem recolher ou exfiltrar conteúdo privado do cliente. O motor comportamental avalia *o que um programa está a fazer* — quais processos estão a alcançar onde, tendo feito o quê previamente — e nada disso requer abrir o ficheiro ou ler o segredo.

Este é o mesmo princípio subjacente à proteção de identidade: o acesso é rastreado e analisado sem que a própria credencial seja acedida.

Onde ocorre a análise

Os caminhos de execução de processos, a linhagem de processos, os indicadores de execução de hardware e os estados de integridade da memória são analisados **localmente no endpoint**. Quando a gestão assistida por nuvem ou centralizada está ativada, a telemetria administrativa de saída é estritamente limitada aos indicadores operacionais necessários para a monitorização da saúde do sistema e para os relatórios de segurança.

Qual é a diferença entre a telemetria do sistema e os dados do cliente?

Resposta curta: A telemetria do sistema descreve como o software está se comportando — qual processo iniciou qual, como se apresenta a memória, se os padrões de execução são anómalos. Os dados do cliente são o conteúdo que a sua empresa cria e mantém — ficheiros, e-mails, registos de bases de dados, credenciais. A Cyber Crucible analisa o primeiro e nunca recolhe o segundo.

Uma forma útil de pensar sobre isto

A telemetria é metadados sobre o *comportamento da máquina*. O conteúdo é a *informação em si*.

Saber que o `processo A` gerou o `processo B`, que depois tentou ler um repositório de credenciais do browser enquanto apresentava sinais de modificação em memória, é suficiente para identificar um ataque. Ler o que estava nesse repositório de credenciais não é necessário — e a Cyber Crucible não o faz.

O que isto significa na prática

- A análise comportamental é realizada sobre o acesso à identidade **sem processar a própria informação de identidade**.
- A telemetria que efetivamente sai do endpoint em implementações assistidas por nuvem limita-se a indicadores operacionais para monitorização de estado e relatórios de segurança.
- Os metadados técnicos e comportamentais são tratados como dados pessoais apenas quando podem identificar direta ou indiretamente um indivíduo — e, nesses casos, os identificadores são pseudonimizados ou mascarados.

Controlo do cliente

As fontes de telemetria são configuráveis. As organizações podem definir quais as fontes recolhidas, de modo a que não seja adquirida informação desnecessária. Os campos que não são essenciais para a deteção de ameaças são excluídos ou descartados.

A Cyber Crucible vende ou compartilha dados de clientes com terceiros?

Resposta curta: Não. A Cyber Crucible não compartilha, licencia, comercializa ou divulga informações de clientes ou telemetria a terceiros, e os dados de clientes não estão, sob nenhuma circunstância, à venda.

Os compromissos

- **Zero compartilhamento com terceiros** — nenhum compartilhamento, licenciamento, comercialização ou divulgação de informações de clientes ou telemetria a terceiros.
- **Proibição de monetização comercial** — os dados de clientes não estão à venda, sob nenhuma circunstância.
- **Nenhuma corretagem de dados de identidade ou telemetria** — não são comercializados, licenciados ou monetizados com qualquer parte.

Por que isso é arquiteturalmente confiável

Muitos fornecedores fazem a promessa de não vender dados. O que torna esta diferente é que grande parte do material sensível simplesmente não é coletado, em primeiro lugar. Uma empresa que nunca detém suas chaves de descryptografia, credenciais ou arquivos não tem nada nessas categorias para vender, compartilhar ou perder — independentemente da política.

A política pode mudar. A arquitetura é mais difícil de reverter.

“Veja também: *"O que a Cyber Crucible pode divulgar se obrigada por um governo ou tribunal?"*

O que a Cyber Crucible pode divulgar se for obrigada por um governo ou tribunal?

Resposta curta: Nada nas categorias que mais importam, porque ela nunca as detém. A Cyber Crucible não coleta, armazena nem retém chaves de decifração, credenciais de usuário ou arquivos de clientes — portanto, não há nada desse tipo para ser entregue a nenhuma parte privada, governo ou potência estrangeira. Como qualquer empresa dos EUA, ela permanece sujeita à legislação aplicável, mas não pode entregar dados que nunca possuiu.

"Nada a divulgar por design"

Trata-se de uma posição arquitetônica deliberada, e não de uma promessa jurídica. Um processo legal pode obrigar uma empresa a entregar aquilo que ela possui. Não pode obrigá-la a produzir aquilo que nunca foi coletado.

Como a Cyber Crucible não coleta nem retém chaves de criptografia, credenciais ou conteúdo privado, essas categorias estão vazias por design.

Por que isso importa mais do que antes

Arquiteturas de segurança centralizadas criam um ponto de agregação de alto valor. Um fornecedor que armazena as chaves e tokens de sessão de milhares de clientes é um alvo tanto para criminosos quanto para atacantes patrocinados por estados — e pode ser acessado por meio de coerção legal, às vezes sem o conhecimento do cliente.

A posição da Cyber Crucible sobre custódia de chaves segue o mesmo raciocínio: ela deliberadamente não mantém um repositório central de chaves, de modo que não existe um único ponto de falha a ser violado ou intimado judicialmente.

Um limite honesto

A Cyber Crucible é uma empresa dos EUA e está sujeita às leis norte-americanas. A afirmação aqui é restrita e específica: ela não pode divulgar dados que não possui. Trata-se de uma declaração sobre arquitetura, não de uma alegação de imunidade a processos legais.

Como os dados da Cyber Crucible são protegidos em trânsito?

Resposta curta: Todas as comunicações entre o agente e o servidor aplicam TLS 1.3. Os payloads de dados operacionais utilizam adicionalmente JSON Web Encryption (JWE) com pares de chaves criptográficas exclusivos por agente, de modo que os payloads não possam ser interceptados ou manipulados em trânsito. O acesso administrativo requer autenticação baseada em chaves, além de validação de token OAuth 2.0.

As camadas

- **Canais criptografados** — todas as comunicações entre o agente e o servidor aplicam TLS 1.3.
- **Criptografia de payload por agente** — os payloads operacionais utilizam JWE com pares de chaves exclusivos por agente. Como cada agente possui seu próprio par de chaves, o comprometimento de um circuito de trânsito não expõe os demais, e a interceptação ou manipulação inline é evitada.
- **Administração autenticada** — o acesso ao sistema requer autenticação individual de usuário baseada em chave e validação de token OAuth 2.0, restringindo as ações administrativas a pessoal autorizado.

Por que as chaves por agente são importantes

A criptografia de transporte, por si só, protege apenas o canal. A criptografia de payload por agente protege o *conteúdo da mensagem* de forma independente do canal — de modo que um atacante posicionado inline, ou um intermediário comprometido, ainda assim não consegue ler ou alterar o que o agente enviou.

Infraestrutura compartilhada

Quando ambientes de nuvem pública ou de nuvem privada virtual são utilizados para a administração de back-end, a Cyber Crucible aplica um rigoroso isolamento lógico de locatários (tenants), juntamente com criptografia de payload de ponta a ponta. Os provedores de nuvem e operadores de infraestrutura têm **visibilidade zero** sobre os payloads de dados operacionais ou os estados dos sistemas dos clientes.

Onde os meus dados são processados e podem permanecer dentro do meu país?

Resposta breve: Sim. A infraestrutura da Cyber Crucible pode ser configurada para que o processamento ocorra geograficamente próximo ou dentro da sua jurisdição legal, e uma implementação totalmente no local (on-premises) e isolada (air-gapped) mantém tudo dentro do limite da sua própria rede, com zero telemetria de saída.

Configuração soberana

A infraestrutura pode ser posicionada para manter o processamento dentro — ou geograficamente próximo — da jurisdição legal do cliente. Isto foi concebido para apoiar a conformidade com mandatos de residência de dados, incluindo o Regulamento Geral sobre a Proteção de Dados (RGPD) da UE, a Lei de Proteção de Dados Pessoais (PDPL) da Arábia Saudita, o Decreto-Lei Federal dos EAU n.º 45/2021, e a Lei de Proteção de Dados do Quênia.

A opção mais robusta

Para organizações que exigem isolamento total, o modelo on-premises executa todo o software de gestão de backend dentro dos seus próprios racks de servidores fisicamente protegidos. Zero telemetria e zero dados saem do limite da sua rede soberana.

Como a avaliação de ameaças e a interdição de processos ocorrem localmente no endpoint, tipicamente em menos de 200 milissegundos, a proteção não depende de qualquer ligação externa. A soberania não custa nada em termos de capacidade defensiva.

“ Ver também: *"Que modelos de implementação estão disponíveis para a soberania de dados?"*

Quais modelos de implantação estão disponíveis para a soberania de dados?

Resposta curta: Dois. Um modelo local totalmente isolado (air-gapped), no qual nada sai da sua rede, e um modelo hospedado ou híbrido assistido por nuvem, com comunicações TLS criptografadas por JWE para servidores organizados regionalmente. Ambos oferecem a mesma prevenção local em menos de 200 milissegundos.

Comparação

	Local Soberano (Air-Gapped)	Hospedado / Híbrido Assistido por Nuvem
Limite de trânsito de dados	100% contido dentro dos racks de servidores fisicamente seguros do cliente	Comunicações TLS criptografadas por JWE para servidores de aplicação regionais
Fluxo transfronteiriço	Nenhum fluxo de rede externo; nenhuma telemetria de saída	Organização geograficamente localizada para atender aos limites regionais
Alinhamento regulatório	Suporta requisitos rigorosos de residência e soberania de dados nacionais	Projetado para se alinhar com diretivas globais de privacidade (GDPR, PDPL e outras)

Como escolher entre eles

O modelo air-gapped é adequado para governos, defesa, infraestrutura crítica e qualquer organização sujeita a mandatos rigorosos de residência nacional ou que opere em ambientes desconectados.

O modelo híbrido é adequado para organizações que desejam gerenciamento centralizado e relatórios entre frotas, mantendo ainda os dados dentro de um limite regional.

A prevenção é idêntica em ambos. O ciclo local de Detect-Decide-Respond é executado no kernel do endpoint, independentemente do modelo de implantação — a diferença está apenas em onde reside a infraestrutura de gerenciamento e relatórios.

Como a Cyber Crucible gerencia riscos da cadeia de suprimentos e riscos internos?

Resposta curta: Por meio de acordos mútuos de confidencialidade (NDA) vinculantes para todo o pessoal com acesso potencial, acesso administrativo estritamente restrito à necessidade de conhecimento e limitado a colaboradores previamente avaliados, e um mandato de tolerância zero para isolar ou desvincular imediatamente qualquer fornecedor, prestador, contratado ou colaborador que represente um risco para os clientes ou sua propriedade intelectual.

Os controles

- **Acordos de confidencialidade obrigatórios** — todo o pessoal com acesso potencial aos dados operacionais dos clientes ou aos sistemas de gestão está legalmente vinculado por um NDA mútuo antes da integração.
- **Acesso restrito à necessidade de conhecimento** — o acesso administrativo às instâncias de gestão dos clientes é restrito exclusivamente a pessoal previamente avaliado, e apenas quando necessário para realizar uma operação de negócios ou suporte validada.
- **Mandato de desvinculação de fornecedores e recursos** — se qualquer fornecedor, fornecedor de software, contratado ou colaborador representar um risco de segurança, privacidade ou propriedade intelectual para os clientes, a Cyber Crucible gerencia e isola ativamente esse risco ou desvincula o recurso imediatamente.

Por que os riscos internos e da cadeia de suprimentos estão relacionados

Ambos representam o mesmo problema visto de ângulos diferentes: alguém com acesso legítimo sendo o vetor. Controlá-lo requer limitar quem tem acesso, vincular essas pessoas contratualmente e estar disposto a romper rapidamente uma relação quando surge um risco — incluindo uma relação comercial.

O mandato de desvinculação é a parte que as organizações mais frequentemente não possuem. Contratos e NDAs estabelecem obrigações; a disposição de rescindir imediatamente com um fornecedor é o que as torna significativas.

A Cyber Crucible incorpora bibliotecas de terceiros ou código estrangeiro?

Resposta curta: Não. Os sensores de kernel, drivers e modelos comportamentais de Genetic AI são desenvolvidos internamente. Nenhum SDK patrocinado por estados estrangeiros, biblioteca de terceiros não verificada ou mecanismo oculto de telemetria está incorporado no software. Os drivers de kernel do Windows são submetidos para certificação no âmbito do Windows Hardware Compatibility Program (WHCP) da Microsoft.

O diferencial de engenharia

Construir sensores de kernel e modelos comportamentais internamente é caro e demorado. A maioria dos fornecedores monta componentes em vez de desenvolvê-los. É precisamente nessa montagem que o risco de cadeia de suprimentos entra em um produto de segurança — a ferramenta com os privilégios de sistema mais profundos é também aquela em que uma dependência não verificada causa mais danos.

Os componentes da Cyber Crucible são proprietários e mantidos internamente, o que elimina essa categoria de exposição em vez de apenas geri-la.

Validação externa

Todos os drivers de kernel do Windows passam por testes internos de garantia de qualidade e são submetidos para certificação no âmbito do Windows Hardware Compatibility Program (WHCP) da Microsoft — uma validação independente de qualidade e resistência a adulterações para código em execução no nível do kernel.

Sem telemetria oculta

Não existem mecanismos ocultos de telemetria. O que o software coleta está documentado, e as categorias que ele nunca coleta estão explicitamente enumeradas.

O que significa neutralidade geopolítica em software de segurança?

Resposta curta: Significa que o software é construído para proteger a sua organização sem incorporar backdoors estratégicos estrangeiros, parcerias de inteligência com estados estrangeiros ou dependências obrigatórias de nuvem — de modo que a sua utilização não importe os interesses estratégicos de outro país para a sua infraestrutura.

O problema que aborda

As ferramentas de segurança legadas frequentemente dependem de modelos centralizados de recolha em nuvem que exfiltram continuamente telemetria de endpoints, detalhes de contas e artefactos do sistema de ficheiros através de fronteiras nacionais e geopolíticas. Isso é lento face a ataques à velocidade das máquinas e cria exposição de conformidade e segurança ao abrigo do GDPR, da Saudi PDPL, da Lei Federal por Decreto n.º 45/2021 dos EAU e da Lei de Proteção de Dados do Quénia.

Também cria uma questão que a maioria dos processos de aquisição nunca coloca: *em que jurisdição acaba a minha telemetria, e quem mais lhe consegue aceder aí?*

Os três componentes

1. **Ausência de backdoors estratégicos estrangeiros** — sem componentes de código patrocinados por estados nem SDKs estrangeiros não verificados.
2. **Ausência de parcerias de inteligência com estados estrangeiros** — a telemetria do cliente não é partilhada com terceiros, incluindo governos.
3. **Ausência de dependência obrigatória de nuvem** — o software funciona totalmente offline, pelo que nenhum dado precisa de atravessar uma fronteira para que o produto funcione.

O terceiro ponto é o que torna os dois primeiros aplicáveis. Um produto que *exige* uma ligação à nuvem não pode prometer de forma credível que os seus dados permanecem no local.