SPINNAKER SUPPORT

Software Publisher Patches vs. Spinnaker Shield

SOFTWARE PUBLISHER PATCHING

Software patches are code changes for software that are designed to eliminate bugs, fix security vulnerabilities, and improve usability or performance. Software publishers include patches as part of their paid maintenance to ensure their clients continue relying on their support services. SAP is a notable exception, as it provides security patches to all customers, irrespective of support status.

Most publishers package multiple fixes and release them 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 managemente, however, the benefits of patching are more open to question, even while the publisher extensively promotes them as the ideal security solution.

THE SHORTCOMINGS OF PUBLISHER PATCHES FOR SECURITY

For years, publisher patches were the only 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 to be a wholesale scurity solution. [1]This is because:

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

As for the timeliness and quality of patches, a recent large-scale empirical study from UC 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 of their 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 limitations described above, customers may be apprehensive about the loss of quarterly security patches.

Spinnaker Support addresses those concerns with our standard Spinnaker Shield Solution, which exceeds the performances of patches as a CVE solution. From day one of the customer experience we use a multilayered approach to replace security patches and updates, including:

Preparing new customers for an upgraded security posture by conducting custom risk review and implementing attack surface reduction - both of which help customers to properly configure and harden applications, operating systems, servers, databases, and networks.

Virtual Patching not only responds far more quickly to overt or suspected attacks than traditional publisher patches, but it also helps maintain compliance with laws, statutes, and governance policies (like HIPAA and PCI DSS).

Providing responsive and ongoing vulnerability management that's tailored to reach customer's needs and delivered when they need it. We prioritize security-related support tickets and bring our global team of security experts into the conversation from the start.

SECURITY IS A STANDARD

We invest in your security and compliance measures with the same exacting standards we apply to our own organization. Spinnaker Support has achieved both ISO / IEC 27001:2013 certification for managing sensitive company information and ISO 9001:2015 certification for quality managemente 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. Armed with proven processes, tried-and-true security solutions, and a robust staff of industry experts, Spinnaker Support continually investigates issues and hardens and protects your application environment, delivering timely fixes and remediations throughout your customer experience.

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

For more information on Spinnaker Shield, please contact us at **spinnakersupport.com**

ABOUT US

Today's leaders are navigating an increasingly uncertain and ever-changing world. They can't be held back by restrictive, ineffective, or complicated software systems as they move their organizations forward. Spinnaker optimizes software ecosystems through services designed for sustainable transformation, maximizing software investments and freeing up the capital and resources leaders need to navigate the future with certainty.