SPINNAKER SUPPORT

Security

TABLE OF CONTENTS

Executive Summary 3

Security Comes Standard with Third-Party Support 4

Two-Fold Security Philosophy 5

Seven-Point Security Solution 6

Discover and Harden, Incident Response, and Threat Intelligence 7

Proactive Security Tooling 8

Seven-Point Security vs. Software Publisher Patches 9

Spinnaker Support compared to Oracle, SAP, and 3PS Providers 10

Examples of Security Issues 11

Holistic Security Approach 13

Glossary 14

As the rate of ransomware attacks continue to rise and new attack vectors open as technology ecosystem trend towards increasing interoperability and cloud migration, organizations are finding it difficult to keep up with evolving security needs. Spinnaker Support brings a holistic approach to security through a broad defense in depth approach that aligns with industry standards and frameworks. Understanding the threat of CVEs (Common Vulnerabilities and Exposures) to client's ecosystem, our vulnerability management utilizes best-in-class compensating controls to properly mitigate risk without waiting for a patch. We will continually investigate issues and harden your system to better protect your application environments while delivering timely fixes and remediations.

Our global security team monitors and reports actionable vulnerabilities and actively advises on security concerns. When it comes to your data and critical systems, we adhere to the core concepts of "discover, harden, and protect."

SECURITY COMES STANDARD WITH THIRD-PARTY SUPPORT

BREAK/FIX

GLOBAL TAX, REGULATORY AND COMPLIANCE (GTRC)

GENERAL INQUIRY

SECURITY AND VULNERABILITY MANAGEMENT

TECHNOLOGY ADVISOR SERVICES

ARCHIVING SERVICES

Our comprehensive third-party support (3PS) covers everything from software errors to general product questions to technology advice. Security is an integral part of our organization from our support offerings to managed services and consulting. Our security services for third-party support focuses on our seven-point security solution we have tailored specifically for this type of support. We focus on the core concepts of discover, harden, incident response, and threat intelligence to protect your data and critical systems.

We treat every reported security incident as a P1 ticket, responding within 15 minutes, and continuing to work until the risk has been properly addressed. One weak point is all it takes for a threat actor to get into your system.

98.1%

According to a recent customer satisfaction survey, 98.1% of customers reported **higher satisfaction** after moving to Spinnaker Support's third party software services.

TWO-FOLD SECURITY PHILOSOPHY

WE DELIVER A LAYERED, DEFENSE IN DEPTH APPROACH

1

Our security specialists target the weakness category, or common weakness enumeration (CWE), providing layered system protection. Vendor Patches focus on addressing each published CVE by individual product.

Security vulnerabilities in products often go unannounced and patches are often not released for extended periods of time.

(e.g., Oracle Patches 3-Year-Old Java Deserialization Flaw in April Update (eweek, April 2019)).

FUTURE PROOF YOUR ENVIRONMENT

2

Our team will provide you with a system analysis, based on DISA-STIG and CIS standards and benchmarks. Based on the analysis, we'll deliver tailored hardening techniques and compensating controls to ensure that your systems can pass penetration testing and auditing.

SEVEN-POINT SECURITY SOLUTION

DISCOVER AND HARDEN

1 | CUSTOM RISK REVIEW

We conduct a risk assessment on your systems, providing reports with recommendations on configurations, encryption, access management, best practices, and guidelines. This gives a top-level view of your current attack surface.

2 | ATTACK SURFACE REDUCTION

Our specialist advises on where the attack surface can be reduced at a user, data, and application level, leaving attackers with fewer ways to exploit known vulnerabilities.

3 | COMPLIANCE AUDIT SUPPORT

Consultative services designed to adjust your audit controls, to comply with attestations such as SOC2, HIPAA, GDPR, and PCI.

INCIDENT RESPONSE

4 | VULNERABILITY SUPPORT

We deploy compensating controls (external to application code) to mitigate your security risk. Submit a ticket at any time for security-related issues.

5 | SECURITY RESOURCE LIBRARY

Includes white papers, blogs, and solutions briefs on a wide range of topics on security.

THREAT INTELLIGENCE

6 | PROACTIVE SECURITY TOOLING

A portfolio of security products designed to implement our holistic philosophy on security.

7 | RISK ASSESSMENT BULLETIN

We monitor a variety of source for new vulnerabilities of supported systems, then publish periodic email bulletins and alerts to customers with best practice recommendation to address these potential threats.

DISCOVER AND HARDEN, INCIDENT RESPONSE, AND THREAT INTELLIGENCE

DISCOVER AND HARDEN

One of our top priorities is to help future-proof your security for the technology environment we help support. When a customer partners with us for the first time or adds additional systems and/or applications to their support contract, we have the capability to perform custom risk assessments on your system to review possible vulnerabilities and weaknesses.

Utilizing the reported results, which includes recommendations for hardening your systems against potential attacks. Spinnaker Support can also advise on helping implement the necessary changes to your environment.

INCIDENT RESPONSE

Whether you have been breached or are concerned over a possible vulnerability, the solution begins with submitting a support ticket. We're always available to assess and discuss security issues, and we've developed a deep library of white papers, solution briefs, and blogs for our clients.

Since we focus on categories of weakness rather than individual common vulnerabilities and exposures, we can often supply a solution that also protects against similar known, or yet undetected, vulnerabilities.

THREAT INTELLIGENCE

Spinnaker Support continually monitors a variety of sources for new vulnerabilities and exposures. Some of these vulnerabilities are critical enough to merit widespread attention. We publish periodic bulletins and alerts, depending on the CVE and its impact to a client's systems.

PROACTIVE SECURITY TOOLING

MIDDLEWARE

Waratek monitors and protects the application at the Java virtual-machine level.

The Waratek “Java agent” is a specially crafted jar file. It uses the instrumentation API that the JVM provides to alter existing bytecode that’s loaded in a JVM.

Waratek’s surveillance is performed on all-Java code within the just-on-time compiler inside the runtime. This enables Waratek to help mitigate attacks such as cross-site request forgery, deserialization, HTTP open redirects, session fixation, libraries loaded from untrusted sources, cross-site scripting, and WebSocket vulnerabilities.

DATABASES

Database Defender, powered by Trellix, is our virtual patching solution. Database Defender detects and prevents attempted attacks and intrusions in real time, shielding databases from the risks presented by unpatched vulnerabilities.

This tool provides comprehensive coverage for a wide array of databases, including Oracle Database, Microsoft SQL Server, IBM Db2, SAP ASE, SAP IQ, SAP SQL Anywhere and SAP Advantage Server, and SAP HANA databases. It runs on Windows, Linux, and Unix environments.

OPERATING SYSTEMS

Trend Micro is a network intrusion detection and prevention system (IDS/IPS). This tool provides protection at the network level, sniffing TCP/IP and UDP data transfer.

If Trend Micro detects a suspicious or forbidden action, the system will use pre-defined rules to either nifty network administrators or execute rule-based proactive measures.

Trend Micro adds a layer of protection beyond network firewalls and the web application firewalls by protecting from attacks on DNS, SMTP. TELNET, RDP, SSH, and FTP.

SEVEN-POINT SECURITY VS. SOFTWARE PUBLISHER PATCHES

Some enterprises considering third-party support are concerned about the loss of quarterly software patches for critical vulnerabilities and exposures.

Patches are an excellent first line of defense for code vulnerabilities, but they can be flawed – just like the software they are meant to fix – and are often released by product, so not all products get patches at the same time. By solving for areas of weakness, we address the uses at the infrastructure layer rather than by individual products.

	SOFTWARE PATCHING	SEVEN-POINT SECURITY
TIMING	Patches are not timely and can take months or even years to be released.	Virtual patching tools plus proactive monitoring provides near-immediate protection.
SPECIFICITY	Patches are one-size-fits-all and may be problematic for customizations.	Receive only the fixes you need.
VERSIONS	Patches may not be available for older versions and applications.	By addressing issues at the infrastructure level, you protect the entire tech stack, regardless of app versions.
TESTING	Patches require valuable time to test and install.	For critical vulnerabilities and exposures, methods such as virtual patching save valuable time by diminishing testing and installation.
APPLICATION	Many organizations do not patch or patch regularly due to operational constraints.	Organizations must remain vigilant for critical vulnerabilities and exposures and not rely on patches that may not actually resolve the issue.

Recent studies of Oracle patches have shown that for many products, a large percentage of patches failed to resolve the original issue, requiring Oracle to publish additional patches for the same CVE. In 2020, 69% of all Oracle Database patches were repeats, and 25% of all Weblogic patches were repeats.

Patches are an excellent first line of defense for code vulnerabilities, but they can be flawed – just like the software they are meant to fix – and are often released by product, so not all products get patches at the same time. By solving for areas of weakness, we address the issue at the infrastructure layer rather than by individual product.

SPINNAKER SUPPORT COMPARED TO ORACLE AND SAP?

Oracle and SAP heavily promote patching and utilize it as a best practice for resolving security issues related to vulnerabilities. As mentioned previously, patching alone can be a flawed solution, especially when clients are unable to install every patch or commit the necessary resources to a patch management program.

Spinnaker Support Security Solutions are responsive, on-demand, and multi-layered. Our seven-point security solution replaces relying solely on patches and creates a stronger framework to cover a wider range of possible security issues. While software publishers can take months or even years to patch a vulnerability, we begin to assess and resolve the threat immediately.

THIS INCLUDES:

HOW DOES SPINNAKER SUPPORT COMPARE TO ITS MARKET COMPETITORS?

All third-party support vendors offer some form of security as a standard feature for their services. This typically involves a reliance on security tooling and virtual patching, which comes as a separate line item and additional cost.

Spinnaker Support includes security tooling as an option, but our security solution relies primarily on the layered set of defensive and proactive approaches described above. This sets us apart and ahead of our competitors since we can respond more quickly and with personalized service. We continue to expand our global security team and invest in the research, communication tools, and processes to keep your environment secure.

EXAMPLES OF SECURITY ISSUES

Closing A Breach Used By A Bitcoin Mining Program

A customer discovered a rogue process on one of its payment processing servers. The customer killed the process and removed the program, but it kept re-installing itself. At that point, we were brought in to help.

We confirmed that it was a Bitcoin mining program that someone had surreptitiously installed via a little-known and little-used Web service library. Our security team provided the customer with a plan to determine whether this library was being used for business purposes and, if so, determine a way to remove it safely. After executing our plan, the customer reported that the issue was resolved, and it has not returned.

Educating On Critical Vulnerabilities

During the Spectre / Meltdown incident of 2018, several customers approached us to help them understand the potential scope and impact on their systems and for advice on how to handle the CPU bugs. We drafted a whitepaper detailing the background and mitigation methods and shared it with the customers.

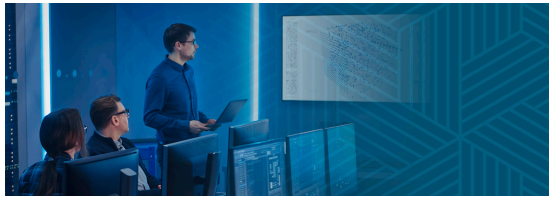
As security topics develop, we author whitepapers and other reference materials for the benefit of all of our customers. We also develop position papers on specific areas of customer interest such as interoperability and virtualization.

Providing Hardening Advice

During a customer's transition to Spinnaker Support, we discovered that the customer had its development database fed directly by the production environment. Failure of the production environment could potentially impact both production and dev databases, and there would be no way to test solutions to fix problems for the production database.

We advised the customer as to the proper architecture and procedures and recommended creating three unique and isolated environments.

EXAMPLES OF SECURITY ISSUES



Addressing The Apache Log4J-Flaw

On December 10, 2021, “Log4Shell” was disclosed by security researchers with CERT New Zealand and logged into the National Vulnerability Database as CVE-2021-44228. This vulnerability in the Java logging framework Log4j is described as a zero-day (easily exploitable) arbitrary code execution (you can run any commands), with a rare score of 10-out-of-10 on the CVSS v3 rating scale.

The offending program is an open-source, publicly accessible library, distributed and managed by the Apache Foundation. On the day of the disclosure, we researched the CVE and sent out a risk assessment bulletin to affected customers. We then published documents on this vulnerability and added them to our security resource library. We were able to mitigate the CVE definitively by having customers remove the offending class files from the jar file or upgrade their Log4j version.

As we received tickets from concerned clients, we were able to provide immediate vulnerability support. For those who needed more hands-on assistance, we provided step-by-step help via video or conference call. We also published a blog to provide additional information and links to trusted and publicly available security sources.

Our security team had access to the same information as Oracle, and yet we passed the information and our solution along to our customers faster than Oracle was able to provide its fix.

OUR HOLISTIC SECURITY APPROACH

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.

ISO 9001 Quality

ISO 27001 2022

CYBER ESSENTIALS

PRIVACY SHIELD

CIS SecureSuite® Membership

LEARN MORE

Our security leaders and team are always available to discuss our techniques and overall security solution.

Reach out to Spinnaker Support today to start a conversation.

GLOSSARY

CIS benchmarks

The Center for Internet Security Best-practice Security Configuration Guide, with benchmarks that are consensus-based and accepted across governments, industry, and academia, is an industry-standard way to measure security effectiveness.

CVE

Common vulnerabilities and exposures – an actual discovered vulnerability.

CWE

Common weakness enumeration – a category of classification of CVE.

Compensating controls

Something put in place to prevent a vulnerability from being exploited.

Defense in depth

More layers mean more protection.

DISA - STIG

Defense Information System Agency – Security Technical Implementation Guides. These are available through the DoD Cyber Exchange.

Hardening

The process of eliminating potential attack vectors through the reduction of a system's attack surface.

IPS (IDS)

Intrusion prevention system (intrusion detection system).

Security posture

A phrase used to describe an organization's overall approach to security.

Types of tools

Trellix – Database; Waratek – Middleware; TrendMicro – Operating Systems

Virtual patching

Implementing layers of security policies and rules that prevent and intercept an exploit from taking network paths to and from a vulnerability.

Zero-day vulnerability

Vulnerability in a system or device that has been disclosed but is not yet patched.