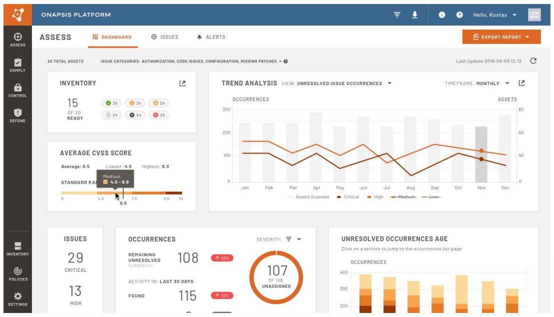
ONAPSIS

Datasheet

Onapsis Defend

Continuous threat monitoring and pre-patch protection for business-critical SAP applications.

Customizable research-based alerts, anomaly detection, descriptions of root cause, and remediation guidance accelerate analysis and incident response.



> “By integrating Defend with IBM QRadar...our SOC teams are armed with the information they need to understand the threat and what corrective actions to take.”
>
> — Global Lead of SAP Operations, F500 Biopharmaceutical Co.

Business-critical applications are the lifeblood of an organization, supporting financial, supply chain, sales, and other business processes. Security teams have traditionally relied on defense-in-depth strategies in an attempt to protect the application layer. Unfortunately, this layered approach is no longer sufficient for many reasons, including digital transformation and modernization initiatives eroding the perimeter. Adding insult to injury, most enterprises lag behind in applying important patches to their most critical systems.

The result is that the critical application layer is now more exposed than ever before. Threat actors have taken notice, targeting this layer directly through a variety of attack vectors and at an accelerated pace. To protect their critical business operations and data, organizations need continuous threat monitoring designed specifically for these applications. Existing defense-in-depth models surround, but ultimately neglect this layer, creating a large security blindspot. Without this visibility and context, organizations are unable to identify potential threats, understand the risk, and effectively protect their ERP systems.

Onapsis Defend uniquely addresses these challenges by enabling continuous threat monitoring, detection, and response for business-critical applications. Powered by the industry-leading Onapsis Research Labs, Defend acts as an early warning system for unauthorized changes, data access/extraction, misuse, or cyberattacks targeting these applications. Security Operations Centers (SOCs) can automatically monitor for more than 2,500 threat indicators, including exploit activity against zero-days and known, unpatched vulnerabilities, providing “pre-patch” protection for an organization’s critical systems. Real-time alerts, easily integrated into SIEMs, provide valuable details on severity, anomaly score, root cause, and recommended remediation steps. These context-rich incident alerts turn SOC teams into instant SAP experts. Defend empowers teams to accelerate analysis and incident handling to support meeting new disclosure timelines (e.g., NIS2, SEC) and minimize minimize potential DLP violations, the risk of IP theft, related compliance costs, and reputational damage .

SAP® Endorsed App
Premium Certified

How Onapsis Defend Works

Sensors are deployed - either on-premises or in the cloud - to target SAP systems. Defend discovers critical assets across the full landscape and extracts data to analyze for notable security events and user activity. Full visibility into the details of each incident includes the context, severity, anomaly score, root cause, and recommended action for remediation. Incidents can be managed within the console or assigned to external tools and shared with additional stakeholders. The integration framework and configuration interface allows system incidents within SAP to be exported into SIEM and syslog tools for further investigation.

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

- Defend for SAP ABAP/JAVA systems
- Defend for SAP HANA systems
- Defend for SAP BTP
- Defend for SAProuter

Subscription includes access to all updates available for the respective software license, including Onapsis Research Labs threat insights, technical support, and a dedicated account manager.

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

- **Network Detection Rule Pack:** This subscription license grants access to regular updates of Snort®* rules for the most critical and network-detectable threats. These vendor-agnostic rules can be imported across an enterprise security stack into existing network security products to provide organizations with an additional layer of defense.
- **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 Defend 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 platform invited to the SAP Endorsed Apps Program.

* Snort is a registered trademark of Cisco. All rights reserved.

Table 1: Onapsis Defend Features And Benefits

Description	Benefits
Detection Rules	2,500+ detection rules across a wide range of SAP assets (e.g., ABAP, JAVA, HANA, SAProuter, SAP BTP) identify notable security events, including inappropriate privilege escalation, system misconfigurations, indicators of compromise or known exploits, dangerous RFC or program executions, data/table downloads, user access misuse or abuse, and more.
Zero-Day Detection Capabilities	Detection rules triggered by the potential exploitation of vulnerabilities for which SAP has not yet released a security note ('patch"), and which have not been publicly disclosed. This gives users protection from attacks against critical vulnerabilities as early as possible.
Predefined Incident Profiles	Defend includes several predefined incident profiles to help users get started with monitoring SAP systems. These profiles will create an incident to notify users when the actions specified in the profile have occurred on the targeted assets (e.g., an intrusion attempt or other negative behavior).
Customizable Incident Profiles	Define the criteria used to trigger incident notifications, so users are only alerted to activity that they have deemed significant enough to require notification, immediate action, or further investigation. This includes customization to mitigate threats related to user actions such as key operations, authorization assignments, and data downloads.
Root Cause Identification and Recommended Actions	Incident context, severity, root cause, and recommended mitigation actions are provided for each event and incident to support and accelerate investigation and response efforts.
AI-based Anomaly Detection	Each recorded activity includes an anomaly score (0-100) based on machine learning models developed by the Onapsis Research Labs, with higher scores denoting larger threats and business impact. These scores can also be used to further customize and create incident profiles unique to your organization.This helps users better direct mitigation and remediation efforts to the most suspicious or anomalous threats facing their business.
Compensating Controls	Address the risk of open vulnerabilities (e.g., until patches can be applied, on older systems that aren't easily updated) by monitoring for exploit activity. Support compliance efforts and help meet regulatory requirements by adding additional controls around user access.

Table 1: Onapsis Defend Features And Benefits (Continued)

Description	Benefits
Onapsis Research Labs Threat Intelligence	Detection rules automatically incorporate the deep research from the Onapsis Research Labs. Updates with the latest threat intelligence and other security guidance from the Onapsis Research Labs are included at no cost. This provides advanced notifications on critical issues, configurations and pre-patch protection, ahead of scheduled vendor updates.
SIEM Integrations	Import Defend issues and incidents into existing SIEMs and workflows used by the SOC. The integration allows system incidents within SAP to be incorporated into the wider security management and incident response process.
Defend for SAP BTP	Continuously monitor SAP BTP subaccounts with out-of-the-box detection rules designed for BTP. Gain an early warning system for indicators of compromise or insider threat with alerts for critical configuration changes (e.g., creation of new trusted domains) and incorrect or over-privileged role assignments.
Defend for SAProuter	Continuously monitor SAProuter with out-of-the-box detection rules designed for SAProuter. Identify unapproved or unexpected changes to the Access Control List (ACL) and detect unauthorized user access faster with targeted alerts for logins by specific users, logins from external networks, and unsuccessful login attempts.
Network Detection Rule Pack	Includes regular updates of Snort* rules defined by the Onapsis Research Labs. These rules extend Onapsis threat intelligence to network security applications, augmenting their ability to detect (and potentially stop) the most critical, Onapsis-researched threats to ERP applications. Snort rules are open source and vendor agnostic, allowing broader distribution across multiple layers of an organization's defense-in-depth security stack.
Threat Intel Center	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. Consolidated results from across your Onapsis products provide a faster read on your risk and exposure, and make it easier to communicate risk with other stakeholders across the company.

Table 2: Onapsis Defend Components and Description

Technology Component and Description	Details
Supported Business-Critical Systems	All SAP applications that run: SAP NetWeaver - ABAP SAP NetWeaver - JAVA SAP HANA Database SAProuter SAP BTP
Console - Provides the management and reporting interface for the Onapsis Platform. Deployable on-premises or in the cloud.	Hardware requirements: HD: 200 GB CPUs: 8 cores (2+GHz) 16 recommended RAM: 16 GB
Sensors - Virtual devices that find and analyze systems. Deployable on-premises or in the cloud. 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.	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)
ABAP and Java Add-Ons (SAP-Certified) - Discovers ABAP and Java systems and extracts technical information for analysis in the Onapsis Platform.	The add-on runs as a component on top of your SAP systems and, therefore, does not interact with any functional (business-related) SAP modules.
Browser Compatibility	Supported browsers: Google Chrome* Microsoft Edge Mozilla Firefox Apple Safari *recommended

Table 2: Onapsis Defend Components and Description (Continued)

Technology Component and Description	Details
SIEM and Syslog Integration - Integration profiles can be created to import incident data to Security Information and Event Management (SIEM) and Syslog tools for correlation, reporting and investigations	Supported integrations with: Splunk Microsoft Sentinel IBM QRadar ArcSight Enterprise Security Manager Elasticsearch Kibana Other integrations possible if SIEM can listen for incoming syslog traffic and ingest LEEF, CEF, JSON formats.
Network Detection Rule Pack^	Vendor-agnostic, open-source rules formatted to support Snort* 2.0+

^ Requires purchase of premium add-on Network Detection Rule Pack license
* Snort is a registered trademark of Cisco. All rights reserved.