SPINNAKER SUPPORT

Third-Party Support and Information Security

Business Challenges

Security is usually a hot topic for those who are considering a switch to third-party SAP or Oracle support. Organizations that utilize software vendors for software support feel they might be exposed from a security perspective should they transition to Spinnaker Support. Prospective clients often question us regarding vulnerability and patch management. They want to understand how we proactively alert our clients when new vulnerabilities are detected. While we can challenge the assumption that there's a critical exposure here, this is a valid concern that we can address.

Spinnaker Support Solution

Points to consider regarding Spinnaker Support's approach to security:

- We have built a global security monitoring and advisory team to help our customers maintain more secure application environments. This growing team monitors and reports actionable security vulnerabilities and develops resolutions when required. We work with these systems all day, every day, in over 100 countries. We hire the best of the best for our team. We have built a unique ability to monitor and report on security issues, often before software vendors "approve" them as vulnerabilities.

- Spinnaker Support has access to the same public vulnerability databases as Oracle, SAP, and other vendors. We use these databases to drive our security alerting process.

- Spinnaker Support has a legal team of experts monitoring and accessing the very same security vulnerability information that Oracle, SAP, and other vendors utilize to provide security alerts to clients.

- As part of our standard support contract, we allow our customers to log security related concerns for issue resolution and advisory guidance. This cross-pollinates our substantial security knowledgebase. We leverage this cross pollination to alert our other clients when a security ticket becomes more than a specific client related issue.

- Our security experts become an extension of our client's team of security professionals. While security teams of the software vendors can act as unique and disparate functions within their own companies, our security support team works closely as an integrated part of our client's security and support teams. Engaging us is partnering with us.

Security Guidelines

Compliance is just another risk we need to manage and knowing the landscape of security compliance can help us make better decisions on how and when to address its risks. When we look at the ERP landscape and challenges our clients face in the realm of security, there are a few basic guidelines that we always bear in mind:

1. If it ain't broke, don't fix it: ERP managers invest a lot of time and effort to get their systems functioning per their organizational needs. A top concern is the stability of the system, stability that, in their mind, can be at risk upon implementation of new security fixes.

2. Patches are not always a solution: Patches are simply patches. Patching a system is important but it is far from being a structured, well designed and long lasting solution. It is what it is, a patch. Patches are one-off solutions that, in the eyes of an ERP manager or Database Administrator, can potentially open a can of worms for which they didn't prepare.

3. Not all patches are relevant: When vendors such as Oracle and SAP communicate a patch package it can feel like there's no other viable alternative but to follow the herd and apply the patch. Not quite true. Not all patches are relevant to all clients. Companies use different versions, different modules, and even different implementation methodologies for the same version of ERP

Where Security Meets Third-Party Support

Industry Examples:

For security compliance, Spinnaker Support is addressing a range of challenges related to specific industry standards, such as the Payment Card Industry Data Security Standard (PCI DSS). PCI is one of the more technically-driven security standards in the credit card industry. Year after year and with every new revision that comes out, we see PCI incorporating more technical requirements from organizations that work in this industry. We help clients regarding their PCI compliance efforts. We address these issues the way any compliance issue should be addressed – as a risk. Risks need to be managed.

To clarify, our clients that run SAP applications do not lose their ability to access SAP security patches when they transition to Spinnaker Support. However, our clients that run Oracle applications do lose their ability to access Oracle security patches upon leaving Oracle-provided support. Thus, we become the go- to vendor for security advice and patches on the Oracle front and a supplemental avenue on the SAP front.

We often recommend using existing PCI controls as a set of compensating controls. Recurring activities such as quarterly vulnerability scans, semi-annual penetration tests, and other security audit and monitoring controls gives the organization the capability to address those known vulnerabilities with a much more thorough approach. Compensating controls are, as they should be, more than a tick in a box. Spinnaker Support is able to resolve customer issues in a timely manner by introducing our different approach, developed specifically for each customer.

HIPAA is another standard that we team with customers to address. For example, a regulated Biotech company in the healthcare industry developed an amazing technology to enhance in-home patient care. This technology allows remote treatment for the patient from anywhere at any time. The patient never has to leave the house. This was a significant breakthrough and subsequently became the next big thing in the industry. However, before our involvement, the biotech firm had failed to sufficiently address the fact that protected health information (PHI) must be collected and stored throughout the system. To comply with HIPAA requirements, the company had to shut down its production line for 3 months.

Here, just like in the PCI scenario, an out of the box approach was needed, and we developed a way for this customer to resume production, while satisfying all HIPAA requirements for security. We started by implementing encrypted data in transit. This stopped the bleeding. Next we identified and enhanced existing security controls we could immediately work within the environment, providing layered security that decreased risk to an acceptable level. We then worked with our customer to develop and execute a roadmap that eventually reduced risks to an even lower level, while satisfying all HIPAA requirements.

Spinnaker Support is a world leader for third-party support security management. We deliver tremendous value to clients by addressing security as a unique solution to a specific need rather than a universal patch or a package. We see a great opportunity to help our clients expand their approach to gain truly effective ERP security.

About Us

Spinnaker Support is the leading global provider of third-party support and managed services for Oracle and SAP enterprise software products. Spinnaker Support clients gain more comprehensive and responsive service, save an average of 62% on their support fees, and can remain on their current software release indefinitely. They trust Spinnaker Support to keep their enterprise applications running at peak performance and to help them navigate from on-premise to hybrid to cloud.

Spinnaker Support operates from ten regional operational centers located in Denver, Dubai, London, Mumbai, Paris, Sao Paulo, Singapore, Seoul, Tel Aviv, and Tokyo. Our award-winning blend of services span SAP, BusinessObjects, Oracle E-Business Suite, JD Edwards, Siebel, Oracle Database, Oracle Technology and Middleware products, Hyperion, Agile PLM, ATG/Endeca, and more.

SPINNAKER SUPPORT

SPINNAKERSUPPORT.COM