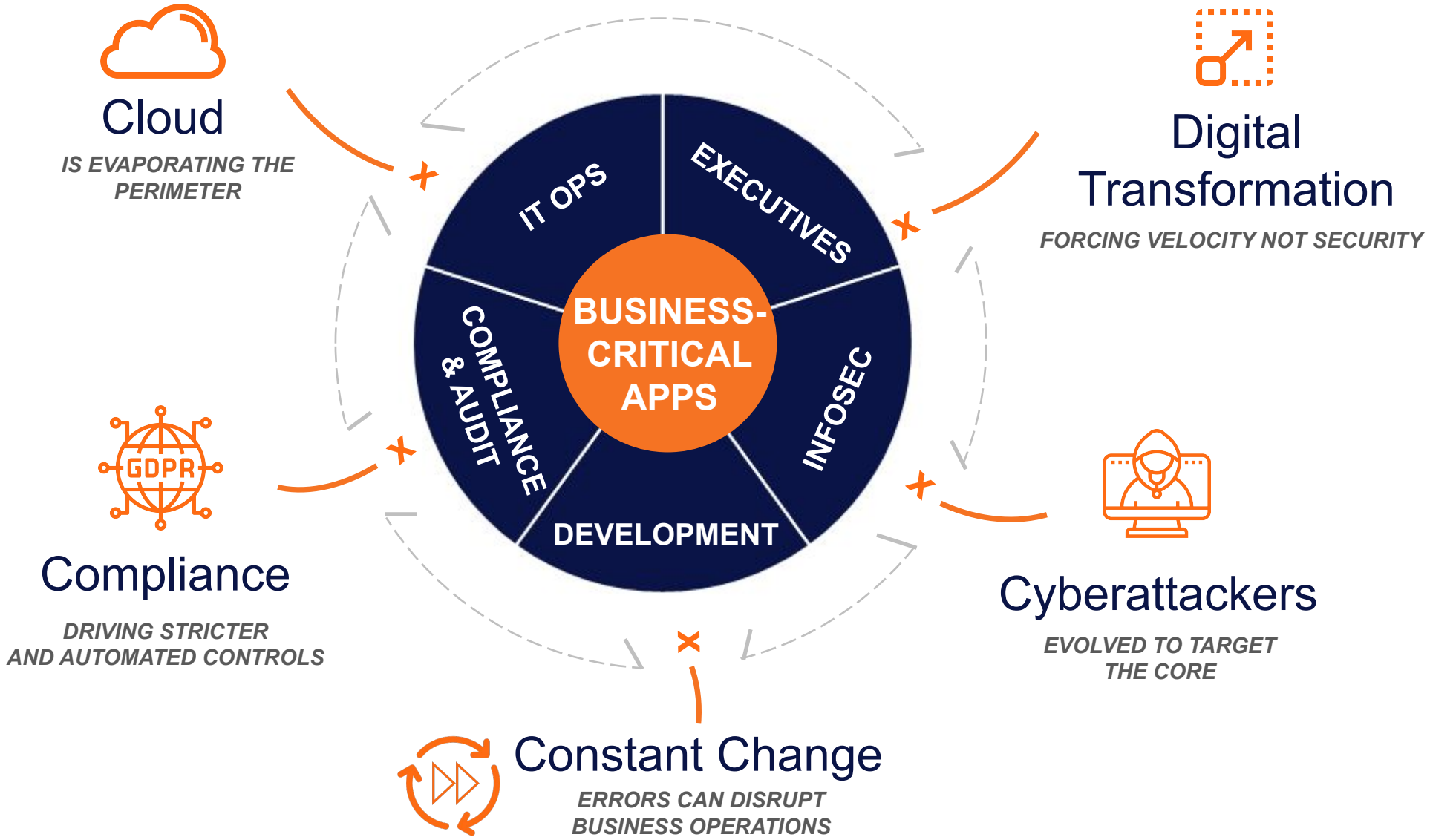
SAP Security 101 | 5 Things Every Leader & Organization Should be Doing to Secure SAP

Jordan Thompson – Strategic Account Manager

WE'RE FACING A PERFECT STORM OF COMPLEXITY



Cloud

IS EVAPORATING THE PERIMETER

Digital Transformation

FORCING VELOCITY NOT SECURITY

Compliance

DRIVING STRICTER AND AUTOMATED CONTROLS

Cyberattackers

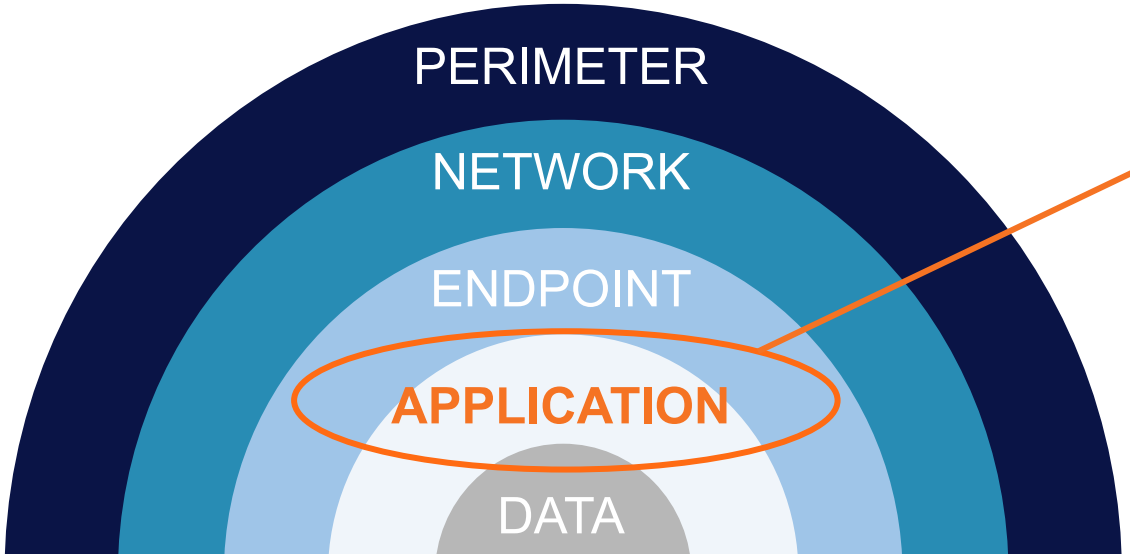
EVOLVED TO TARGET THE CORE

Constant Change

ERRORS CAN DISRUPT BUSINESS OPERATIONS

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

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

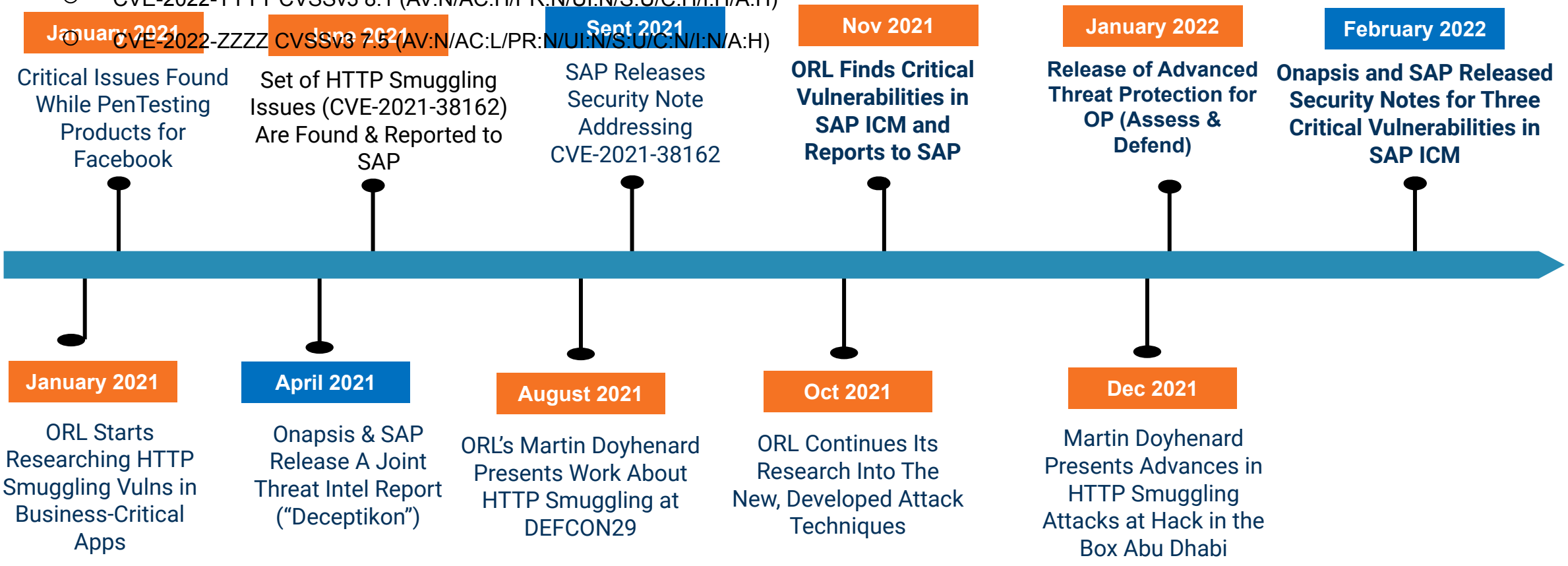
2021
PUBLIC EXPLOIT
SAP SolMan

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

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

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



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

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

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

“Rainbow” Field
Parts of Green, Brown and every color of the rainbow to meet business requirements

Project Delays

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

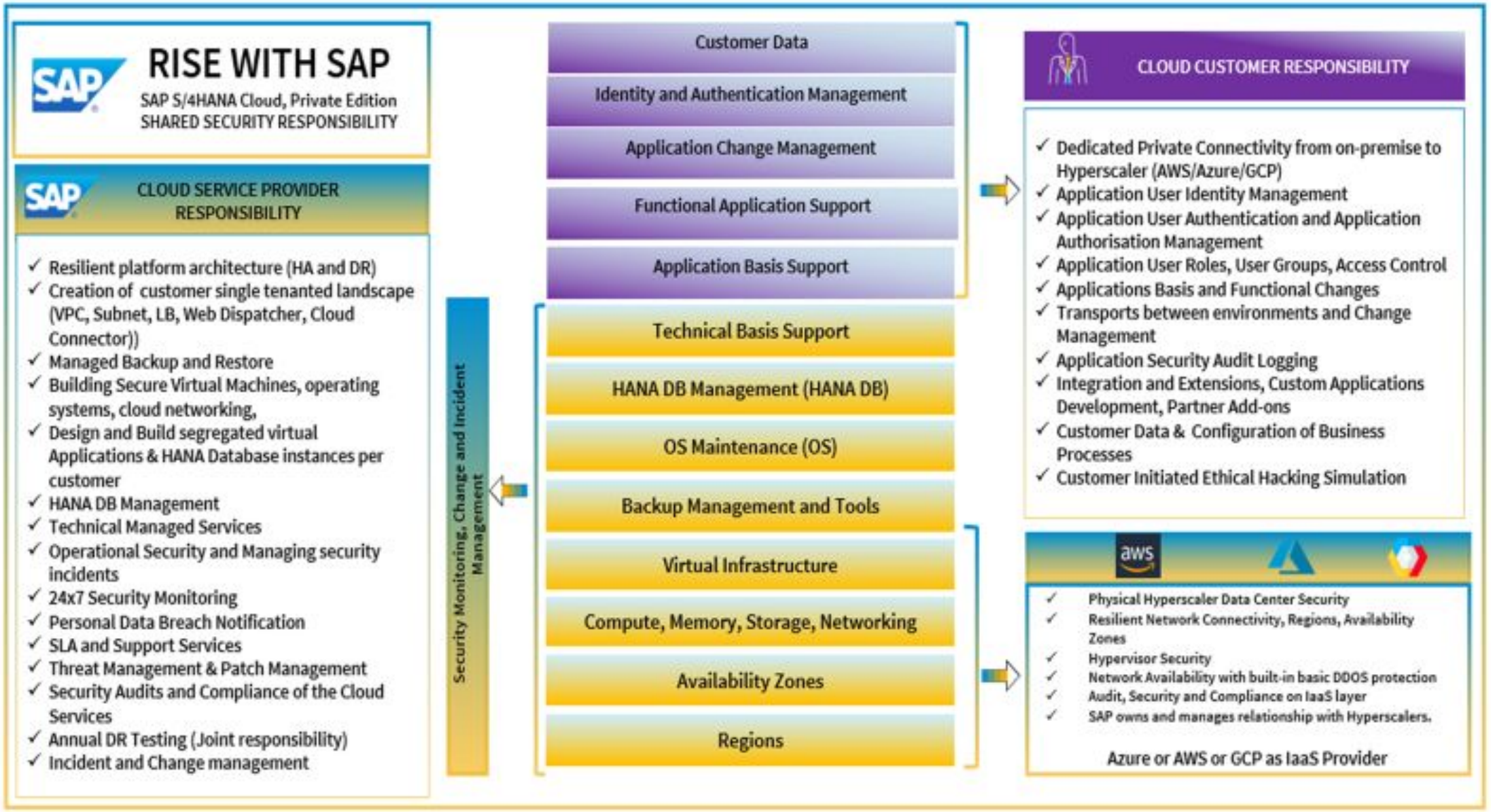
Reputation Damage

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]

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

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

ASSESS | VULNERABILITY & SECURITY POSTURE MANAGEMENT

- **Visibility** into vulnerabilities, misconfigurations, authorization errors, and security posture
- **Understand risk** and business impact
- **Manage issues** with built-in workflows and integrations with external ticketing systems

servicenow

- **Streamline remediation** with detailed step-by-step technical solutions
- **Report** on vulnerability and security posture over time via dashboards and exportable exec summaries
- **In short,** Assess prioritizes patches based off your systems and validates if patches/security notes have been applied correctly. The efficiencies gained, according to our customers, traditionally equates to around ~$37.5K per basis resource

60%	Decrease in remediation efforts
75%	Issue investigation time eliminated due to low false positive rate
95%	Less time identifying and investigating vs manual efforts
60%	Time saved preparing executive reports
80%	Time saved scheduling patches with built-in prioritization

Fortune 500 Utility Company

COMPANY

2K Employees

$2B revenue

INDUSTRY

Energy

> ***Onapsis removes the mystery around SAP security by increasing visibility.*** *We can see ...misconfigurations, missing patches or unusual user activity - what risk they post and how to fix them*
>
> *- CISO*

CHALLENGE: A labor intensive patch and vulnerability management process created visibility and security gaps within SAP for a small team

SOLUTION: Onapsis Assess and Defend to scan and continuously monitor its SAP environment for vulnerabilities, misconfigurations, missed patches, and new threats.

RESULT: Gained visibility into SAP, including activity of third party contractors; streamlined and automated the patch and vulnerability management process, allowing the team to scale and refocus

CONTROL FOR CODE | SAP APPLICATION SECURITY TESTING

- **Identify** security, compliance, and quality issues in “real-time” or in batches before release
- **Understand** business risk and criticality
- **Manage** issues via built-in approval workflows
- **Resolve** with detailed step-by-step remediation guidance
- **Mass correction** services available to automate the fix of bulk issues
- **In short,** Control for code automates the code review efforts by approximately 80% and developer efficiencies by 20-40%

25x	Faster than manual review processes
1 minute	Scan up to 150,000 lines of code
<5%	False positive rate
75%	Reduction in errors making it into production
50 -80%	Common findings automatically fixed with optional service

COMPLY | AUTOMATED COMPLIANCE TESTING & VERIFICATION

- **Automate evidence collection** to prepare for internal/external audits
- **Automate testing and validation** of IT controls against customizable policies
- **Prioritize** issues based upon criticality and compliance impact
- **Understand** effectiveness of IT controls and business impact of identified issues
- **Continuously assess** to proactively measure risk, stay ahead of audit cycle, and maintain compliance
- **Avoid** deficiencies and material findings
- **Customer Testimonial:** A Fortune 100 company saves over 1,000+ hours a year on audits alone, equating to roughly $75,000 per year

92% | Of tasks associated with controls testing can be automated

90% | Reduction in time spent testing IT controls

$100K | Saved per year compared to manual audit processes

Thank You!

jordan.thompson@onapsis.com

linkedin.com/company/onapsis

ONAPSIS.COM

ONAPSIS

Onapsis Quantitative / ROI Benefits (Control for Code)

- Code Review module:
- By providing immediate code review capabilities to each developer, “Control for Code” can reduce the reaction time between code development and code improvement from several days to a few seconds; This increases developer productivity and reduces time for unit-tests and time from development requests to delivery, especially in case of smaller objects such as reports
- In short, “Control for Code” helps to increase developer efficiency by 20%-40% and reduces delivery time for minor developments from weeks to days
- ***Simple math : 30% of Developer ~150K = 45K savings per developer***

Onapsis Quantitative / ROI Benefits (Code Review)

- Code Review module:
- A medium detailed ABAP code review will require approximately 1 senior developer for every 4–8 developers; With “Control for Code”, you can automate these reviews and the communication with the developers saving 70% - 90% of the reviewing man-power while significantly improving the accuracy, especially close to project milestones, where high work-load is typical
- In short, “Control for Code” can automate the code review effort by approximately 80% while increasing accuracy significantly
- ***Simple math : 80% of Sr. Developer ~200K = 160K savings per year***

Onapsis Quantitative / ROI Benefits (Vuln Mgmt)

- Full Platform / General:
- Reduce amount of SAP security/basis/support, development, and audit resources procured from third-parties or in SOWs
- Vulnerability module:
- Automation of security note patch management every SAP Patch Tuesday (Which SAP security notes are applicable to Sompo and what priority do they receive?) This manual, human error-laden process can take 1-4 weeks or longer according to our customers; Automating the vulnerability Management review process decreases the time from weeks to minutes with the click of a button
- ***Simple math : ~ 12 weeks of SAP Basis ~150K = 37.5K savings per Basis***

Onapsis Quantitative / ROI Benefits (Compliance)

- Compliance module:
- Automation of manual testing procedures for ITGC compliance reporting (Transitioning from gathering screenshots, spreadsheets, and table data for SOX and security audits of SAP; can take several hours per external audit season or per quarter for SAP Basis/security to gather this info for internal and external audit, which takes away their time for other projects, and is manual with human error, so there could be deficiencies or weaknesses in financial statements)
- Specific customer example saves them 1,000 hours annually by automating the above processes
- ***Simple math : ~1000 hours = ½ FTE = ~150K *50% = 75K savings per year***