

Software Patching Is Critical to Stay Secure: Are You Prepared?

Is your security strategy secure and comprehensive? Don't risk it.

"Oracle Support provides levels of capability and security that are far above offerings from third-party, non-Oracle software support vendors." ¹

Why Patching?

Global technology research firm Omdia's most recent annual survey identified **managing security, identity, and privacy** as the most important top-three trends.

Failure to perform proper software patching and maintenance puts your company's bottom line and reputation at risk.

Threats you may face:



Theft



Financial Loss



Damaged Brand Reputation



Fraud



Fines

Patching is a key measure for your proactive protection strategy and critical to all good IT security governance. Ensuring regular software patching and maintenance is imperative for every enterprise.

"Timely application of vendor software patches is the indispensable foundation of avoiding the risk arising from the presence of unmitigated security vulnerabilities." ²

Benefits of Patching

There are plenty of reasons to regularly patch your software. Oracle believes that these two are critical:

- 1. To maintain strong software security:**
A rigorous software security and maintenance program requires ongoing vigilance and upkeep.
- 2. To meet IT governance and compliance needs:**
A strong foundation and culture of compliance cannot exist without regular software patching and maintenance services.

"[Keeping your] estate up to date with vendor-supplied patches is the primary and timeliest means of protecting against software-related threats." ³

The Federal Trade Commission (FTC) recommends updating and patching third-party software, heeding any security warnings from vendors and addressing them immediately.



How Do You Incorporate a Software Patching Strategy?

These are the patching guidelines that lead to **stronger security**:

- 1. Foster a culture change** to ensure patching is considered an essential element of organizational well-being.
- 2. Prioritize patches based on business and technical risk.**
- 3. Commit to execute patching as a key part of your regular security maintenance.**
- 4. To avoid risk, only patch with your software vendor.**

"Companies should be working closely with their software vendors, because they have the most experience and expertise when it comes to patching, supporting, and securing their own products." ⁴



Why is a Trusted Partner Crucial?

Companies must partner with a trusted provider to put procedures in place to keep their **software security current** and address **potential vulnerabilities**.

There are **three characteristics** that help you identify a trusted partner, like Oracle.

- | | | |
|--|---|--|
| <p>Trusted ✓</p> <p>Possesses knowledge and expertise in securing data in an enterprise IT environment.</p> <p>Has long term experience handling enterprise-class security and support.</p> | <p>Secure ✓</p> <p>Is experienced in securing the entire IT stack.</p> <p>Is an expert in providing proactive and real-time support resources.</p> | <p>Comprehensive ✓</p> <p>Provides a full, integrated suite of security and support offerings that's constantly evolving and improving.</p> <p>Is able to help you establish a culture focused on IT security and compliance.</p> |
|--|---|--|

What Are You Missing with Third-Party Support?



1. Security fixes:

Third-party vendors cannot provide key security fixes because:

- They cannot alter portions of Oracle's source code.**
- They are unfamiliar with the technical details of the vulnerabilities that Oracle fixes.**



2. Ongoing security assurance efforts:

Oracle Support customers benefit from Oracle's security assurance efforts in ways third-party support customers do not because:

- Previous fixes and patches are incorporated into each subsequent Oracle software release.**

"Therefore, a considerable level of care is important when relying on any third-party services relationship for provision of software support. Inadequate definition of requirements could allow a service provider to get away with implementing "workarounds" as partial solutions to vulnerabilities to close down ticketed support requirements." ⁵

The Bottom Line

Security software patching is essential to secure enterprise software, including Oracle's. **If you don't have sufficient rights to the code, you can't access or update it.** This leaves your software exposed to attacks and your business open to risk.

Third-party support and self-maintenance mean:

- ✗ Inadequate security updates**
- ✗ Inadequate security fixes**
- ✗ Inadequate elimination of vulnerabilities**

Get Strong Security with Oracle

Ensure mission-critical security updates and protection for your Oracle software, while satisfying IT governance and compliance needs. With Oracle, you get:

- A regular patching schedule** and a strong emphasis on IT security company-wide that provides assurance that its systems are less vulnerable and more secure.
- Reliable security updates** to the source.
- Proactive change management** processes.

[Read the full Omdia Report](#)

[Visit Oracle Premier Support](#)

¹⁻⁵ Omdia. (2023). Sustainable Software Patching: Critical for Solid Security, Reduced Risk, and Meeting Compliance Challenges.

