ONAPSIS

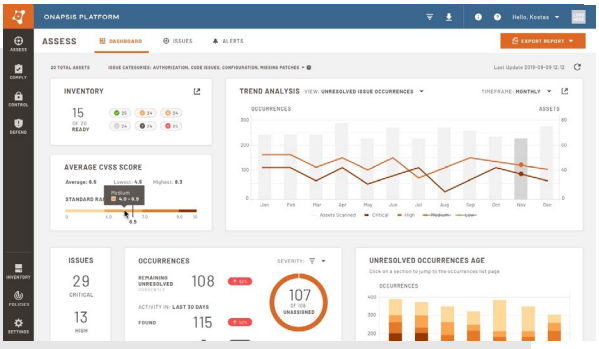
DATASHEET

ONAPSIS ASSESS

Vulnerability management for business-critical applications such as SAP and Oracle, including deep visibility into the entire application landscape, automated assessments with detailed solutions and descriptions of associated risk and business impact.

VISIT US AT WWW.ONAPSIS.COM

> 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 applications are the lifeblood of an organization, supporting financial, supply chain, sales, and other business processes. An attack against them has the potential for a devastating impact across the organization. Traditionally, organizations have relied on a "defense-in-depth" security model to protect these critical systems. Unfortunately, this layered approach is no longer sufficient for many reasons, including modernization and digital transformation initiatives eroding the perimeter.

However, InfoSec professionals are still responsible for evaluating their organization's risk and overall cybersecurity posture, including vulnerability management and application security. They frequently lack visibility into their organization's most critical business applications because the tools they traditionally rely on don't adequately cover these systems. Security administrators are typically responsible for vulnerability management for the business. However, their tools don't cover business critical applications and they often rely on cohorts within application teams for remediation.

A lack of visibility and tools aren't the only challenge, the applications themselves are also complex. The frequency of releases, the complexity of patching processes, and size of application landscapes mean enterprises are facing a growing backlog of patches and lack prioritization tools.

Onapsis Assess directly addresses these challenges for enterprise teams. It provides focused and comprehensive vulnerability management for business-critical applications like those from SAP and Oracle. It provides deep visibility into the entire application landscape, automated assessments with detailed solutions, and descriptions of associated risk and business impact. Onapsis Assess aligns InfoSec and IT Teams and lets them make empowered decisions on how to respond to incidents, reduce investigation and remediation times, and achieve greater risk reduction with less effort.

ONAPSIS

HOW ONAPSIS ASSESS WORKS

Sensors are deployed - either on-premises or in the cloud - which provide deep scanning of assets at the system, application, and code level. Assess runs scans with preset and customizable policies and modules which search assets for a comprehensive and regularly updated set of known issues, missing patches, vulnerabilities, and zero-days. 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 vulnerability identified contains an explanation of the business impact, a 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 27001:2013, SOC 1 Type 1, SOC 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 on Onapsis cloud environment, as a SaaS. Technical components needed to support each deployment type are described in Table 2 below.

LICENSING

Onapsis Assess is licensed as an annual subscription based on the number of target systems. Subscription includes access to all updates available for the respective software license, technical support, and a dedicated account manager. Onapsis Assess currently features two license tiers - Assess and Assess Baseline. The Assess Baseline license focuses on helping customers jumpstart their vulnerability 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.

Additional premium licenses for Onapsis Assess are available to extend its capabilities:

- Threat Intel Center: This subscription license grants access to a centralized repository of new and ongoing threat research, directly from the Onapsis Research Labs, within the Onapsis Platform. The Threat Intel Center provides a detailed, high-impact view of the evolving SAP threat landscape with one-click access to a comprehensive research library within the Onapsis Platform.

THE ONAPSIS PLATFORM

Onapsis Assess is part of the Onapsis Platform. The Platform focuses on four pillars of business-critical application security that directly targets interconnected risk - vulnerability management, threat monitoring, compliance automation, and application security testing.

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, Salesforce and others. They have discovered over 800 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.

ONAPSIS

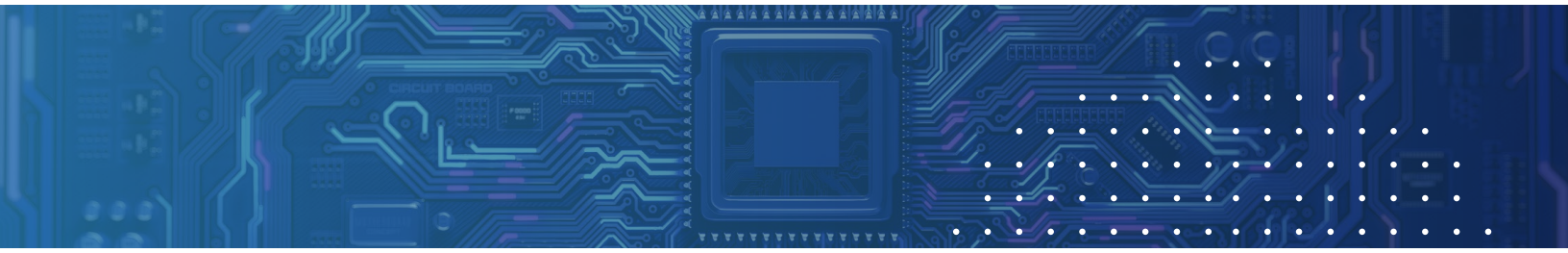


TABLE 1: ONAPSIS ASSESS FEATURES AND BENEFITS

Feature	Description and Benefits
Agentless Scanning	Virtual devices are deployed on premises or in the cloud to provide deep scanning of assets at system, application and code levels and analyze 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 the target system (e.g., SAP, Oracle), allowing for full vulnerability scanning of your business-critical applications
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.
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, accelerate 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.
Exportable Executive Reports	Summary reports demonstrate current risk standing, status over time, and mitigation efforts, allowing results of vulnerability 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.
Onapsis Research Labs Threat Intelligence	Vulnerability checks are regularly updated and added based on the latest investigation results from the Onapsis Research Labs.
Premium Add-on License: Threat Intel Center	Delivers a regularly-updated and curated library of new and ongoing threat research, directly from the Onapsis Research Labs. The Threat Intel Center provides one-click access to comprehensive research designed for both the education of cybersecurity team members and providing organization-specific business impact for cybersecurity leaders.

*Custom policies and modules not available with Assess Baseline License

ONAPSIS

TABLE 2: ONAPSIS ASSESS TECHNOLOGY COMPONENTS AND DESCRIPTIONS

Technology Component and Description	Details
Business Critical Systems Supported	**All SAP Applications that run**: SAP Netweaver - ABAP SAP Netweaver - JAVA SAP HANA DataBase SAP SuccessFactors SAP Business Objects (BOBJ) **Oracle E-Business Suite (EBS)**
Console for Onapsis Platform On-premises: Onapsis Virtual Appliance provides the management and reporting interface for the Onapsis Platform and control for all sensors. Can also be deployed in the cloud.	**Hardware requirements:** HD: 200 GB CPUs: 8 cores (2+GHz) 16 recommended RAM: 16 GB
Sensors for Onapsis Platform On-premises: Onapsis Virtual Appliances, virtual "headless" devices that perform workloads to find and analyze system vulnerabilities. Each installation requires at least one sensor. The number of sensors needed is based on landscape size, complexity, and network segmentation. The sensor receives updates from the console. Can be deployed on premises or in the cloud.	**Hardware requirements:** HD: 200 GB CPUs: 8 cores (2+GHz) 16 recommended RAM: 16 GB
Virtualization Technology: The console and sensor(s) are delivered in a pre-built virtual appliance in Open Virtualization Appliance (OVA) format. The OVA is self-contained and includes a Linux-based OS and the Onapsis solution.	**Supported virtualization platforms:** VMware KVM Microsoft Hyper-V Supported cloud platforms: Amazon Web Services (AWS), Microsoft Azure and Google Cloud Platform (GCP)
Onapsis SaaS Connector: Required for SaaS deployments; allows the Onapsis Platform to interact with your systems.	**Technical requirements:** Ubuntu 20.04 CPUs: 1 RAM: 1 GB
Browser compatibility	**Supported browsers:** Google Chrome* Microsoft Edge Mozilla Firefox Apple Safari *recommended

Version Date - 11.18.2022