

Protecting SAP applications from Malware uploads –

How **Henkel** does it with SAP VSI

Markus Hille, Henkel

Joerg Schneider-Simon, bowbridge

SAPinsider
2023



In This Session

- Learn about file-based threats to your SAP applications
- Get to know the SAP Virus Scan Interface VSI.
- Explore how Henkel implemented VSI-based protection on-prem and in RISE.

Agenda

- Application-layer malware scans? Why?
- Henkel's Journey with SAP VSI
- Solutions for On-Prem and Cloud
- Q & A




Agenda

- Application-layer malware scans? Why?
- Henkel's Journey with SAP VSI
- Solutions for On-Prem and Cloud
- Q & A



Reason #1: Because SAP Recommends It



9 Virus Scanning

Basic Concepts

We recommend installing and running a VSI 2.x-compliant virus scanner in your landscape. The SAP S/4HANA code calls this scanner using a dedicated interface during different stages of processing - during upload, download, and passage through the Gateway, and so on. You can customize the interface with the help of scan profiles.

We recommend running VSI scans for:

- Signature scans
All files should be checked against an up-to-date list of known virus signatures.
- Mime-type detection
Only trusted file types should be allowed.
- Active content detection
Files with active content should be blocked (for example, PDF files containing JavaScript).

For more information about virus scan profiles and customizing, go to https://help.sap.com/s4hana_op_2022, enter **Virus Scan Interface** into the search bar, press **Enter**, and open the search result with that title.

Additional information is available in SAP Notes [786179](#) and [1494278](#).

For virus scanning in SAP Content Server, see SAP Note [1585767](#).

PUBLIC
Document Version: 3.0 – 2023-05-26

Security Guide for SAP S

© 2023 SAP SE or an SAP affiliate company. All rights reserved.

9.1 Virus Scanning in File Uploads

Example

The system allows uploading of files. For example, users can add an attachment to business documents. Also, you can upload template files, such as e-mail HTML templates, which can be used to render data on a UI. Once uploaded into SAP S/4HANA, such documents may be displayed in SAP Fiori apps without further security-related checks. If a document contains malicious content, unintended actions could be triggered when the item is downloaded or displayed. This can lead to situations, such as cross-site scripting vulnerabilities. That is why proper virus scanning at upload time is an essential first line of defense against (stored) XSS attacks.

For a technical description of this problem see the *ABAP Platform Security Guide*.

Go to https://help.sap.com/s4hana_op_2022, enter *Preventing Cross-Site Scripting From Uploads* into the search bar, press **Enter**, and open the search result with that title.


It is clear that uploaded files need to be scanned for malware. Also, their type needs to be verified against a allowlist of MIME-types. You can meet both these requirements by installing and running a VSI 2.x-compliant virus scanner in your landscape.

Examples of File-based Threats


- Malware
 - Viruses
 - Trojans
 - Ransomware, etc.
- File-type filter bypass
 - e.g. Upload of arbitrary content by changing/removing the extension
- Active Content
 - Macros, OLE, DDE
 - Executables, Screensavers, DLLs, shell-scripts
 - PDF with JavaScript, XML with JavaScript, etc.

Home


Open and Close Posting Periods
FAGL_EHP4_T001B...



Procurement Overview



Accounts Payable Overview



Overdue Payables Today

Critical O... 651.53M EUR

↻ 30 min. ago

Days Payable Outstanding Last 12 Months

| | |
|---------|--------|
| 06/2023 | 0 |
| 11/2022 | 237.34 |
| 10/2022 | 557.13 |


↻ 30 min. ago

Overdue Receivables Today


100%

↻ 30 min. ago


Create Dunning Notices




My Dunning Proposals



Display Dunning History



Post Incoming Payments



Reason #2: because your auditor will flag the SAL warnings

- Warnings in Security Audit Log for
 - File uploads and downloads that were not scanned
 - Standard with SAP_BASIS 757 and/or SAP note 3165706 and 3165707

| Security Audit Log - Evaluation | | | | | | | | | | |
|--|----------|-----|-------|-------------|-------|---------------|------------|-------|------------|---|
| Evaluation File List Statistics SAL Configuration | | | | | | | | | | |
| Evaluation of Security Audit Log | | | | | | | | | | |
| Period Requested 17.07.2023 00:00:00 - 17.07.2023 23:59:59 | | | | | | | | | | |
| Period Selected 17.07.2023 19:18:54 - 17.07.2023 19:23:27 | | | | | | | | | | |
| Server vhcals4hci | | | | | | | | | | |
| Events Read | | | | | | | | | | |
| - Critical 17 | | | | | | | | | | |
| - Severe 42 | | | | | | | | | | |
| - Other 200 | | | | | | | | | | |
| Date | Time | Cl. | Event | User | Group | Terminal Name | Peer | TCode | ABAP Sourc | Audit Log Msg. Text |
| 17.07.2023 | 19:23:20 | 100 | FU9 | S4H_FIN_DEM | | 10.0.10.37 | 10.0.13.69 | S000 | SAPMHTTP | Virus scan profile /SIHTTP/HTTP_UPLOAD not active. Scan was not executed. |
| 17.07.2023 | 19:23:20 | 100 | FU9 | S4H_FIN_DEM | | 10.0.10.37 | 10.0.13.69 | S000 | SAPMHTTP | Virus scan profile /SCMS/KPRO_CREATE not active. Scan was not executed. |
| 17.07.2023 | 19:23:27 | 100 | FU9 | S4H_FIN_DEM | | 10.0.10.37 | 10.0.13.69 | S000 | SAPMHTTP | Virus scan profile /SIHTTP/HTTP_UPLOAD not active. Scan was not executed. |
| 17.07.2023 | 19:23:27 | 100 | FU9 | S4H_FIN_DEM | | 10.0.10.37 | 10.0.13.69 | S000 | SAPMHTTP | Virus scan profile /SCMS/KPRO_CREATE not active. Scan was not executed. |

Reason #3: because your red-team/pen-tester will report findings



[PROJECTS](#) [CHAPTERS](#) [EVENTS](#) [ABOUT](#) [Q](#)

[Member Login](#)

Unrestricted File Upload

Description

Uploaded files represent a significant risk to applications. The first step in many attacks is to get some code to the system to be attacked. Then the attack only needs to find a way to get the code executed. Using a file upload helps the attacker accomplish the first step.

The consequences of unrestricted file upload can vary, including complete system takeover, an overloaded file system or database, forwarding attacks to back-end systems, client-side attacks, or simple defacement. It depends on what the application does with the uploaded file and especially where it is stored.

Reason #4: because your OS-level Security does not even see it

• OS-level anti-virus

The screenshot shows the SAP for Me user interface. The top navigation bar includes the SAP logo, 'SAP for Me' text, a search bar, and icons for notifications (125), shopping cart, and user profile. The left sidebar contains navigation links: Home, Calendar, DASHBOARDS, Customer Success, Finance & Legal, Partner Solutions, Partnership, Portfolio & Products, Sales & Marketing, and Services & Support. The main content area displays '106267 - Virus scanner software on Windows' with a version of 18 and a release date of 15.06.2021. Below the title are tabs for Description, Software Components, References, Attributes, and Available Languages. The 'Description' tab is active, showing a paragraph about access errors and a red-bordered box with a recommendation to exclude SAPLOC and SAPMNT file shares from virus scanner monitoring. Below this, it lists 'Known errors in connection with virus scanners on Windows Server operating systems:' followed by a bulleted list of specific error messages and a note about malware detection in SAP source code.

106267 - Virus scanner software on Windows
SAP Note, Version: 18, Released On: 15.06.2021

Description Software Components References Attributes Available Languages

the customer. At the same time, customers can check whether the access error to files or remote resources also occurs when the defender virus scanner. In the experience of SAP Support, these errors no longer occur in 95% of all cases. If the error can also be reproduced then, the customer can open a case with Microsoft so that Microsoft can determine the exact cause of the access error - if necessary using a full memory kernel dump.

We recommend excluding the file shares SAPLOC and SAPMNT from the monitoring by the real-time scan engine of the virus scanner. The same applies for all directories of the database (data files, log files, archive logs, and so on).

Known errors in connection with virus scanners on Windows Server operating systems:

- Access error to the file system, local or remote:
 - Sporadic error messages stating that a file or a folder cannot be found, even though it exists
 - Error when deleting files, usually access problems (*access denied*)
 - Error when reading large files, sporadic error "The device is not ready" or similar error messages
- The virus scanner solution blocked the start of processes because malware was determined in the SAP source code, and this was caused due to incorrect virus scanner signatures.

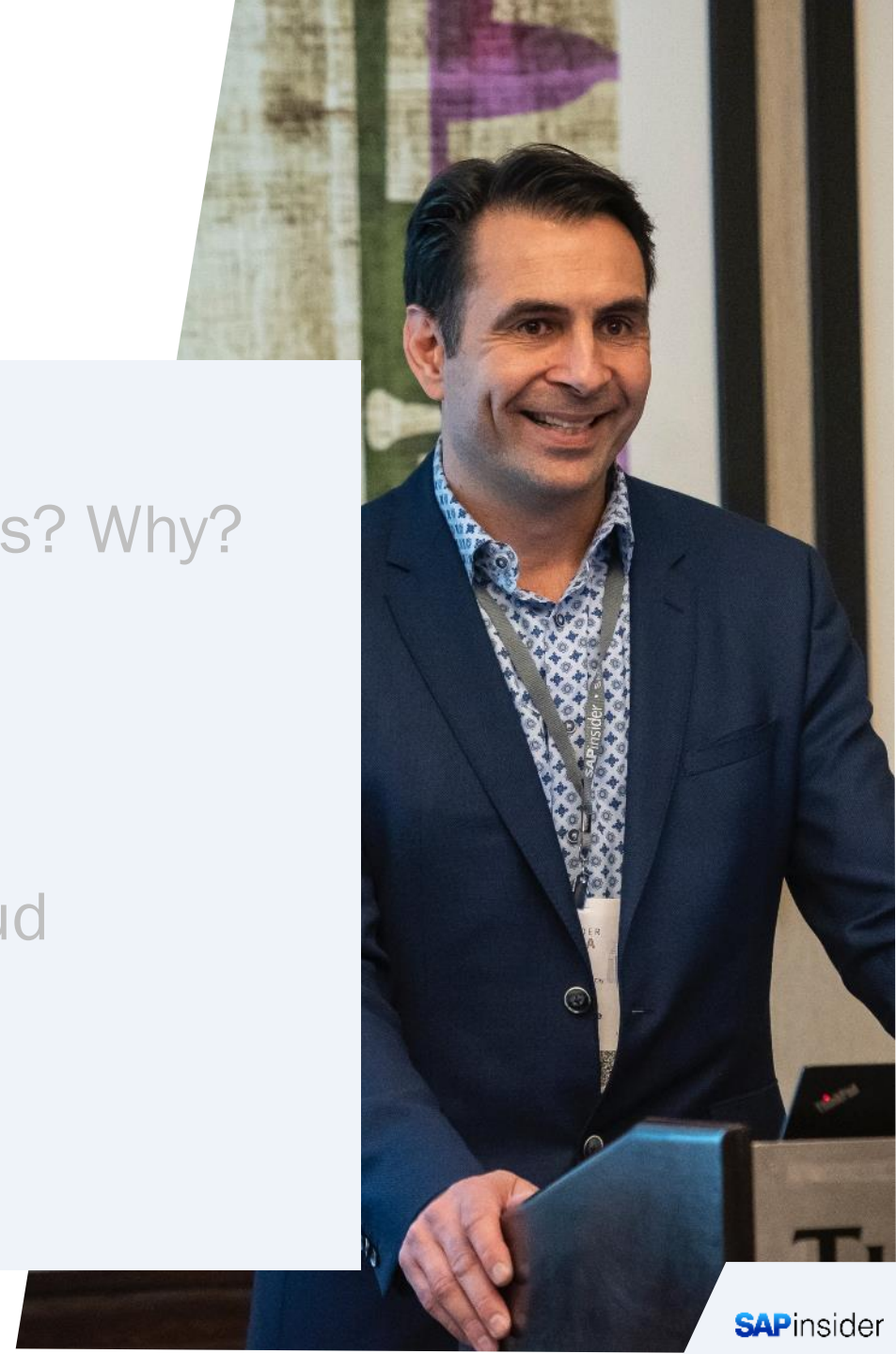
• Cannot monitor RFC connections

Reason #5: because your company may be liable for damages

- Most cybersecurity regulatory frameworks require organizations to implement state of the art malware protection:
 - ISO 27002:2022, Control 8.7
 - UK's Cyber Essentials Scheme and Security Standard SS-015
 - PCI DSS
 - HIPPA
 - German BSI Cloud Computing Catalogue – C5:2020
- SAP VSI exists since 2005 – it is considered state of the art
- Failure to implement VSI-based solutions can be found **negligent**
 - Entitles persons and organizations to compensation for damages

Agenda

- Application-layer malware scans? Why?
- Henkel's Journey with SAP VSI
- Solutions for On-Prem and Cloud
- Q & A



SALES

€22.4_{BN}

€2.3_{BN}

ADJUSTED OPERATING
PROFIT (EBIT)

146 YEARS

SUCCESS WITH
BRANDS AND
TECHNOLOGIES

WE EMPLOY MORE THAN

50,000

PEOPLE FROM
124 NATIONALITIES

-55%

CO₂ EMISSIONS FROM
OUR OPERATIONS¹

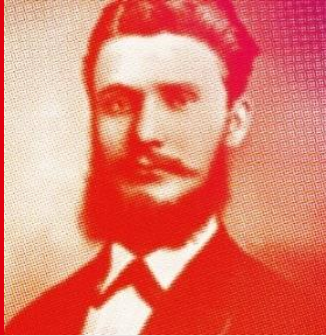
SOCIAL PROJECTS
IN 2022

2,055

AROUND

39%

WOMEN IN
MANAGEMENT



¹ Per ton of product, compared to the base year 2010

LEADING POSITIONS IN INDUSTRIAL AND CONSUMER BUSINESSES



ADHESIVE TECHNOLOGIES



CONSUMER BRANDS

LOCTITE

TECHNOMELT

BONDERITE

Persil

Schwarzkopf

all

syoss

Henkel

How it started...

From: [REDACTED]
Sent: Thursday, January 12, 2023 11:39 AM
To: Andreina [REDACTED]@henkel.com>; [REDACTED]@henkel.com>
Subject: [EXT] Virus on the platform!!!!!!

This message is from an EXTERNAL SENDER – be CAUTIOUS, particularly with links and attachments

Dear Andreina and Erik

While working on the platform we noticed some problems with some files:

IDH FG 2884084 – TBV IDH 2883809

DH FG 2884086 – TBV IDH 2883813

You probably have a virus on the platform.

Please forward this message to the appropriate person.

Some screenshots are attached.

How it started...

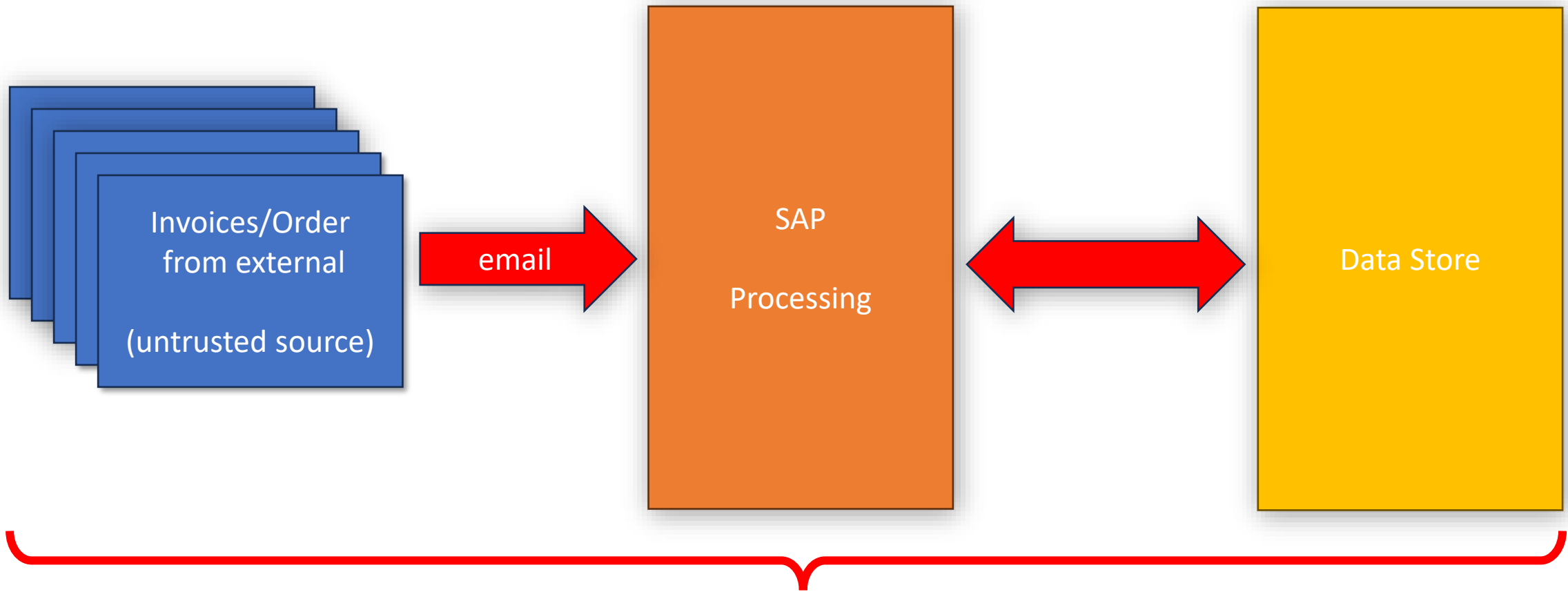
ES ET ENDPOINT ANTIVIRUS

Wykrycia

| Godzina | Skaner | Typ ob... | Obiekt | Wykrycie | Czynność | Użytkownik | Informacje | Skrót | Pierwsze wys |
|---------------------|-----------|-----------|--------|---|--|---------------------------|--|--------------|--------------|
| 12.01.2023 11:06:17 | Ochron... | plik | | \Downloads\TBV_2883809(1).doc | Win32/Exploit.CVE-2017-11882.BOR koń trojański | wyleczone przez usunięcie | Zdarzenie wystąpiło podcza... B268BA14FB75A197496708B... | 12.01.2023 1 | |
| 12.01.2023 09:16:13 | Ochron... | plik | | \Desktop\uaktualnienia tymczasowe 16.11.2022\28840... | Win32/Exploit.CVE-2017-11882.BOR koń trojański | wyleczone przez usunięcie | Zdarzenie wystąpiło podcza... 0032A9CAC5DA1864428AF0... | 12.12.2022 1 | |
| 12.01.2023 08:59:53 | Ochron... | plik | | \Downloads\TBV_2883813.doc | Win32/Exploit.CVE-2017-11882.BOR koń trojański | wyleczone przez usunięcie | Zdarzenie wystąpiło podcza... 711FF2102A489050F7650CC... | 12.01.2023 C | |
| 12.01.2023 08:59:30 | Ochron... | plik | | \Downloads\TBV_2883813.doc | Win32/Exploit.CVE-2017-11882.BOR koń trojański | wyleczone przez usunięcie | Zdarzenie wystąpiło podcza... 711FF2102A489050F7650CC... | 12.01.2023 C | |
| 12.01.2023 08:58:51 | Ochron... | plik | | \Downloads\TBV_2883813.doc | Win32/Exploit.CVE-2017-11882.BOR koń trojański | wyleczone przez usunięcie | Zdarzenie wystąpiło podcza... 711FF2102A489050F7650CC... | 12.01.2023 C | |
| 12.01.2023 08:56:40 | Ochron... | plik | | \Jane\HENKEL\OCEAN\2884086\Specyfikacje\TBV_28838... | Win32/Exploit.CVE-2017-11882.BOR koń trojański | wyleczone przez usunięcie | Zdarzenie wystąpiło podcza... 0032A9CAC5DA1864428AF0... | | |
| 12.01.2023 08:50:09 | Ochron... | plik | | \Downloads\TBV_2883813.doc | Win32/Exploit.CVE-2017-11882.BOR koń trojański | wyleczone przez usunięcie | Zdarzenie wystąpiło podcza... 711FF2102A489050F7650CC... | 12.01.2023 C | |

☐ Filtrowanie

Where it started - Invoice & Order Process



No dedicated malware protection

This time it was a False Alarm, but....

We realized there was a gap - technically and legally:

- **Legally - Reversal of the burden of proof**
 - In the event of litigation, we need to be able to demonstrate the files downloaded from our systems were NOT infected at the time of the download
- **Technically – let's dive into it...**

Technical Analysis

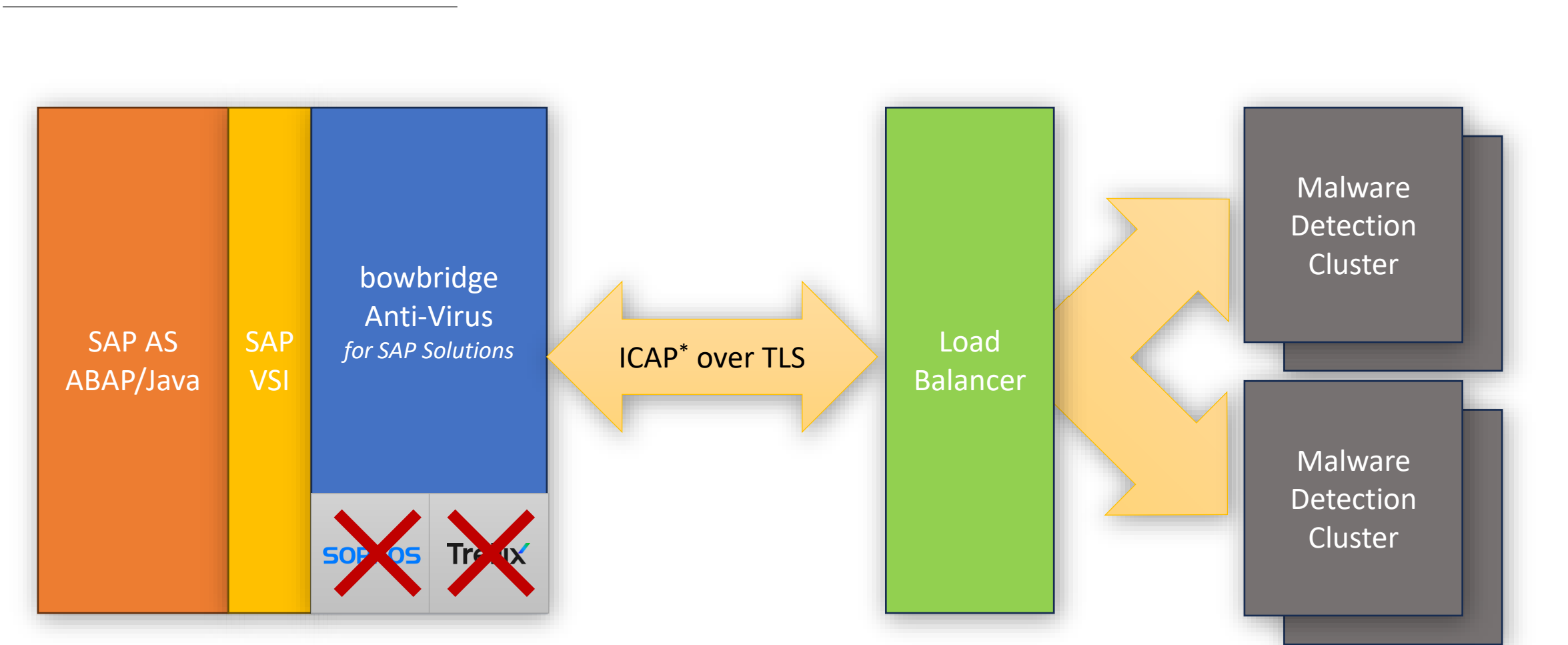
Key Finding: File-Ingestion into SAP was not properly protected

- Several file ingestion vectors exist, some interactive and some automated
 - Email (for example invoice handling)
 - GUI and HTTP uploads by users
 - eFolder
- Even if anti-virus is deployed on the OS, uploads into SAP are not scanned
- Vulnerability Management Department was unaware of this “blind spot”

Selection Criteria for a possible Solution

- Must be available for ABAP (R/3 & S/4)
- Must be SAP-certified for NW-VSI 2.x
- Must be available on multiple OS platforms
 - Linux x86_64
 - IBM AIX
- Must be a commercial solution with professional support

Solution Building Blocks



* ICAP: Internet Content Adaptation Protocol, RFC 3507

Why ICAP?

PROs:

- ICAP product was already licensed, no need to introduce a new AV engine
- Separation of operational responsibilities
- Automatic monitoring and well-established processes around malware

CONs:

- slightly lower scanning throughput than with a local scan engine on the AS
- Not critical for our scan volume (most scans are “background scans”)

Roll-out – OS-Layer installation

Solution rollout consists of 2 steps:

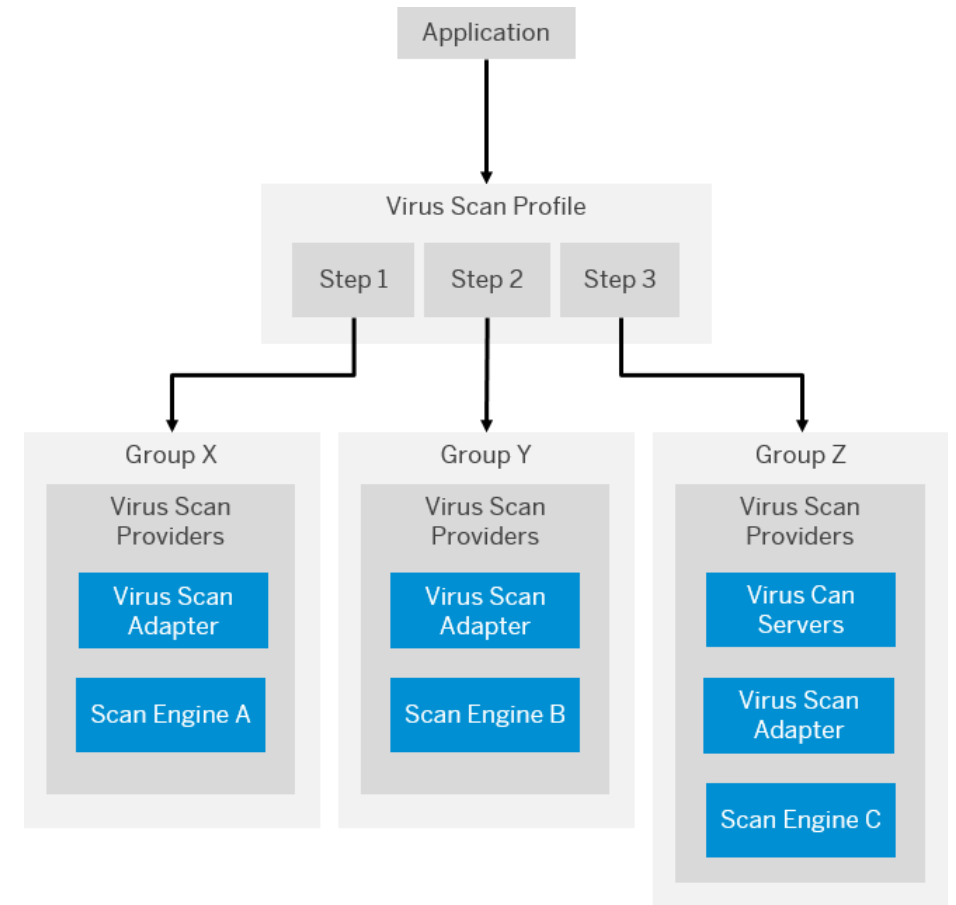
- OS-Layer Installation
 - Performed by Henkel's OS-team and provider
 - Command-line installer
 - Interactive
 - "Silent", unattended option
 - Newly deployed systems on RISE



SAP Virus Scan Interface - configuration

SAP VSI introduces 3 abstraction layers for:

- Maximum transparency for the application
- Availability, redundancy
- Increased security



SAP-Layer configuration – Virus Scanner Group

- Transaction VSCANGROUP
- “Container” for initialization parameters
 - Groups one or more Virus Scan Providers
 - Load-balances providers, if there are more than one
 - Watch out with paths, so the configuration can be transported and applied to DEV/QA/PROD.

DE

to

SAP-Layer configuration – Virus Scan Provider

- Transaction VSCAN
- Connects to SAP VSI
 - Shared Library/DLL
 - Loaded into the Work-Processes / jstart process
 - One per Instance
 - Monitored by CCMS

SAP-La

- Trans
- Conn
- Sh
- Lo
- On
- Mo

Table View Edit Goto Selection Utilities System Help

Display View "Virus Scan Provider Definition": Details

Provider Type: ADAPTER (Virus Scan Adapter)
Provider Name: VSA_VHCALS4HCI
Status: ☒
Start Stop

Virus Scan Provider Definition

Scanner Group: DEFAULT Display
Status: Active (Application Server)
Server: vhcals4hci_S4H_00
Trace Level: Errors Only
Interval Reinit: 1 Hours Last Initialization: 21.09.2023 09:10:42 Load
Adapter Path: /opt/bowbridge/libbbAV.so.4
Configuration:

Engine Data

| | |
|---------------|--|
| Version | 4.0 |
| Version Text | bowbridge Anti-Virus for SAP Solutions (SHM) |
| Date | Sun Sep 17 14:23:17 2023 |
| Known Viruses | |

Loaded Drivers

| Version | Driver Name | Date | Known Viruses |
|---------|--------------------------|--------------------------|---------------|
| 5.42 | MIME scan | Sun Sep 17 14:34:03 2023 | |
| 23.2 | Archive extraction | Sun Sep 17 14:34:03 2023 | |
| 23.2 | Active content detection | Sun Sep 17 14:34:03 2023 | |
| 23.2 | ICAP client | Sun Sep 17 14:34:04 2023 | |

Adapter Data

| | |
|--------------|--|
| Manufacturer | bowbridge Software GmbH |
| Product Name | Anti-Virus for SAP Solutions, wrapper v.4.0.1 Build 74 |
| Version | 4.0 |

One entry chosen

SAP

SAP-Layer configuration – Virus Scan Profiles

- Transaction VSCANPROFILE
- Scan is triggered by Function Modules
 - Any application using the module automatically scans file transfers
 - No application changes required
- SAP provides several virus scan profiles out of the box
- Admins may create own reference profiles
- Configure individual scan settings for each profile

SAP-La

- Transa
- Scan is
 - Any
 - No
- SAP pr
- Admin
- Config

Table View Edit Goto Selection Utilities System Help

Display View "Virus Scan Profile": Overview

Dialog Structure

- Virus Scan Profile
 - Steps
 - Step Configuration
 - Profile Configuration
 - MIME Types

| Virus Scan Profile | Active | Default Pr... | Profile Text |
|-------------------------|--------------------------|--------------------------|-----------------------------|
| /CBGLMP_API/WWI_GET_C | <input type="checkbox"/> | <input type="checkbox"/> | GLM Plus: Load Image File |
| /CBUI/WWI_REPORT_GEN | <input type="checkbox"/> | <input type="checkbox"/> | EHS: WWI Report Genera |
| /COND_PUBLIC_MAINTEN... | <input type="checkbox"/> | <input type="checkbox"/> | |
| /HCM_TMC/DOCUMENT_U... | <input type="checkbox"/> | <input type="checkbox"/> | File Upload Using the Met |
| /IC_CCS_MCM/ICI_MAIL | <input type="checkbox"/> | <input type="checkbox"/> | Virus Scan Profile for Emal |
| /IWBEF/CP/ODATA_DOW... | <input type="checkbox"/> | <input type="checkbox"/> | |
| /IWBEF/V4/ODATA_UPL... | <input type="checkbox"/> | <input type="checkbox"/> | |
| /MDG_BS_FILE_UPLOAD... | <input type="checkbox"/> | <input type="checkbox"/> | |
| /PAOC_EIC_APPL_COMM... | <input type="checkbox"/> | <input type="checkbox"/> | Employee Interaction Cen |
| /PAOC_RCF_BL/HTTP_U... | <input type="checkbox"/> | <input type="checkbox"/> | SAP E-Recruiting: File Upk |
| /PC01/SVINCOMING | <input type="checkbox"/> | <input type="checkbox"/> | Scanning Incoming Status |
| /PLMU/UI_SPC_BAS/MS... | <input type="checkbox"/> | <input type="checkbox"/> | |
| /SAPC_RUNTIME/APC_W... | <input type="checkbox"/> | <input type="checkbox"/> | |
| /SAPC_RUNTIME/APC_W... | <input type="checkbox"/> | <input type="checkbox"/> | |
| /SARC/ARCHIVING_ADK | <input type="checkbox"/> | <input type="checkbox"/> | Virus Protection Using the |
| /SBCOMS/SMTP_INBOUND | <input type="checkbox"/> | <input type="checkbox"/> | SMTP Inbox Processing |
| /SCA/DM_ATTACHMENTS... | <input type="checkbox"/> | <input type="checkbox"/> | |
| /SCA/DM_BRANDING/UP... | <input type="checkbox"/> | <input type="checkbox"/> | |
| /SCA/DM_FTR/UPLOAD_... | <input type="checkbox"/> | <input type="checkbox"/> | |
| /SCA/DM_HELPCENTER/... | <input type="checkbox"/> | <input type="checkbox"/> | |
| /SCA/DM_MFGC/UPLOAD... | <input type="checkbox"/> | <input type="checkbox"/> | |
| /SCA/DM_MYS/UPLOAD_... | <input type="checkbox"/> | <input type="checkbox"/> | |
| /SCET/DP_VS_ENABLED | <input type="checkbox"/> | <input type="checkbox"/> | |
| /SCET/GUI_DOWNLOAD | <input type="checkbox"/> | <input type="checkbox"/> | |
| /SCET/GUI_UPLOAD | <input type="checkbox"/> | <input type="checkbox"/> | File Upload Using CL_GUI_ |
| /SCMS/KPRO_CREATE | <input type="checkbox"/> | <input type="checkbox"/> | |
| /SCMS/KPRO_XML_CREA... | <input type="checkbox"/> | <input type="checkbox"/> | |
| /SCWN/MIME_NOTE_INS... | <input type="checkbox"/> | <input type="checkbox"/> | |

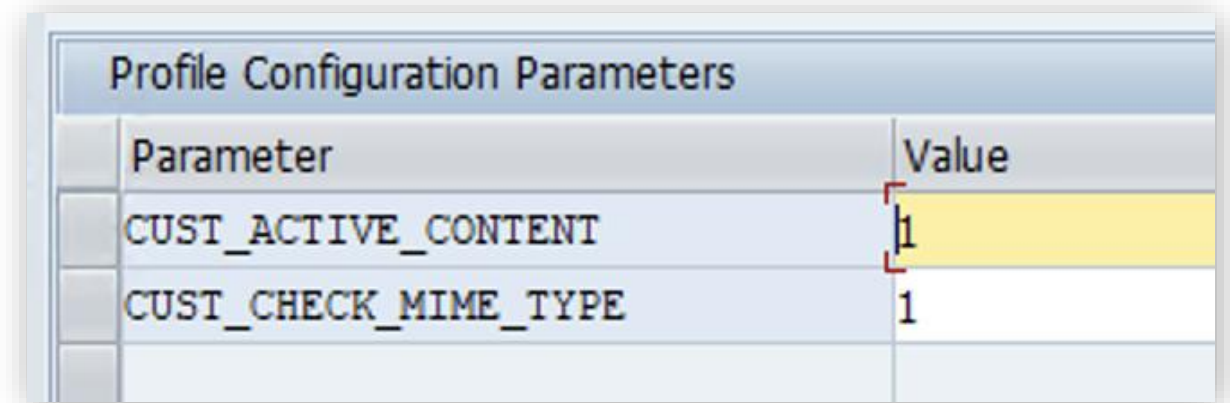
Position... Entry 1 of 45

SAPinsider

Scan Options

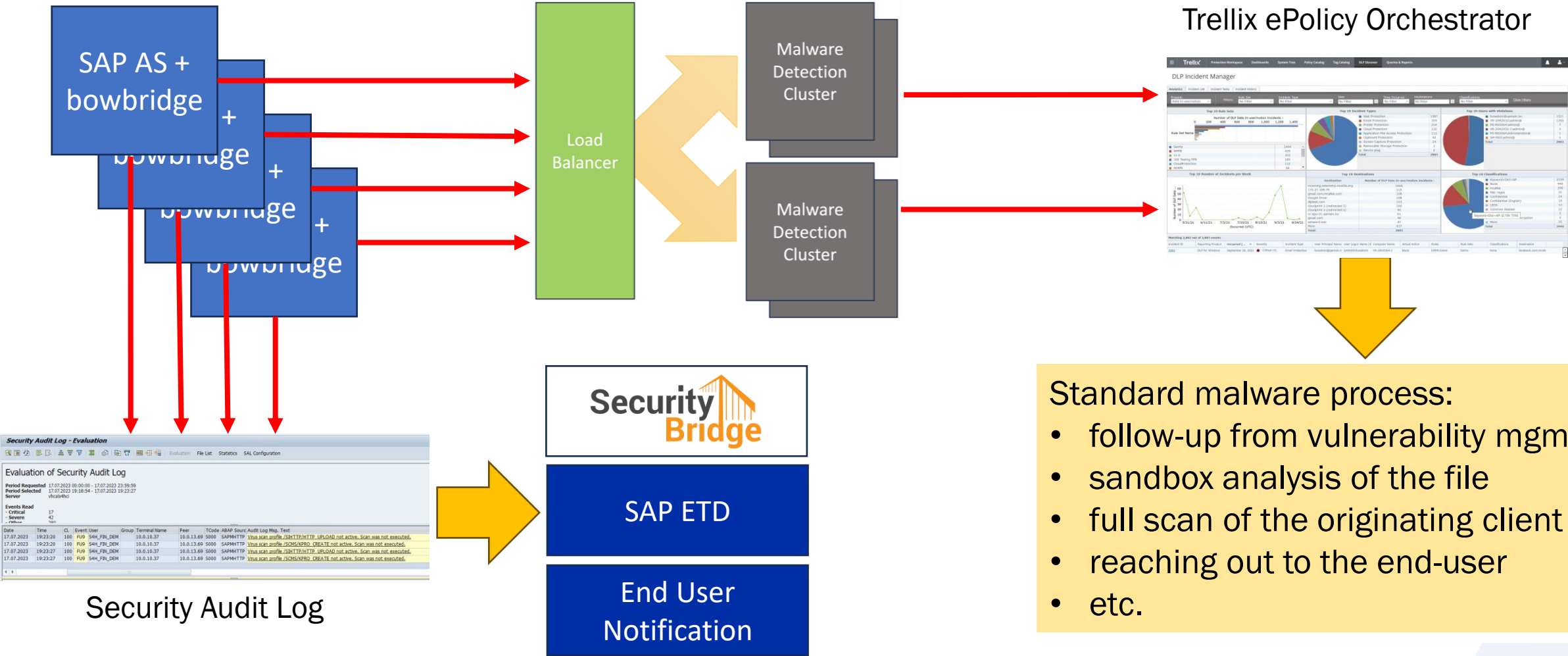
In addition to malware-scanning Henkel's policy is to

- Enforce matching of file content and file extension
 - Block files where the extension does not match the content ("notepad.pdf")
- Block active content in files
 - Macros in Office documents
 - JavaScript in PDF/HTML/XML/SVG, etc.
 - Shell scripts
 - Executables, etc.



| Profile Configuration Parameters | |
|----------------------------------|-------|
| Parameter | Value |
| CUST_ACTIVE_CONTENT | 1 |
| CUST_CHECK_MIME_TYPE | 1 |
| | |

Integrations for monitoring and post-detection measures



Operations

Current implementation:

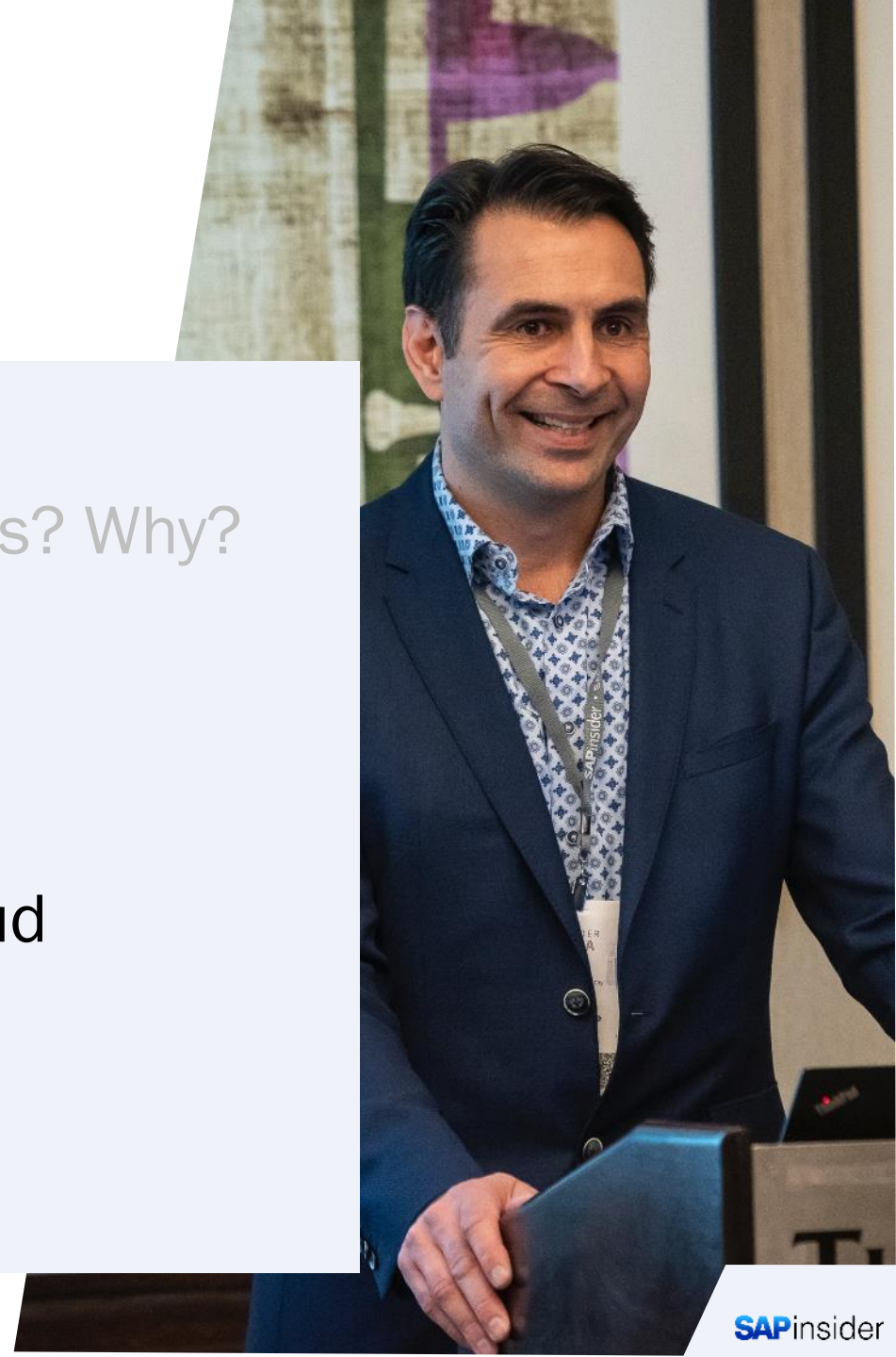
- VSI in use on 70 Instances
 - On-Premises
 - On RISE with SAP
- Securing several applications, for example:
 - Ordering
 - Inbound email
 - eFolders
 - Files received by middleware (e.g. SAP CPI)
 - CRM (File exchange)
- Scanning thousands of files per day

Lessons learned – unexpected value

- Fewer detections of **malware** than expected
- More detections of **active content** than expected
 - e.g. download of executables from SAP to execute on local machine
- We gained a lot of **VISIBILITY**
 - e.g. into how users and developers are (mis-) using data / file transfers
- We increased the **quality of data processing**
 - e.g. by detecting/blocking corrupted files
- Overall improved **Data Hygiene**

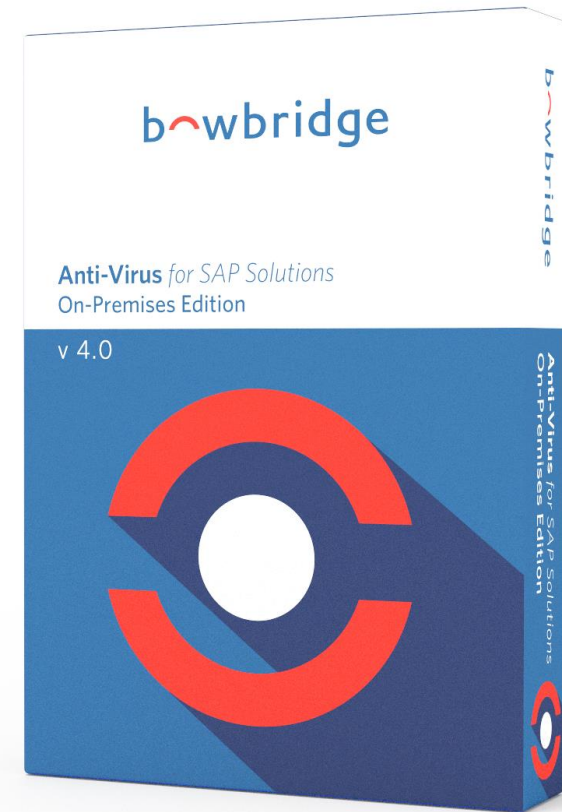
Agenda

- Application-layer malware scans? Why?
- Henkel's Journey with SAP VSI
- Solutions for On-Prem and Cloud
- Q & A

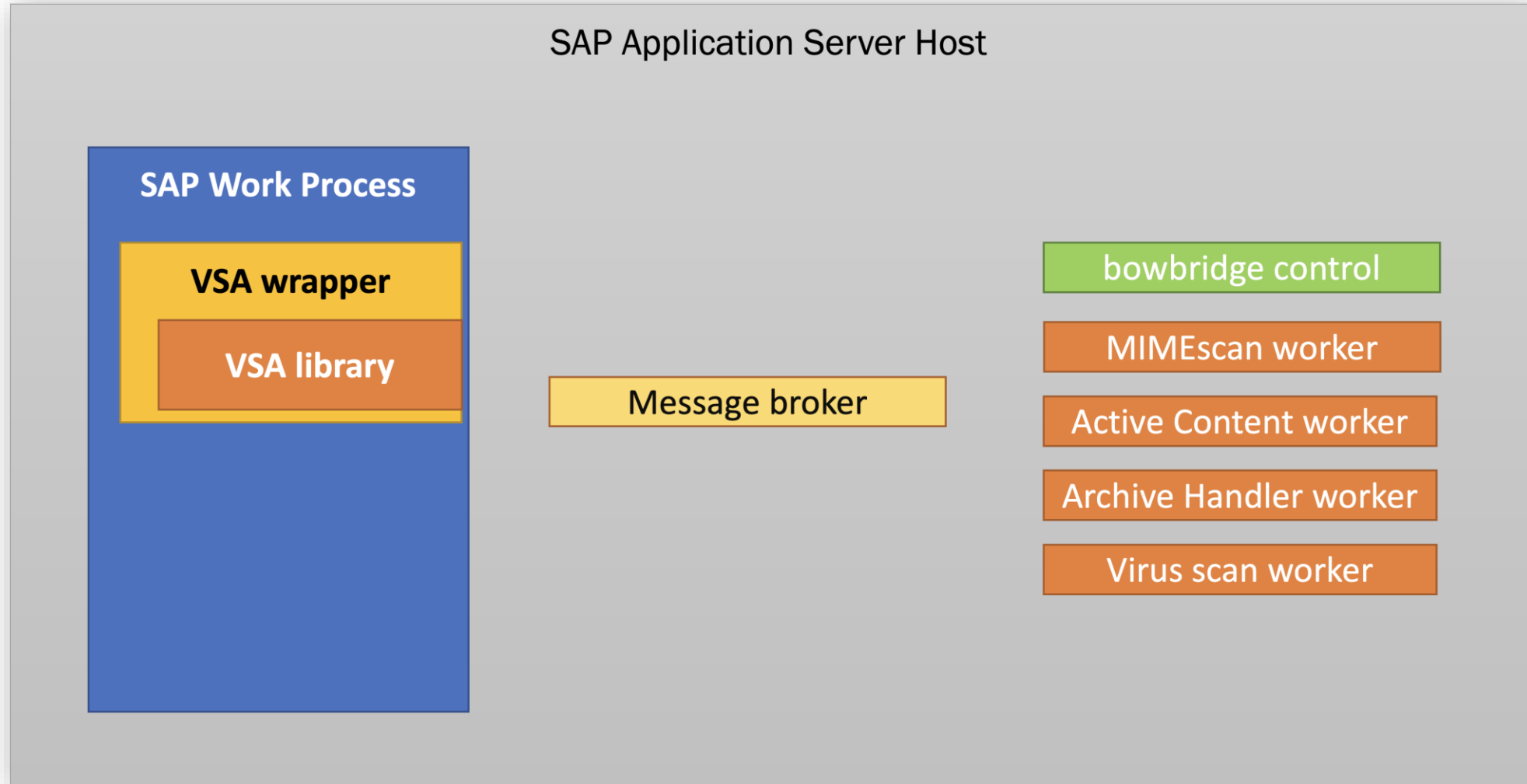


bowbridge Anti-Virus 4.0 – launching at SAPinsider EMEA

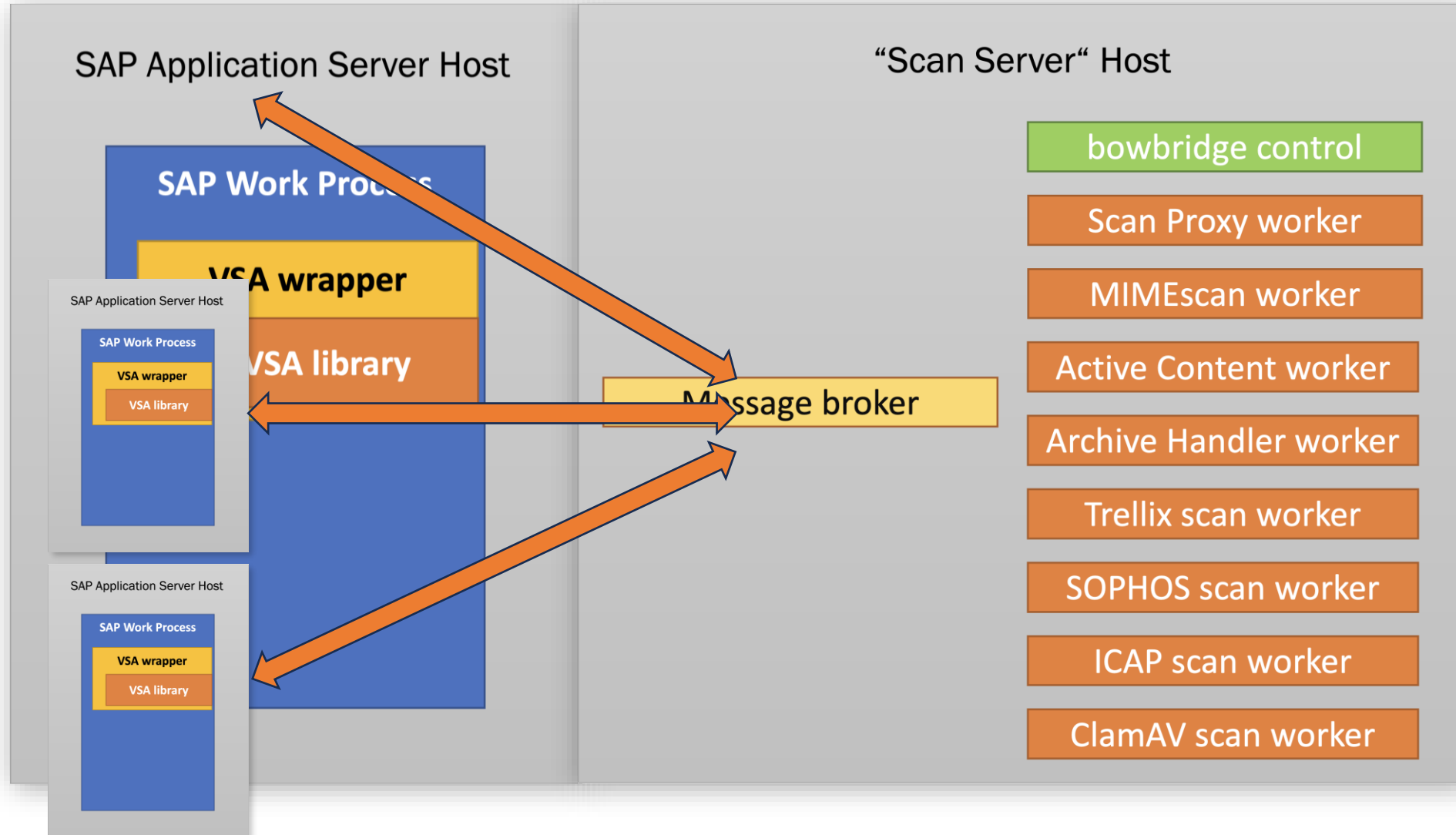
- Latest version of bowbridge Anti-Virus
- Increased Modularity
- Flexible Deployment Options
- Horizontal Scalability
- Cloud-Ready
- Hybrid SaaS-Ready



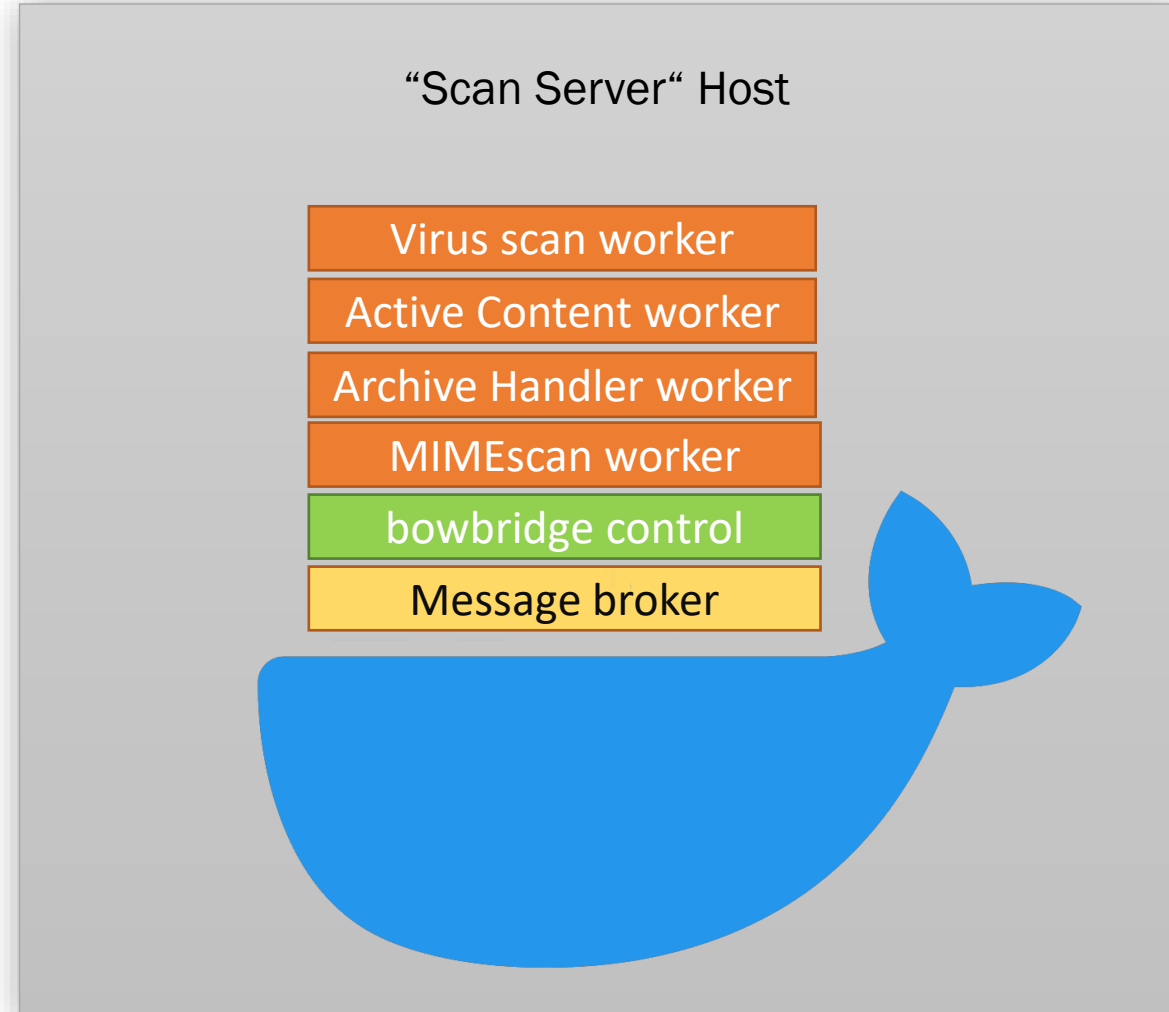
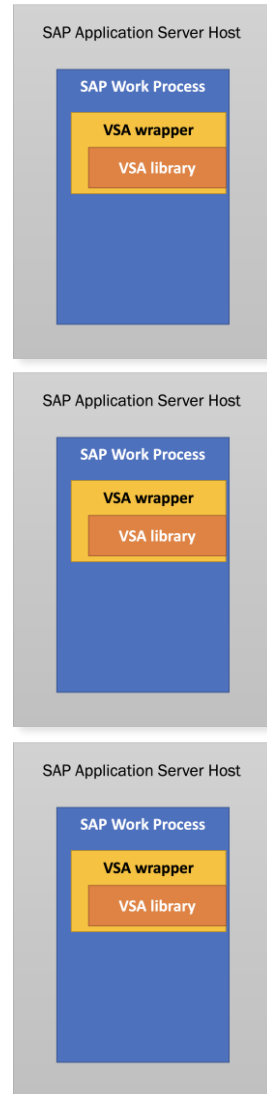
Deployment options – All local



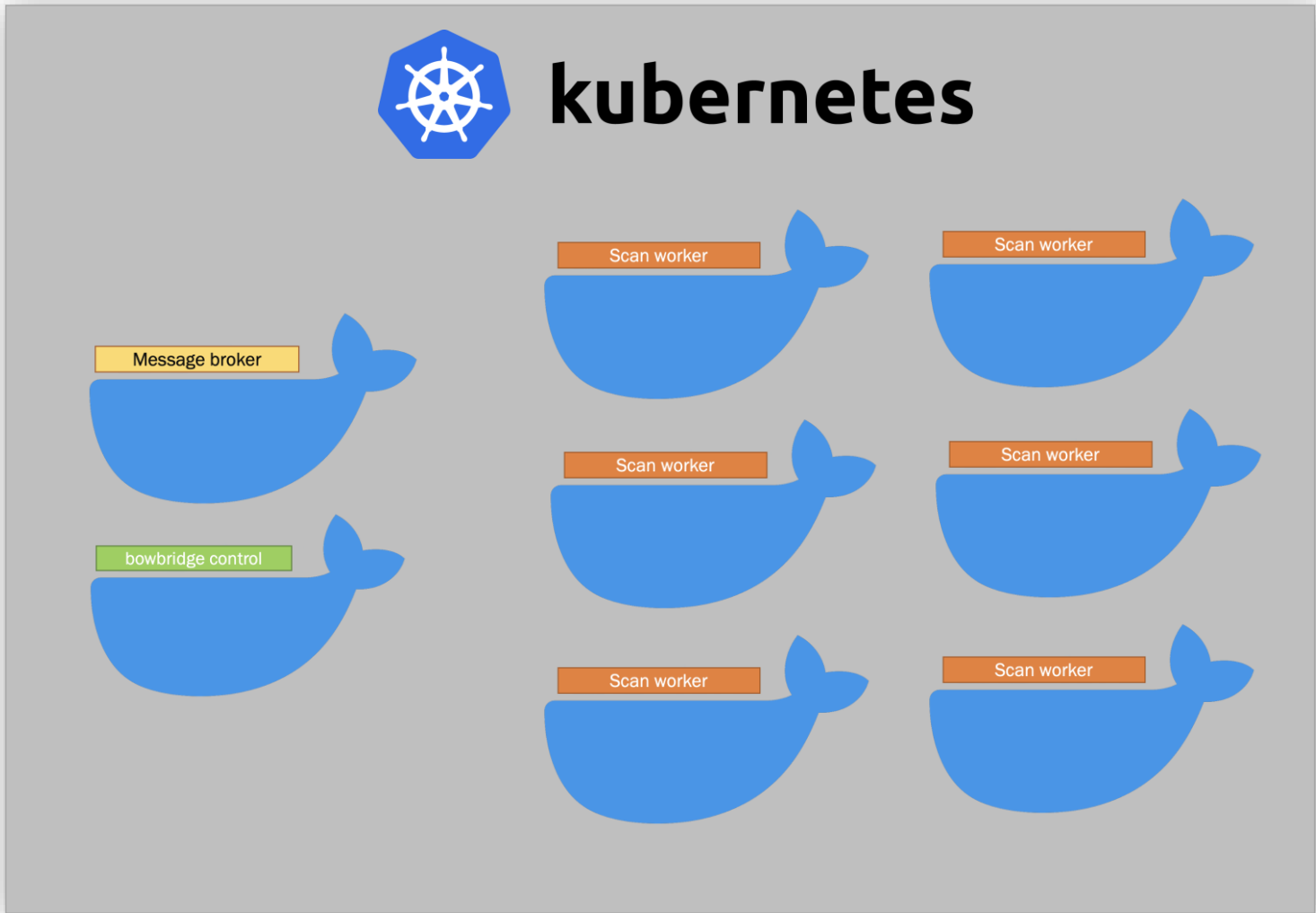
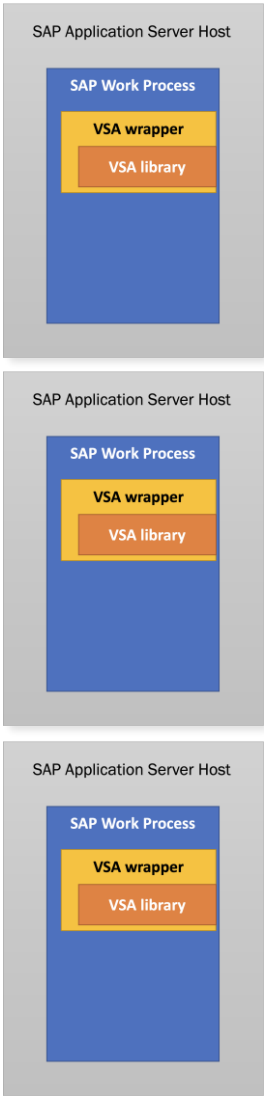
Deployment options – Scan Server



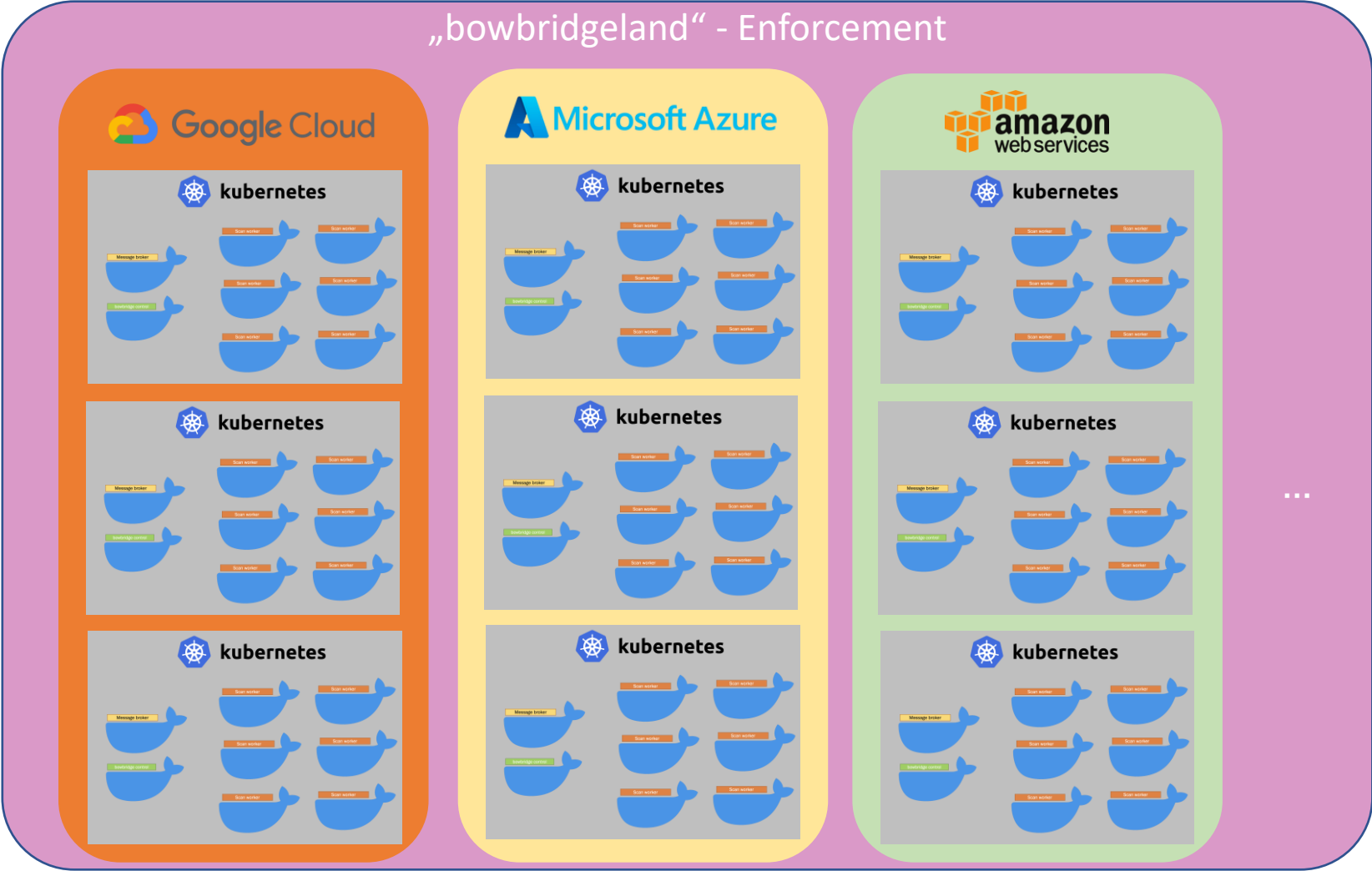
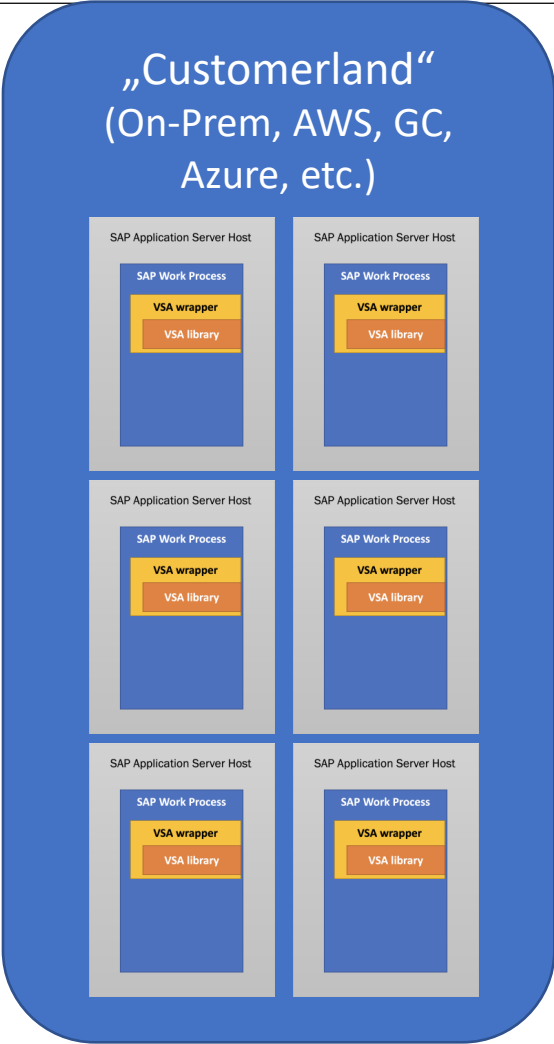
Deployment options – Scan Server on Docker



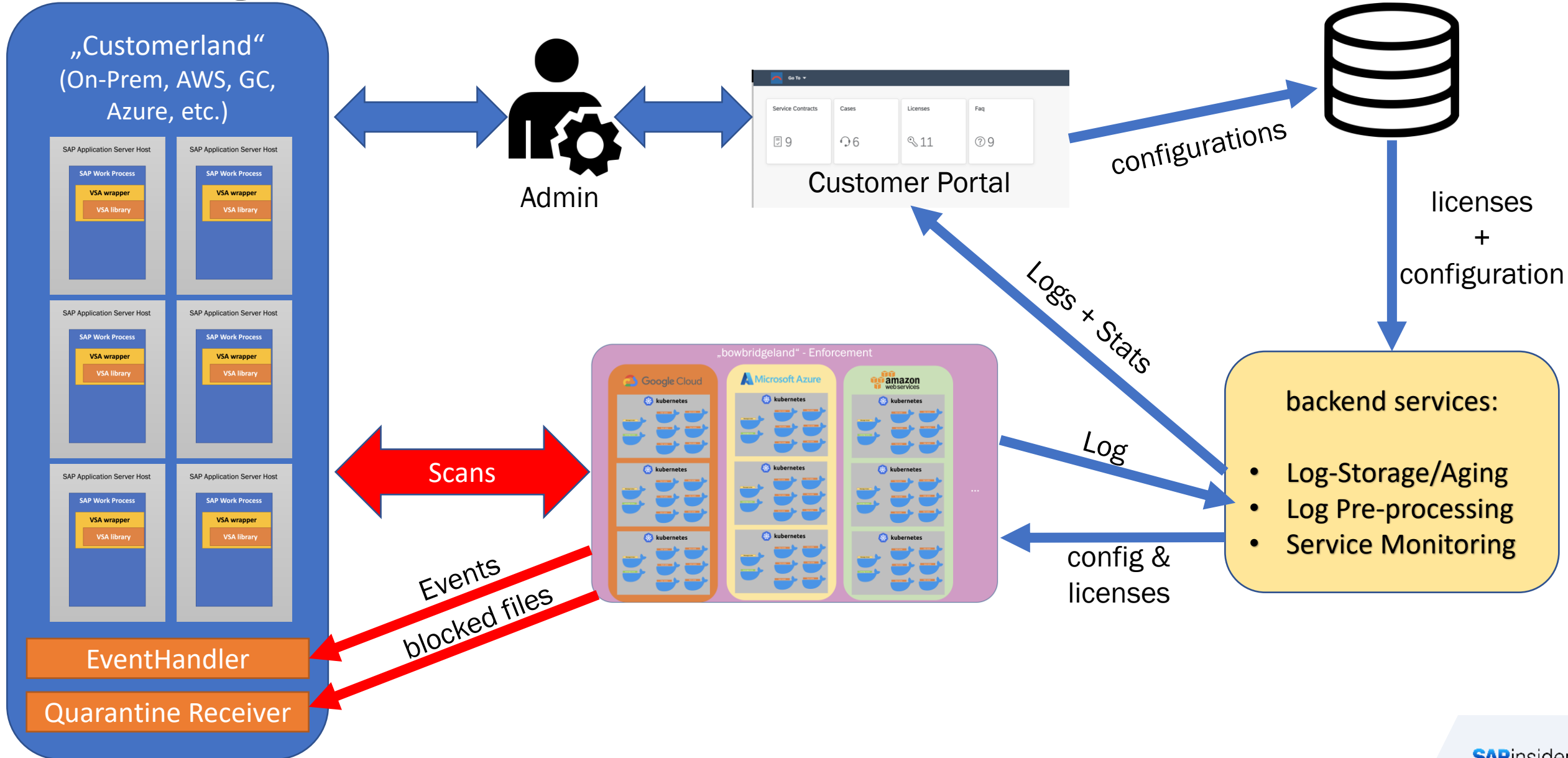
Deployment options – Scan Server on kubernetes



bowbridge in the Cloud



bowbridge in the Cloud



Get Hands-On Experience:

Join us for our hands-on labs on VSI tomorrow:

- 10:00-12:00: SAP VSI + bowbridge In OnPrem Scenarios
- 13:00-15:00: SAP VSI + bowbridge In Cloud Scenarios

Participants will be issued a bowbridge Certificate of Participation

Outlook / Roadmap

- Anti-Virus v4 – On Premises Edition: SAP-certified and available
- Anti-Virus v4 – (Hybrid) SaaS Edition: ETA Q2, 2024
- bowbridge Anti-Virus – BTP Edition: ETA Q3, 2024
 - Leverage bowbridge scanning from any application
 - Simple API (think "VSI over HTTPS")
 - Integrated with bowbridge SaaS backend services for logs, reports, alerting, ...

Wrap up

- SAP VSI helps solving content-security challenges
 - Malware
 - Active content
 - MIME-type filtering
- VSI + bowbridge implementation at Henkel
 - Tightly integrated with vulnerability management processes
 - Leverages existing ICAP infrastructure
 - Clear delineation of responsibilities
 - Implemented on-premises and on RISE with SAP
 - **Result:** improved security, visibility, and data hygiene

Where to Find More Information

- SAP Virus Scan Interface
 - https://help.sap.com/docs/ABAP_PLATFORM_NEW/1531c8a1792f45ab95a4c49ba16dc50b/4e2606c3c61920cee10000000a42189c.html
- SAP S/4 HANA 2022 Security Guide
 - https://help.sap.com/doc/d7c2c95f2ed2402c9efa2f58f7c233ec/2022/en-US/SEC_OP2022.pdf
- bowbridge Anti-Virus for SAP Solutions, v4
 - <https://www.bowbridge.net/en/anti-virus-for-sap-solutions/>
- Top 5 reasons to implement application-layer malware scanning
 - <https://www.bowbridge.net/wp-content/uploads/2023/09/Top-5-Reasons-to-Implement-Application-Layer-Malware-Protection-.pdf>

Key Points to Take Home

Top 5 reasons to implement VSI-based scanning:

- Recommended by SAP
- Prevents expensive findings during audits
- Addresses pen-test/red-team findings
- OS-level anti-virus does not help
- Reduces liability risk

Markus Hille, Henkel

markus.hille@henkel.com

Jörg Schneider-Simon

j.schneider-simon@bowbridge.net

VISIT US AT
BOOTH #1110

Please remember to complete
your session evaluation.

SAPinsider



SAPinsider.org

PO Box 982Hampstead, NH 03841
Copyright © 2023 Wellesley Information Services.
All rights reserved.

SAP and other SAP products and services mentioned herein as well as their respective logos are trademarks or registered trademarks of SAP SE (or an SAP affiliate company) in Germany and other countries. All other product and service names mentioned are the trademarks of their respective companies. Wellesley Information Services is neither owned nor controlled by SAP SE.

SAPinsider comprises the largest and fastest growing SAP membership group worldwide, with more than 750,000 global members.
