ONAPSIS

PROTECTING THE BUSINESS-CRITICAL APPLICATIONS THAT RUN YOUR BUSINESS

RANSOMWARE - SAP SECURITY THREAT LANDSCAPE

21 OCTOBER 2021 | JONATHAN COOPER

Agenda

SAP Endorsed App
Premium Certified

Challenges

Risk based approach

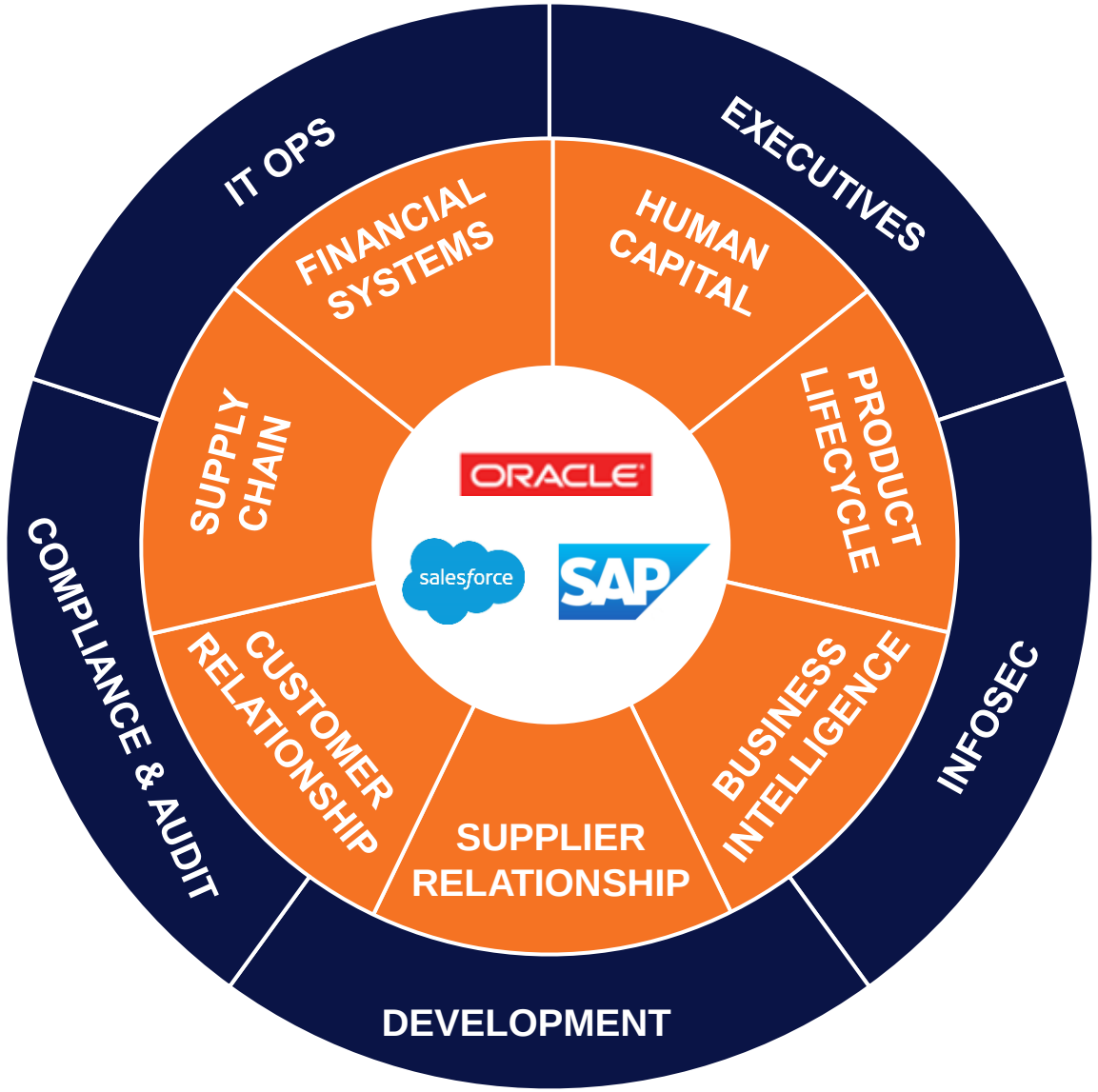
Why Onapsis

Demo

SAP Cyber Security Maturity

Key Takeaways

BUSINESS-CRITICAL APPLICATIONS POWER YOUR BUSINESS



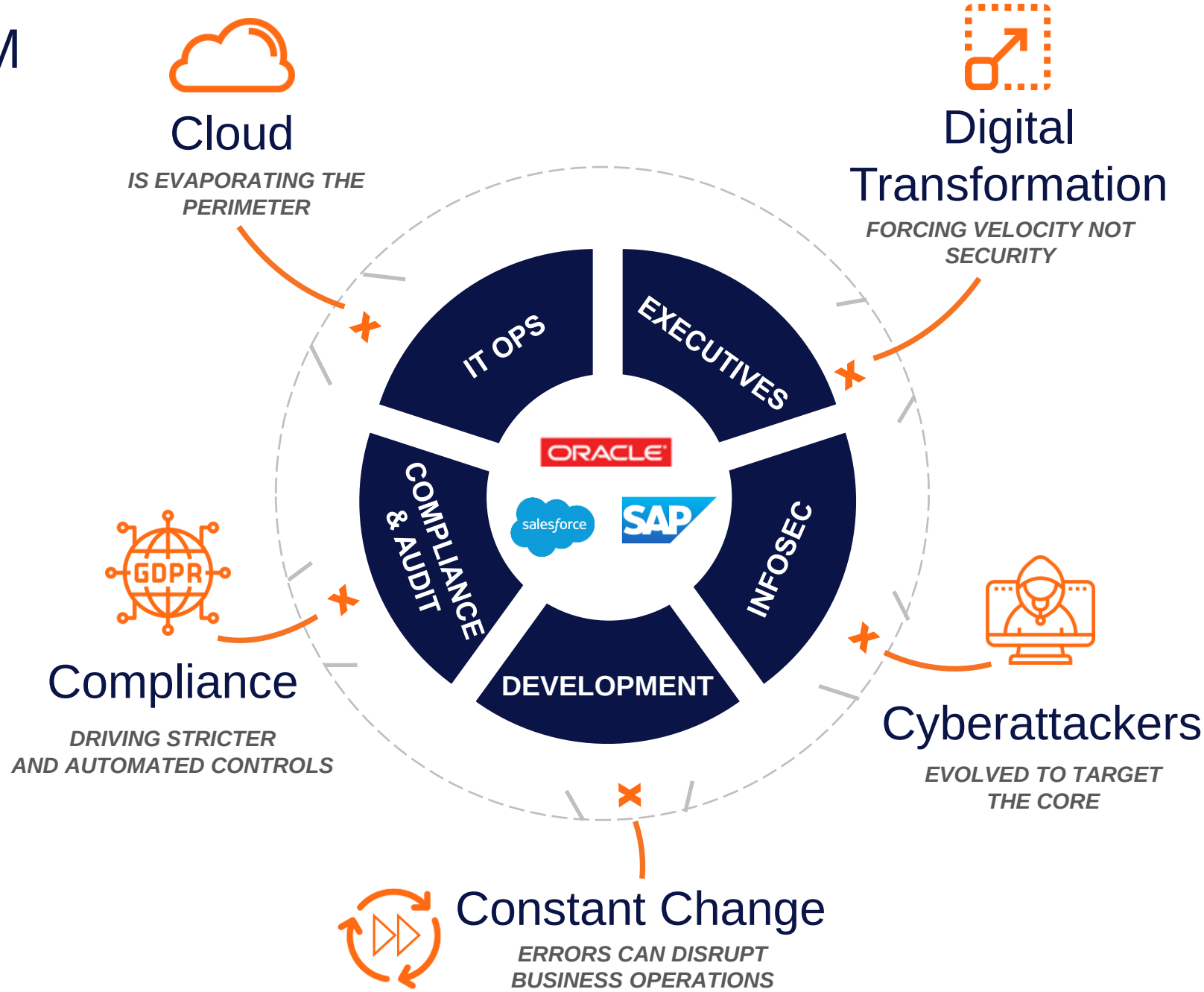
92% of the Global 2000 use SAP or Oracle[1]

77% of the world's revenue touches these systems[2]

1 in 5 enterprise applications are SaaS-based[3]

A PERFECT STORM

New Industry Dynamics and Emerging Cyber Threats Are Threatening Your Mission-Critical Applications



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 10K

B

LAZE
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

DHS US-CERT ALERT

ONAPSIS THREAT INTEL

Risk = Likelihood x Impact

ONAPSIS & SAP THREAT INTEL | NOVEL EVIDENCE OF ONGOING ATTACKS ON SAP APPLICATIONS IN THE WILD

300+
CONFIRMED EXPLOITATIONS

107+
HANDS-ON ATTACKS

18
UNIQUE COUNTRIES
* may include VPS / TOR

<72hs
SAP PATCH RELEASE TO EXPLOITATION

<3hs
NEW SYSTEM ONLINE TO BEING EXPLOITED

"*Hackers are targeting certain versions of enterprise software from SAP SE that haven't been updated with recent security patches. Successful hacks can '**lead to full control of unsecured SAP applications**,'"*

WSJ

About SAP SE / SAP News Center / **Ecosystem**

SAP and Onapsis Proactively Notify and Help Customers Protect Mission-Critical Applications from Active Cyber Threats

SAP

"*Impacted organizations could experience:*
- *theft of sensitive data,*
- *financial fraud,*
- *disruption of mission-critical business processes,*
- *ransomware, and*
- *halt of all operations.*"

CYBERSECURITY & INFRASTRUCTURE SECURITY AGENCY — CISA

WHAT HAPPENS IF YOU DON'T FIX THIS?

Data Loss or Breach

74% Of breaches involved access to privileged account[1]

28% Of breaches are due to missing application patches[2]

System Outages

52% Of security events caused operational outage that affected productivity[3]

over $50k/ hour Average cost of ERP application downtime[4]

Compliance Findings

$5M Average yearly cost of business disruption due to non-compliance[5]

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

Project Delays

52% Of cloud migrations are delayed due to security concerns[6]

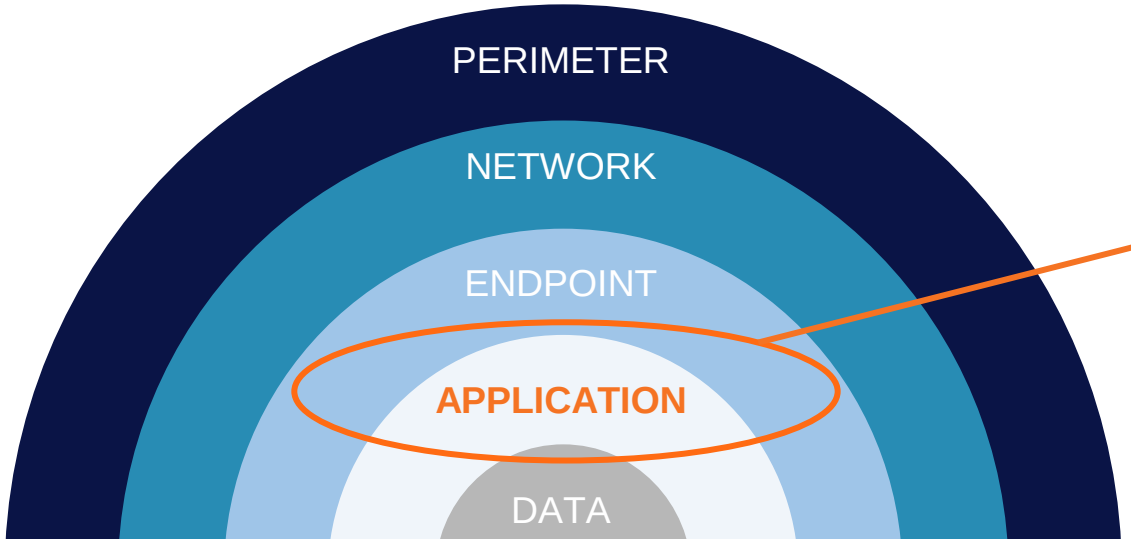
Reputation Damage

7.3% Average decrease in stock price following a security breach[7]

[1]Centrify
[2]DarkReading
[3]Fortinet
[4]Onapsis
[5]Ascent
[6]TechRepublic
[7]Forbes

Why Onapsis

"*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.*" Gartner



SAP Application Security

- Single Sign On, IDM, ID Access Governance/Service,
- Role Based Access Control, ABAC
- SolMan, Early Watch, Focused Run
- Code Vulnerability Analysis, Code Inspector, ATC
- SAP GRC AC, PC, RM, AM, BIS, UI Mask/Log, ETD

Traditional SAP controls can be bypassed by cyber attacks

Ripped from the Headlines...

CYBERSECURITY

Meat supplier JBS paid ransomware hackers $11 million

PUBLISHED WED, JUN 9 2021•7:43 PM EDT | UPDATED WED, JUN 9 2021•8:42 PM EDT

NBC NEWS | Kevin Collier

SHARE

Signage outside the JBS Beef Production Facility in Greeley, Colorado, U.S., on Tuesday, June 1, 2021.

Michael Ciaglo | Bloomberg | Getty Images

Colonial Pipeline Paid Roughly $5 Million in Ransom to Hackers

The payment clears the way for gas to begin flowing again, but it risks emboldening other criminal groups to take American companies hostage by seizing control of their computers.

The Way Organizations Commonly Respond Isn't Working...

Challenge: Commonly, people think of endpoints, cyber education, network detection tools, and backups when they hear the word "ransomware". Lots of reacting...

Where Do We Want Organizations Focusing?

Goal: Onapsis needs to help organizations focus on ***proactive*** measures to directly secure the “crown jewels”. Onapsis needs to drive increased product awareness of how we can identify attack vectors and help mitigate disruptive attacks to business-critical applications.

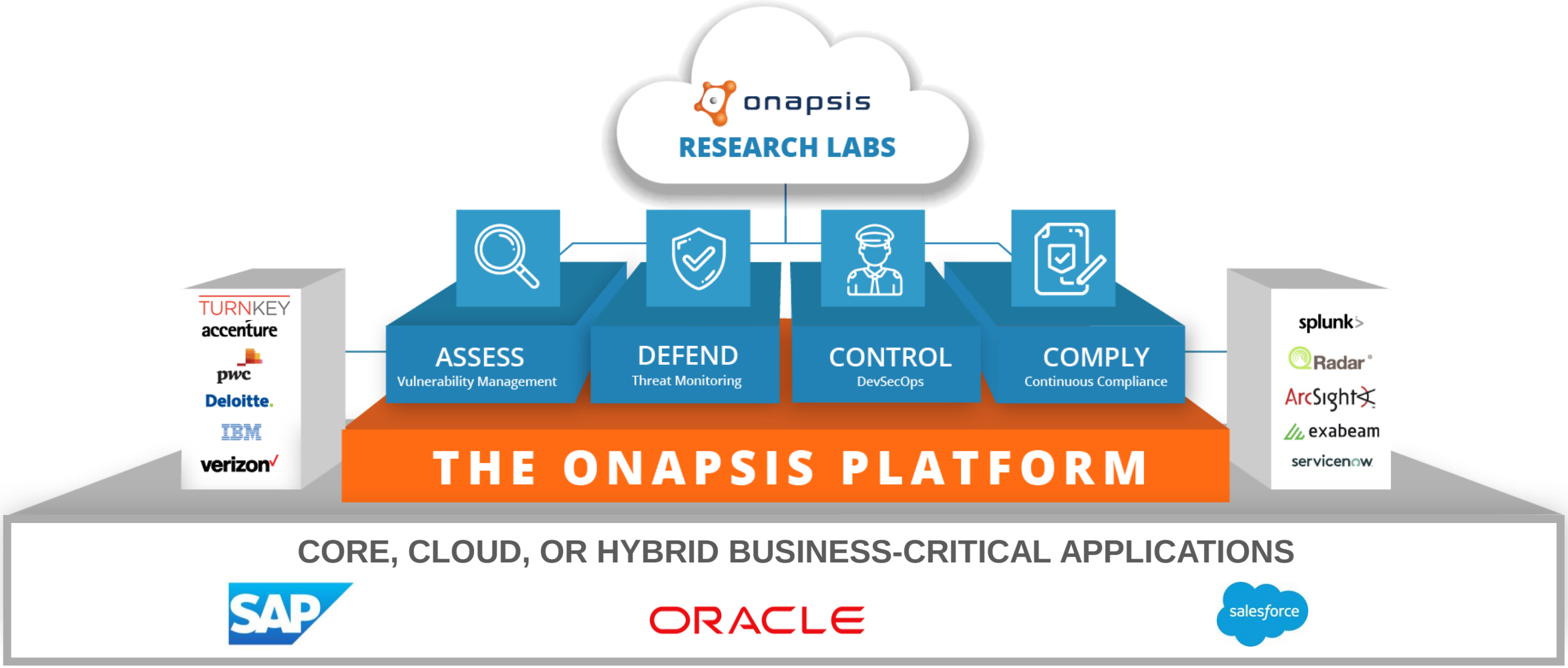
Ransomware for Mission Critical Applications

- Connected Applications Introduce More Weaknesses and Vulnerabilities.
- Getting Back to Basics Means Good Security Hygiene.
- Speed and Sophistication of attacks
- Surface area of attack has increased

“Implement a risk-based vulnerability management process that includes threat intelligence. Ransomware often relies on unpatched systems to allow lateral movement. ***This should be a continuous process. The risk associated with vulnerabilities changes as vulnerabilities are exploited by attackers.*** Gartner

ONAPSIS BRINGS BUSINESS-CRITICAL APPLICATIONS INTO SCOPE

Unprecedented visibility into business-critical applications across your enterprise



Demonstration

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

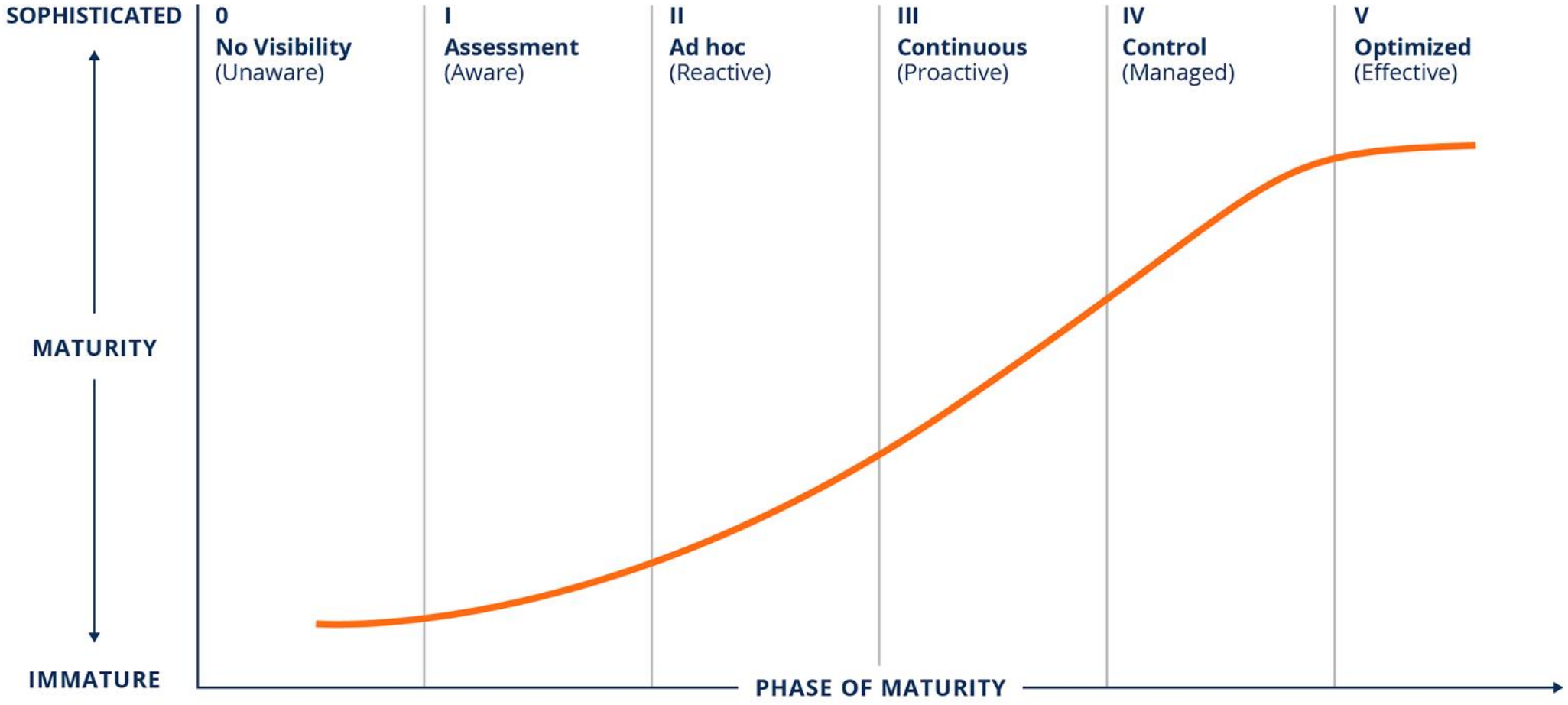
Continuous Compliance

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

MANAGEMENT FUNCTIONALITY

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

SAP CyberSecurity Maturity



ONAPSIS RESEARCH LABS

Stay ahead of ever-evolving cybersecurity threats with the world's leading threat research on business-critical applications

- 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
800+
zero-day vulnerabilities in business-critical apps

14
Out-of-the-box compliance policies, plus ability to customize

5
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 HIGHLIGHTS

#1
Market Category Leader

400+
Global Employees

300+
Customers, 20% Fortune100

94%
Customer Retention

SAP® Endorsed App
Premium Certified

INFOSEC AWARDS WINNERS CYBER DEFENSE MAGAZINE 2020

CYBERSECURITY BREAKTHROUGH AWARD 2020

CYBER DEFENSE GLOBAL AWARDS CYBER DEFENSE MAGAZINE 2019 WINNER

THANK YOU

Jonathan.cooper@onapsis

linkedin.com/company/onapsis

ONAPSIS.COM

ONAPSIS

ASSESS | VULNERABILITY & SECURITY POSTURE MANAGEMENT

- **Visibility** into vulnerabilities, misconfigurations 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

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

DEFEND | THREAT DETECTION & RESPONSE

- **Continuous monitoring** and real-time alerts for over 3,000+ threat indicators
- **Prioritize alerts** based on stakeholder risk posture and/or systems
- **Respond quickly** to active threats via detailed alarm notifications
- **Analyze Root Cause** by sending threat information to SIEMs and correlating with other system logs

75%	Improved incident response times
50%	Reduced forensic investigation time
100%	SAP log forwarding enables correlation with other logs

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

25x	Faster than manual review processes
1 minute	Scan up to 900,000 lines of code
<1%	False positive rate
75%	Reduction in errors making it into production
50 - 80%	Common findings automatically fixed with optional service

CONTROL FOR TRANSPORT | SAP TRANSPORT INSPECTION

- **Comprehensive inspection** of all SAP transports (including third-party)
- **Resolve** with detailed step-by-step remediation guidance
- **Integrate** with existing change and transport management systems
- **Prevent** import errors, business outages, downgrades, security vulnerabilities, and compliance violations
- **Protect** sensitive data from manipulation and espionage

100%	Automated transport inspection lifts the burden of a manual review process
75%	Reduction of unexpected outages
100%	Visibility into 3rd party transports without importing into SAP
462 Hours	Saved per system per year on investigating and fixing transport errors
$35K	Saved per system per year by eliminating import errors in production

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

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

ONAPSIS PARTNERS | APPLICATION PROTECTION ECOSYSTEM

TECHNOLOGY ALLIANCES

SAP Endorsed App
Premium Certified

ORACLE Gold Partner

ArcSight An HP Company

servicenow

AZURE Sentinel

Radar

splunk>

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