IIS267

Secure the Intelligent Enterprise with SAP Enterprise Threat Detection

Michael Schmitt, Arndt Lingscheid, SAP

Disclaimer

The information in this presentation is confidential and proprietary to SAP and may not be disclosed without the permission of SAP. Except for your obligation to protect confidential information, this presentation is not subject to your license agreement or any other service or subscription agreement with SAP. SAP has no obligation to pursue any course of business outlined in this presentation or any related document, or to develop or release any functionality mentioned therein.

This presentation, or any related document and SAP's strategy and possible future developments, products and or platforms directions and functionality are all subject to change and may be changed by SAP at any time for any reason without notice. The information in this presentation is not a commitment, promise or legal obligation to deliver any material, code or functionality. This presentation is provided without a warranty of any kind, either express or implied, including but not limited to, the implied warranties of merchantability, fitness for a particular purpose, or non-infringement. This presentation is for informational purposes and may not be incorporated into a contract. SAP assumes no responsibility for errors or omissions in this presentation, except if such damages were caused by SAP’s intentional or gross negligence.

All forward-looking statements are subject to various risks and uncertainties that could cause actual results to differ materially from expectations. Readers are cautioned not to place undue reliance on these forward-looking statements, which speak only as of their dates, and they should not be relied upon in making purchasing decisions.

Agenda

Why you need SAP Enterprise Threat Detection

- SAP Enterprise Threat Detection (ETD) and generic SIEM systems
- SAP Enterprise Threat Detection – preventing cyber attacks
- How does SAP Enterprise Threat Detection work
- Details & Benefits of SAP Enterprise Threat Detection
- SAP Enterprise Threat Detection — Architecture

Live Demo SAP Enterprise Threat Detection

Hands on SAP Enterprise Threat Detection

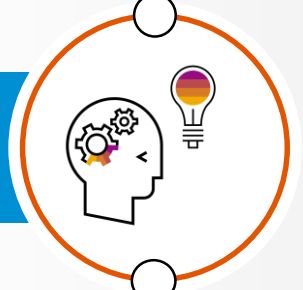
Divider page

Stop security breaches

Challenge

- Stop security breaches **in** today's SAP business applications.

Solution

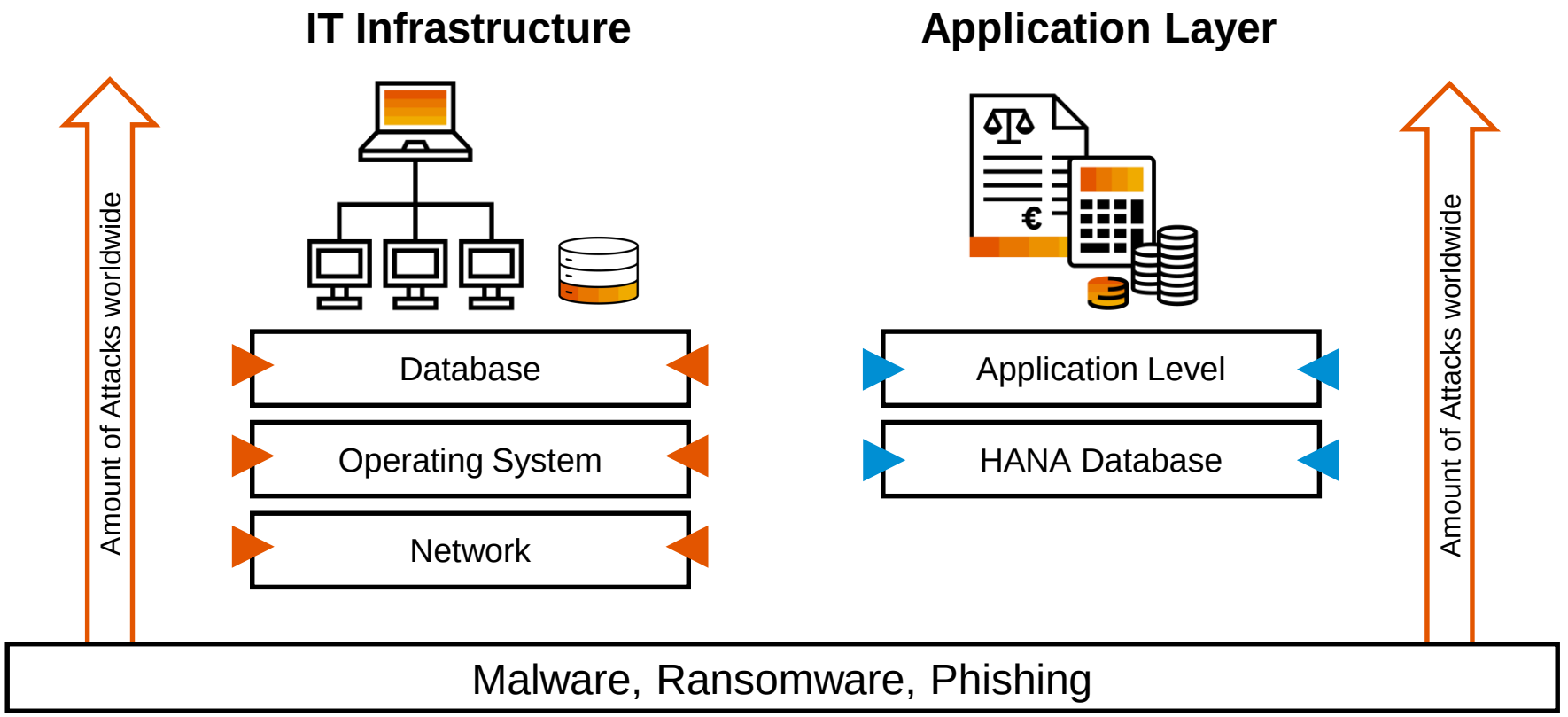


- Enterprise Threat Detection gives transparency in real time to suspicious (user) behavior an anomalies in SAP business applications to identify and stop security breaches in real-time.
- SAP Enterprise Threat Detection understands the semantic events coming from the inside of the SAP application layer.

Benefits

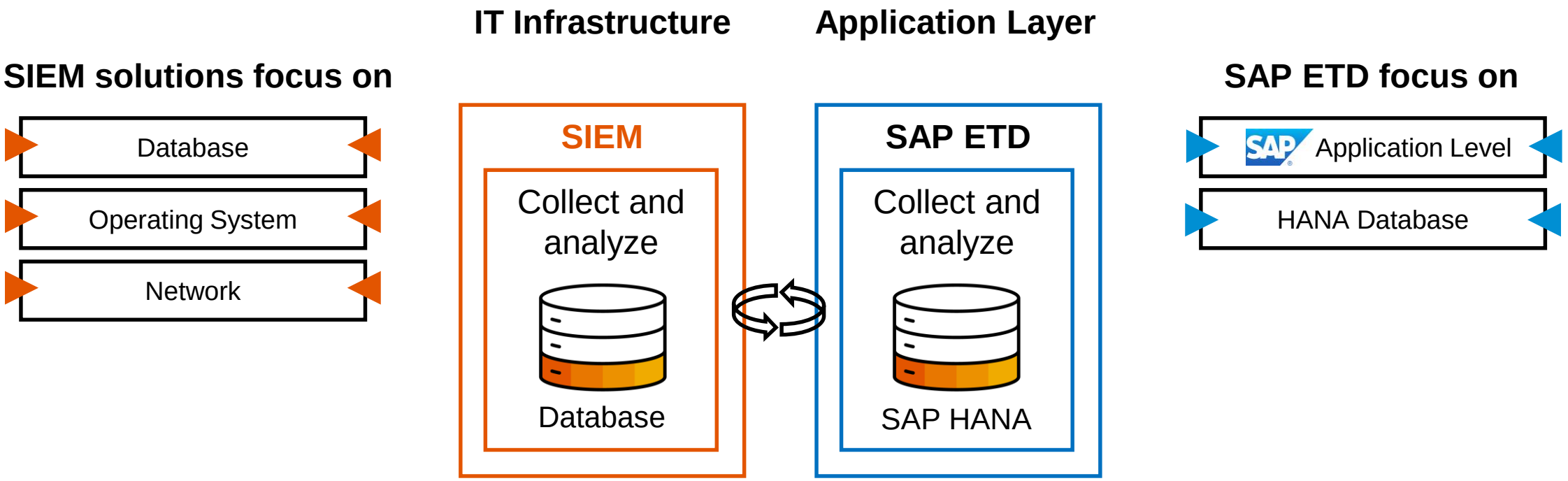
- Minimize the risk of suffering a severe data breach.
- Protect the Business future.
- Protect the intellectual.
- Protect the sensitive data of an enterprise.
- Protect your enterprise against reputation loss due to data breach.

What cyber attacks do we see



Analysts e.g. from ensurance companies rate cyber attacks as the biggest risks for enterprises worldwide within the top 10 Business Risks.

SAP Enterprise Threat Detection (ETD) and generic SIEM systems



Continue use of proven security incident reporting

+

Real time monitoring of business critical SAP applications & data

Integration of SAP ETD with all leading SIEM solutions (HP Arcsight, IBM Q-Radar, Splunk) available

Processing all SAP log events in a non-SAP SIEM solution

Challenge

- Tremendous costs since other SIEM solutions are licensed based on the log volume.
- Log implementation projects since the semantic understanding must be implemented in SIEM solution.

Solution

- Use SAP Enterprise Threat Detection.
- License is based on monitored users.
- SAP delivers the semantic understanding as pre-defined patterns.

Benefits

- SAP Enterprise Threat Detection gives transparency to the inside of the application layer out of the box.
- SAP Enterprise Threat Detection saves costs analyzing a huge amount of log data.
- SAP Enterprise Threat Detection bridges the gap between IT infrastructure monitoring an in application monitoring of the SAP applications.

NIST Framework

Identify

Asset Management

Business Environment

Governance

Risk Assessment

Risk Management Strategy

Supply Chain Risk Management

Protect

Access Control

Awareness and Training

Data Security

Information

Maintenance

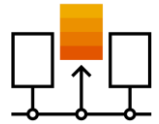
Protective Technology

Detect

Anomalies and Events

Continuous Security Monitoring

Detection Processes



Respond

Response Planning

Communications

Analysis

Mitigation

Improvements

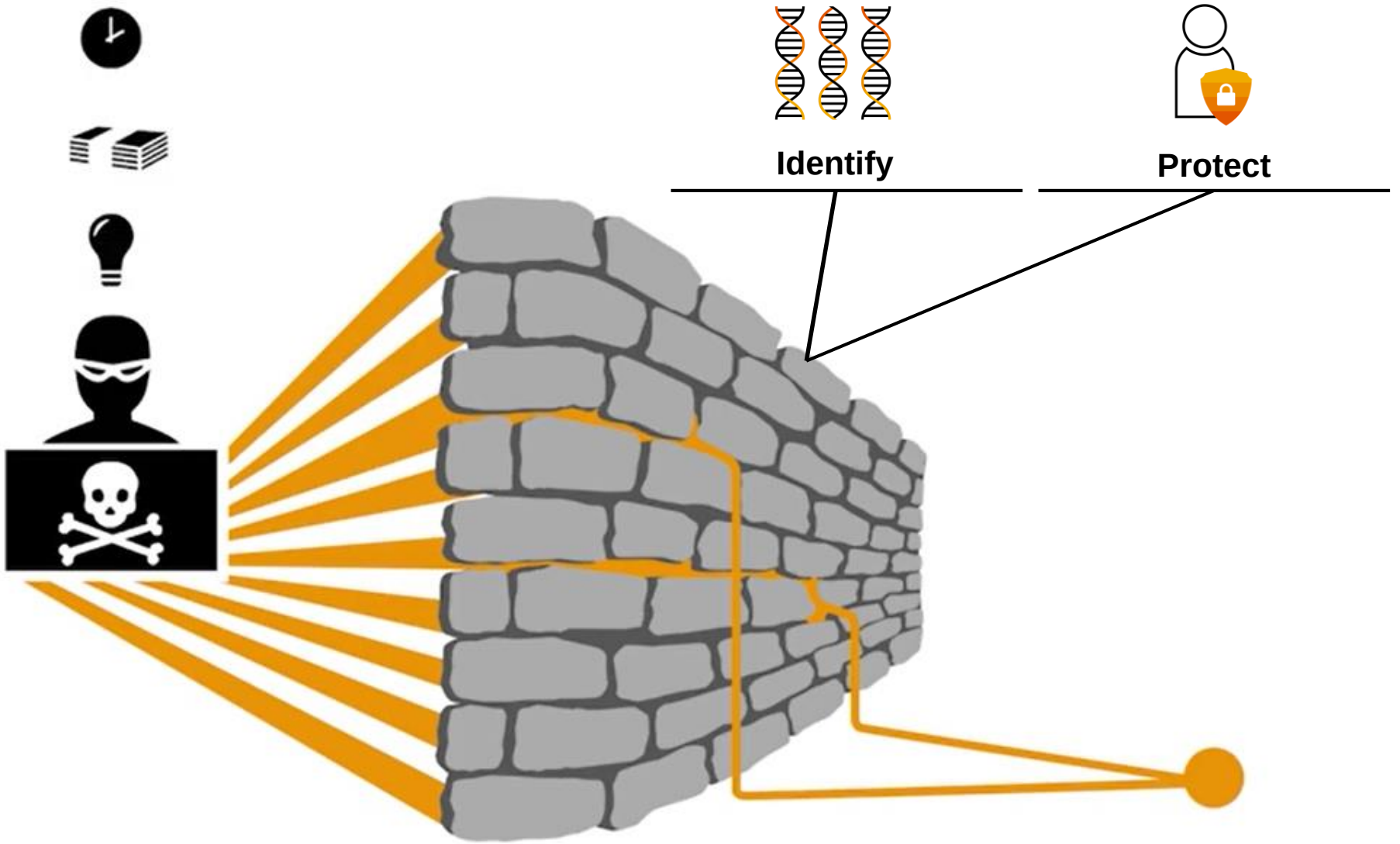
Recover

Recovery Planning

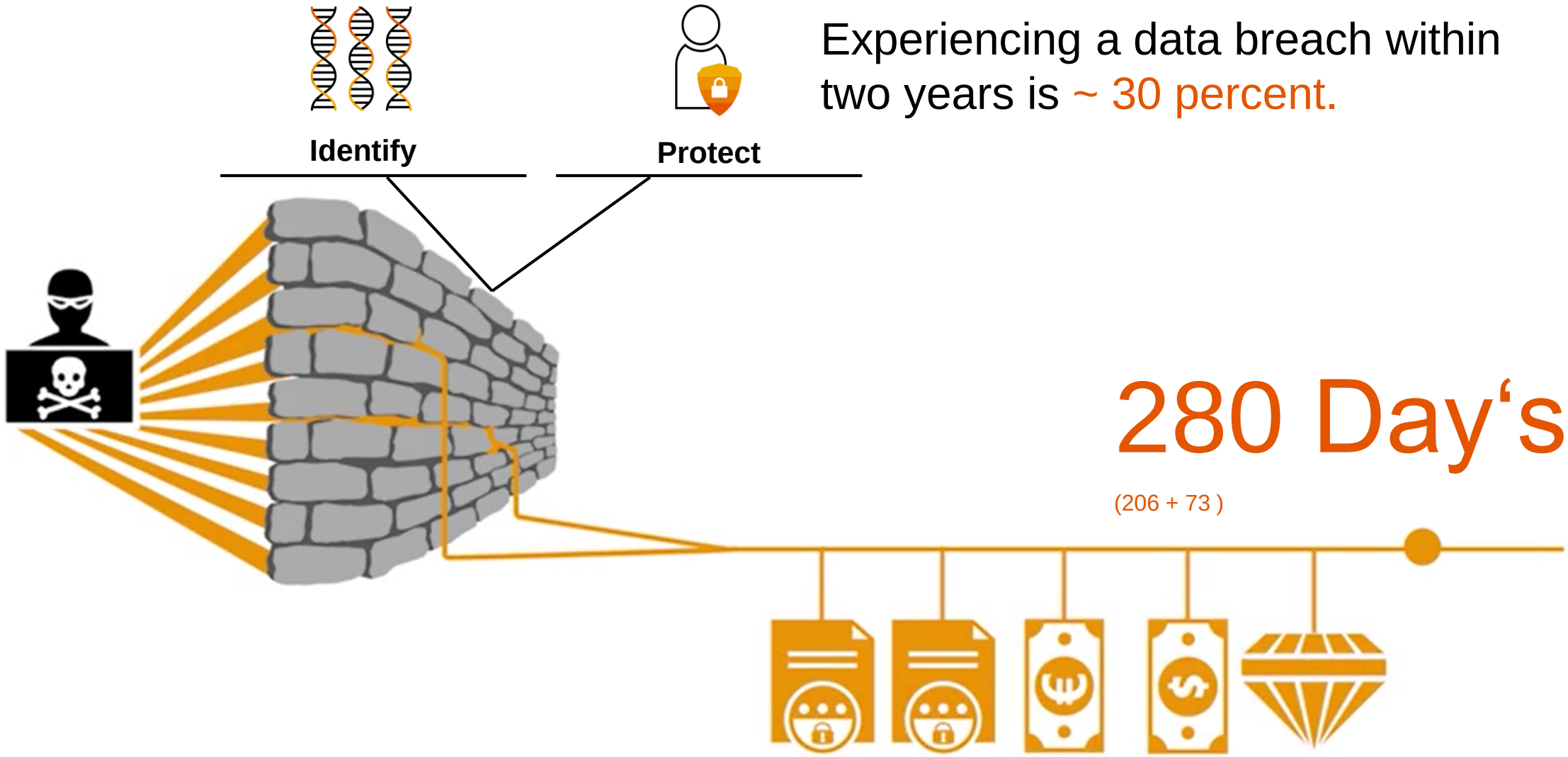
Improvements

Communications

SAP Enterprise Threat Detection – preventing cyber attacks



SAP Enterprise Threat Detection – preventing cyber attacks

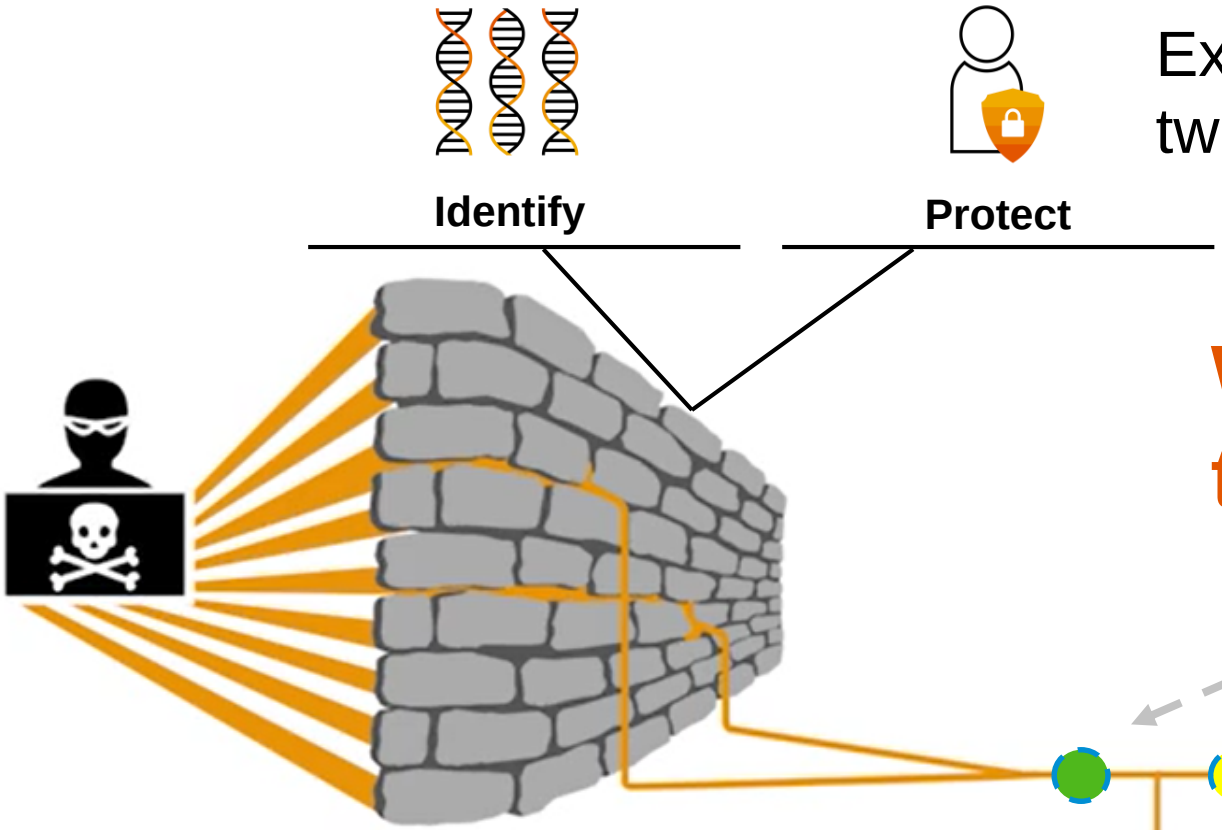


Experiencing a data breach within two years is ~ 30 percent.

280 Day‘s

(206 + 73)

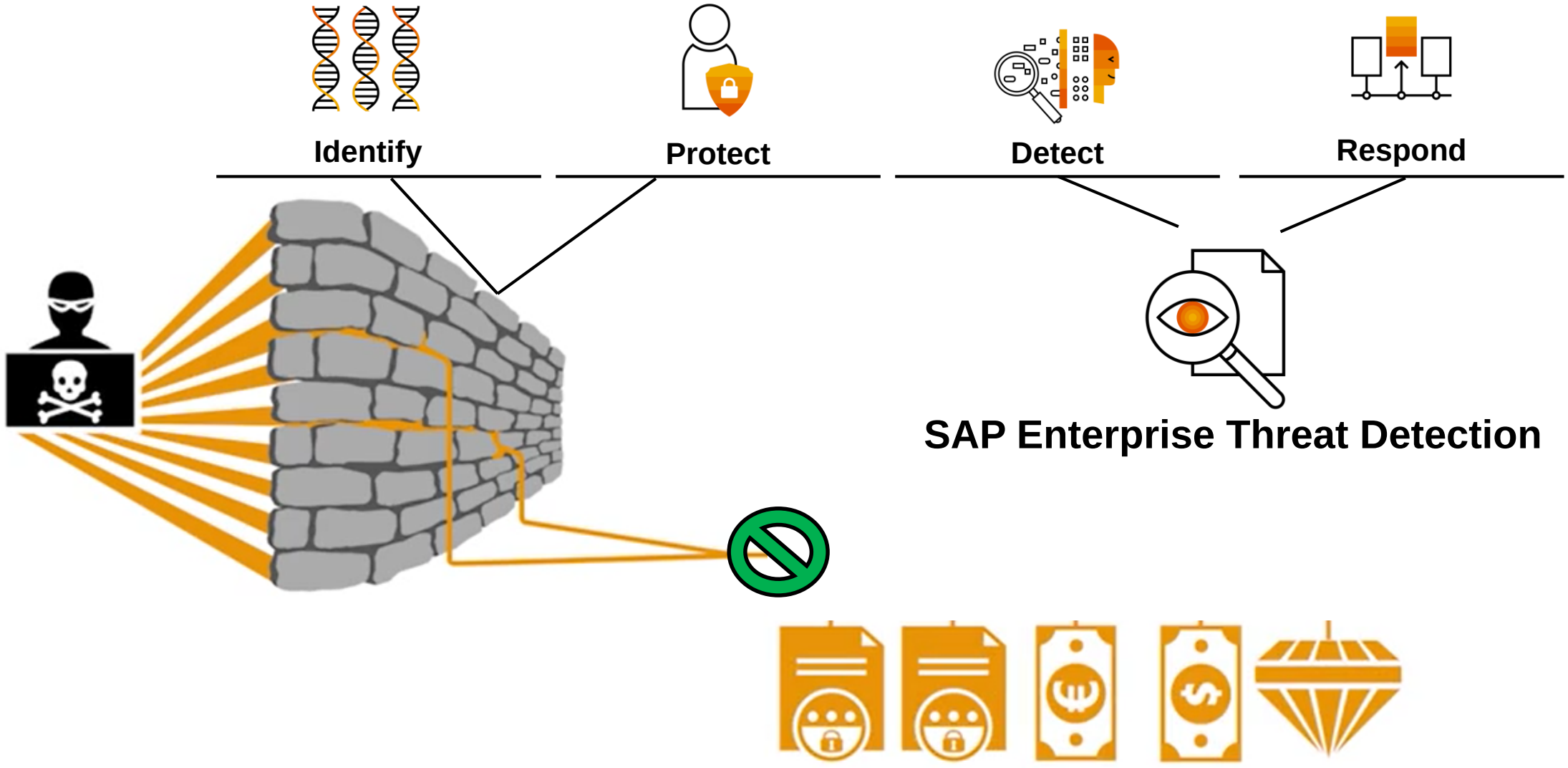
SAP Enterprise Threat Detection – preventing cyber attacks



Experiencing a data breach within two years is ~ 30 percent.

When are you able to stop a breach ?

SAP Enterprise Threat Detection – preventing cyber attacks



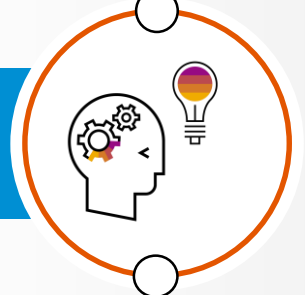
Security Audit Log compliance

Challenge

- Complex configuration
- Causes performance problems
- Must be filtered
- Cannot be read by humans
- Cannot be searched in an efficiant way
- Cannot be stored for Audit purpose

Incompliante

Solution



- Direct transfer of all information belonging to the Security Audit log to SAP Enterprise Threat Detection

Benefits

- Manipulation safe Audit Log
- No additional configuration
- All Security Audit Log entries are available
- Continuous automated analysis
- Manual human analysis possible
- Audit proof at any time

Compliant

Preventing Fraud & Cyber Attacks

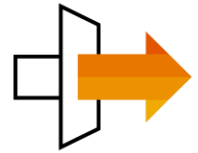
Debugging DEV System

Discover SM59 connections

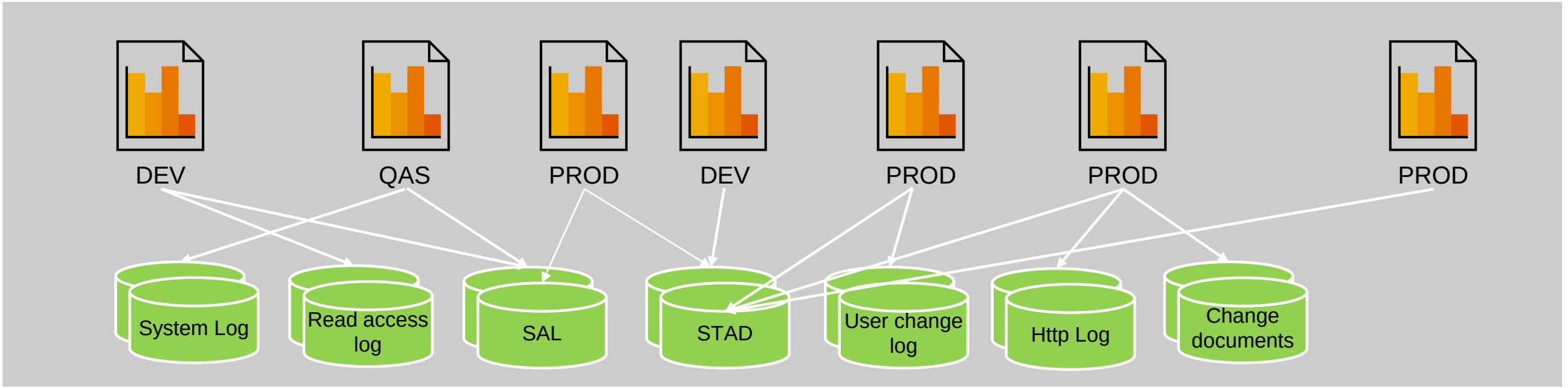
RFC to change passwd

Change vendor

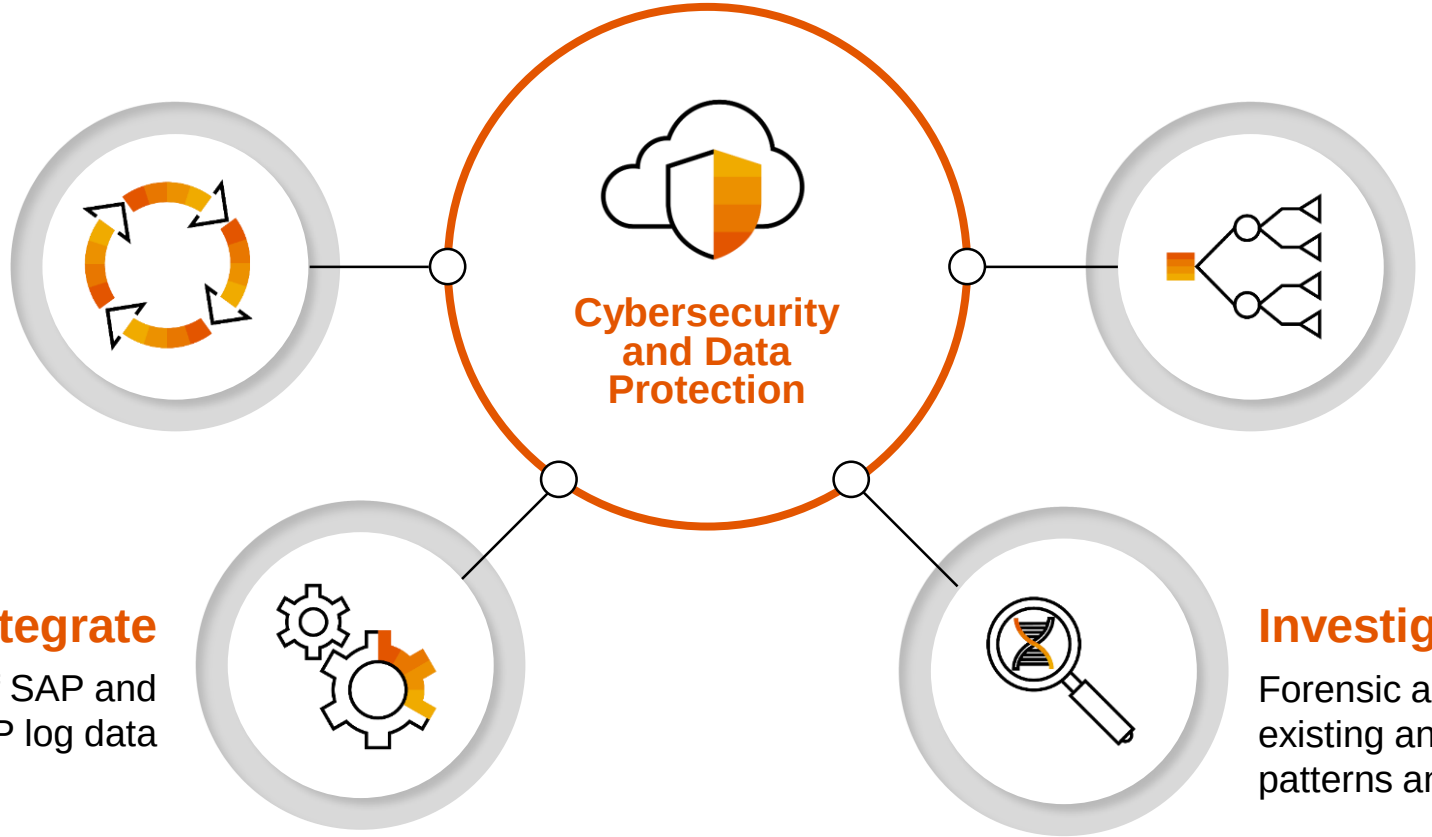
Outgoing payments



01.2020 | 06.2020 | 03.2021



How does SAP Enterprise Threat Detection work



Analyze

Efficiently enrich, analyze, and correlate logs

Evaluate

Automatically evaluate attack detection patterns with real-time alerting

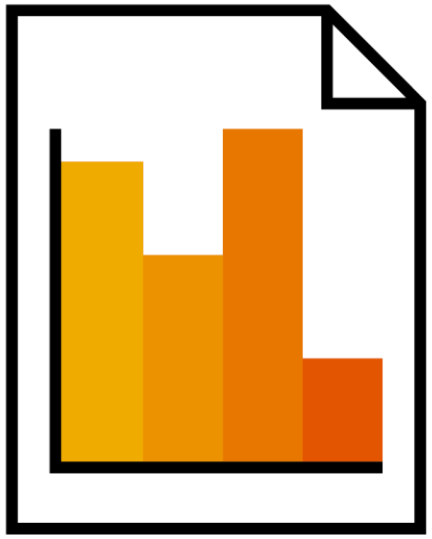
Integrate

Integration of SAP and non-SAP log data

Investigate

Forensic analysis and modeling of existing and new attack detection patterns and dashboards

Log Data Supported by ETD



SAP Netweaver/ S/4 Log Types

- System Log
- Security Audit Log
- Business Transaction Log
- HTTP Server Log
- RFC Gateway Log
- User Change Log
- Change Document Log
- Read Access Log / UI Log
- SOAP based Web Services Log

SAP Netwaever Java

- HTTP Access Log (Java)
- Security Audit Log (Java)
- Security Log (Java)

HANA DB

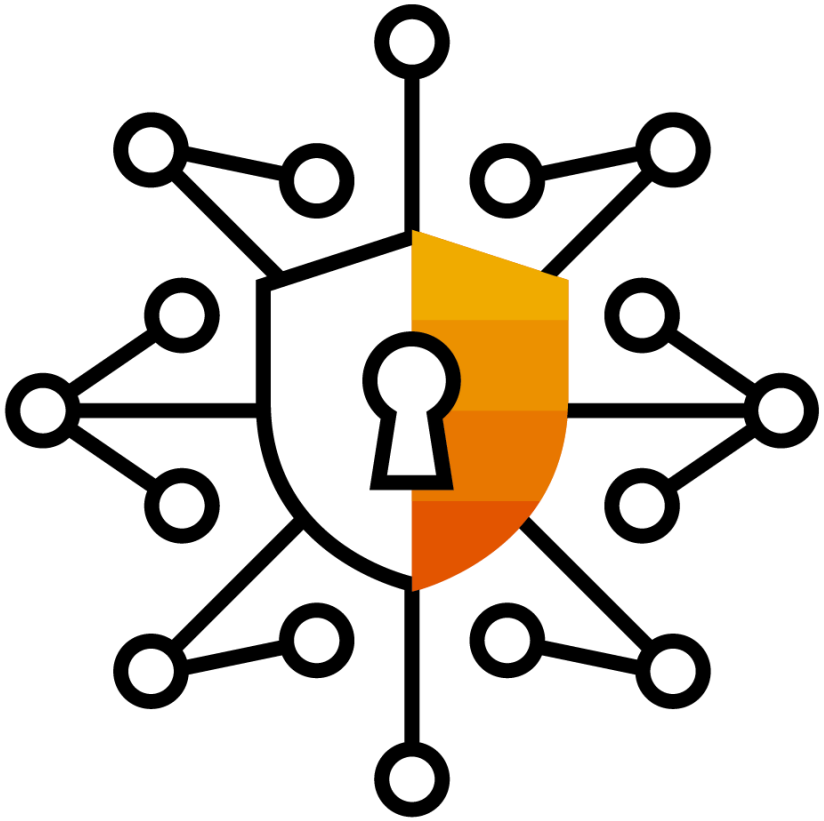
- HANA Audit Trail

SAP Cloud Platform

- SAP Cloud Platform Audit Logs (Neo +CF)

Unique benefits of Enterprise Threat Detection

- Forensic Analysis, Threat Hunting, Anomaly detection
- All SAP logs unfiltered, normalized, readable to be used by Audit
- Analysis of Read access logging logs, SOAP based web services logs, UI Logging Logs
- Any log type can be added
- Continuous automated detection, analyze and neutralize cyber-attacks in real time
- Real time manipulation save data transfer to Enterprise Threat Detection
- Look at all log types and correlate the complete picture, not only a few small puzzle peace’s
- Analysis of e.g.: What else did the user do?
- Generic approach (not based on fix test cases)



Use cases samples

- Activation of high privilege accounts (Type Firefighter, SAP_ALL)
- An unauthorized user assigned a critical SAP role to same user / different user
- Newly created user logs on via the same terminal as of the user was just created
- Switching off the SAL (including Security configuration is changed)
- A critical transaction is unlocked
- Use of critical transactions such as SE16 or similar
- Miss-use of debugging and error-analysis
- Monitoring locking/unlocking of production for direct changes
- e.g. HR data is accessed (read only)
- e.g. HR data is accessed (and changed)
- Monitoring whether the logging to the monitored components is activated or not
- Account sharing is detected
- SAP debugging is used for bypassing transaction authorizations

- Activation of high privilege accounts (Type Firefighter, SAP_ALL)
- An unauthorized user assigned a critical SAP role to same user / different user
- Newly created user logs on via the same terminal as of the user was just created
- Switching off the SAL (including Security configuration is changed)
- A critical transaction is unlocked
- Use of critical transactions such as SE16 or similar
- Miss-use of debugging and error-analysis
- Monitoring locking/unlocking of production for direct changes
- e.g. HR data is accessed (read only)
- e.g. HR data is accessed (and changed)
- Monitoring whether the logging to the monitored components is activated or not
- Account sharing is detected
- SAP debugging is used for bypassing transaction authorizations

SAP Enterprise Threat Detection

More than 220 SAP customers worldwide in all industries protect their SAP landscape with SAP Enterprise Threat Detection.

Most of those companies are listed within the DAX 30, DOW 30, or come e.g. from the defense sector. Please address the authors or your SAP account manager for more details about our reference customers.

SAP Enterprise Threat Detection is supported by the world leading auditing companies.

We have implementation partners in many regions of the world.

Partners are e.g.:

- Ernst & Young,
- KPMG,
- Turnkey,
- IBS Schreiber,
- Asconsit,
- PWC,
- SAPNS2,
- Deloitte
- Accenture,
- Infosys,
- Xiting…

Benefits of SAP Enterprise Threat Detection

SAP system Transparency with respect to Security- and Compliance-Events

Single Source of truth for centrally audited SAP Security Controls improves compliance

Audit logs are easy to read and transparent

Real Time Threat Visibility in Complex SAP Scenarios

Proactive Threat Monitoring and Treat Hunting leads to an Early Interception of Threats

High Manipulation Safety of SAP Systems

Improved monitoring of user activity and auditing

Intellectual Property

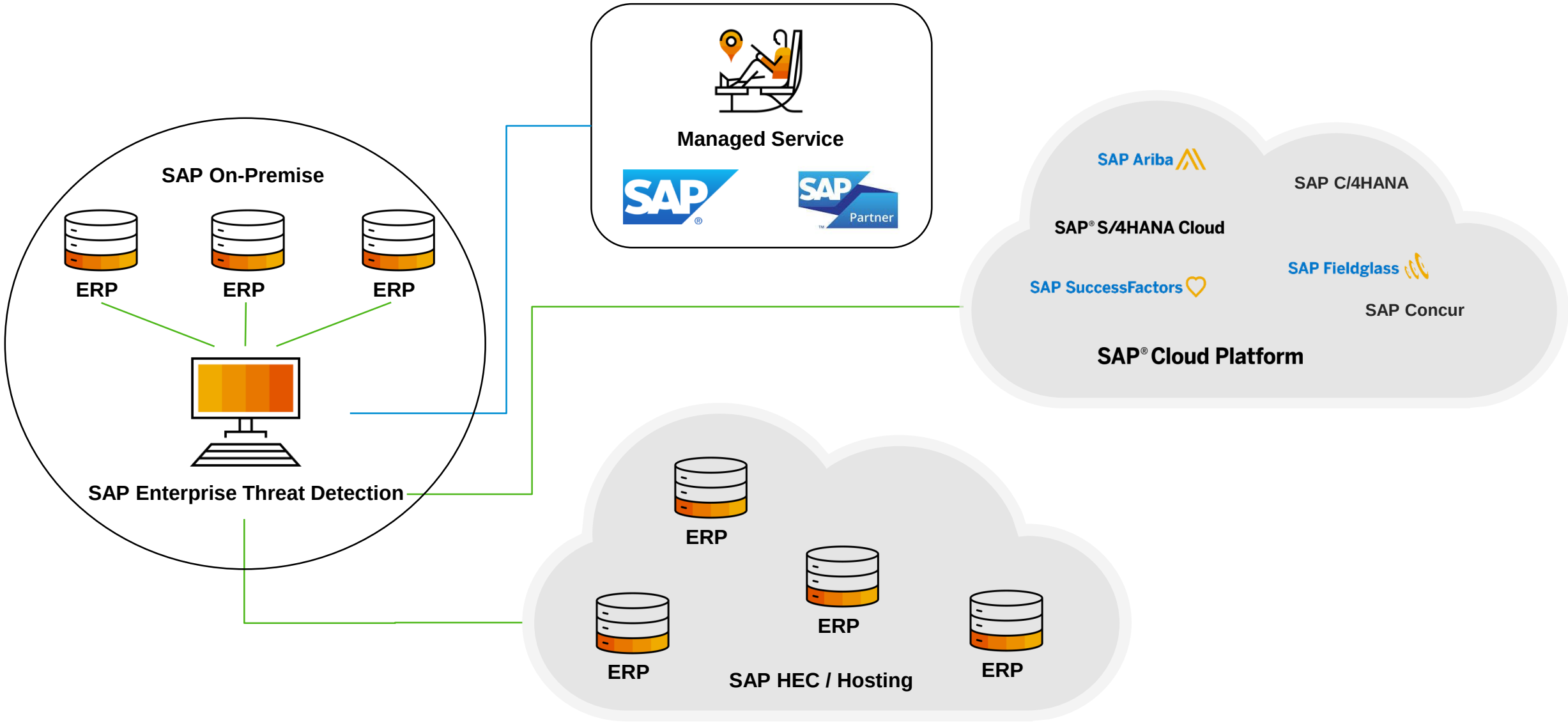
Reputation

Sensitive Data

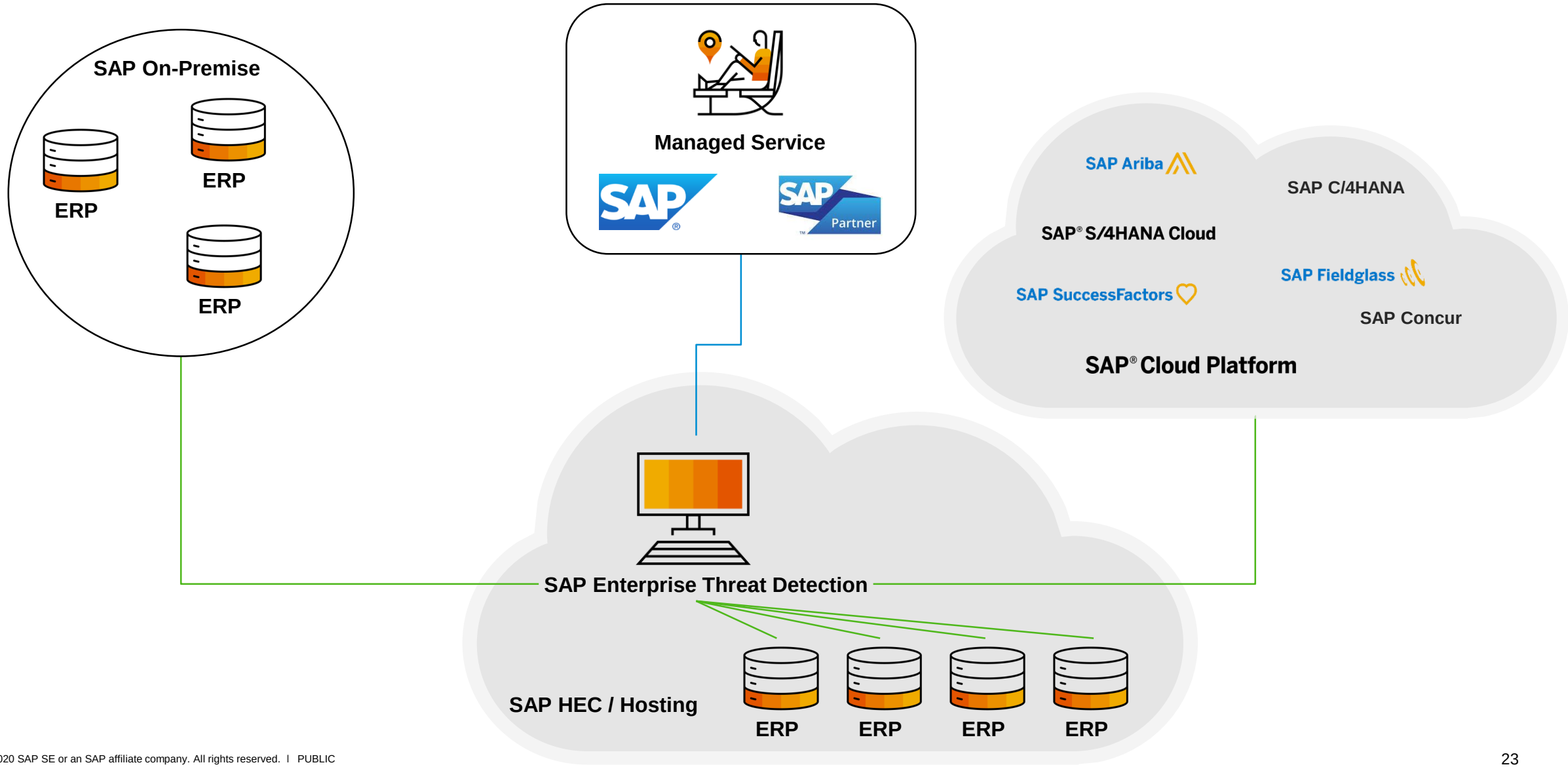
Severe Penalties

Business Future

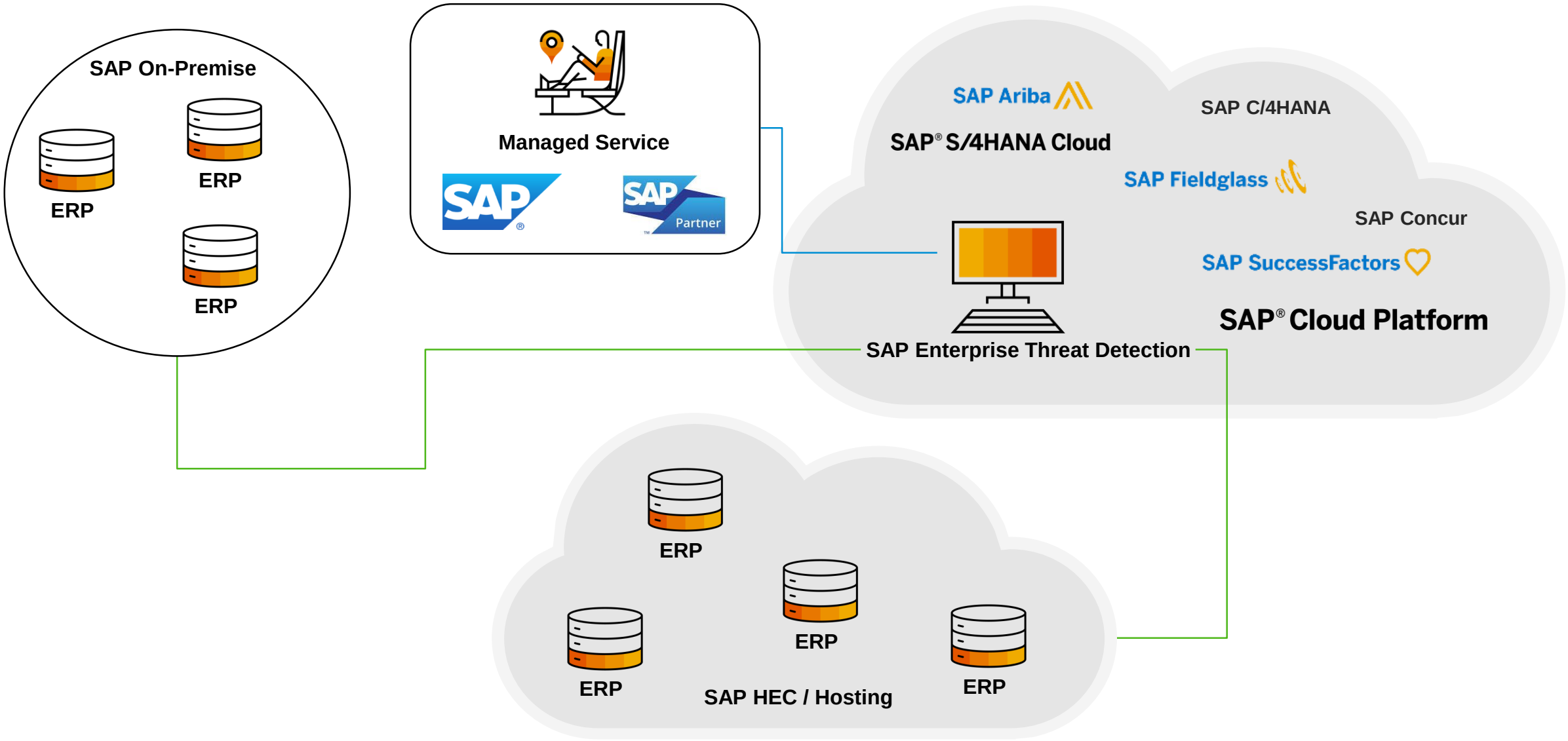
SAP Enterprise Threat Detection — Architecture



SAP Enterprise Threat Detection — Architecture



SAP Enterprise Threat Detection Cloud Edition (2021) — Architecture



P.S.: Save trees: please do not print out your application logs

Demo

Attack and defend

Hands on

Go to GitHub …..

….

….

…..tbd

More information

Related SAP TechEd sessions

- IIS125 – Security Roundtable

Public SAP Web sites

- SAP Community: https://community.sap.com/topics/enterprise-threat-detection
- SAP products: https://www.sap.com/germany/products/enterprise-threat-detection.html
- SAP Focused Run: https://support.sap.com/en/alm/sap-focused-run.html
- SAP Code Vulnerability Analyzer: https://community.sap.com/topics/abap-testing-analysis/code-vulnerability-analyzer

Continue your learning experience from SAP TechEd in 2020

Your exclusive path to build and maintain SAP solution skills anytime, any place

Get empowered with access to relevant, up-to-date digital learning for SAP TechEd participants through a complete enablement solution that drives adoption and innovation.

Deepen your learning experience from SAP TechEd

Activate your free access to SAP Learning Hub, event edition, for:

- **Learning Journey** illustrations to guide you through **complementary** self-paced learning content
- **Content specific to SAP TechEd** in the online **SAP Learning Room for SAP TechEd**
- Access to SAP experts in **special live sessions**

Deepen and validate your SAP solution skills

Subscribe to SAP Learning Hub, solution editions, for:

- **Solution-specific Learning Journey guides, content, collaborative learning,** and **hands-on practice** for your role and goals
- Drive performance and business success with validated solution expertise from the **SAP Global Certification** program

Your benefits

- Gain insight into the latest innovations, and master software proficiency
- Keep skills up-to-date, and enable performance and business success with help from SAP solution experts
- Achieve competitive advantages and digital transformation success with trusted certifications

500,000+
Learners in SAP Learning Hub

100+
Experts getting certified per day

150+
SAP Global Certifications

Thanks for attending this session.

Contact for further topic inquiries

Arndt Lingscheid
Product Manager
SAP Enterprise Threat Detection
a.lingscheid@sap.com

Michael Schmitt
Product Manager
SAP Enterprise Threat Detection
m.schnmitt@sap.com

Follow us

www.sap.com/contactsap

THE BEST RUN SAP®