Fortune 500 Utility Company Partners with Onapsis **to Build Security into Their RISE with SAP Transformation and Achieve Secure, On-Time, On-Budget Go-Live**

Industry
Utilities, Gas & Electric

Company Size
2K+ employees, >$2B revenue

Challenge

A Fortune 500 utility company operating a twenty-year-old, on-premises SAP system chose the RISE with SAP program to more efficiently migrate to SAP S/4HANA and modernize their systems. Due to the age and complexity of their legacy systems, the company opted for a greenfield approach so they could start over and start clean in their new RISE environment. With the knowledge that the company was still responsible for their application security and compliance under the shared security responsibility model of RISE, this company recognized that their existing staff - while very good - required new skills and insights to navigate SAP security and compliance in the cloud. They recognized that they needed greater understanding of their roles and responsibilities for security under RISE. This utility company very much wanted a partner who could offer significant SAP security technology capabilities to help them today, deep R&D teams for both threat insights and product innovation to protect them tomorrow, and knowledgeable resources with deep hands-on expertise in guiding large enterprises with security planning and execution for large, multi-year RISE deployments.

Fortunately for this company, they had been partnering with Onapsis for many years to secure their on-premises systems, so they already recognized the value of Onapsis technology for securing their SAP landscape and wanted that to continue in RISE. However, when they learned that Onapsis also offered hands-on RISE experts for enterprises to help augment their staff as they journey to RISE, they quickly realized they could get everything they wanted from their partner that knew both themselves and SAP security the best.

Overall Results

With the help of Onapsis technology, this utility company achieved their goal of building security into their RISE with SAP transformation seamlessly, without interfering with their tight delivery timelines. They expanded their security visibility to their new RISE systems as well as point-in-time vulnerability scanning and continuous monitoring for SAP BTP and SAProuter, while simultaneously protecting their legacy systems as they executed a phased rollout of new systems on RISE. Everything - both legacy on-premises and RISE assets - were all centralized in the Onapsis Platform dashboard which simplified security and compliance for their teams. The research-driven analysis built into the Onapsis Platform paired with efficiencies from security automation helped them eliminate a significant amount of manual processes throughout the project as well as make project decisions much faster, resulting in both better security and greater risk reduction and significant time and cost savings.

By far, the biggest advantage this utility company had during their RISE transition was enlisting the Onapsis RISE experts to augment their existing staff and guide them along the way. From the initial project discussions with SAP through the build phases and go-live, the utility company had SAP-security-focused experts on their team to help them address challenges as they arose, recommend best practices, troubleshoot with GSIs, SAP, and the hyperscale, prevent scope creep, and mitigate or avoid security or compliance project delays.

"In the five years we've worked with Onapsis to secure our on-premises systems, we've not only experienced the day-to-day value of their technology - cutting our investigation times in half and reducing our mean-time-to-remediate by over 75% - but we've come to rely on them as ***true expert partners*** *in shaping and optimizing our SAP security strategy. We knew we had to have them involved from the start when we began our RISE discussions and* ***their guidance was invaluable****, helping us to not only navigate but anticipate potential security and compliance obstacles so we could get ahead of them and avoid unexpected project delays.*

The automation and risk-based analysis provided by their solutions made it easy to build security checks into each stage of the product, so we could find and fix things quickly, our teams were aligned, and we were ultimately able to ***deliver our RISE project on time and on budget****."*

- VP of Security, Utility Company

With Onapsis, the utility company achieved both greater risk reduction and significant time and resource savings throughout their RISE transformation project, including:

68%
reduction in time spent reviewing code by replacing manual checks

97%
reduction in time spent checking for missing Security Notes across entire landscape

88%
reduction in time spent analyzing and collecting information about missing Security Notes (saving at least 2 hours of time on each Note)

99%
reduction in time spent testing controls across entire landscape (what used to take 55 hours each quarter, now only takes 5 minutes)

Before

Planning for a Secure Greenfield SAP S/4HANA Transformation

CHALLENGE	SOLUTION
Shared Security Model Under RISE with SAP, the customer organization is responsible for a number of areas, such as quality and security of custom code, user access and behavior, certain areas of patch management, security monitoring and incident response, and compliance. The utility company wanted to have technologies in place from the start of the project that would help them address those areas throughout the transformation and beyond.	Having used Onapsis products to secure their legacy, on-premises SAP landscape for over five years, the utility company was confident that Onapsis was the answer for addressing their security requirements in the new RISE environment and made Onapsis usage a non-negotiable stipulation in their RISE contract negotiations with SAP. Onapsis solutions for application security testing, vulnerability management, continuous monitoring, and audit automation would help the utility company better manage their security responsibilities under RISE.
Security-by-Design without Interfering with Overall Project Goals The utility company wanted to build security into the project from the start to avoid surprises and delays at go-live. But, security and compliance couldn't get in the way of delivering the project on time and on budget.	Onapsis technology and services would be embedded into each phase of the project and aligned with the SAP Activate methodology, allowing the utility company to identify and address issues early and incorporate security and compliance milestones into each phase gate check to avoid unexpected delays and costly rework in future phases. Onapsis RISE Experts embedded with the utility company's teams and helped them better construct a comprehensive SAP security plan from the start, saving them from costly, unplanned security and compliance project delays The robust automation and AI delivered by Onapsis products replaced manual efforts and enabled the utility company to de-risk and accelerate their project while avoiding interference with broader delivery goals.
Access to Necessary App Information Since SAP would be managing certain technical components of the utility company's applications (e.g., Client 000), SAP would need to provide access to the application logs for security monitoring and incident response purposes, plus any other data needed for security tools to ingest.	Having navigated these requirements in RISE projects before, Onapsis experts knew exactly what to do to ensure that the new RISE assets were set up properly to share the information the utility company would need to run successful security programs in their new RISE environment.

During

Building Their New RISE Environment Securely

CHALLENGE	SOLUTION
Establishing and Maintaining DevSecOps "Best Practices" to "Start Clean" with new Custom Code: The utility company outsources new code development to a global systems integrator (GSI), but under RISE with SAP, they are still ultimately responsible for the security and quality of the custom code in their systems. They needed a way to follow appropriate DevSecOps best practices to enforce code security and quality for the GSI in a way that won't interfere with the GSI's application delivery goals.	The utility company contractually obligates their GSI's development teams to run Onapsis Control as the code is being written to ensure clean and high quality code. Since Control plugs directly into the development environment the GSI developers are using, any issues are identified in real-time with detailed remediation guidance and pre-written code suggestions provided to accelerate the testing and fixing process. Control's automated scans replace manual effort to save significant time, reduce the risk of human error, and improve the quality of the code without interfering with delivery goals.
Validating Quality & Security of Third-Party Custom Code: The utility company also needed a way to easily test any code provided by 3rd parties to ensure it's of the highest security and quality, as they are ultimately responsible for custom code in their SAP systems, according to the shared security responsibility model.	The utility company leverages **Onapsis Control** bulk scanning functionality to test the GSI-created custom code before new code is imported into new PRD environments. Context-rich scan results help them easily understand any identified issues, so they can make informed decisions on what issues are of the highest priority to revert to the GSI.

"We've saved so much time and energy on DevSecOps efforts by using Onapsis Control. It has enabled our GSI's developers to write better code faster, right in the development environment they're already using. And, we're able to easily perform our own round of checks to make sure nothing was overlooked and that it meets our quality and security standards."

During

CHALLENGE	SOLUTION
Verifying Security Notes SLA Compliance: The utility company maintains an SLA of no missing critical ("HotNews") or High Priority Security Notes in any system, so they needed an easy way to verify that this SLA is being met.	The utility company uses **Onapsis Assess** automated vulnerability scans to identify any missing High Priority or HotNews Security Notes across their entire landscape. Results can easily be shared with the appropriate party (e.g., SAP for implementation into DEV, internal teams for implementation into QA/PRD).
Identifying Non-HotNews Patches to Request from SAP: In a standard RISE, SAP and the company share responsibility for Security Notes. While SAP may assist with preparing a transport for ABAP security notes in DEV, they will only automatically do so for HotNews. All other Notes (i.e., < CVSS 9.0) must be requested by the customer with an SAP support ticket. The utility company needed an easy way to identify and prioritize which Non-HotNews Notes to request.	The utility company uses **Onapsis Threat Intel Center's** monthly **Patch Tuesday** report to understand which Non-HotNews Notes have been released. Detailed descriptions of the Note, including potential business impact and prioritization for their unique landscape, help them determine if or when they want to submit a support request for SAP.
Validating Security Note Application by SAP: Under RISE, SAP is responsible for implementing HotNews Security Notes to DEV. The utility company needed a way to validate that this was happening in a timely manner, especially so they could begin quality testing of the patches as they moved the patch through their change management process.	The **Onapsis Threat Intel Center** has a report for each month's Patch Tuesday that shows the results for the utility company's landscape indicating which systems are missing which Notes from that month's release. They can easily see if any DEV systems are missing any HotNews Notes and export this information to be shared with SAP for follow-up.
Validating Security Notes Application by Customer Teams: The utility company also needed to validate that their own internal teams were adhering to their SLA and were taking the SAP-prepared HotNews Notes from Dev through to Production.	The utility company uses the same monthly Patch Tuesday report from the **Onapsis Threat Intel Center** to validate that any HotNews Notes have been carried through beyond DEV systems (e.g., QA, PRD).

"The Onapsis Threat Intel Center has been invaluable in helping us manage our responsibilities and internal SLAs around patching. Right on one page, we can easily validate - 1) if SAP has applied the HotNews Notes that they were supposed to in DEV; 2) if our teams have carried that work through to our production systems; and 3) if there are any other Notes we need to request from SAP. This is saving us hours and hours of tedious work each month."

During

CHALLENGE	SOLUTION
Identifying Insecure Application Configurations: Under RISE with SAP, application configuration remains the responsibility of the customer. The utility company needed a way to ensure their new S/4HANA applications are configured to best practices and remain that way.	The utility company uses **Onapsis Assess** automated vulnerability scans to identify insecure configurations. Detailed scan results, including step-by-step fixes, prioritize and accelerate remediation efforts.
Controls Testing & Audit Preparation: The utility company has over 50 controls they need to test on each system for audit purposes. Doing so manually was taking them about 5 hours per system each quarter (adding to over 3000 hours of wasted manual effort every year), so they sought a way to do this much more quickly and also reduce the risk of mistakes.	Onapsis experts assisted with the creation of a custom **Onapsis Comply** policy with custom modules that mapped to the controls the utility company needed to test. Now, they use that scan to quickly test their controls across their entire landscape, reducing the process to a matter of minutes and greatly improving the accuracy and repeatability of the results.
Avoiding Future Audit Findings: The utility company recently had an audit finding related to the assignment of a highly privileged SAP role and needed an easy way to avoid unexpected audit findings in the future.	The utility company uses **Onapsis Defend** as a real-time compensating control to monitor for privileged role assignments and other user behavior so they are alerted and can respond before any unauthorized assignments or behavior are found in an audit.
Monitoring for Potential Indicators of Compromise: Under RISE with SAP, the customer is responsible for application security threat monitoring and incident response.The utility company needed a way to be alerted to potential threats and security issues, to bring those alerts into their existing SIEM, and to give their security analysts the context they need to know what to prioritize and how to respond.	The utility company uses **Onapsis Defend** to continuously monitor their RISE landscape for exploit activity and other indicators of compromise (IoCs). **Defend** alerts, along with detailed explanation and mitigation guidance, are forwarded to their SIEM to inform and accelerate incident response. **Onapsis Defend** is regularly updated with the latest insights and observations from the Onapsis Research Labs, ensuring the utility company is monitoring for the latest techniques, tactics, and procedures used by threat actors targeting SAP.
Keeping Their Legacy Systems Protected in the Meantime: While the utility company built their new RISE environment, they needed to ensure their existing, on-premises systems remained protected and functioning properly to continue powering the business.	The utility company is using a range of Onapsis products on their legacy systems: • **Onapsis Assess** to maintain their SLA of no missing HotNews or High Priority Security Notes, identify any lower priority Notes that warrant prioritization, detect insecure configurations, and automate controls testing • **Onapsis Assess for Code** to scan custom code running in production and make sure it is still clean • **Onapsis Defend** to continuously monitor for IoCs and suspicious or unauthorized user behavior All of this security visibility for on-premises systems is combined with the assets from their RISE landscape in the Onapsis Platform giving them one easy, single view of the hybrid landscape for security.

After

Keeping Their New and Expanding RISE Environment Clean and Protected

CHALLENGE	SOLUTION
Staying Clean: The utility company needs a way to ensure that any new custom code developed by their GSI - including for SAP BTP development in the future - and any code running in production continues to be high quality and secure.	The utility company's GSI will continue to use **Onapsis Control** to automatically check custom code as it's being written across all their integrated development environments (IDEs), including those for SAP BTP. This allows them to identify and fix any code issues in a timely, efficient manner, before they reach production systems. The utility company will also leverage **Onapsis Assess for Code** to identify any security issues in code that's running in production (e.g., an issue made it past AppDev and QA; or a new vulnerability has been discovered since the code was originally tested and deployed).
Ongoing Controls Testing & Audit Preparation: The utility company needs an easy way to routinely validate their controls and identify any potential violations or audit findings ahead of their audit cycle.	On a quarterly basis, the utility company will use the customized **Onapsis Comply** policy created by Onapsis experts that maps to their specific controls to validate their controls and automate evidence collection ahead of their audit cycle. This process only takes a few minutes (as compared to the 50+ hours it used to take manually) and will allow them to find and address any potential violations before they are discovered by the auditors.

"I can't overstate the value Onapsis Assess has provided when it comes to controls testing. We used to spend over fifty hours a quarter manually going into each of our systems and checking off on a list of controls. We can now do those checks for our ENTIRE LANDSCAPE in about five minutes. Plus, we have Onapsis Defend running so we get alerted if there are any changes or user activity that might be a violation of those controls. Onapsis has completely reinvented our process for testing controls. We're so much more confident going into an audit that there won't be any unexpected findings."

After

CHALLENGE	SOLUTION
Validating SAP's Security Notes Application & Knowing Which Non-HotNews Notes to Request: The utility company needs a way to ensure that SAP continues to meet their obligations regarding implementing HotNews Notes to DEV. They also need a way to know which non-HotNews Notes to request that SAP implement.	The team will use **Onapsis Threat Intel Center's** monthly Patch Tuesday report to view that month's list of relevant Security Notes for the landscape, allowing them to quickly identify if any HotNews notes are missing from any DEV systems and easily communicate this to SAP. The Threat Intel Center will also guide them on which non-HotNews Notes they need to request from SAP.
Maintaining Security Notes SLA: The utility company needs a way to easily see if their SLA of no missing HotNews or High Priority Security Notes across their entire landscape is being met and communicate any missing notes to SAP.	The utility company will use **Onapsis Assess** automated vulnerability scans to identify and understand any missing Notes across their systems, allowing them to quickly see if they are missing any HotNews or High Priority Notes and inform their requests to SAP.
Ensuring Applications Remain Securely Configured: Application configuration is the responsibility of the RISE customer, so the utility company needs a way to identify configuration drift or any new misconfigurations that have been discovered since the applications were built.	The utility company will run **Onapsis Assess** automated vulnerability scans monthly to identify any new misconfigurations across their landscape. They will set up Assess alerts so they are notified if anything is discovered.
Ongoing Monitoring for Suspicious or Unauthorized User Behavior: With hundreds of users performing countless activities in SAP every day, the utility company needs a way to easily monitor this activity for anything unauthorized or suspicious.	**Onapsis Defend** will run 1000+ user detection rules against the utility company's application logs to detect indicators of account compromise or behavior anomalies. They will receive targeted alerts for the most suspicious behavior with anomaly scores to help them find potential threats or control violations even faster.
Monitoring for Exploit Activity Before Patches Can Be Applied: While the utility company waits for SAP to implement Security Notes to DEV, or in cases where the Note will never be applied, they need a way to address this risk of open vulnerabilities in their systems.	**Onapsis Defend** uses 600+ exploit rules and targeted alerts for the fastest exploit detection possible. **Defend's** ruleset is regularly updated, including after every Patch Tuesday and zero-day rules to provide protection before Security Notes are made available.
Keeping up with the latest threats to SAP: The utility company needs to "future-proof" their security investments and be confident that they will be able to detect and respond to the latest vulnerabilities and threat actor TTPs as they arise.	**All Onapsis products** are regularly updated with the latest vulnerability and threat intel from the Onapsis Research Labs. The utility company will also leverage the **Onapsis Threat Intel Center, Defend's pre-patch protection, and expert briefings** for details on the biggest security news from the Onapsis Research Labs.
Securing New RISE Assets: The utility company needs to be able to easily expand their security scope to cover new systems as needed, such as SAP BTP which is already on their roadmap.	**Onapsis products** provide the most comprehensive coverage of the SAP landscape and tech stack available in the market today. The utility company will easily be able to bring new systems and capabilities, including **SAP BTP**, into their existing SAP vulnerability management, application security testing, and continuous security monitoring programs.

Conclusion

With the Onapsis partnership, the utility company saw great success by starting early and building security into their **RISE with SAP** transformation project. The risk-based analysis, automated processes, and expert guidance provided by Onapsis not only de-risked the project and improved overall security, but also offered significant time and cost savings.

The partnership helped them finish the project ahead of schedule with practically no delays due to security or compliance issues, and they will continue to leverage **Onapsis RISE** experts and technology to ensure their expanding RISE landscape stays clean and protected.