

O Seu Software É Vulnerável A Crimes Cibernéticos?

O suporte terceirizado e a automanutenção não protegem o seu sistema — a solução verdadeira está na origem

O Crime Cibernético É Real US\$ 23 Trilhões

Estimativa do custo anual com danos causados por crimes cibernéticos no mundo todo até 2027¹

↑ Ataques cibernéticos e violações de dados continuam a crescer exponencialmente²

A média de custo de uma violação de dados foi de
US\$ 4,88 milhões
desde 2024³

Ataques Ransomware
são uma ameaça constante que afeta todas as indústrias⁴

Muitas empresas nunca se recuperam do impacto

- Informações confidenciais particulares
- Interrupção operacional
- Restauração de arquivos e sistemas
- Multas e processos judiciais
- Danos à reputação e à marca
- Confiança dos clientes e funcionários

Não Se Engane Com Métodos De Segurança Oferecidos Por Provedores De Suporte Terceirizados Ou Automanutenção

1 O “patching virtual” não resolve nada

O patching virtual é uma solução paliativa que, na verdade, não corrige nem atualiza o seu software.

- ▶ Solução temporária
- ▶ Negligencia a raiz do problema
- ▶ Ignora o escopo completo das vulnerabilidades

Departamento De Defesa Dos Estados Unidos

“É necessário que todas as organizações estabeleçam um processo eficiente de gerenciamento de patches para garantir que sejam tomadas medidas preventivas contra possíveis ameaças.”

<https://www.cisa.gov/>

2 Firewalls não são à prova de fogo

As estratégias de segurança voltadas para o perímetro deixam o seu software vulnerável a ataques.

- ▶ Suscetível a violações internas
- ▶ Visibilidade mínima das ameaças na rede
- ▶ Ignora a segurança real do software

Regulamento de Proteção de Dados Gerais da UE

Um conjunto único de regras para melhorar a privacidade dos dados e garantir a segurança de dados pessoais e do processamento de dados.

- ✓ Aplica-se a todas as organizações que têm acesso a dados de residentes da UE
- ✓ Em vigor a partir de 25 de maio de 2018
- ✓ A violação ou não conformidade poderá resultar em multas altas

https://ec.europa.eu/info/law/law-topic/data-protection/eu-data-protection-rules_en

3 Automanutenção = possível responsabilidade

Fazer você mesmo deixará seus softwares sem atualizações essenciais de segurança.

- ▶ Sem a capacidade de (legalmente) corrigir vulnerabilidades
- ▶ Sem acesso a novos patches e atualizações
- ▶ Recursos limitados para fazer a manutenção e cuidar da segurança de maneira confiável

Conclusão

Os patches de segurança são essenciais para proteger softwares corporativos, inclusive da Oracle. Se você não tiver acesso ao código fonte, não poderá desenvolver patches para ele. Isso deixa seu software vulnerável a ataques e sua empresa sujeita a riscos.



- ▶ Atualizações de segurança inadequadas
- ▶ Correções de segurança inadequadas
- ▶ Proteção inadequada contra vulnerabilidades

Proteja Softwares da Oracle com o Oracle Support

O Oracle Support é a melhor maneira de receber legalmente a proteção e as atualizações de segurança essenciais para o seu software da Oracle.



Oracle desenvolve o código fonte e é proprietária dele

- ▶ As vulnerabilidades e ameaças emergentes são identificadas e resolvidas na origem
- ▶ Atualizações de segurança confiáveis na origem



A Oracle oferece segurança em todos os níveis

- ▶ Patches em todas as camadas da pilha de software
- ▶ Testes de regressão em toda a pilha



A Oracle tem as ferramentas, a experiência e o conhecimento

- ▶ Processos proativos de gerenciamento de mudanças
- ▶ Processo uniforme de gerenciamento de versões
- ▶ Inovação confiável, contínua e inigualável

Com a Oracle você ganha muito mais.

Quando sua empresa está em risco, não há nada melhor do que um suporte confiável, seguro e abrangente.

[Acesse Oracle Premier Support](#)

Fontes:
1. <https://www.techtarget.com/whatis/34-Cybersecurity-Statistics-to-Lose-Sleep-Over-in-2020>
2. <https://www.securitymagazine.com/articles/100335-cyberattack-attempts-increased-104-in-2023>
3. <https://www.ibm.com/security/data-breach>
4. <https://assets.sophos.com/XZ4WTUEQ/at/9brg5n44hqvgsp5f5bqcps/sophos-state-of-ransomware-2024-wp.pdf>

Direitos autorais © 2025, Oracle e/ou suas afiliadas. Todos os direitos reservados. Oracle e Java são marcas registradas da Oracle e/ou de suas afiliadas. Outros nomes poderão ser marcas registradas de seus respectivos proprietários. Versão 1.04

