ORACLE

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

$6 trillion

The estimated annual cost of cybercrime damages worldwide by 2021[1]

65% of organizations
say their in-house security capabilities are adequate[2]

Yet **80%** have been negatively
affected by a cybersecurity attack in the past year[2]

+82,000 cybercrime incidents estimated globally in 2016[3]

- **+250,000** including unreported incidents[3]
- **4,149** confirmed data breaches[4]
- **4.2 billion** records exposed[4]

The average cost of a data breach in 2016 was **$3.6 million**[5]

Many businesses never recover from the fallout

- Sensitive, proprietary information
- Operational disruption
- System and files restoration
- Fines and litigation
- Reputation and brand damage
- Customer and employee trust

Don't be fooled by third-party support providers and self-maintenance security methods

1 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

U.S. Department of Homeland Security

"It is necessary for all organizations to establish a strong ongoing patch management process to ensure the proper preventive measures are taken against potential threats."

www.dhs.gov/cybersecurity

2 "Holistic security" isn't whole; firewalls aren't fireproof

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

- Susceptible to internal breaches
- 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
- Enforceable May 25, 2018
- Noncompliance or violation can lead to heavy fines

www.eugdpr.org

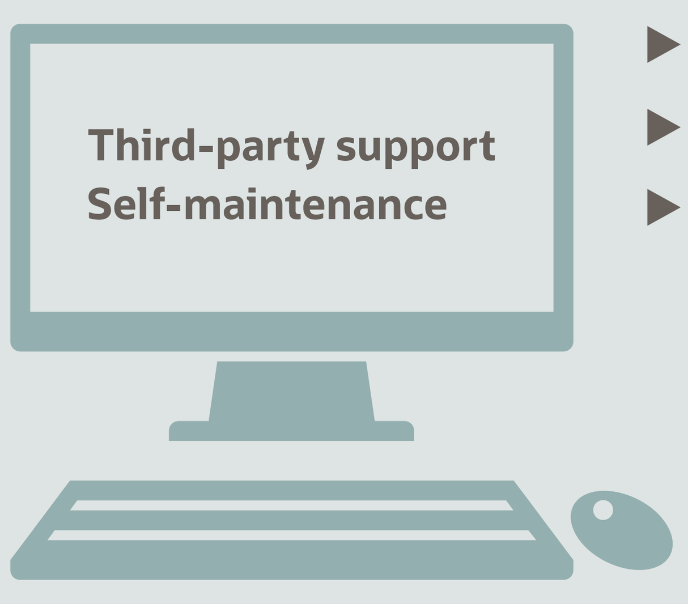
3 Self-maintenance = potential liability

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

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

The Bottom Line

Security patching is essential for securing enterprise software, including Oracle's. If you don't own the code, you can't access or update it. That leaves your software open to attack and your business open to risk.



- No security updates
- No security fixes
- No elimination of vulnerabilities

Only Oracle Can Secure Oracle Software

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

Oracle creates and owns the source code

- Vulnerabilities and emerging threats identified and addressed at the source
- Reliable security updates to the source

Oracle provides security at every level

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

Oracle has the tools, experience, and knowledge

- Proactive change management processes
- Uniform release management process
- Dependable, ongoing, and unparalleled innovation

Get more from Oracle.

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

Visit Oracle Premier Support

Sources:
1. https://cybersecurityventures.com/hackerpocalypse-cybercrime-report-2016/
2. https://www.business.att.com/cybersecurity/docs/vol4-threatlandscape.pdf
3. https://www.accenture.com/t20171006T095146Z__w__/us-en/_acnmedia/PDF-62/Accenture-2017CostCybercrime-US-FINAL.pdf#zoom=50
4. https://www.justice.gov/criminal-ccips/file/872771/download
5. https://otalliance.org/system/files/files/initiative/documents/2017_cyber_incident_breach_response_guide.pdf