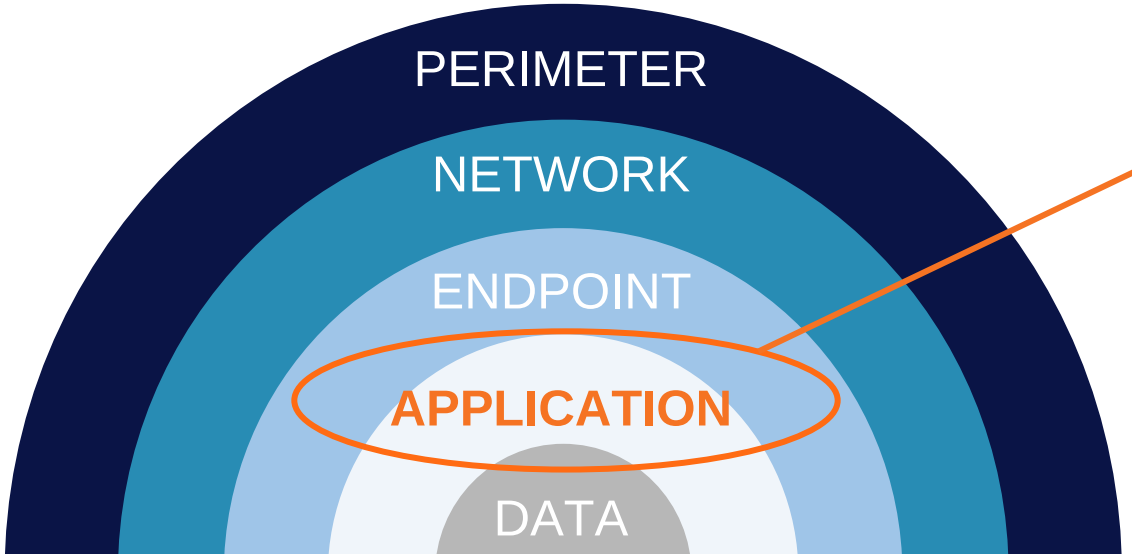
ONAPSIS

SAP Security 101 | 5 Things Every Leader & Organization Should be Doing to Secure SAP

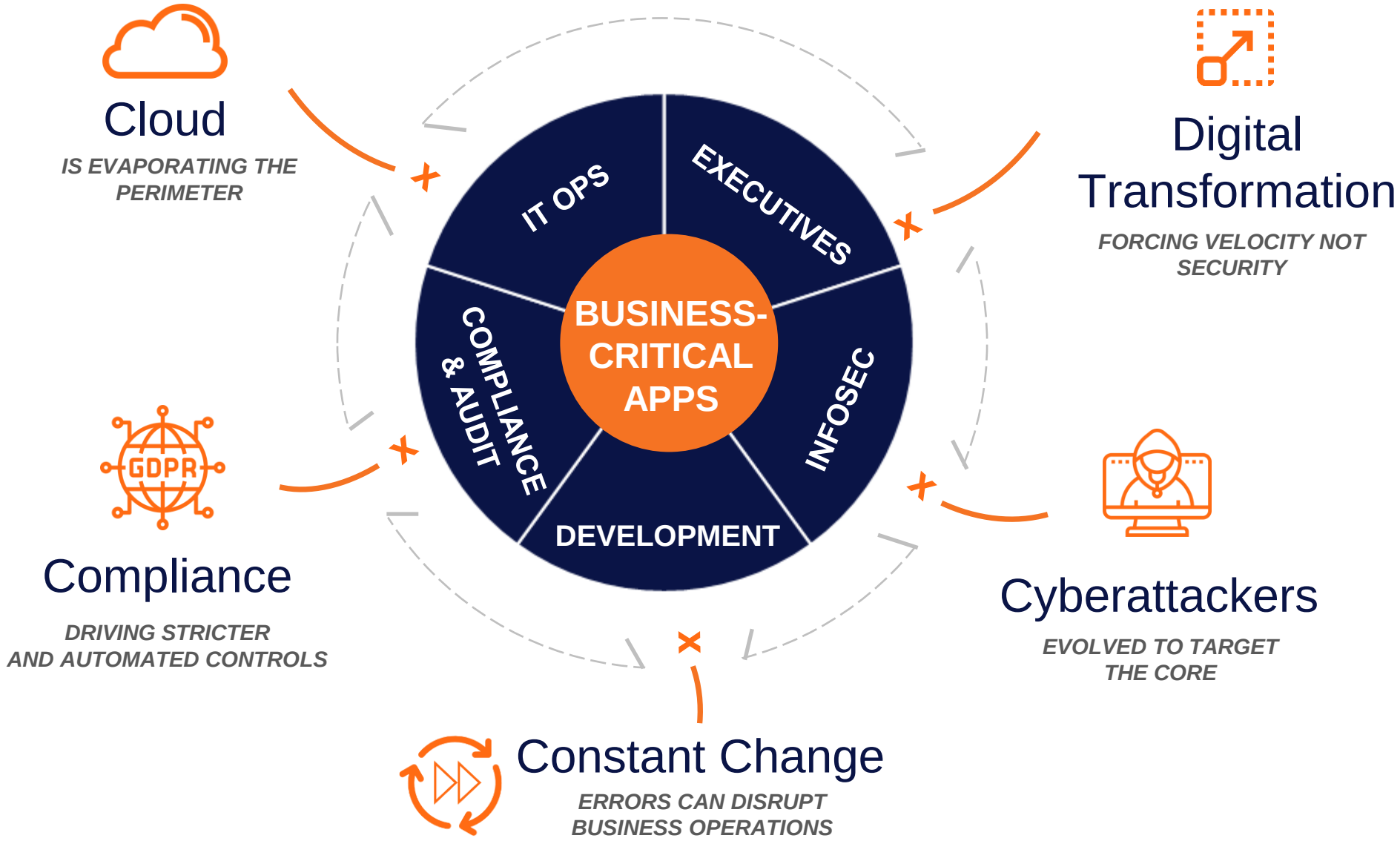
WHY AREN'T TYPICAL SECURITY EFFORTS EFFECTIVE HERE?

Defense-in-Depth Models Surround but Ultimately Neglect That Critical Application Layer.



- **Attacks on the application layer** are the #1 concern of CIOs, which increased YoY
- **Over 70%** say their application portfolio has become **more vulnerable** in the past year
- Almost **two-thirds of organizations have a backlog** of application vulnerabilities

WE'RE FACING A PERFECT STORM OF COMPLEXITY



EVOLUTION OF BUSINESS-CRITICAL APPLICATION CYBERATTACKS

64% ***OF ERP SYSTEMS HAVE BEEN BREACHED IN THE PAST 2 YEARS***

IDC ANALYZE THE FUTURE

2012
HACKTIVIST GROUPS
1st public exploit targeting SAP applications

2013
CYBER CRIMINALS CREATING MALWARE
SAP targeted malware discovered

2014
PUBLIC EXPLOIT
Chinese hacker exploits SAP NetWeaver

2015
NATION-STATE SPONSORED
Chinese breach of USIS targeted SAP

2016
1ST DHS US-CERT ALERT
for SAP Business Applications

2017
INCREASED INTEREST ON DARK WEB
Onapsis helps Oracle secure critical vulnerability in EBS

2018
2ND DHS US-CERT ALERT
for SAP Business Applications

2019
3RD DHS US-CERT ALERT
for SAP 10KBLAZE Vulnerability

PAYDAY
Oracle Vulnerabilities

2020
EXPLOIT TOOLKIT
SAP RFCpwn

BigDebIT
Oracle Vulnerabilities

4th DHS US-CERT ALERT
for SAP RECON Vulnerability

2021
PUBLIC EXPLOIT
SAP SolMan

5th DHS US-CERT ALERT
on malicious activity targeting SAP applications

2022
6th DHS US-CERT ALERT
SAP ICMAD Critical Vulnerabilities

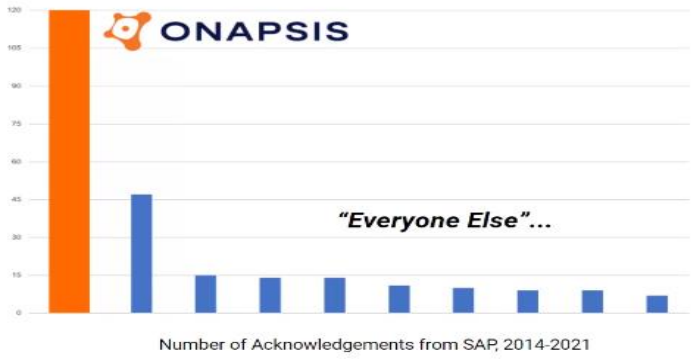
How Did We Quantify This? Well, We Built the ONAPSIS **THREAT INTELLIGENCE CLOUD**

Synthetic targets,
Real attacks from real threat actors.

STAY AHEAD OF EVER-EVOLVING CYBERSECURITY THREATS WITH THE WORLD'S LEADING THREAT RESEARCH ON BUSINESS-CRITICAL APPLICATIONS

ONAPSIS RESEARCH LABS

- Onapsis products automatically updated with latest threat intel and security guidance
- Receive advanced notification on critical issues and improved configurations
- **Get pre-patch protection ahead of scheduled vendor updates**



Number of Acknowledgements from SAP, 2014-2021

Discovered
1000+
zero-day vulnerabilities in business-critical apps

40%
Of critical SAP Security Notes in 2020 were influenced by Onapsis Research Labs

6
US DHS critical alerts based on our research

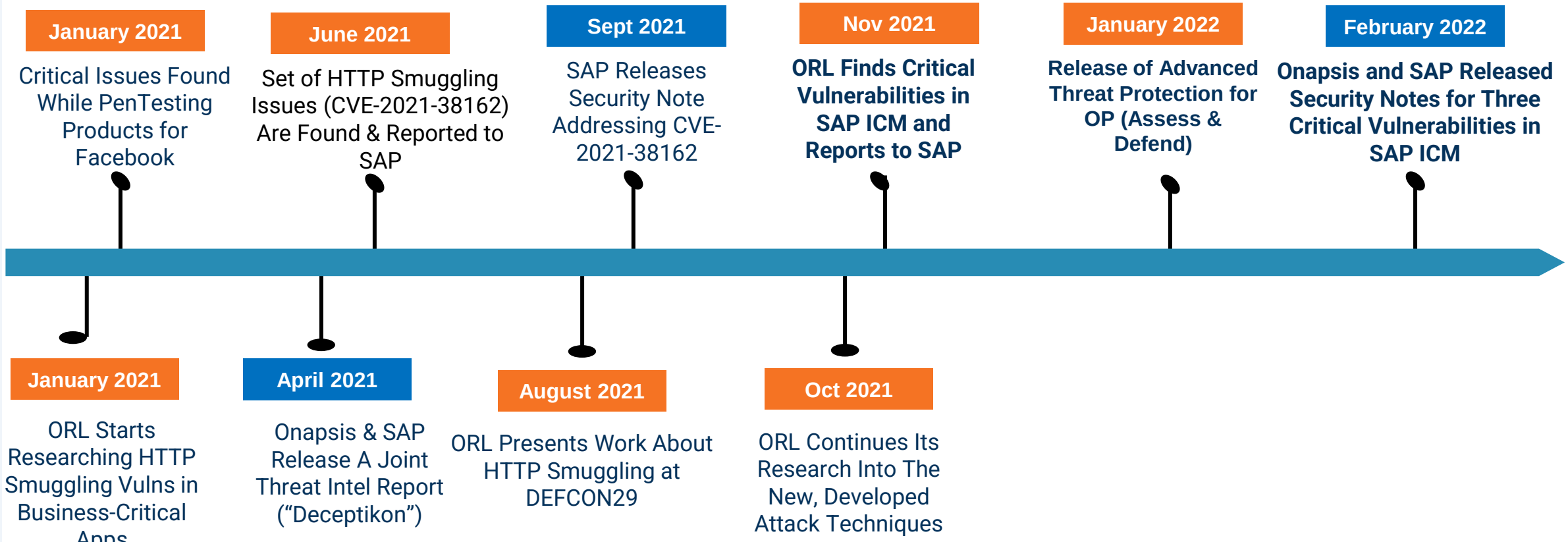
17
Patents, 8 issued & 9 pending

Knowledgebase of
10,000+
vulnerabilities and attacks on business applications

ICMAD Vulnerability Timeline

- SAP Internet Communication Manager (ICM) is affected. “The gate to the outside world” for SAP systems
- ORL found **three vulnerabilities affecting** this component, Almost every productive system exposed to the Internet can be affected
  - CVE-2022-XXXX CVSSv3 10.0 (AV:N/AC:L/PR:N/UI:N/S:C/C:H/I:H/A:H)
  - CVE-2022-YYYY CVSSv3 8.1 (AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:H/A:H)
  - CVE-2022-ZZZZ CVSSv3 7.5 (AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H)

- Leveraging these vulnerabilities, a **Remote Unauthenticated Attacker** can steal…
  - Cookies / user sessions
  - Username and passwords
  - Sensitive information



What is your SAP Transformation journey?

Choose your adventure…(or maybe you already have)

Green Field
Start from the beginning and use SAP best practices

Brown Field
Lift and shift to a Hyperscaler to gain operational efficiency

Project Delays

52% Of cloud migrations are delayed due to security concerns[1]

Reputation Damage

7.3% Average decrease in stock price following a security breach[2]

Financial Ramifications

$2M Average yearly cost of fines and penalties due to non-compliance[5]

THE ONAPSIS PLATFORM | PRODUCTS & FUNCTIONALITY

ASSESS

Vulnerability Management

- System misconfigurations, missing patches
- Authorization issues, default accounts/roles
- Assess if systems are configured in line with best practices

Integrations with workflow services:

servicenow

DEFEND

Continuous Threat Monitoring

- Real-time attack alerts
- Monitor for exploits, user activity / transactions, privilege misuse
- Alert for dangerous program executions

Integrations with SIEMs:

splunk> ArcSight Radar exabeam

CONTROL

Application Security Testing & Transport Inspection

- Identify security, compliance, and quality errors in SAP custom code
- Identify SAP transports that would cause import errors, outages, downgrades, security or compliance issues

Integrations with change management and development environments:

SAP ChaRM, TMS, HANA Studio, Eclipse, Web IDE, ABAP development workbench

COMPLY

Continuous Compliance

- Evaluate compliance impact of system vulnerabilities, misconfigurations, patches, authorizations, deployed code (SAP)
- Out-of-the-box & custom policies
- Evaluate and verify IT controls

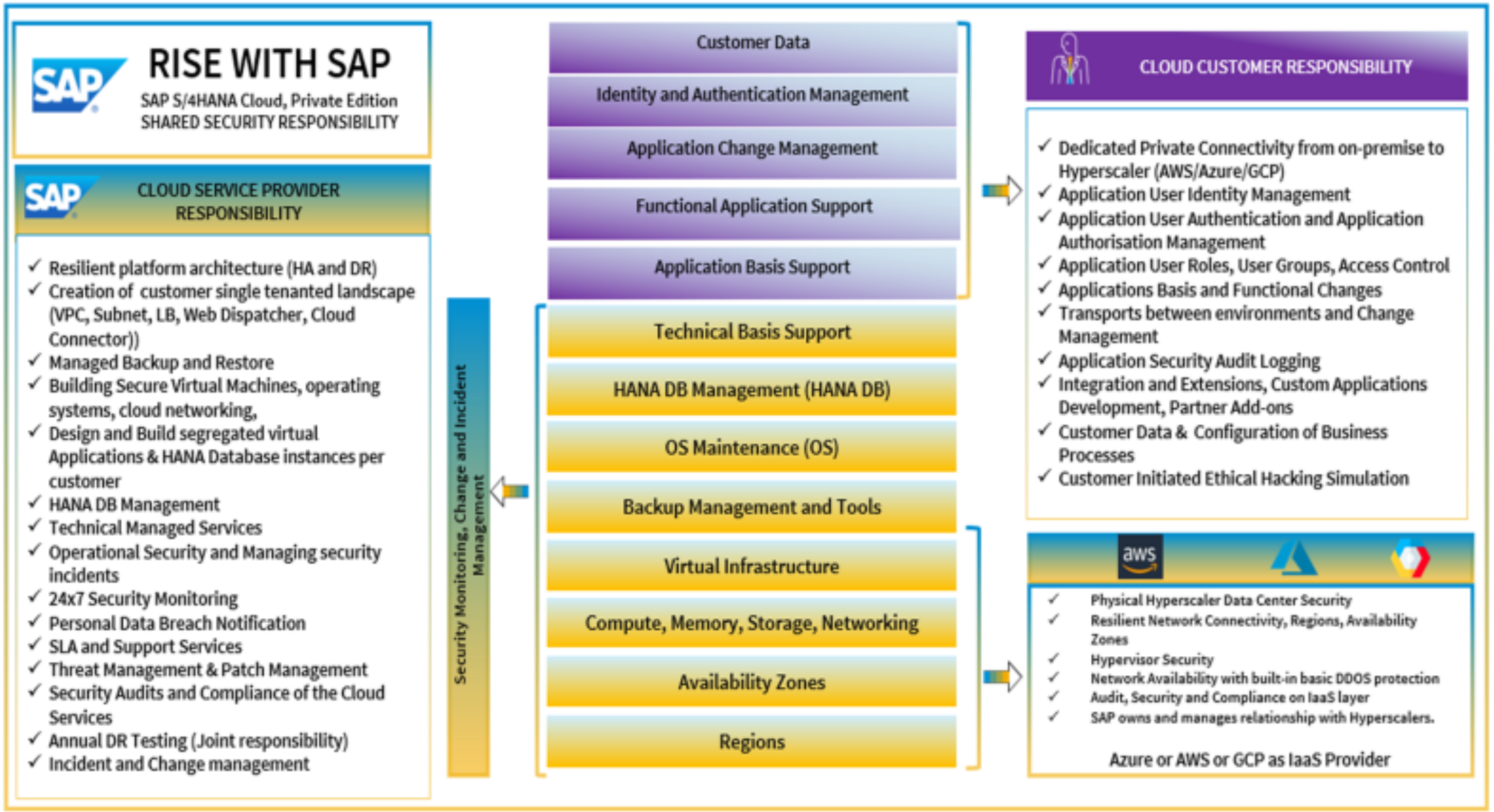
Integrations with compliance automation solutions:

SAP Process Control

MANAGEMENT FUNCTIONALITY

Reporting & Analysis | Ticketing/SOC Integration | Scheduling & Workflows | Asset Discovery | Users & Role Management

RISE with SAP: Shared Security Responsibility for SAP Cloud Services



This Means We May Have a Gap with Understanding The **True Risk** to Our ERP Journey… and Our Organization

Vulnerabilities?

- ERP systems are frequently managed by other teams, with little to no visibility for InfoSec
- More processes moving to SaaS applications
- Increasing reliance on code or apps developed by contracted third-parties

Threat Monitoring?

- No meaningful monitoring of ERP, with little to no visibility for the SOC
- Reliance on manual log reviews to identify threat activity in ERPs
- No ability to establish compensating controls

Code Optimization?

- Security is frequently “bolt on” and not “built in”
- Reliance on manual code reviews
- Problems aren’t identified until they hit production

…And Five Things To Do Today

1. Treat Business-Critical Apps Like OT Critical Infrastructure
2. Timely Patch Management
3. Continuous Monitoring of Vulnerabilities and Threats to Your ERP Applications
4. Secure Your Custom Code in ERP Applications
5. Commit to Control and Governance

Thank You!

linkedin.com/company/onapsis

ONAPSIS.COM

ONAPSIS