A White Paper Analysis from Orasi Software and Saltworks

Customizing Your SAP Platform: Put Security First

orasi

Saltworks
An Orasi Company

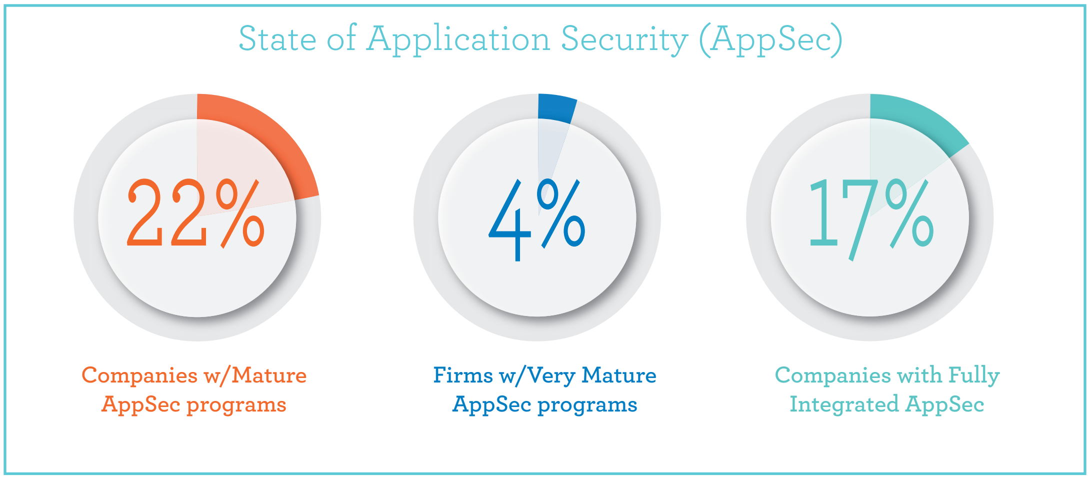
Contents

Executive Summary

With vulnerabilities in web-connected applications presenting one of the greatest risks for a breach (and web app attacks, specifically, remaining the single biggest case of breach data loss), the vulnerability of organizations running connected enterprise resource planning (ERP) platforms such as SAP is indisputable. At the same time, only 17% of developing organizations have fully mature, integrated application security (AppSec) plans and approaches, and even those with mature programs have fallen victim to cyber attacks.

Furthermore, the security safeguards that SAP builds into its platform are not designed to protect organizations that develop, customize, or integrate in-house or third-party components, apps and front-end sites with SAP. These organizations are responsible for their own app security—and statistics prove that remediating vulnerabilities in production is not enough.

To reduce the odds of a potentially crippling breach, such firms must implement robust security programs managed by trained specialists—and deploy software that can identify and report on vulnerabilities beginning at the earliest stages of the software development lifecycle. The circumstances that have led to this imperative—and the means to achieve it—are the subject of this paper.



Software Security Matters More than Ever

It's been more than a decade since the first application security products hit the market. Yet, in many ways, organizations are no closer to locking down applications than they were then. Since that time, security experts have stopped suggesting that organizational networks and systems can completely avoid penetration. Rather, the focus has turned to mitigation—minimizing security holes and then identifying attacks and stopping them, hopefully before they cause damage.

Over that period, cybercrime organizations have gone from being loosely connected groups of hackers to extremely well-organized, well-funded criminal enterprises with resources greater than that of many nations. Exacerbating the problem, some unscrupulous security researchers have been lured by curiosity or greed into selling the vulnerabilities they discover to the highest bidder.

Cybercrime has become so lucrative that criminal enterprises now compete to find and exploit vulnerabilities before anyone else does—and before the company where they reside can identify and close them. Most evidence indicates the criminals are winning the race.

Application Security: Better, but Not Enough

In this threat-fraught environment, organizations are attempting to protect themselves, but AppSec remains one of many problems. In its 2016 "State of Application Security: Skills, Configurations and Components," the SANS Institute noted that AppSec is "maturing for most organizations." Yet, the study found that only 26% of respondents said their programs were "Mature" or "Very Mature," and only 17% felt they had fully integrated AppSec into their overall security, risk management, and incident response programs.

Even among firms with an AppSec program in place, development efforts may not be immune to compromise. A number of issues can impede positive outcomes:

- The security team implements the plan it feels will work and tries to force developers to work within it, but it isn't compatible with the developer's workflow. Under pressure to meet expedited deadlines, developers dismiss the plan as too complicated or time consuming and attempt homegrown solutions or simply do nothing.
- The security team, anxious to get solutions flowing, issues reports without vetting them. Developers don't have any guidance regarding priorities and become even more reluctant to act.
- Application testing happens as specified and vulnerabilities are found, but nothing gets done due to lack of time, willingness, an appropriate plan, and/or ranking of vulnerabilities by importance.

In all of these scenarios, application security is neither efficient nor effective. Frustration mounts as security efforts impede the speed, integration, and automation expected in the software development lifecycle (SDLC) of modern applications. Developers (and/or corporate stakeholders) perceive security as a barrier to innovation. The organizational approach continues to be, “Find and fix (and often ignore) errors in production,” or the program is abandoned altogether.

For companies that are not operating under a blanket of AppSec protection, the problem is even worse. These firms are often purely reactive and fix issues as they are reported by users or discovered by team members. The firm continues to operate on borrowed time, never truly accepting that a reactive approach will not solve the problem—but it likely will lead to disaster.

Vulnerability by the Numbers

Software exploits remain one of the foremost vectors allowing remote code execution and privilege escalation (which affords a higher level of rights than would normally be allowed)—in many cases, using exploits that were discovered years earlier. Among all applications, web and mobile apps remain top players, despite years of attacks and attempts to thwart them.

Web App Attacks

Still account for more than 40% of data breach incidents and remain the single-biggest source of data loss.[1]

Critical Vulnerabilities

In March 2017, Apache released a bulletin on a critical remote code execution vulnerability, “Struts-Shock.” The Struts 2 framework in which it exists is widely used in Java applications, and attackers were exploiting it at discovery.

Mobile and Web Exploits

In terms of exploits, Android and Java rank number two and three, at 18% and 12%, respectively. (Microsoft Windows is number one.) [2]

Android Threats

More than 10,000 new threats discovered daily, and old vulnerabilities still haunt security teams. One example is “CVE-2012-6422”—a Samsung processor privilege escalation vulnerability that allows read/write to the system memory[2]. Discovered in 2012, that vulnerability was still responsible for 24% of exploits three years later[3].

[1] 2016, Verizon [2] 2016 HPE [3] 2015, Reversing Labs

The Vulnerability of a Connected World

Until now, we’ve been talking about application vulnerability and security in general. Perhaps you are wondering, “What’s the connection to SAP?” The answer is just that—connection. In the current environment, a large portion—if not the majority—of ERP activities conducted by employees, partners, providers, and customers are Internet enabled and therefore extremely vulnerable. That percentage is only going to increase. Organizations running SAP customizations that retrieve information from other sites or services, or that build/integrate SAP apps or front-end sites for customers, employees, partners, or providers, cannot safely achieve meaningful business goals with the platform without best-practices security.

Consider some of the top customizations for SAP and the potential threat becomes pretty clear:

- Shopping carts
- Customer service websites
- Order tracking and fulfillment websites
- Partner portals
- Medical records systems
- Mobile apps for remote employee time tracking, report generation, work order fulfillment, etc.

Vulnerable Externally Connected SAP Enhancements

Shopping Carts · Customer Service Sites · Order Tracking/ Fulfillment Sites · Partner Portals · Medical Records · Remote Worker Apps

We are not suggesting SAP is a bigger risk than any other ERP system or, for that matter, any enterprise-grade solution. The decision makers at SAP have made security a priority, securing their modules to the highest extent possible. Nevertheless, when organizations have hundreds, thousands, or even just dozens of external users interacting with web applications and mobile devices, these activities present a giant attack surface.

No matter how secure SAP's products are, as soon as a developer writes code for a custom application—or for a component, app, or web service integration—that person has opened an inviting hole in the system's attack surface. If appropriate security mechanisms aren't in place, it becomes a beacon to cybercriminals everywhere. Given that SAP customizations and services are prone to process and store not only personally identifiable information (PII) but also sensitive corporate data, a single breach could be disastrous.

SAP S/4HANA: What's the Big Deal?

SAP S/4HANA presents opportunities for customization that go well beyond the norm for earlier versions of SAP. As such, security must be handled with extra care. The platform, which is built on SAP HANA—an advanced, powerful in-memory platform—has the ability to rapidly organize and process Big Data—gargantuan datasets of structured and unstructured data. SAP S/4HANA also offers SAP Fiori, a consumer-grade, personalized user experience, so users can visualize and consume data in near-real-time.

With any platform optimized to process big data and visualize it on public-facing devices, effective security testing and vulnerability remediation would be an imperative.

In the case of SAP S/4HANA, the situation is exacerbated by the many third-party add-ons that developers are releasing, many of which target Fiori.

Deploying and customizing organizations must be highly vigilant with code that they are writing for the new platform. They must also ensure customizations in existing SAP deployments are scrubbed of vulnerabilities before they port them over to the SAP S/4HANA platform.

Reengineering a Broken Process

As many company leaders realize, the endless cycle of code remediation for individual bugs is expensive and labor intensive. Even sophisticated, industry-engineered countermeasures such as data execution prevention (DEP) no longer keep attackers out. (DEP marks memory regions as executable or non-executable so that data-related commands won't execute in regions where it is prohibited.) With code bases reaching millions of lines of code, the next vulnerability is always just around the corner.

Moreover, with the Ponemon Institute reporting that the average cost to mitigate the damage of stolen confidential or sensitive data is $158 per record—excluding lawsuits and penalties—many organizations simply will not survive a major breach. Even if they do, erosion of customer confidence and brand reputation will likely cause substantial damage.

Finally, with SAP customizations and integrations offering a very broad attack surface for intensely sensitive information, enterprises must prioritize best-practices security for their custom SAP deployments. If they are running customized versions of SAP S/4HANA, the importance of robust security escalates from essential to extreme.

To minimize the odds of becoming an ugly statistic, organizations customizing any version of SAP should take concrete, proactive steps:

- Accept that after-the-fact mitigation of security flaws discovered in production is a losing game that could result in corporate disaster.
- Apply in-house resources or hire outsourced expert assistance to analyze current security approaches.
- Identify resources, inside the firm or out, to develop and implement a Software Security Assurance (SSA) program for every externally connected application or service integrated with SAP. (For more about SSA elements, refer to the box below.)

Elements of a Best Practices SSA

1. Security is integrated into the app development process across the SDLC, beginning at the earliest stages of code development.
2. The approach is functional for everyone—and is written to work with the way developers operate rather than vice versa.
3. Security testing and QA occur with every code change (before the build) for new applications, updates, integrations, and all other components interacting with SAP.
4. Robust tools quickly identify vulnerabilities and stay abreast of them until they are closed. (For reasons we will disclose, we recommend HPE Security Fortify.)
5. All team members have appropriate training on systems, practices, and tools, with periodic monitoring to ensure consistent, practical application.

Building a Secured Future

Frequently, organizations do not have the resources to initiate or complete a best-practices security program. Consequently, management postpones the effort, thinking that there will be time “down the road.” The reality of software development is that the situation is growing worse, daily. The acceleration of digital platforms for user- and customer-facing activities is not helping.

Fortunately, organizational leaders and software managers do not need to find the resources to develop a security program. Companies with expertise in these efforts can do it for them with minimal disruption. Saltworks Security, an Orasi company, specializes in application security. They have helped many organizations develop effective application security programs and plans while minimizing cost and disruption. This is how we do it:

- Our security experts come to the customer’s site and help stakeholders design an application security program.
- Saltworks’ technical pros develop methodologies that integrate security into the SDLC.
- We deploy the tools and technologies that make it easy for teams to get code analyzed.
- Our on-site team trains everyone in tools and best practices that ensure software security.
- We partner with security, development, and audit teams until the program is stable and then can either provide ongoing support services to manage the program or turn the effort over to the firm’s designated point team.”

Is there a charge for this work? Of course. But, company leaders often tell us that they recoup most, if not all, of their expenditure through reduced budgets for development, remediation and compliance—and increased team productivity. This payback doesn’t even take into account the sharply reduced risk of a financially crippling security breach.

HPE Fortify Spotlight:

Healthcare Organization Protects Customer Data; Cuts AppSec Test Costs by 800%

When one of the nation’s largest healthcare enterprises sought to safeguard its customer data and business reputation from attack, it chose Saltworks and HPE Fortify to provide a solution. The result?

- AppSec testing time dropped from 7 days to under 48 hours while testing 10 times the applications and reducing false positives.
- AppSec testing costs were reduced by 800%.
- The risk of cyber breaches was minimized, promoting data safety and aiding compliance.

Huge Problems; Reasonable Solutions

To help organizational stakeholders understand more about HPE Fortify and how it enables teams to remediate vulnerabilities, HPE experts compiled and analyzed sample datasets from static scans (327 applications) and dynamic scans (301 applications). The results, presented in the HPE Security Research Cyberrisk Report 2016, illustrate lack of awareness about the realities of extreme risk—and highlight the value in remediating "easy fix" vulnerabilities.

Vulnerability Findings

Non-Mobile Applications

35%+

Mobile Applications

75%+

At least 1 critical or high-severity vulnerability

Over one-third (35%) of the non-mobile applications that HPE Fortify scanned exhibited at least one critical- or high-severity vulnerability. Among mobile applications, that number jumped to 75%.

HPE Fortify Scan Results

Static Scans

Dynamic Scans

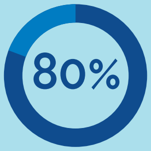
Static Scans		Dynamic Scans	
35% Issues Resolved 0-30 Days (1st scan range)	90% Issues Resolved 0-120 Days (1st four scan ranges)	32% Issues Resolved 0-30 Days (1st scan range)	79% Issues Resolved 90-120 Days (End of 4th scan range)

Most critical-severity issues were addressed by the second range of scans (6 to 11 scans, or 31 to 60 days).

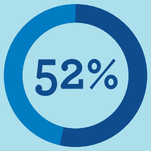
System Information Leaks: Big Issue; Easy Fix

Most low-severity vulnerabilities found in HPE Fortify's static scans **were fixed by teams early on**. Many of these vulnerabilities were system information leaks, where too-detailed error messages leak system data.

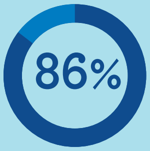
These leaks generally are not critical and are relatively simple to fix. However, if leaked externally, they can help attackers gain visibility into the system and facilitate critical attacks.



Percent of Vulnerable Instances Where External Leaks Are a Factor



Percent of Non-Mobile Apps with System Leaks
97% Leak Externally



Percent of Mobile Apps with Leaks
24% Leak Externally

Fortifying Application Security

As we mentioned in Elements of a Best Practices SSA, the fourth "leg" of the program is ongoing code monitoring and analysis, for which we recommend HPE Security Fortify. This ecosystem of security solutions and tools is targeted to sharply reduce the potential for successful exploits while promoting software quality and reliability and accelerating time-to-market. Specifically, the solution:

- Allows security testing to be done very early during the SDLC.
- Targets vulnerabilities proactively, by type rather than by incident.
- Conducts ongoing scans that not only identify the existence of vulnerabilities but also confirm their disappearance once code changes are complete.
- Helps pinpoint the time teams take to correct flawed code, enabling organizations to identify and correct deficiencies in security practices.

On-Demand Scanning: A Key Piece of the Puzzle

A valuable tool within the HPE Security Fortify family is HPE Security Fortify On Demand, an application security-as-a-service offering. With this powerful, as-needed code analysis tool, teams submit code as they develop it, receive feedback on vulnerabilities, and can then take immediate action. HPE Fortify On Demand incorporates a Static Code Analyzer (SCA) that analyzes source code during the build phase and identifies security vulnerabilities at the earliest stages. It delivers, through an interactive dashboard, accurate, risk-ranked results with remediation guidance, enabling teams to prioritize remediation work by severity.

HPE Fortify On Demand also incorporates dynamic application security testing. Dynamic scans are used not only for preproduction but also for production monitoring—identifying vulnerabilities and risk profile changes, discovering rogue applications, and detecting run-time security events in applications. Offering both types of analysis enables HPE Fortify On Demand to cover the entire spectrum of code, from early snippets under development to applications, post-release.

How the SCA Engine Works

1. Source code is translated into a specialized code model that is optimized for analysis by the SCA engine.
2. The SCA engine loads the model into memory, after which six different analyzers examine the code for problems with data flow, control flow, code structure and process execution (semantics), configuration, and buffer activity.
3. Each analyzer finds different types of vulnerabilities, and the results are reported for evaluation and remediation.

Achieving the Possible

We hope we have illustrated not only the depth of vulnerability to which customizing SAP organizations are exposing themselves, but also the relative ease and efficiency with which they can thwart attackers while ensuring product security. Developing organizations must be as adaptable and determined as cyberattackers if they hope to survive.

About Us

Orasi Software, Inc.
Orasi is a leading provider of software, support, training and consulting services. Through strategic industry partnerships, Orasi offers market-leading automated testing, application performance management/intelligence, test data management and coverage, continuous delivery/integration, big data, and mobile technologies to enable customers to focus on a complete software quality lifecycle. For more than 15 years, Orasi has helped customers successfully implement and integrate software testing environments to reduce the cost and risk of software failures.

Saltworks Security, LLC
Saltworks Security, LLC (Saltworks) is a joint venture of application security experts Saltworks Security, Inc. and Orasi Software, Inc., providing the combined software and security talent and proficiency of both. Saltworks offers organizational stakeholders end-to-end consulting expertise for securing software, beginning with strategic planning and program development, through identifying, purchasing, and deploying the right combination of security tools, to personnel training and follow-up reporting, auditing, and more.

Saltworks' experts have specialized competency in a full spectrum of security programs and tools, not only for application development but also for varied corporate activities associated with it. These include both static and dynamic code testing, penetration testing, encryption, and secure email. Working with Saltworks, organizations and their customers gain the reassurance of following standards that lead to consistently secure application development, testing, deployment, and lifecycle management.

For more information, contact Orasi and Saltworks

www.orasi.com | 678.819.5300 | www.saltworkssecurity.com

orasi

{S} Saltworks
An Orasi Company

Hewlett Packard Enterprise
Platinum Partner