ONAPSIS

Case Study

LEADING BIOTECHNOLOGY COMPANY USES ONAPSIS TO PROTECT ITS BUSINESS-CRITICAL SAP APPLICATIONS

INDUSTRY

Biotechnology

COMPANY SIZE

>20,000 employees worldwide, >$20B total revenue

BUSINESS-CRITICAL APPLICATION PLATFORM

SAP

As one of the world's leading independent biotechnology companies, the company depends on their SAP systems to manage their supply chain, international trade, financial and other business-critical applications to achieve their mission of serving patients around the world.

Given the growing number of security vulnerabilities and public exploits on SAP systems, the organization knew their global ERP systems were a potential target for cyberattacks and posed a huge risk to their corporate mission and patient safety. To combat this, they created a cybersecurity program dedicated to their SAP systems and sought a solution provider that would enable them to find, fix and prevent vulnerabilities, misconfigurations and custom-code issues.

REQUIREMENTS

- Identify critical vulnerabilities to SAP and reduce exposure by streamlining the remediation process
- Continuously monitor and protect SAP before patches have been released
- Provide real-time alerts if SAP systems are under attack with integration to IBM QRadar
- Prevent SAP systems, code and transports from becoming insecure or non-compliant

CHALLENGE

Harden SAP against internal and external threats, operationalize risk remediation.

SOLUTION

The Onapsis Platform continually assesses SAP systems, code and transports for vulnerabilities and misconfigurations, provides actionable remediation and mitigation strategies and protects against unauthorized changes to ensure that the company's mission-critical applications stay online, secure and compliant.

Case Study

A threat to our SAP applications is a threat to the patients that rely on our products. Onapsis helps us protect our SAP systems by keeping them online, stable and available, allowing us to be proactive with our SAP security on both a system and code level. We can now prevent performance, stability and data loss issues before they happen, further reducing our risk exposure and saving our Basis team a ton of time.

GLOBAL LEAD OF SAP OPERATIONS,
BIOTECHNOLOGY COMPANY

SOLUTION

The company found its ideal solution with Onapsis to protect its global SAP environment. The Onapsis Platform provides visibility into their SAP system, code and transport configurations and continuous assessment of misconfigurations and vulnerabilities across the entire SAP landscape. An initial Onapsis assessment identified over 80 vulnerabilities, more than 20 critical or high, within their systems.

With actionable insight from Onapsis, they prioritized remediation and reduced vulnerabilities by 75%, including all 20+ critical/high ones, ahead of its migration to HANA. Due to configuration changes during the migration process, follow-up assessments with Onapsis revealed 30 new vulnerabilities within its SAP systems. These findings stressed the need for ongoing assessment, monitoring and mitigation options.

Using The Onapsis Platform, they are now able to continuously monitor for vulnerabilities, prioritize remediation based on risk assessment, receive notifications of internal misuse or external attack and prevent changes that would leave their systems insecure. Onapsis provides the product capabilities and SAP expertise they need to ensure their critical applications remain stable, secure and compliant. By leveraging Onapsis, they have significantly reduced SAP vulnerabilities. In fact when the 10KBLAZE exploits went public, they quickly validated that they were not vulnerable.

RESULTS

- Reduced vulnerabilities and remediation time from more than six months to less than one (less than a week for emergencies) by automating vulnerability checks, measuring security risks of each vulnerability and prioritizing fixes
- Applied compensating controls for unmitigated risks to ensure SAP is continuously protected, even between patches
- Received immediate notifications with IBM QRadar integration of an SAP system attack, including insight into whether the attack was successful and corrective actions
- Achieved visibility into system and security settings, with the ability to automatically prevent unapproved changes

ADDITIONAL CUSTOMER INITIATIVES WITH ONAPSIS

- Given the success of the SAP cybersecurity project, the organization continues to expand its use of The Onapsis Platform to further strengthen their overall SAP security posture and ensure compliance with the following initiatives:
- Code Analysis—Automate code reviews for 100% of development artifacts, eliminating time-consuming manual code reviews and improving overall quality and productivity
- Transport Analysis—Onapsis's integration with SAP ABAP Test Cockpit (ATC) and Solution Manager CHaRM prevents promotion of transports with code that did not pass the company's security checks
- Vulnerability Lifecycle Tracking—Onapsis's integration with ServiceNow enables a formal approach to SAP vulnerability remediation and mitigation
- Compliance Automation—Automate recurring compliance checks, including SOX controls, through custom "compliance policies"

ABOUT ONAPSIS

Onapsis protects the business-critical applications that power the global economy including ERP, CRM, PLM, HCM, SCM and BI applications from SAP®, Oracle® and leading SaaS providers. Onapsis proudly serves more than 300 of the world's leading brands including 20% of the Fortune 100 and partners with leading consulting and audit firms such as Accenture, Deloitte, IBM, PwC and Verizon. The Onapsis Research Labs is responsible for the discovery and mitigation of more than 800 zero-day business-critical application vulnerabilities.