

# LARGE UTILITY COMPANY USES ONAPSIS TO IMPROVE SAP SECURITY AND PREPARE FOR S/4HANA MIGRATION

**INDUSTRY**

Energy

**COMPANY SIZE**2,000+ employees, serving  
850k+ customers,  
>\$2B revenue**BUSINESS-CRITICAL  
APPLICATION PLATFORM**

SAP

## CHALLENGE

Create a security foundation for transformation projects, including Fiori and S/4HANA migration.

## SOLUTION

The Onapsis Platform assesses SAP for vulnerabilities and misconfigurations to understand potential business impact, define remediation strategies and set baselines. With Onapsis, the company was able to build security into projects from the start, continually monitor their entire landscape and prevent configuration drift, ensuring their business-critical applications stay secure and online.

This large American utility company relies on a centralized, highly customized SAP system for their business-critical functions, including HR, legal, customer service and finance.

Given this, the utility company needed to focus attention on its security measures and knew traditional practices, like segregation of duties, weren't enough. This was especially pressing due to increased use of third-party developers, Fiori exposing SAP to the internet and a looming S/4HANA migration—all of which could introduce new risks to their critical applications. An SAP cybersecurity program would help protect their critical systems, keep them working properly and ensure the success of future digital transformation projects.

To create this program, they needed a solution to provide visibility into SAP configurations, including those created by third-party developers, identify misconfigurations and other vulnerabilities and help streamline patching and remediation processes.

*ONAPSIS REMOVES THE MYSTERY AROUND SAP SECURITY BY INCREASING VISIBILITY. WE CAN SEE ISSUES— MISCONFIGURATIONS, MISSING PATCHES OR UNUSUAL USER ACTIVITY—WHAT RISK THEY POSE AND HOW TO FIX THEM. WE WERE ABLE TO ESTABLISH AND MAINTAIN SECURITY BASELINES AND CAN NOW BUILD THEM INTO TRANSFORMATION PROJECTS FROM THE START. ONAPSIS ENABLES US TO KEEP SAP SECURE WITHOUT IMPACTING SYSTEM PERFORMANCE OR INTERFERING WITH BASIS TEAMS.*

**ENTERPRISE SECURITY MANAGER,  
UTILITY COMPANY**



Scanned and remediated vulnerabilities quickly



Decreased number of code corrections required



Improved developer skills



Reduced effort and time spent on code reviews



Ensured ALL code meets security and compliance requirements

## REQUIREMENTS

- Discover critical vulnerabilities across SAP landscape; understand their business risk and how to remediate
- Establish consistent security baselines across entire SAP landscape without interfering with Basis teams or impacting system availability
- Visibility into SAP to help detect financial fraud and monitor configurations set by third-party contractors
- Simplify the patching process, which was complicated and time consuming due to legacy customization

## SOLUTION

Onapsis delivered the visibility and intelligence capabilities that they needed to implement their SAP cybersecurity program and protect their business-critical applications long-term. With The Onapsis Platform, they discovered system security issues and their business impact and received expert remediation guidance.

This enabled them to determine their SAP threat landscape and appropriate security baselines for their risk posture. With Onapsis, they can now continually monitor systems against these baselines, preventing changes that may make them non-compliant, build them into digital transformation projects from the start, preventing roadblocks due to security concerns, and allow Basis teams to develop with confidence.

The organization has also significantly improved their patch process. Previously it was manual and time consuming, due to the high level of customization and often resulted in missed patches. The Onapsis Research Lab's monthly analysis of SAP Security Notes has helped them determine which notes to prioritize, the best way to implement and if they are missing any critical patches.

## RESULTS

- Gained visibility into SAP configurations and controls, reducing reliance on the small team who manages the systems and enabling oversight of third-party contractors
- Established SAP cybersecurity program and baselines that will serve as a foundation for Fiori and S4/HANA migration projects, enabling transformation with confidence
- Reduced SAP threat landscape by continuously monitoring for unusual activity (internal or external), vulnerabilities, misconfigurations, missing patches and other security issues that could result in data loss, tampering, fraud or system outages
- Streamlined the patching process by relying on Onapsis's SAP Security Note guidance

## 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. For more information, visit [www.onapsis.com](http://www.onapsis.com).