SOLUTION BRIEF

SecurityBridge - Transport Center

Simplify and secure your SAP change and transport management process

COMPONENTS

- Transport Center

SOLUTION BENEFITS

- Prevent unplanned outages caused by erroneous transports
- Workflow based import approval system for immediate and release-based transports
- Use the Transport List builder for complex project cutovers
- Secure your transport deployment process
- When a transport does fail SecurityBridge enables a full rollback of the deployment

Available on the SAP App Center

Executive Summary

Configuration and development changes in SAP are applied in development and promoted to the production system using SAP standard transport requests. Attackers can use the SAP transport layer to inject malware or manipulate objects with malicious intension. Additionally, when a transport deployment fails, this can lead to functional impact to even a full system outage. Use SecurityBridge Transport Center to detect threats to your SAP systems.

Challenge

SecurityBridge Transport Center secures the SAP transport deployment process by enhancing the Transport Management System with capabilities not available in SAP. It comes with an innovative algorithm that prevents system downtimes as it detects and warns for version mismatches, downgrade protection, missing objects, configuration dependencies and much more. Using a configurable review and approval workflow, segregation of duties can be enforced before deploying changes into production. A central user interface provides a unified view for controlling complex transport landscapes. Transport Center is integrated in the SecurityBridge Platform to manage the SAP transport layer and protect it against malicious code injections or object manipulation.

Solution Description

Transport Center compliments the SecurityBridge cybersecurity platform by adding transport security and by simplifying the operational processes of SAP running enterprises. This light-weight solution adds missing features to the SAP Transport Management system.

For many years, organizations of all sizes have been relying on Transport Center to simplify their SAP transport deployment processes.

The integration of the SecurityBridge Cybersecurity platform provides a holistic combination of features:

- Seamless integration with Code Vulnerability Scanning
- Scan and report on malicious transport contents
- Real-time monitoring via SecurityBridge Threat Detection
- Comply with compliance regulations, enforce and document 4-eye approvals

Solution Components

Selected SecurityBridge Transport Center capabilities:

- **Dump Prediction:** Scan and detect transports on completeness and highlight hidden interdependencies
- **Import List Builder:** Manage and sequence complex cut-over lists, identify and resolve errors prior to project go live.
- **System Rebuilder:** Synchronize transports after a system copy with a click of a button
- **RE.Do:** A unique feature which allows rolling back a transport after it has been deployed

Use Cases

Version conflict – Developer 1 has changed object A. During the acceptance test phase, object A requires a set of corrections, executed by developer 2. If the sequence of transports is not respected at go-live, the initial version containing the identified flaws, may become active. A version conflict may result in disrupted business processes or a full system outage.

Malicious code – Transport Center introduces an additional quality gate to ensure transport requests (containing custom and 3rd party content) does not introduce unknown risks into the receiving systems. A code vulnerability scan can be activated as a prerequisite for importing new and changed code.

REQUEST-DEMO FROM 1st BASIS