SOLUTION BRIEF

SecurityBridge - Interface Traffic Monitor

SAP systems exist within a complex communication network.
This combination of complexity and a lack of transparency lead to unseen attack vectors and vulnerabilities.

COMPONENTS

- Interface Traffic Monitor
- Threat Detection

SOLUTION BENEFITS

- Graphical visual showing the entire system landscape
- Easy to identify non-responding connections
- Simple to see the critical access path

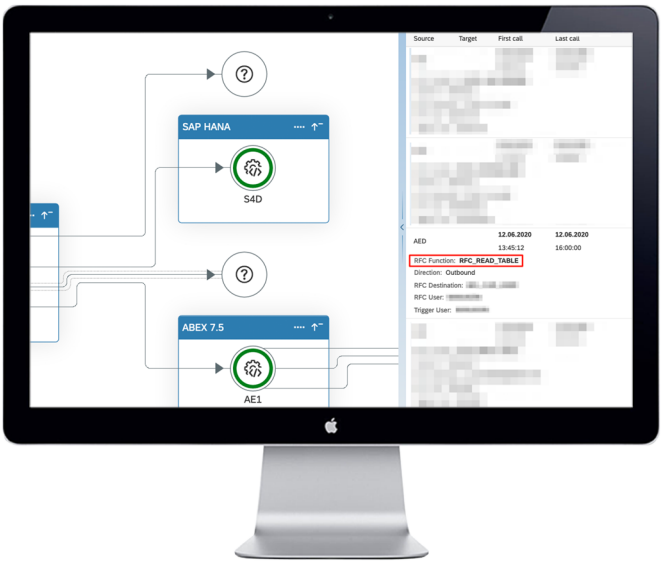
Available on the SAP App Center

Executive Summary

Undocumented or obsolete interfaces are significant security risks, while outdated and incompatible interfaces can lead to severe disruptions in business operations. With the rise of digitalization, the degree of machine-to-machine communication has increased. SAP systems process enterprise critical data that they receive or share with other systems. Robust integration, transparent monitoring and encryption of communication data is essential to ensure confidentiality, integrity, and availability. SecurityBridge Interface Traffic Monitor generates an interactive communication map which provides all the insight that is needed to implement effective governance, and to identify and eliminate existing attack vectors even in complex environments.

Solution Description

SecurityBridge deploys a holistic cyber-security platform for SAP. The solution fills the existing gap between the security departments and the SAP competence centers. While the Interface Traffic Monitor is a component of the platform, it also provides capabilities for



- Real-time Threat Detection,
- Vulnerability Management,
- Code Vulnerability Analysis,
- Patch Management for SAP.

With the help of the Interface Traffic Monitor, customers can analyze complex integration landscapes based on an interactive graphical map.

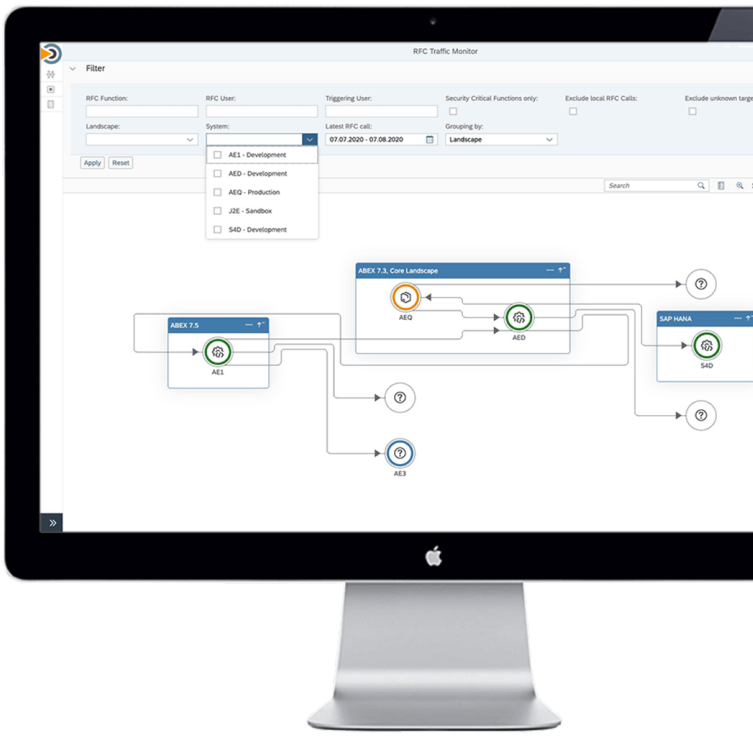
Communication between SAP systems and non-SAP can be reviewed in a very simple and transparent manner. At the click of a button, you can zoom in to find all relevant information needed to assess communication. Find direct connections between development and production stage by use of a simple to use grouping.

Solution Components

The Interface Traffic Monitor enables accurate, software-based identification of all your SAP interfaces across the entire landscape. This provides a real-time, updated view into your SAP interfaces at any time with minimal effort.

During an intrusion detection, SecurityBridge collects inbound and outbound communication. Creating the interface map does not require additional system analysis and resources, as the data needed is shared across the platform's modules.

The component is available instantly at no additional cost and integrates seamlessly with other components of the platform. An open architecture allows for the creation of an incident to document and process the findings to ensure a constant security posture.



Use-Cases

Non-responding endpoints: Attackers explore the environment to find gaps within the established lines of defense, so the risk of a successful exploitation can be minimized by reducing the attack surface. Non-responding endpoints can be used by attackers to gain access to your environment, so from a security perspective it's better to remove them.

Identify tier-up communication: A direct interaction between lower staging level systems with production instances should be avoided. Attackers frequently infiltrate low security instances to perform lateral movements until they reach valuable data.

Always Up To Date: Don't waste the limited time of highly skilled experts to manually create an interface overview. SecurityBridge Interface Monitor will do this for you, and it's always up to date.

Reach out to 1st Basis for a free demo.

Request a Free Demo from 1st Basis