

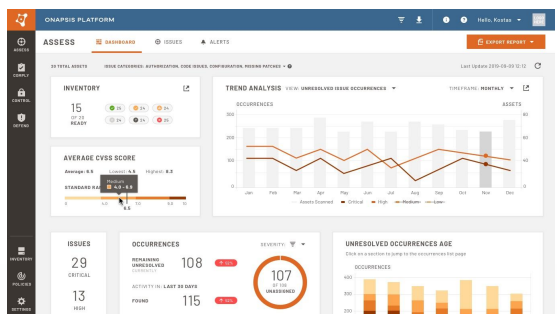


Datasheet

Onapsis Assess

Next-gen exposure management for business-critical SAP applications.

Identify and prioritize risk across your SAP landscape with AI-powered contextual analysis and real-time threat intelligence. Focus on what matters most, accelerate SAP hardening, and leverage trusted application intelligence to power emerging agentic security orchestration.



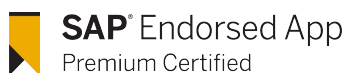
“Onapsis removes the mystery around SAP security by increasing visibility. We can see issues — misconfigurations, missing patches or unusual user activity — what risk they pose and how to fix them.”

– Enterprise Security Manager,
Fortune 500 Utility Company

Business-critical SAP applications are the core engines of the modern enterprise, supporting financial, supply chain, and HR processes. But as SAP landscapes become increasingly interconnected and cloud-connected, their attack surface is expanding and so is the volume of risk organizations must manage. AI-powered scanning tools are accelerating vulnerability discovery, while threat actors increasingly target application-layer weaknesses as a direct path to sensitive business assets. Security teams need a way to separate meaningful SAP exposure from the noise and respond with speed and precision.

Traditional, patch-forward vulnerability management makes that difficult. SAP exposure goes well beyond missing patches, spanning misconfigurations, authorization and user settings, custom code, and other application-level issues. Security teams need to understand these issues in the context of their specific environment and the ways threat actors are targeting SAP applications to know which exposures demand attention first. Without that context, prioritization becomes difficult and remediation slows.

Onapsis Assess directly addresses this gap with purpose-built exposure intelligence for SAP. Powered by insights from Onapsis Research Labs, Assess provides comprehensive visibility across the SAP landscape and combines customer-specific environmental context with real-time threat intelligence to isolate the exposures that matter most. Trusted, high-fidelity insights and precise, actionable guidance help InfoSec and IT/Basis teams align on priorities, accelerate remediation, and systematically harden application and user configurations. This same intelligence provides the foundation for safely integrating SAP into emerging agentic security and orchestration workflows.



How Onapsis Assess Works

Assess runs scans with preset and customizable policies and modules which search assets for a comprehensive and regularly updated set of known issues, including missing patches, unsecured or incorrect configurations, risky user authorizations/permissions, and issues in deployed custom code*. With any licensed Comply pack, Assess can run scans for compliance with IT General Controls related to various regulations and frameworks, such as Sarbanes-Oxley, GDPR, and NIST. Custom policies and modules allow alignment with organizational policies and best practices. The results are displayed in a single dashboard to prioritize risks and identify action for mitigation. Each identified issue contains an explanation of the business impact, severity, contextual risk score, and remediation steps for resolution.

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.

Deployment Options

Onapsis Assess can be deployed on-premises, in your cloud environment (all major cloud providers supported), or in the Onapsis cloud environment, as SaaS. Technical components needed to support each deployment type are described in Table 2.

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 SAP applications. 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.

*Requires Assess for Code license

Licensing

Onapsis Assess is licensed as an annual subscription based on the number number and type of target systems. Licenses include:

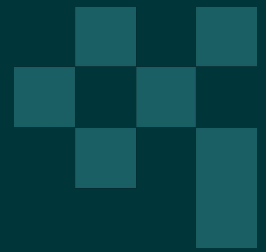
- Assess for ABAP*/JAVA/BOBJ systems
- Assess for SAP HANA systems
- Assess for SAP BTP (incl. Cloud Connector)
- Assess for SAProuter
- Assess for SAP SuccessFactors
- Assess for SAP Web Dispatcher

Subscription includes access to all updates available for the respective software license, technical support, and a dedicated account manager.

*Onapsis Assess for ABAP currently features two license tiers - Assess and Assess Baseline. The Assess Baseline license focuses on helping customers jumpstart their exposure management process quickly and easily by addressing issues aligned with the officially published SAP Security Baseline Template and supported by the insights of the Onapsis Research Labs.

Expand and enhance your Assess deployment with additional, premium capabilities:

- **Assess for Code:** Licensed as an annual subscription based on the number of target systems, this provides access to vulnerability scanning for issues in custom code previously deployed to production. InfoSec teams gain much-needed visibility into security issues within custom code and a more complete view of the SAP application attack surface.
- **Comply Packs:** Licensed as an annual subscription based on the number of target systems, these policy packs provide right-sized, frictionless audit packs that automatically audit ERP IT general controls against various regulatory requirements, eliminating 1000s of hours of manual work. Available policies include Sarbanes-Oxley (SOX), Data Privacy (GDPR), NIST/ISO (ISO:27001, NIST 800-53, NIST 800-171), NERC CIP, and PCI.
- **Threat Intel Center:** This subscription license grants access to a centralized repository of new and ongoing threat research and adversary behavior, directly from the Onapsis Research Labs, within the Onapsis Platform. Get high-impact overviews of latest attack campaigns, Onapsis honeypot observations and threat activity, monthly Patch Tuesday analysis, and more. Plus, get an immediate read on your organization's exposure with a consolidated view of affected assets and potential Indicators of Compromise^.



The Onapsis Platform

Onapsis Assess 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 targets interconnected risk - exposure management, threat monitoring, compliance automation, and application security testing.

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



^Requires Defend license

Table 1: Onapsis Assess Features And Benefits

Description	Benefits
Agentless Scanning	Onapsis unified appliance, deployed on premises or in the cloud, provides deep scanning of assets at system, application and code levels and analyzes system vulnerabilities without sacrificing system performance.
Out of-the-Box Vulnerability Scanning	Thousands of vulnerability checks are ready to go out of the box and are grouped into standard policies based on target system, allowing for full vulnerability scanning of your business-critical applications, including assets like SAProuter, SAP Web Dispatcher, SAP Business Technology Platform (BTP) & Cloud Connector.
Custom Policy Creation*	Users can create custom policies to include the set of vulnerability checks that meets their needs.
Standard and Custom Vulnerability Checks*	Onapsis provides predefined vulnerability checks, called modules, but also enables the ability to define custom checks.
Unified Single Dashboard	Shows issue data and trends from recent scans, with graphical visualizations to provide quick insights into system issues.
SAP Notes Command Center	Provides centralized management and dynamic views of SAP Note implementation status across the entire landscape. This focused visibility accelerates patching by making it easier for customers to scope, prioritize, assign, and validate patching efforts.
Contextual Risk Scoring	Each issue occurrence includes a multi-factor risk score to facilitate prioritization. The risk score is based on several characteristics of the occurrence, including severity, asset role, age, category, the availability of a public exploit, and whether a compensating control is currently in place via Onapsis Defend.
Risk and Remediation Guidance	Detailed explanations of the business impact of identified problems within each system, along with an associated risk score and step-by-step remediation instructions, accelerates time to resolution.
Integrated Workflows and ITSM Integration	Built in workflow capability allows for issue assignment and acceptance either manually via an automated workflow engine. Integration with IT Service Management tools enables automatic ticket creation for faster remediation.
Onapsis Agentic Gateway	A standardized interface based on the Model Context Protocol, allowing corporate-sanctioned AI agents (e.g., Microsoft Copilot, Anthropic Claude, Google Gemini, OpenAI ChatGPT, and custom-built agents) to securely invoke Onapsis' trusted, deterministic application data and fuel agentic workflows for autonomous SAP application security and compliance.

*Not available with Assess Baseline license

Table 1 (Continued): Onapsis Assess Features And Benefits

Description	Benefits
Onapsis Security Advisor	Leveraging AI and 16+ years of Onapsis' security data and expertise, this feature acts as a personalized security advisor, helping IT and security leaders assess and improve their SAP security posture. It establishes better security goals, guides ERP security journeys, and tracks progress against baselines and industry peers. Trended metrics and benchmarking save you time on reporting, make it easier to prove value, and simplify budget justification.
Onapsis Research Labs Threat Intelligence	Vulnerability checks are regularly updated and added based on the latest investigation results from the Onapsis Research Labs.
Exportable Executive Reports	Summary reports demonstrate current risk standing, status over time, and mitigation efforts, allowing results of exposure management efforts to be more easily shared with stakeholders across the business.
Custom Reporting	Create custom reports via the Onapsis Platform API in order to share reports regarding risk posture trends and assessments.
Premium Add-on License: Assess for Code	Extends vulnerability scanning to custom code deployed to production. This gives security teams a more complete view of their SAP application attack surface.
Premium Add-on License: Onapsis Comply packs*	Adds right-sized, frictionless SAP audit packs to the Assess scanning engine to automatically test ITGCs against popular regulatory frameworks.
Premium Add-on License: Threat Intel Center*	Delivers a regularly-updated and centralized library of new and ongoing threat research and adversary behavior, directly from the Onapsis Research Labs, within the Onapsis Platform. The Threat Intel Center provides high-impact overviews of the latest attack campaigns, Onapsis honeypot observations and threat activity, monthly Patch Tuesday analysis, and more. And, it provides an immediate read on your organization's exposure with a consolidated view of affected assets and potential Indicators of Compromise [^] . With the Threat Intel Center, you get a real-time look at what threat actors are actively targeting right now and where you're exposed, so you know exactly where to focus your efforts.

*Not available with Assess Baseline license

[^] Requires Defend license

Table 2: Onapsis Assess Technology Components and Description

Technology Component and Description	Details
Business Critical Systems Supported	All SAP applications that run: - SAP NetWeaver - ABAP - SAP NetWeaver - JAVA - SAP HANA Database - SAProuter - SAP SuccessFactors - SAP Business Objects (BOBJ) - SAP Business Technology Platform (BTP) - SAP Cloud Connector - SAP Web Dispatcher
Onapsis Unified Appliance: Provides the management and reporting interface for the Onapsis Platform. Can be deployed on premises or in the cloud.	Requirements for standard deployment[^]: Supports: up to 200 target assets (e.g., SAP SIDs) vCPU: 16 Cores Memory: 64 GB Swap Space: 32 GB Storage: 200 GB [^]Sizing can be scaled up or down based on your SAP footprint
Onapsis Platform Connector: A lightweight, cloud-connector-style architecture delivers secure, agentless monitoring across segregated network segments without the burden of heavy virtual machines.	Operating system: Enterprise Linux via RPM package CPU: 1x vCPU RAM: 0.5 GiB minimum Storage: No specific disk space requirement due to its lightweight nature
Virtualization Technology: The Onapsis Unified Appliance is delivered as a fully self-contained package that includes both the OpenSUSE operating system and the Onapsis solution. No additional OS is required.	Available in the following formats: - On-premises: Open Virtualization Appliance (OVA) file - Cloud deployments: Cloud-native machine image Supported cloud platforms: Amazon Web Services (AWS), Microsoft Azure, and Google Cloud Platform (GCP)
Browser Compatibility	Supported browsers: - Google Chrome* - Microsoft Edge - Mozilla Firefox - Apple Safari *recommended