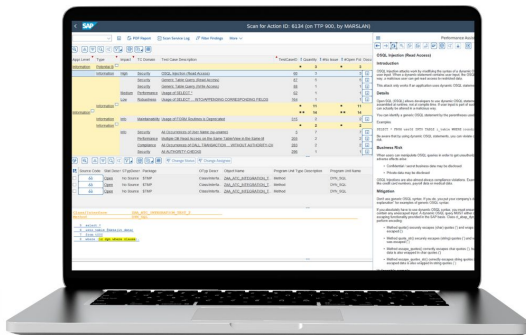




Datasheet

Onapsis Control

Establish better DevSecOps for SAP and accelerate RISE projects with the most comprehensive application security testing available for SAP. Our automated code scans secure both human- and AI-generated code across more languages, platforms, and IDEs than any other vendor. Control keeps SAP application development moving and mitigates unexpected, costly delays.



“Onapsis helps us gain deeper visibility into code and transport vulnerabilities so we can prioritize our mitigation efforts and reduce risk to our systems.”

– Director SAP Application Development, Fortune 100 Manufacturing Company

Organizations are increasingly focused on hardening their applications against attack, starting with the development process. A research¹ demonstrated a 400% increase in ransomware incidents that involved compromising SAP systems and data at victim’s organizations within three years. This increased threat level is especially concerning because these business-critical SAP applications contain highly valuable corporate data and support the essential operations of the enterprise.

These applications are also at the core of digital transformation projects, such as RISE with SAP. To accelerate these initiatives, organizations increasingly rely on AI-generated code. However, migrating legacy systems and securely building SAP custom applications remains a challenge. Relying on highly error-prone manual reviews, often a fallback due to a lack of automated testing solutions for SAP environments, is not sustainable.

The rapid pace of transformation forces teams to balance speed and security—with security frequently tabled to meet tight deadlines. This pressure drives the adoption of third-party code libraries and AI tools like SAP Joule or SAP Build Code to maximize productivity. Yet, this introduces new risks. With limited visibility into huge volumes of external or AI-authored code, organizations face a growing backlog of manual reviews to prevent new security vulnerabilities.

Onapsis Control addresses these challenges by delivering the most comprehensive, award-winning application security testing available for SAP. It seamlessly integrates into existing workflows to scan code in Dev (within IDEs and SAP Build Code), at rest (in Git repositories), and in motion (across CI/CD pipelines). By automatically scanning and fixing code from all sources—whether internal, third-party, or AI-generated—Control ensures consistent security, accelerating and de-risking your RISE with SAP projects.



¹[Ch4tter: Threat Actors Attacking SAP for Profit](#)

How Onapsis Control Works

Centrally deployed and managed, Onapsis Control works by inspecting code directly within integrated development environments (IDEs and SAP Build Code) or code repositories such as Git. Control flexibly scans code across multiple stages: inline as developers work, via large batch scans of projects and packages—including high volumes of AI-generated code—or embedded within your change management and transport processes. With a focus on vulnerable, insecure code, Control leverages extensive test cases across multiple domains based on best practices and in-depth SAP security research from the Onapsis Research Labs.

Millions of lines of code can be automatically scanned in minutes, and remediation guidance is provided to keep pace with accelerated development cycles. You can leverage automatic bulk code identification and empower developers with step-by-step guidance to resolve code errors efficiently before deployment.

Security And Compliance

Onapsis' highest priority is the security of our software and the confidentiality, integrity, and availability of customer information as it flows through that software. We embed the strongest possible security measures into our software development life cycle (SDLC) and into the operating system, database, web security, and logging layers of our products. Onapsis contracts with accredited, third-party, auditing companies who have audited our SDLC process and we have the following certifications: ISO 9001, ISO 20243:2018, ISO 27001:2013, SOC 1 Type 1/2, SOC 2 Type 1/2, and Veracode Verified Program. Our product design and development requirements follow the OWASP ASVA v4 framework or other industry standard guidelines.

Onapsis Professional Services

Achieve your business objectives at every stage of your journey. Onapsis' comprehensive professional services offerings target:

Implementation: A paired delivery approach to accelerate time-to-value

Education: Knowledge for teams to successfully operate our platform

Optimization: Enable continuous improvement and alignment to business needs

Administration: Alleviate resource constraints

Onapsis Research Labs

The award-winning Onapsis Research Labs is a team of cybersecurity experts who combine in-depth knowledge and experience to deliver security insights and threat intel affecting mission critical applications from SAP, Oracle, and SaaS providers. They have discovered over 1,000 zero-day vulnerabilities and multiple critical global CERT alerts have been based on their novel research. Onapsis automatically updates its products with the latest threat intelligence and other security guidance from the Onapsis Research Labs. This provides customers with advanced notification on critical issues, comprehensive coverage, improved configurations and pre-patch protection ahead of scheduled vendor updates.

Licensing

Onapsis Control offers extensive flexibility in licensing, allowing organizations to customize their Control Central package based on targets, landscape, and preferred languages. All licenses are available as annual subscriptions based on the number of target systems. Subscriptions include access to all updates available for the respective software license, technical support, and a dedicated account manager.

Expand and enhance your Control Central deployment with the following add-ons:

Git Repository Scanning

Licensed by annual per-customer subscription, it provides batch scanning capabilities by connecting directly to Git repositories, ideal for modern DevOps workflows. It scans ABAP and UI5 repositories (supporting GitLab, GitHub, Azure Repos and Bitbucket for gCTS, abapGit and SAPUI5), showing results on an independent web UI.

Pipeline Integrations

Licensed by annual per-customer subscription as an Add-on for Git Repository Scanning, it enables seamless integration into CI/CD pipelines, supporting Azure Pipelines, SAP Project Piper, SAP Continuous Integration and Delivery Service, and SAP Cloud Transport Management service (cTMS). It scans related ABAP and UI5 CI/CD pipelines, stopping the build process for mandatory findings and showing results on an independent Scan Service Web UI.

On Change Control

Licensed as an annual subscription based on the number of target systems, it provides a detailed security scanning and approval framework for change management that integrates with SAP® ChaRM. It offers a single view of detailed security scans, approvals, and notes related to system changes in addition to improving approval and process workflows with automatic notifications, secondary approvals, and more.

The Onapsis Platform

Onapsis Control is one-third of the Onapsis Platform. The Platform provides complete attack surface management for ERP landscapes, focused on business-critical application security that directly target interconnected risk - vulnerability management, threat monitoring, compliance automation, and application security testing.

Onapsis is proud to be an Oracle partner and the only application security and compliance vendor invited to the SAP Endorsed Apps Program.



Table 1: Onapsis Control Central Features and Benefits

Description	Benefits
Highly secure, lightweight architecture (NGA) centered around a single, unified virtual appliance.	Deployed as Infrastructure as Code (IaC), this automated, fully code-deployable infrastructure enables rapid setup and fast time-to-value. Organizations benefit from a significantly lower Total Cost of Ownership (TCO), reduced operational complexity, and considerable savings in maintenance and administration.
Centralized Management with Lightweight Sensors	Control Central is centrally managed from one centralized system, drastically reducing deployment and maintenance times as well as load on satellite scanned systems. User access, policies, and test cases are centrally managed as well, enabling organizations to ensure consistency and quality from their code scanning and QA regardless of who is coding or where the code rests.
Out-of-the-Box Custom Code Scans	Save time by scanning millions of lines of code in minutes for ABAP, Fiori, and HANA Native applications. Scans performed for HANA Native include code languages such as SAPUI5, CDS, and XSJS. Scans performed for Fiori include code languages such as ABAP and SAPUI5. New ABAP syntax is supported as well as older objects such as SAP LSMW.
Multi-layered Scan Engine	Powerful scan engine that employs multiple scanners running in parallel with hundreds of automated, predefined test cases across a wide swath of use cases. Prioritize code issues based on probability and impact to accelerate your time-to-resolution. Can be connected with SAP Cloud Connector.
Onapsis Global Data and Control Flow Analysis	Onapsis' patented analysis capabilities deliver more accurate detection and significantly lower rates of false positives for code issues, saving valuable time and resources for application development teams.
SAST (Static Analysis)	Based on patented global data and control flow analysis
DAST (Dynamic Analysis)	Identifies vulnerabilities that are not part of the expected result set including incomplete/erroneous code
IAST (Interactive Analysis)	Continuous process custom built to check code in SAP development environments against analysis engine for processing in runtime environment
Support for RISE and SAP Business Technology Platform (BTP)	Delivers robust code scanning capabilities for code in development, at rest, and in transit for SAP BTP, including support for ABAP, ABAP Cloud, UI5, and more. Integrates directly with SAP-BTP-recommended IDEs such as Eclipse with ABAP Development Tools, Microsoft Visual Studio Code, and SAP Business Application Studio in BTP. Requires specific licensing for SAP BTP.
Git Repository Scanning	Scans custom ABAP, ABAP Cloud, UI5, and other non-ABAP code for S/4HANA and BTP development, residing in Git repositories. It integrates with GitLab, GitHub, Azure Repos, and Bitbucket for technologies like abapGit, gCTS, and SAPUI5. Requires specific licensing for Git repositories.
CI/CD Pipeline Integrations	Enables seamless integration for automated scanning within popular CI/CD pipelines, including SAP Project Piper, Azure DevOps, SAP CI/CD Service, and SAP cTMS. This capability is offered as an add-on to Git Repository Scanning.

Table 1 (Continued): Onapsis Control Central Features and Benefits

Description	Benefits
Broadest Set of Predefined Test Cases Across Multiple Domains	Hundreds of test cases are available out-of-the-box and maintained by the SAP security experts at Onapsis. Test case domains include but are not limited to security, compliance, data loss prevention, code performance, robustness, and maintainability.
Market-Leading Support for SAP Development Environments	Use Control Central wherever you currently develop applications, including support for SAP ABAP Development Workbench, Eclipse with ABAP Development Tools, Microsoft Visual Studio Code, and SAP Business Application Studio (BTP).
SAP Application Process Integrations	Seamless integration with SAP ABAP Test Cockpit (ATC), SAP Change Request Management (CHaRM), and SAP Transport Management System (TMS)
Premium Add-on License: On Change Control	A detailed security scanning and approval framework for change management that integrates with SAP Change Request Management (CHaRM)

Table 2: Onapsis Control Central Components and Description

Technology Component and Description	Details
Scan Service: Scans custom source code for security vulnerabilities. Clients communicate with the Scan Service through a REST API	Minimum Hardware Requirements: CPU: AMD64/EM64T 64-bit mode compatible multi-core CPU (eight-core minimum) Hard Disk: 128 GB hard disk space (above what is required for the operating system) RAM: 32 GB Software Requirements: Ubuntu 22.04/24.04 or Red Hat (RHEL) 9 Java 17 or 21 OpenSSL 1.1.1n SAP JCO library files for Linux (64-bit) version 3.1.2 or higher
SAP Systems: Supported Versions for Control Central System (The Hub) Requirement: Must be a Unicode SAP system	S/4HANA (1909 through 2025) S/4HANA Foundation (any version) ABAP Foundation on HANA (any version) S/4HANA Cloud Extended Edition (EX)
SAP Systems: Supported Versions for Control Client System (Satellite Systems)	SAP NetWeaver 7.40 (BASIS_RELEASE 740 SP 17+) or higher S/4HANA (1709 through 2025) S/4HANA Foundation (any version) ABAP Foundation on HANA (any version) S/4HANA Cloud Extended Edition (EX)