

Onde são processados os dados da Cyber Crucible — são armazenados na nuvem?

Resposta breve: A análise de ameaças e a resposta ocorrem localmente no endpoint, não na nuvem. A Cyber Crucible não coleta arquivos, credenciais ou chaves dos clientes, e não armazena conteúdo dos clientes com um provedor de nuvem pública terceirizado. O backend de gestão e relatórios é executado em infraestrutura operada pela Cyber Crucible, localizada nos Estados Unidos, e uma implantação totalmente on-premises ou isolada (air-gapped) está disponível para organizações que exigem fluxo zero de dados externos.

Por que o processamento local é importante

- **A decisão de proteção nunca sai do dispositivo.** O Detect-Decide-Respond é executado no kernel, no próprio endpoint, tipicamente em menos de 200 milissegundos, sem ida e volta à nuvem no caminho crítico.
- **Proteção independente do backend.** Uma interrupção no backend de gestão não reduz a proteção do endpoint.
- **Escolha de implantação.** Organizações com mandatos rigorosos de residência ou soberania de dados podem executar a Cyber Crucible inteiramente dentro de sua própria infraestrutura segura.

No que um revisor pode confiar

Como o conteúdo dos clientes nunca é coletado, a pergunta "para onde vão os nossos dados?" tem uma resposta simples para as categorias de maior risco: eles não vão para lugar nenhum. Informações detalhadas sobre infraestrutura e subprocessadores são fornecidas aos revisores mediante acordo de confidencialidade (NDA).