ONAPSIS

The Threat Landscape is Transforming: Understand The Importance of Business-Critical Application Protection and Associated Compliance

Roger Egle | Strategic Account Manager

Jason Braun | Vice President West

ONAPSIS | PROTECT YOUR BUSINESS-CRITICAL APPLICATIONS

VULNERABILITY MANAGEMENT

Visibility at application level

Understand Business Risk

Prioritize Remediation

CONTINUOUS THREAT MONITORING

Real-time Alerts

Root Cause Analysis

SIEM Integrations

AUTOMATION

Reduce Costs & Resources

Automated Code Analysis

“Real-time” & Batch Scanning

Dev Environment Integrations

APPLICATION SECURITY TESTING

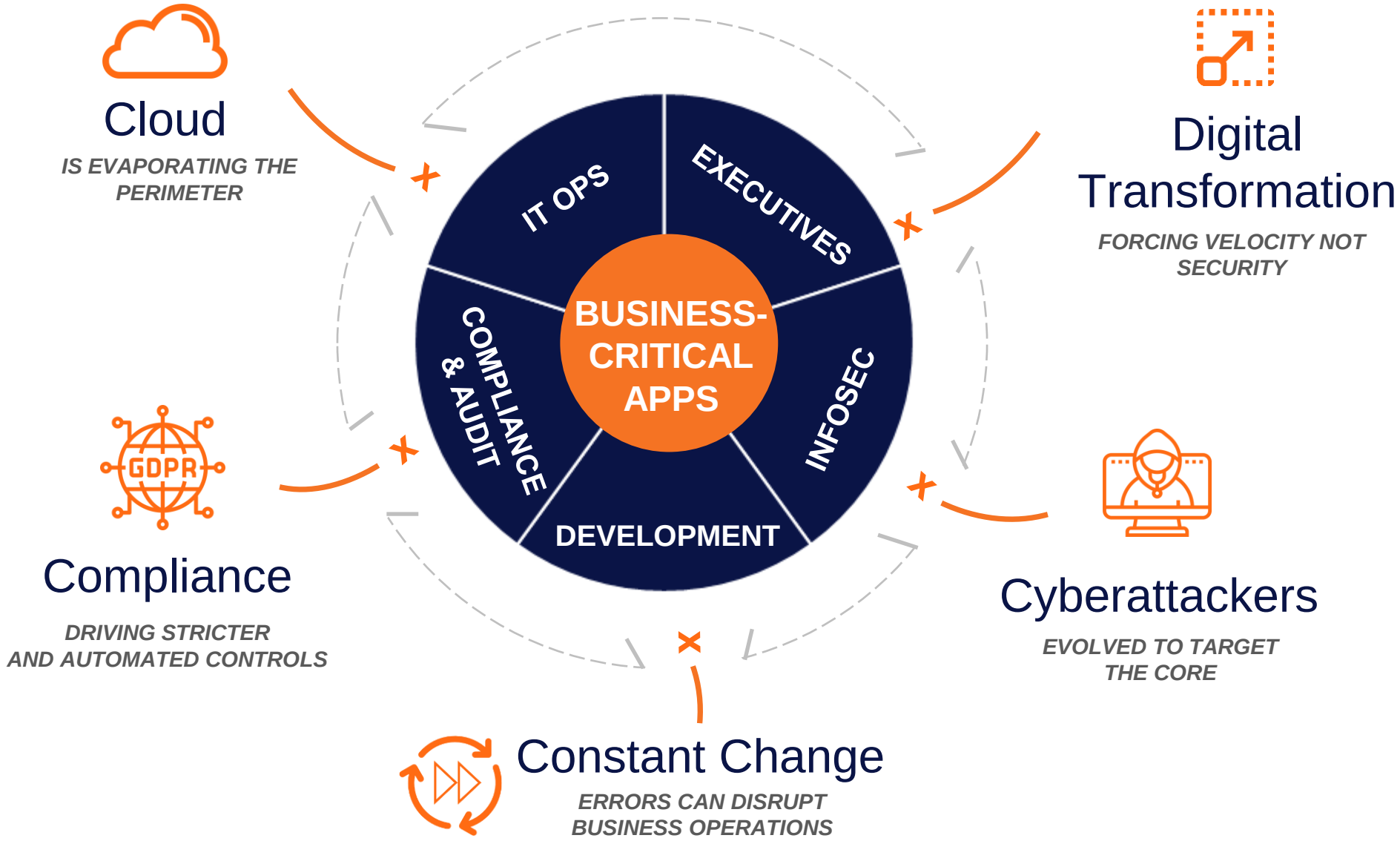
Detect privilege misuse or changes

Identify privileged & default users

Monitor for risky behavior

ROLE & ACTIVITY AUDITING

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 Do This? Well, We Built the ONAPSIS **THREAT INTELLIGENCE CLOUD**

Synthetic targets,
Real attacks from real threat actors.

NOVEL **EVIDENCE** OF SOPHISTICATED THREAT ACTORS **ACTIVELY EXPLOITING SAP APPLICATIONS IN-THE-WILD**

400+
CONFIRMED EXPLOITATIONS

107+
HANDS-ON ATTACKS

7
TRACKED THREAT VECTORS

18
UNIQUE COUNTRIES
* may include VPS / TOR

Data based on direct observation of threat activity against OTIC, upon unmarked systems becoming online. Data is not based on exploitation on SAP customers' environments.

SMALL WINDOW TO DEFEND

Rapid patching and secure Cloud provisioning is critical

<72hs

SAP PATCH RELEASE TO EXPLOITATION

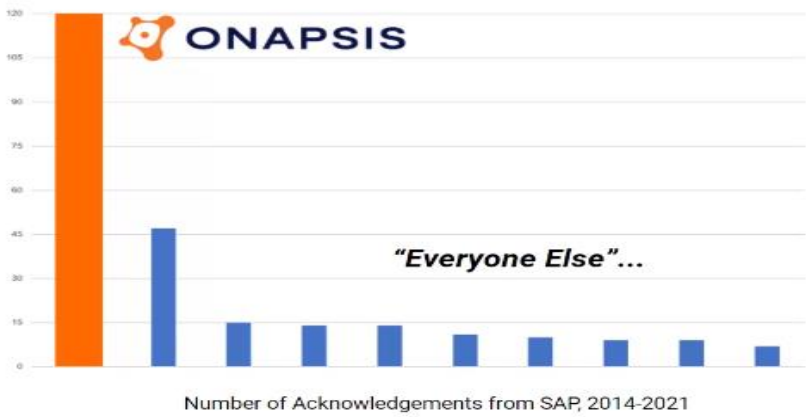
<3hs

NEW SYSTEM ONLINE TO BEING EXPLOITED

Data based on direct observation of threat activity against OTIC, upon unmarked systems becoming online. Data is not based on exploitation on SAP customers' environments.

ONAPSIS RESEARCH LABS

- **Onapsis influences 40%+ of SAP's critical notes and 60% of ALL Hana notes**
- 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

800+

zero-day vulnerabilities in business-critical apps

14

Out-of-the-box compliance policies, plus ability to customize

6

US DHS critical alerts based on our research

17

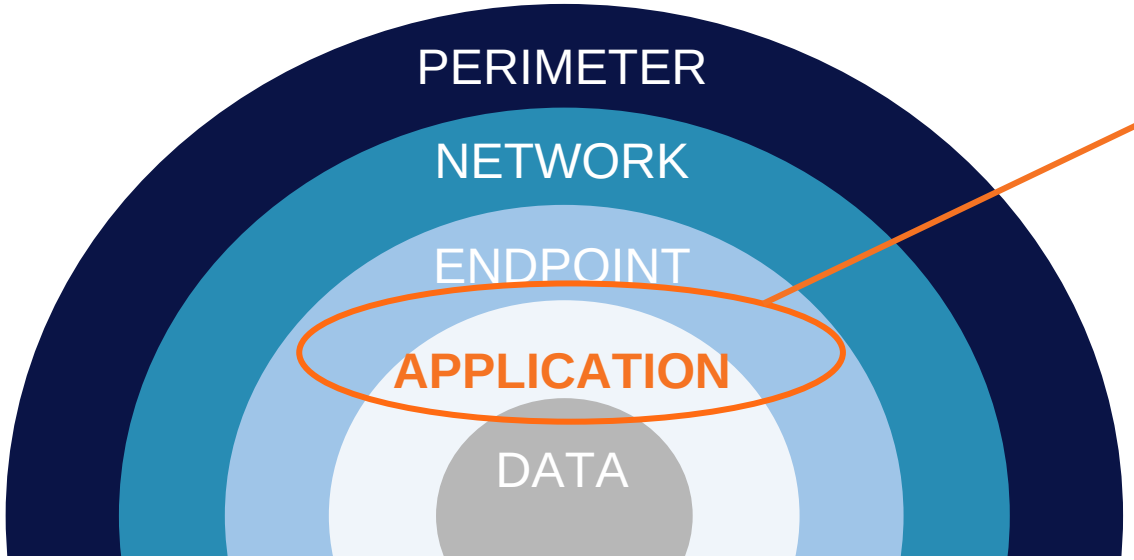
Patents, 8 issued & 9 pending

Knowledgebase of

10,000+

vulnerabilities and attacks on business applications

Traditional Defense-in-Depth Models Surround But Ultimately Neglect That Critical Application Layer



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

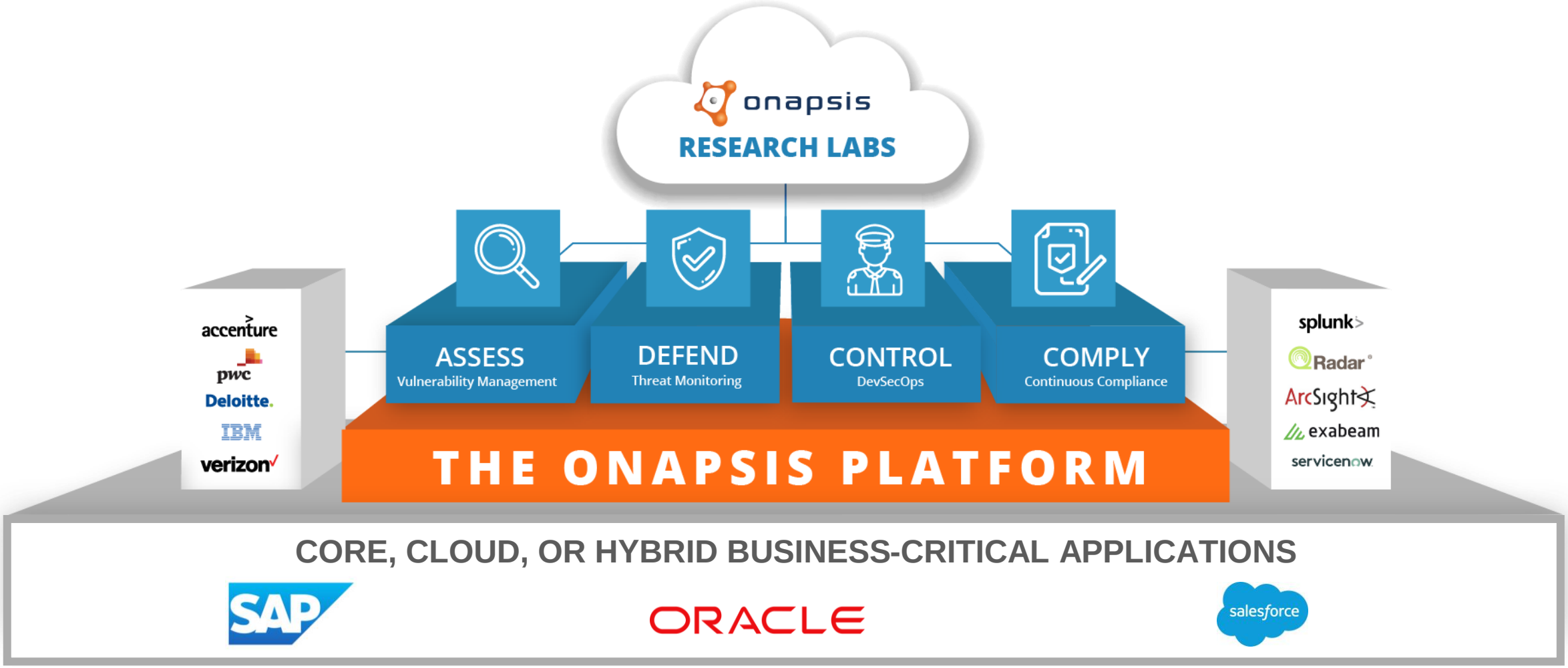
Gartner®

"*In-depth assessments of databases and applications, such as ERP systems (e.g., SAP or Oracle), are* ***not widely supported in traditional Vulnerability Assessment solutions****.*"

https://www.gartner.com/en/newsroom/press-releases/2021-05-17-gartner-forecasts-worldwide-security-and-risk-managem

ONAPSIS BRINGS BUSINESS-CRITICAL APPLICATIONS INTO SCOPE

Unprecedented visibility into business-critical applications across your enterprise



Comply: Key Features & Benefits

- Simplify your compliance efforts with 10+ prepackaged content packs targeting the most in-demand regulations & frameworks and easy customizations to match your unique business needs
- Save time extracting information from SAP to support these regulations
- Identify compliance risks in a timely manner in advance of your auditors and regulators with regularly scheduled jobs
- Take the labor out of manual testing efforts for SOX ITGC with clear results and remediation steps
- SOC 1 Type 2 Attestation (Q1 2022) drives trust with auditors and regulators
- Integration with SAP GRC Process Control
- Content is added and refreshed at least annually

↓80%+ Reduction in time spent collecting information supporting SOX ITGC

300+ Checks that help to manage compliance with SOX ITGC

100+ Customers using Comply to help with their Compliance efforts

ONAPSIS CUSTOMER USE CASES

- Compliance (ICFR/SOX)
  - Patch & Vulnerability Management
  - Default Account/Profile Management
  - Role-based Access Control governance
  - Security Parameter Settings
- Continuous Audit / Monitoring
  - Key controls are monitored in near real-time
    - Integration to SIEM, functional email accounts, etc.
- Role Based Access Control (RBAC)
  - RBAC Governance: 1,000+ hr. audit reduced to dozens of hours PLUS more complete & accurate results
- Internal Audit/External Audit Reliance
  - >10 Controls replaced by platform

ONAPSIS CUSTOMER USE CASES (CONTINUED)

- Cyber Security Threat Detection & Mitigation
  - Alarm profiles alert for active exploits
  - SAP Recon, Log4J, ICMAD
- Assurance for new ERP builds/projects
  - Migration of SAP BW from SAP HEC to Azure
  - New SAP client delivery or future platform upgrades
- Future:
  - Business Use Cases
    - Business Controls for other SAP workstreams (pilot for P2P currently underway)
    - Currently partnered with Controllers function and Onapsis to deliver a broader pilot across SAP workstreams
  - Move other use cases to the Defend module

ONAPSIS HIGHLIGHTS

#1

Market Category Leader

400+

Global Employees

300+

Customers, 20% Fortune100

94%

Customer Retention

SAP® Endorsed App
Premium Certified

ONAPSIS PARTNERS | APPLICATION PROTECTION ECOSYSTEM

TECHNOLOGY ALLIANCES

SAP Endorsed App
Premium Certified

ORACLE Gold Partner

ArcSight An HP Company

servicenow

splunk>

QRadar

Azure Sentinel

exabeam

CLOUD PROVIDERS

Microsoft Azure

Google Cloud

amazon web services

SAP HANA

ORACLE ERP Cloud

SYSTEM INTEGRATORS & MSSP

IBM

Deloitte.

pwc

accenture

Infosys
Navigate your next

verizon

THANK YOU!

Roger.Egle@onapsis.com

linkedin.com/company/onapsis

ONAPSIS.COM

ONAPSIS