SPINNAKER SUPPORT

Maximizing Security with Third-Party Support

PATCHES ARE NO LONGER A SUFFICIENT SECURITY SOLUTION

As the threat landscape continues to evolve and tens of thousands of security vulnerabilities are published each year, businesses look to their enterprise application providers to keep their systems safe from malicious actors. However, the traditional approach of patching that is employed by these vendors turns out not to be the most effective security strategy.

PATCHES ARE SLOW AND REACTIVE

Patches take months or even years in some cases to be issued, leaving businesses vulnerable to breaches. This is particularly problematic for zero-day vulnerabilities, which are vulnerabilities that have been announced publicly before a patch is available.

Vendors take an average of 52 days to fix security vulnerabilities. (**source**)

PATCHES ARE ONE-SIZE-FITS-ALL

Patches are typically issued for only recent software versions, and are designed to work for standard code, not customizations. Businesses running legacy versions or heavily customized solutions may not have access to usable patches.

89% of organizations have modified at least some of their ERP code. (**source**)

PATCHES ARE TIME AND RESOURCE INTENSIVE

Patches can take months to test and implement, posing a significant challenge for resource-constrained IT teams who want to spend their time on strategic technology initiatives.

62% of organizations say patching takes a back seat to other priorities. (**source**)

CVE PUBLISHED

PERFORM ANALYSIS

ORACLE

**this occurs over extended period*

Review all products / versions

Create product patches

User must check for patches

THIRD-PARTY SUPPORT OFFERS PROACTIVE SECURITY

Organizations may consider third-party support for a number of reasons, such as extending the life of their enterprise software investments, maintaining customized software, supplementing constrained internal resources, or simply wanting more responsive and consistent support for a lower cost. But these organizations often question whether a third-party support provider can deliver adequate security and vulnerability protection.

Fortunately, many of the reasons organizations may consider third-party support in the first place are exactly the same reasons that patching isn't the best security approach for them!

Third-party support providers employ proactive risk mitigation strategies to supplement an organization's internal security policies and processes. Instead of waiting for vendor patches, your third-party support provider will work with you from day one to harden your system before vulnerabilities are ever discovered.

AN IDEAL SOLUTION FOR LEGACY AND CUSTOM ENVIRONMENTS

Organizations running legacy software versions or heavily customized solutions are perfect candidates for the proactive security offered by third-party support providers. As described above, these organizations often struggle to implement vendor patches as the vendor may not even have product patches for legacy version, leaving them vulnerable to malicious actors. Third-party support provides security that is tailored to the individual customer, even if they're on an unsupported software version or have customized every line of code.

SPINNAKER SUPPORT SECURITY PHILOSOPHY

Spinnaker Support takes a customer-focused approach to security that is designed to proactively identify risks and harden your system from day one. The result is a security posture that is stronger and more responsive than traditional patching.

PROACTIVE

Spinnaker Support focuses on weaknesses category, not always individual vulnerabilities. By focusing on the weakness category the customer can be protected from all current and future vulnerabilities that fall within that category.

At the beginning of our engagement, we conduct a custom risk review and implement attack surface reduction measures that improve your security posture. When a vulnerability is detected and the vendor issues a patch, it is likely that your system is already protected and no additional measures are needed.

PERSONALIZED

Every customer has unique security needs depending on their software version, customizations, and data privacy requirements. We tailor our security services for your needs so we can deliver precisely the solutions you require, on your timeline, and customized to strengthen your bespoke environment.

98% of customers rated Spinnaker Support's security and vulnerability protection as good or better than that delivered by the publisher

FULL-STACK SECURITY AND VULNERABILITY PROTECTION FROM SPINNAKER SUPPORT

Spinnaker Support offers a Defense-in-Depth (DiD) security solution designed for the ongoing protection of your middleware, database, and application. DiD leverages a series of defensive tactics applied across multiple layers so if one mechanism fails, other mechanisms are there to serve as backup protection.

Our security approach has three pillars: Discover & Harden, Incident Response, and Threat Intelligence. A dedicated team coordinates your personalized security services across these pillars to deliver comprehensive protection and business continuity.

DISCOVER & HARDEN

- **SECURITY ASSESSMENTS** - We perform security assessments based on global standards to identify weaknesses in your system and provide guidance on how to harden and configure your system to achieve desired benchmarks, which reduces attack vectors bad actors use to compromise your system.

- **AUDIT COMPLIANCE** - We run audit compliance checks to help you adjust your audit controls to be compliant with standards and frameworks including HIPAA, GDPR, SOC2, and PCI.

INCIDENT RESPONSE

- **CUSTOMIZED SECURITY SUPPORT** - We provide customized security support so you can submit a ticket any time to receive help from our security staff who can provide relevant information and mitigation strategies. We provide SLAs in line with your break/fix agreements.

THREAT INTELLIGENCE

- **SECURITY TOOLS** - We provide a suite of security tools for your full software stack through partnerships with Waratek, Trellix - McAfee Enterprise, and Trend Micro.

- **SECURITY BULLETINS** - We monitor Oracle CVEs and publish regular email bulletins for customers. These include CVE descriptions and best practice recommendations.

SECURITY IS IN OUR DNA

Security is integral to our operations, and this philosophy and legacy is embedded in how we support our customers. We deliver security solutions designed for unique sets of applications and systems, and we invest in our customers' security and compliance measures with the same exacting standards that we apply to our own operations.

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.

NOT ALL THIRD-PARTY SUPPORT PROVIDERS ARE EQUAL

While any third-party support provider can enhance your security posture, they don't all approach security in the same way. Ask your provider these questions to assess the strength of their security services:

1. **Do you leverage industry standards?** Your third-party support provider should perform a risk assessment and deliver tools and strategies aligned with CIS benchmarks, which are consensus-based and accepted across governments, industry, and academia as an industry standard way to measure security effectiveness.

2. **Will I have an assigned support engineer?** When a weakness or vulnerability is discovered, you need to trust that your provider will resolve it quickly. It is crucial that your third-party support team is responsive and communicative, and that you have a dedicated resource you can call for an update rather than a revolving door of offshore engineers.

3. **What security services are included at no extra cost?** While there may be some advanced strategies and tools worth paying extra for, basic security should not be an add-on or upsell. Look for a comprehensive array of services and tools as part of the standard security package included with your third party support.