SOLUTION BRIEF

SPINNAKER SUPPORT

Software Publisher Patches vs. Spinnaker Support Security

A Comparison of Two Approaches to Reducing Your Security Risk

SOFTWARE PUBLISHER PATCHING

Software patches are code changes for software designed to eliminate bugs, fix security vulnerabilities, and improve the usability or performance. Included as part of paid maintenance, patches are used as an incentive to retain the support services of the software publishers. SAP is a notable exception, as it provides security patches (but not update/enhancement patches) to all customers irrespective of support status.

Most publishers package multiple fixes and release these as downloads on an established schedule, with an occasional one-off alert. Because patches help remedy unexpected code issues, publisher support is a worthwhile investment for newer software products and versions. For risk and vulnerability management, however, the benefits of patching are more open to question, even while the publisher extensively promotes them as the primary security solution.

THE SHORTCOMINGS OF PUBLISHER PATCHES FOR SECURITY

For years, publisher patches were the only a practical method available for managing code-based vulnerabilities. As the volume and variety of threats and vulnerabilities has grown, research has found that a reliance on patching alone often falls short of its promise as a wholesale security solution[1]. This is because:

- Patches are not timely (there can be a time lag of months or years between disclosure and patch).
- Patches don't address zero-day vulnerabilities.
- Patches are one-size-fits-all and may be problematic for customizations.
- Patches may not be available for older product versions and applications.
- Patches require valuable time to test and install.
- Many organizations do not patch regularly or patch at all due to operational constraints.

As to timeliness and quality of patches, a recent, large-scale empirical study from the University of California, Berkeley uncovered some disquieting statistics: A third of all security issues were announced more than three years prior to remediation, nearly 5% of security fixes negatively impacted the associated software, and 7% failed to completely remedy the security hole they targeted[2].

In several research papers, Gartner has recommended against relying on patches alone to address critical vulnerabilities and exposures (CVEs). They state that "security and risk management leaders need to broaden their threat and vulnerability management strategies to apply alternate risk mitigation measures to critical systems and applications that cannot be patched.[3]" Many industry regulations, certifications, or compliance standards have also been updated with appendices that allow for compensating security controls when patches are nonexistent or unavailable.

SPINNAKER SUPPORT'S ANSWER TO PATCHING

When organizations consider switching from publisher to third-party software support, it's common for them to have questions regarding patching and security risk. Despite the real limitations described above, Oracle customers, in particular, may be apprehensive about the loss of quarterly security patches.

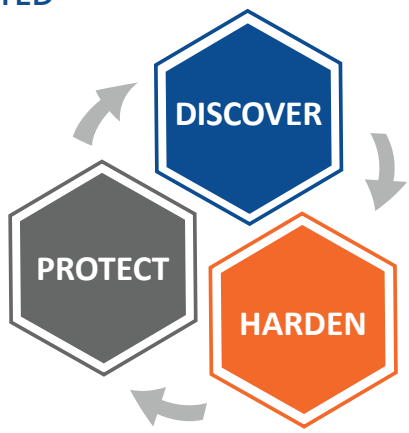
Spinnaker Support addresses those concerns with a Seven-Point Security Solution that is standard for all support customers and exceeds the performance of patches alone as a CVE solution. From Day 1, we offer a multilayered approach to replace security patches and updates, including:

1. **Preparing new customers with a custom risk review and assistance with attack surface reduction**, which helps customers to properly configure and harden applications, operating systems, servers, databases and networks.
2. **Delivering virtual patching and IDS/IPS products from industry leading security vendors.** This not only responds far more quickly than traditional publisher patches to overt or suspected attacks but also helps maintain compliance with laws, statutes, and governance policies like HIPAA and PCI DSS.
3. **Providing responsive and ongoing vulnerability management that's tailored to each customer's needs, delivered when they need it.** We prioritize security-related support tickets and bring our global team of security experts in to the conversation from the start.

Spinnaker Support's security framework addresses vulnerability management for the entire technical stack, replacing the need for general patching with a targeted toolset of security processes and products. This can include Database Defender, Spinnaker Support's virtual patching tool for databases, powered by McAfee.

SPINNAKER SUPPORT HAS YOU PROTECTED

Spinnaker Support takes your data and application security seriously. In our 2019 Satisfaction Survey, **98% of customers who cited security as an issue reported that their security level was improved or unchanged after moving to Spinnaker Support.**



We achieve these results because we reject the one-size-fits-all patching approach, focusing instead on working collaboratively with each customer.

Our global security team monitors and reports on actionable vulnerabilities and actively advises on security concerns. From Day 1, they adhere to the core concepts of discover, harden, and protect for your data and critical system security. They treat every reported incident as a P1 ticket, respond within 15 minutes, and continue to work until the security issue is properly addressed.

[1,3] Claudio Neiva, Adam Hils and Prateek Bhajanka. "When You Can't Patch It, Protect It From the Network," https://www.gartner.com/document/3507617?ref=solrAll&refval= 220253506&qid=386beb2cde3caa5aff4dcfc8

[2] Frank Li and Vern Paxson. "A Large-Scale Empirical Study of Security Patches." 24th ACM Conference on Computer and Communications Security, https://acmccs.github.io/papers/p2201-liA.pdf

SECURITY IS IN EVERYTHING WE DO

We invest in your security and compliance measures with the same exacting standards we apply to our own. Spinnaker Support was the first third-party support provider to achieve both ISO/IEC 27001:2013 certification for managing sensitive company information and ISO 9001:2015 certification for quality management principles. We are Privacy Shield-certified, GDPR compliant, certified for both the EU-U.S. and Swiss-U.S. Privacy Shield Frameworks, and Cyber Essentials certified.

Spinnaker Support delivers security solutions designed for your unique set of applications and systems. Combining proven processes, security products, and a staff of industry experts, Spinnaker Support continuously investigates issues and hardens and protects your application environment, delivering timely fixes and remediations throughout your customer experience.

Have specific concerns or security requirements? Contact us today to discuss to see how we can apply our security framework and solution to support your unique needs.

ABOUT US

Spinnaker Support is a leading and trusted global provider of Oracle and SAP third-party support. Spinnaker Support customers get more comprehensive and responsive service, save an average of 62% on their annual maintenance fees, and can remain on their current software releases indefinitely. We remain the only third-party support vendor to deliver application managed services, technology managed services, and consulting when customers prefer to consolidate with a single vendor. Spinnaker Support's award-winning blend of services span SAP, BusinessObjects, Sybase, Oracle E-Business Suite, JD Edwards, Siebel, Oracle Database, Oracle Technology and Middleware products, Hyperion, and more.

SPINNAKER SUPPORT

SPINNAKERSUPPORT.COM