ORACLE

# Don’t Put Your Business at Risk

## Importance of Software Security Awareness

Oracle firmly believes the software you use to run your enterprise needs to be trusted, secure and comprehensive.

Recently, Rimini Street announced yet another inadequate approach to real-world security challenges. The notion of “holistic security” and “virtual patching” offered by Rimini Street as a solution to protect Oracle systems from vulnerabilities is ridiculous, and will put your business at risk. Oracle believes that neither holistic security nor virtual patching is sufficient to protect your Oracle systems from intrusion in an interconnected network, as neither approach includes security updates that modify the relevant Oracle source code. Only Oracle can provide security at every layer in our software stack because we can modify our source code to deliver updates that address vulnerabilities posed by emerging threats.

In fact, secure software does not happen by itself. Security is a process that requires the continued engagement of development and support organizations. Encompassing every phase of the product development lifecycle, Oracle Software Security Assurance (OSSA) is Oracle’s methodology for building security into the design, build, testing, and maintenance of its products. Oracle’s goal is to ensure that Oracle’s products are helping customers meet their security requirements while providing for the most cost-effective ownership experience.

Oracle Software Security Assurance is a set of industry-leading standards, technologies, and practices aimed at:

### FOSTERING SECURITY INNOVATIONS

Oracle has a long tradition of security innovations. Today this legacy continues with solutions that help enable organizations to implement and manage consistent security policies across the hybrid cloud data center: database security and identity management, and security monitoring and analytics.

### REDUCING THE INCIDENCE OF SECURITY WEAKNESSES IN ALL ORACLE PRODUCTS

Oracle Software Security Assurance key programs include Oracle’s Secure Coding Standards, mandatory security training for development, the cultivation of security leaders within development groups, and the use of automated analysis and testing tools.

## REDUCING THE IMPACT OF SECURITY WEAKNESSES IN RELEASED PRODUCTS ON CUSTOMERS

Oracle has adopted transparent security vulnerability disclosure and remediation policies. The company is committed to delivering the best possible security patching experience through the Critical Patch Update and Security Alert programs.

In summary, there is no substitute for patches that modify code and protect systems from vulnerabilities. There is also no substitute for proactive change management processes. Combining the two together in a consistent release management process is the best way to achieve the levels of security our customers require to protect their systems and data. And in an environment where there is increasing threat posed by hackers, the increasing liability for security breaches, and the increasing interest of government regulators concerning data security, Oracle believes that you are taking a grave risk if you don't take the right steps.

Oracle believes that there is no real dispute that the best way to correct an identified vulnerability within the source code is with a patch provided by the software vendor. The fact remains, only Oracle can do this for Oracle software.

Visit our website for more on Rimini Street and how Oracle trusted support can protect your software from real-world security challenges.


CONNECT WITH US

Call +1.800.ORACLE1 or visit oracle.com.
Outside North America, find your local office at oracle.com/contact.

blogs.oracle.com facebook.com/oracle twitter.com/oracle