ONAPSIS

Managing SAP Application Risk: Before, During and After the SAP Digital Transformation

Plus
Five things every leader and organization should be doing to secure SAP

Brenda King – Solutions Engineer

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]
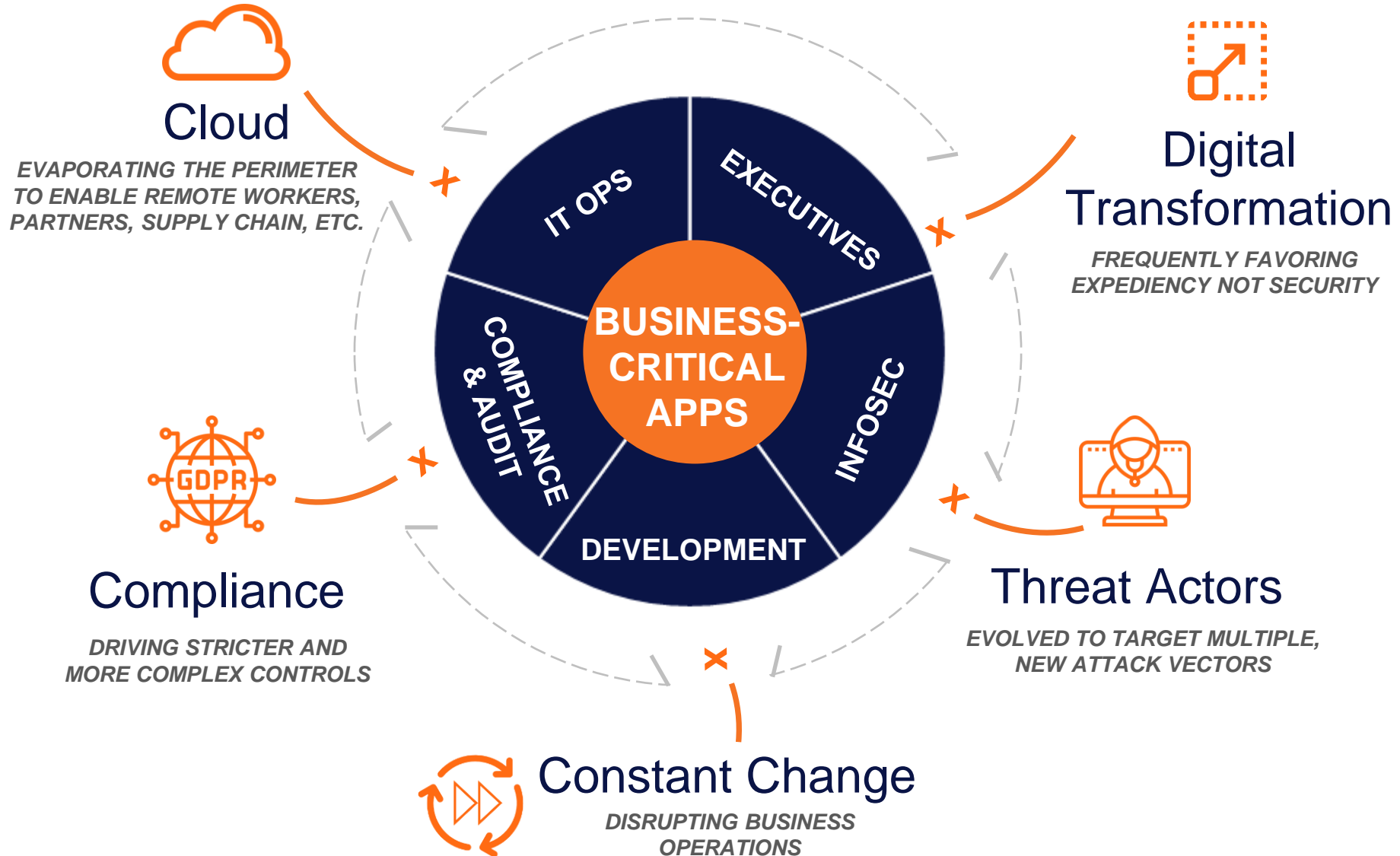
Financial Ramifications

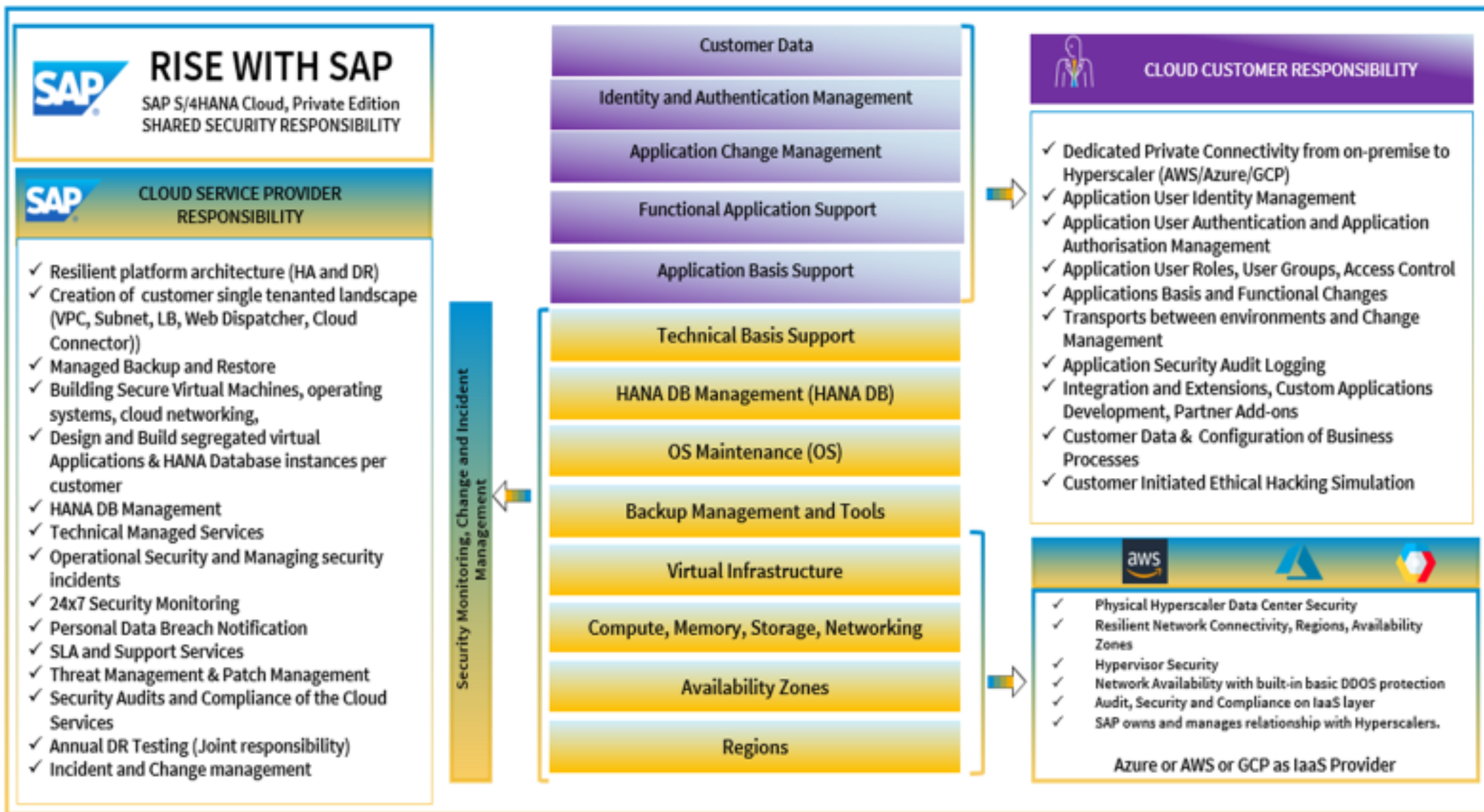**$2M** Average yearly cost of fines and penalties due to non-compliance[5]

Modern Enterprises Are Facing a Perfect Storm of Complexity...

Cloud

EVAPORATING THE PERIMETER TO ENABLE REMOTE WORKERS, PARTNERS, SUPPLY CHAIN, ETC.

Digital Transformation

FREQUENTLY FAVORING EXPEDIENCY NOT SECURITY

Compliance

DRIVING STRICTER AND MORE COMPLEX CONTROLS

Threat Actors

EVOLVED TO TARGET MULTIPLE, NEW ATTACK VECTORS

Constant Change

DISRUPTING BUSINESS OPERATIONS

Center circle:

BUSINESS-CRITICAL APPS

Surrounding segments: IT OPS · EXECUTIVES · INFOSEC · DEVELOPMENT · COMPLIANCE & AUDIT

RISE with SAP: Shared Security Responsibility for SAP Cloud Services

RISE WITH SAP
SAP S/4HANA Cloud, Private Edition
SHARED SECURITY RESPONSIBILITY

CLOUD SERVICE PROVIDER RESPONSIBILITY

- ✓ Resilient platform architecture (HA and DR)
- ✓ Creation of customer single tenanted landscape (VPC, Subnet, LB, Web Dispatcher, Cloud Connector))
- ✓ Managed Backup and Restore
- ✓ Building Secure Virtual Machines, operating systems, cloud networking,
- ✓ Design and Build segregated virtual Applications & HANA Database instances per customer
- ✓ HANA DB Management
- ✓ Technical Managed Services
- ✓ Operational Security and Managing security incidents
- ✓ 24x7 Security Monitoring
- ✓ Personal Data Breach Notification
- ✓ SLA and Support Services
- ✓ Threat Management & Patch Management
- ✓ Security Audits and Compliance of the Cloud Services
- ✓ Annual DR Testing (Joint responsibility)
- ✓ Incident and Change management

Security Monitoring, Change and Incident Management

- Customer Data
- Identity and Authentication Management
- Application Change Management
- Functional Application Support
- Application Basis Support
- Technical Basis Support
- HANA DB Management (HANA DB)
- OS Maintenance (OS)
- Backup Management and Tools
- Virtual Infrastructure
- Compute, Memory, Storage, Networking
- Availability Zones
- Regions

CLOUD CUSTOMER RESPONSIBILITY

- ✓ Dedicated Private Connectivity from on-premise to Hyperscaler (AWS/Azure/GCP)
- ✓ Application User Identity Management
- ✓ Application User Authentication and Application Authorisation Management
- ✓ Application User Roles, User Groups, Access Control
- ✓ Applications Basis and Functional Changes
- ✓ Transports between environments and Change Management
- ✓ Application Security Audit Logging
- ✓ Integration and Extensions, Custom Applications Development, Partner Add-ons
- ✓ Customer Data & Configuration of Business Processes
- ✓ Customer Initiated Ethical Hacking Simulation

aws

- ✓ Physical Hyperscaler Data Center Security
- ✓ Resilient Network Connectivity, Regions, Availability Zones
- ✓ Hypervisor Security
- ✓ Network Availability with built-in basic DDOS protection
- ✓ Audit, Security and Compliance on IaaS layer
- ✓ SAP owns and manages relationship with Hyperscalers.

Azure or AWS or GCP as IaaS Provider

Attacks Against ERP Applications Are Increasing in Frequency and Severity

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

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

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

Code Optimization ?

- Security is frequently "bolt on" and not "built in"

- Reliance on manual code reviews

- Problems aren't identified until they hit production

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

Vulnerabilties ?

- 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

…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

Our Customers Approach and The Onapsis Platform - Visibility and Tools To Protect Your ERP
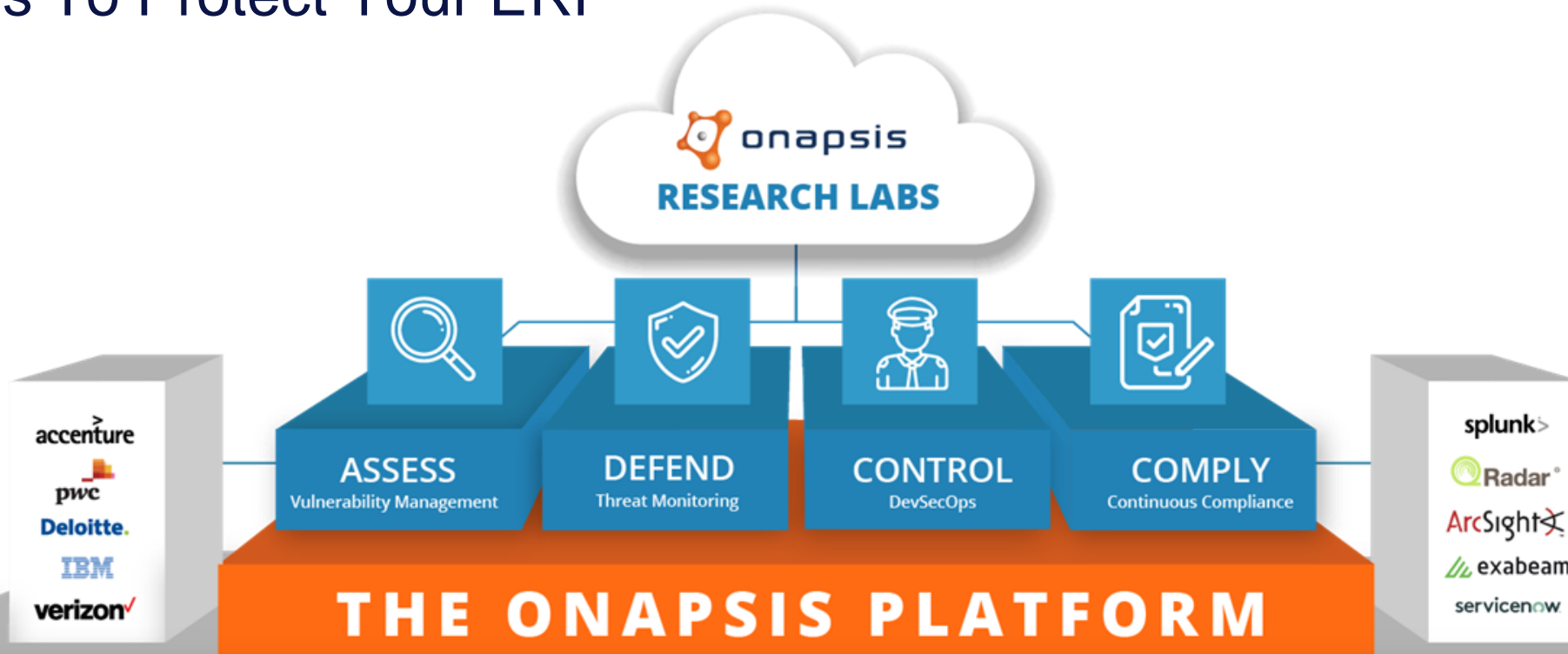
"Prior to using Onapsis, we were **prioritizing simple fixes and ignoring critical vulnerabilities**, of which we identified 600 in 2018. Since we started using Onapsis, we've **remediated 90% of those critical vulnerabilities**, and 70% of the 10,000+ total we initially discovered." - *F100 Biotech*

"Saves time identifying, prioritizing, and remediating security vulnerabilities. **Enables security generalists** to ensure Basis is properly maintaining SAP systems." – F100 Tech Manufacturer

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 Solution Manager 7.2   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   SAP Process Control

MANAGEMENT FUNCTIONALITY

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

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
1,000+
zero-day vulnerabilities in business-critical apps

25%
Of critical SAP Security Notes in 2021 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

Onapsis Quantitative / ROI Benefits (Code Review)

- 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

- 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 example #1 : 30% of Developer ~150K = 45K savings per developer*

- *Simple math example #2 : 80% of Sr. Developer ~200K = 160K savings per year*

Onapsis Quantitative / ROI Benefits (Vulnerability and Compliance Management)

- 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 example #3 : ~ 12 weeks of SAP Basis ~150K = 37.5K savings per Basis*

- 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 example #4: ~1000 hours = ½ FTE = ~150K *50% = 75K savings per year*

Onapsis Family of Customers!

Fortune 500 Utility Company (Lets

conclude with two real customer stories)

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

Thank You!

@onapsis

linkedin.com/company/onapsis

ONAPSIS.COM

ONAPSIS