

Conformidade e Risco

Como a prevenção autônoma e local (on-device) afeta as obrigações regulatórias, a divulgação de violações, a soberania de dados, o seguro cibernético e os relatórios de risco ao nível do conselho.

- [A Cyber Crucible coleta chaves de criptografia?](#)
- [Se um ataque for impedido, ainda precisamos relatar uma violação?](#)
- [Como a Cyber Crucible apoia a conformidade com a HIPAA no setor de saúde?](#)
- [Como a Cyber Crucible apoia a FERPA e a privacidade de dados dos estudantes?](#)
- [O que significa soberania de dados para as implantações da Cyber Crucible?](#)
- [Que risco de conformidade cria o depósito \(escrow\) de chaves de criptografia, e por que a Cyber Crucible não o faz?](#)
- [Como é que a prevenção autónoma afeta o seguro cibernético e os relatórios ao conselho de administração?](#)

A Cyber Crucible coleta chaves de criptografia?

A resposta mais curta é: “Não.”

Houve uma época em que o software da Cyber Crucible não impedia a criptografia de ransomware antes da criptografia. Em vez disso, coletava possíveis chaves de criptografia ou configurações e, em seguida, utilizava uma variedade de técnicas para descobrir o pacote de descriptografia adequado (incluindo as chaves) para descriptografar após um ataque de ransomware.

Do ponto de vista do que coletávamos, uma boa analogia seria uma câmera de vídeo que tirasse fotos de tudo o que pudesse ser uma chave para um cofre. Em seguida, um servidor faria os diversos cálculos para determinar a chave e as configurações corretas para o arquivo adequado. Cientistas da computação chamariam isso de aprendizado de máquina.

Antes de deixarmos para trás o antigo modelo de software “coletar tudo o que possa ser uma chave”, estávamos organizando automaticamente milhares de chaves e configurações de criptografia por máquina durante os ataques.

O módulo de software de análise criptográfica evoluiu agora para um módulo analítico comportamental adicional, que é utilizado como uma das fontes de dados para determinar se um software está tentando acessar indevidamente dados de identidade ou “dados de dados” para roubá-los ou criptografá-los.

Se um ataque for impedido, ainda precisamos relatar uma violação?

Resposta curta: De modo geral, não. Quando um ataque é interrompido antes da execução e nenhum dado é acessado, alterado ou exfiltrado, tipicamente não há violação a ser divulgada. As obrigações de divulgação costumam ser acionadas pelo acesso não autorizado a dados protegidos — e não por uma tentativa que falhou.

Um exemplo real

Na implantação do setor de serviços financeiros em que a Cyber Crucible interceptou quase 10.000 processos maliciosos, o resultado para o CISO incluiu zero divulgação regulatória. Como os ataques foram interrompidos antes da execução e nenhum dado foi tocado, não houve notificações obrigatórias a clientes, fornecedores ou órgãos reguladores governamentais — e nenhuma manchete negativa, o que preservou a confiança dos clientes.

Uma ressalva importante

Os requisitos de divulgação variam conforme a jurisdição, o setor e o contrato, e os fatos específicos de um incidente são relevantes. A Cyber Crucible não é um escritório de advocacia, e isto não constitui aconselhamento jurídico. O princípio confiável é que a prevenção reduz drasticamente a exposição à divulgação em comparação com a detecção após o fato — mas a determinação para qualquer evento específico deve ser feita por sua equipe jurídica e de conformidade.

Como a Cyber Crucible apoia a conformidade com a HIPAA no setor de saúde?

Resposta curta: Toda a análise ocorre localmente, no nível do kernel, portanto as informações de saúde protegidas nunca saem do endpoint para o processamento de segurança. Isso evita a exposição relacionada à HIPAA criada por ferramentas de segurança que enviam arquivos ou chaves sensíveis para nuvens de terceiros, e interrompe os ataques sem tirar os sistemas clínicos do ar.

O problema da segurança hospedada por fornecedores

Muitos acordos de SOC e MDR hospedados por fornecedores exigem o envio de chaves, arquivos ou telemetria sensíveis para bancos de dados em nuvem de terceiros. Para uma entidade coberta, isso cria um risco real de conformidade e amplia o número de partes que lidam com dados protegidos.

Análise local, dados locais

A Cyber Crucible realiza a análise no endpoint. Os ativos sensíveis nunca saem do perímetro seguro do dispositivo — o que apoia tanto a soberania dos dados quanto a postura regulatória associada a ela.

A continuidade importa clinicamente

A contenção que exige isolar uma máquina ou forçar uma reinicialização não é aceitável quando o atendimento ao paciente depende dela. A suspensão seletiva apenas do processo malicioso significa que o ataque é neutralizado em menos de 200 milissegundos, enquanto as operações médicas, os dispositivos conectados e os sistemas clínicos continuam em funcionamento.

Como a Cyber Crucible apoia a FERPA e a privacidade de dados dos estudantes?

Resposta curta: o FortressAI verifica o acesso a dados no dispositivo, para que registos de estudantes e dados familiares não cheguem acidentalmente a uma ferramenta de IA pública. A Cyber Crucible interrompe o ransomware de forma autónoma, sem exigir um centro de operações de segurança (SOC) 24 horas por dia, 7 dias por semana — algo que a maioria dos distritos e instituições não consegue financiar.

Os dois problemas do setor da educação

Escolas e universidades são alvos privilegiados de ransomware, mas raramente dispõem de orçamento para uma equipa de SOC em regime contínuo. Ao mesmo tempo, a adoção de IA nas salas de aula avançou muito mais depressa do que a governação relativa a essa utilização.

Resposta a ambos os problemas

- **Ransomware sem um SOC:** a prevenção autónoma, ao nível do kernel, interrompe ataques em menos de 200 milissegundos, sem necessidade de contratar analistas nem de financiar um contrato de monitorização 24/7.
- **Utilização de IA alinhada com a FERPA:** o FortressAI avalia cada pedido (prompt) no dispositivo, para que registos educativos protegidos e dados pessoais familiares não acabem num sistema de IA público — nem sequer como dados de treino.

Esta combinação protege estudantes e funcionários sem acrescentar uma sobrecarga significativa para a equipa de TI.

O que significa soberania de dados para as implantações da Cyber Crucible?

Resposta curta: Os seus dados permanecem onde forem colocados. A análise e a aplicação ocorrem no endpoint, e a Cyber Crucible pode ser implantada totalmente no local (on-premises) — funcionando em racks de servidores fisicamente seguros em vez de numa nuvem pública, sem plataformas de terceiros, sem acesso externo e sem partilha de dados.

Por que motivo os dados de segurança centralizados representam um risco

As arquiteturas de segurança que centralizam material sensível — chaves de encriptação, tokens de sessão, dados de identidade — criam um único ponto de falha e um alvo de elevado valor tanto para atacantes criminosos como para os patrocinados por estados.

Existe um segundo risco que recebe menos atenção: um governo pode obrigar ao acesso a dados detidos centralmente através de uma intimação classificada ou de uma carta de segurança nacional, sem o conhecimento ou consentimento do cliente. Trata-se de uma exposição profunda em termos de soberania de dados, sem qualquer transparência.

A opção no local (on-premises)

Para organizações que exigem controlo absoluto, a Cyber Crucible oferece uma instalação totalmente no local, incluindo implantação em ambiente isolado (air-gapped) e uma arquitetura multi-tenant adequada para gerir múltiplos departamentos ou agências a partir de uma única instância segura.

Que risco de conformidade cria o depósito (escrow) de chaves de criptografia, e por que a Cyber Crucible não o faz?

Resposta curta: Armazenar chaves de criptografia de forma centralizada cria um ponto único de falha, um alvo de alto valor e exposição à divulgação forçada. A abordagem de prevenção da Cyber Crucible não depende da captura ou do depósito de chaves, portanto não há um repositório central de chaves para proteger, intimidar judicialmente ou violar.

“ Para a resposta direta sobre o produto, consulte o artigo existente **"A Cyber Crucible coleta chaves de criptografia?"** Esta página aborda o raciocínio de conformidade e soberania de dados por trás dessa resposta.

Por que isso é deliberado

A Cyber Crucible originalmente desenvolveu e patenteou uma tecnologia de captura de chaves para defesa contra ransomware. Em 2021, as variantes de ransomware haviam evoluído para derrotá-la — utilizando bibliotecas de criptografia personalizadas, implementações exclusivas por execução e cifras de fluxo imunes à captura de chaves. Apresentamos essa criptoanálise publicamente na BSides Pittsburgh em 2021.

O risco que optamos por não criar

Além de não funcionar mais, a captura de chaves exige o armazenamento centralizado de chaves de criptografia. Isso introduz um ponto único de falha, um alvo de alto valor e a possibilidade de divulgação forçada sem o conhecimento do cliente.

Prevenir o ataque antes que a criptografia comece elimina completamente a necessidade de chaves — o que representa tanto uma defesa mais forte quanto uma superfície de conformidade menor.

Como é que a prevenção autónoma afeta o seguro cibernético e os relatórios ao conselho de administração?

Resposta curta: A prevenção muda aquilo que se reporta. Em vez de documentar incidentes, tempo de inatividade e custos de remediação, reporta-se ataques que foram interrompidos sem interrupção da atividade, sem divulgação e sem pagamento de resgate.

O que realmente interessa ao conselho de administração

Na implementação no setor de serviços financeiros referenciada ao longo desta base de conhecimento, o CISO conseguiu reportar quatro resultados:

- **Zero paragem da atividade empresarial** — ataques suspensos em memória; as operações e as transações legítimas continuaram.
- **Zero divulgação regulatória** — nada foi acedido, pelo que nada exigiu notificação.
- **Zero danos de imagem pública** — sem manchetes, confiança dos clientes preservada.
- **ROI sólido** — uma fração do custo da pilha de tecnologia legada realizou o trabalho que essa pilha não conseguiu fazer.

Sobre pagamentos de resgate

Aproximadamente 90% das vítimas de ransomware pagaram o resgate em 2023. Os clientes da Cyber Crucible não pagaram nada, porque os ataques não chegaram à fase de encriptação.

Para seguradoras

As seguradoras subscritoras perguntam cada vez mais quais os controlos que previnem um incidente, em vez de quais as ferramentas que detetam um. Um controlo autónomo, ao nível do kernel, que opera sem tempo de resposta humano é uma resposta substancial — embora os

termos de cobertura sejam sempre definidos pela sua seguradora.