Is Your Software Vulnerable To Cybercrime?

Third-party support and self-maintenance can't protect you—the real solution is at the source.

Cybercrime is Real

\$10.5 trillion The estimated annual cost of cybercrime damages worldwide by 20251



Cyberattacks and data breaches continue to increase exponentially²

\$4.45 million

Global average cost of a data breach

as of 20233

Many businesses never recover from the fallout

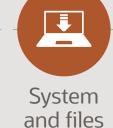
are on the rise⁴

Ransomware attacks









restoration





damage



and employee trust

Don't be fooled by third-party support providers and self-maintenance security methods There's no patching

in "virtual patching" Virtual patching is a workaround that doesn't actually patch or update your software.

▶ Temporary solution Neglects root problem

- Ignores full scope of vulnerabilities

"It is necessary for all organizations to establish a strong ongoing patch management process to ensure the

Security

U.S. Department of Homeland

proper preventive measures are taken against potential threats." https://www.cisa.gov/

Perimeter-focused security strategies leave your software open to attack.

Susceptible to internal breaches

Firewalls aren't fireproof

Minimal visibility into network threats Ignores actual security in the software

- **E.U. General Data Protection Regulation** A single set of rules to enhance data privacy and guarantee the security of personal data and data processing.

Applies to any organization handling EU citizen data

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

Enforceable May 25, 2018 Noncompliance or violation can lead to heavy fines

/eu-data-protection-rules_en

Powerless to (legally) fix vulnerabilities Unable to access new patches and updates Limited resources to reliably maintain and secure

Self-maintenance = potential liability

Doing it yourself cuts your software off from critical security updates.

The Bottom Line Security patching is

business open to risk. Oracle Support is the only way to guarantee mission-critical security updates and protection for your Oracle software.

essential for securing

including Oracle's. If you

don't own the code, you

can't access or update it.

open to attack and your

That leaves your software

enterprise software,

Third-party support

Self-maintenance

Inadequate security

► Inadequate security

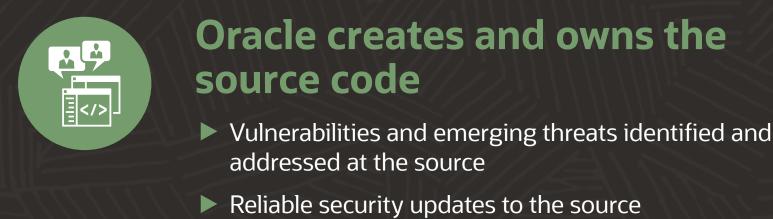
▶ Inadequate protection

against vulnerabilities

updates

fixes

Only Oracle Can Secure Oracle Software



Oracle creates and owns the

Oracle provides security at

Oracle has the tools, experience,

Patches at every layer of the software stack Regression testing across the full stack



and knowledge Proactive change management processes

- Uniform release management process Dependable, ongoing, and unparalleled innovation

Get more from Oracle.

every level

When your business is on the line, there's no substitute for trusted, secure, and

Visit Oracle Premier Support

Sources:

comprehensive support.

- 1. https://cybersecurityventures.com/cybercrime-to-cost-the-world-9-trillion-annually-in-2024/
- 2. https://www.securitymagazine.com/articles/100335-cyberattack-attempts-increased-104-in-2023 3. https://securityintelligence.com/posts/whats-new-2023-cost-of-a-data-breach-report/ 4. https://www.infosecurity-magazine.com/news/ransomware-attacks-skyrocket-q2/

or its affiliates. Other names may be trademarks of their respective owners. Version 1.03

Copyright © 2024 Oracle and/or its affiliates. Oracle, Java, and MySQL are registered trademarks of Oracle and/