ONAPSIS

ONAPSIS DEFEND

Threat Monitoring and Pre-Patch Protection for Business-Critical SAP Applications

Continuously Monitor and Protect Your Most Important Assets from Threats

Challenge

Your Window to Defend Your Business-Critical Applications Is Shrinking

Digital transformation initiatives have left business-critical applications more exposed than ever, and this increased exposure hasn't gone unnoticed. Threat actors are targeting business-critical applications through a variety of attack vectors and at a faster pace than ever before. Attempting to monitor for threat activity by manually reviewing system logs is inefficient and requires extensive internal knowledge. Given the speed at which threat actors operate, this leaves far too much time for successful attacks to take place.

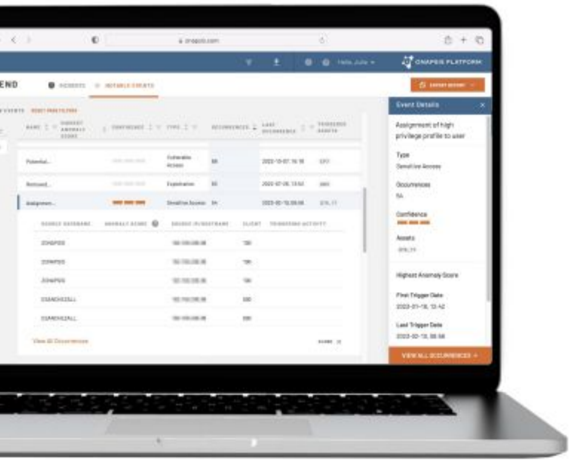
To protect their critical business operations and data, organizations need continuous threat monitoring designed specifically for these applications. They need to identify potential threats in real-time and understand the risk they pose, so they can prioritize incident response. And they need the ability to define and customize criteria for alerts, including threats related to user actions such as authorization and sensitive data access.

<3 hours

for the first exploit attempt on an unprotected system coming online [1]

<72 hours

between release of a patch and first exploit attempts [1]



The Solution

Continuous Threat Monitoring for SAP with Onapsis Defend

Powered by research and insights from the Onapsis Research Labs, Onapsis Defend uniquely provides the visibility and context security teams need to respond faster and smarter to threats targeting their business-critical applications. Onapsis is proud to be the only application security platform in the SAP Endorsed Apps Program.

- Over 2,500 detection rules specific for SAP, including zero days to protect applications from threats prior to patch release
- Detect anomalies, understand root cause and how to mitigate
- Integrate with SIEMs for SOC visibility and cross-system analysis
- Get the latest threat intelligence from Onapsis Research Labs
- Protect RISE with SAP landscapes, including SAP BTP

[1] SAP and Onapsis Threat Report

Understand Threats to Your Critical Systems

Automatically Detect Potential Threats or Suspicious Activity
Eliminate the need for manual log reviews and in-house SAP security expertise to identify threats to critical assets (e.g., ABAP, JAVA, HANA, SAProuter, SAP BTP)

Start Monitoring Immediately and Realize Value Quickly
2,500+ detection rules and 30 pre-configured alarms provide a base level of threat monitoring upon install

Ease the Burden of Security Responsibilities under RISE with SAP
Monitor your RISE landscape, inc. SAP BTP, for anomalous or unauthorized user access and behavior, real-time attacks, and zero-days

> "We're saving over 1000 hours per year by automatically monitoring user access."
>
> – F500 Apparel

Respond Faster and Smarter

> "We're saving 780 hours per year by replacing manual security controls testing."
>
> - F500 Biotech

Reduce Investigation Time and Accelerate Incident Handling
Receive real-time incident alerts enriched with root cause, severity, anomaly score, and business context to context to better guide security incident response and help your organization also meet new material incident disclosure timelines (e.g., US SEC rules, EU NIS2)

Transform SOC Teams into Instant SAP Experts
Easily send curated SAP threat activity and intelligence to your existing SIEM tools; threat explanations and remediation guidance facilitate playbook creation

Extend Onapsis Threat Intelligence to the Network Layer
Augment your existing network security products with vendor agnostic, open-source rules that alert on (and potentially stop) Onapsis-research-based network threats before they reach your ERP applications*

Reduce Risk to Critical Systems

Get the Best SAP Exploit and Zero-Day Protection
Detect more types of exploit activity with 400+ exploit rules across the SAP stack (out of our 2500+ total detection rules), including zero-day rules to protect you before patches are available

Find Suspicious User Behavior Faster
Monitor for insider threats and potential indicators of compromise with targeted alerts and user behavior analysis (UBA) to detect anomalies faster

Easily Implement Compensating Controls
Address the risk of open vulnerabilities by monitoring for exploit activity or help meet regulatory requirements by adding additional controls

> "We're confident our most important assets are protected from zero-days and other emerging threats"
>
> - F500 Chemical Company

SAP Endorsed App
Premium Certified