ONAPSIS

The Threat Landscape is Transforming: Understand The Importance of SAP Business-Critical Application Protection

Al Rosman, Strategic Account Manager | October 6, 2022

albert.rosman@onapsis.com, 414-915-7211

ONAPSIS HIGHLIGHTS

SAP® Endorsed App
Premium Certified

Only cybersecurity vendor endorsed by SAP and in EA

#1
Market Category Leader

400+
Global Employees

300+
Customers,
20% Fortune 100

94%
Customer Retention

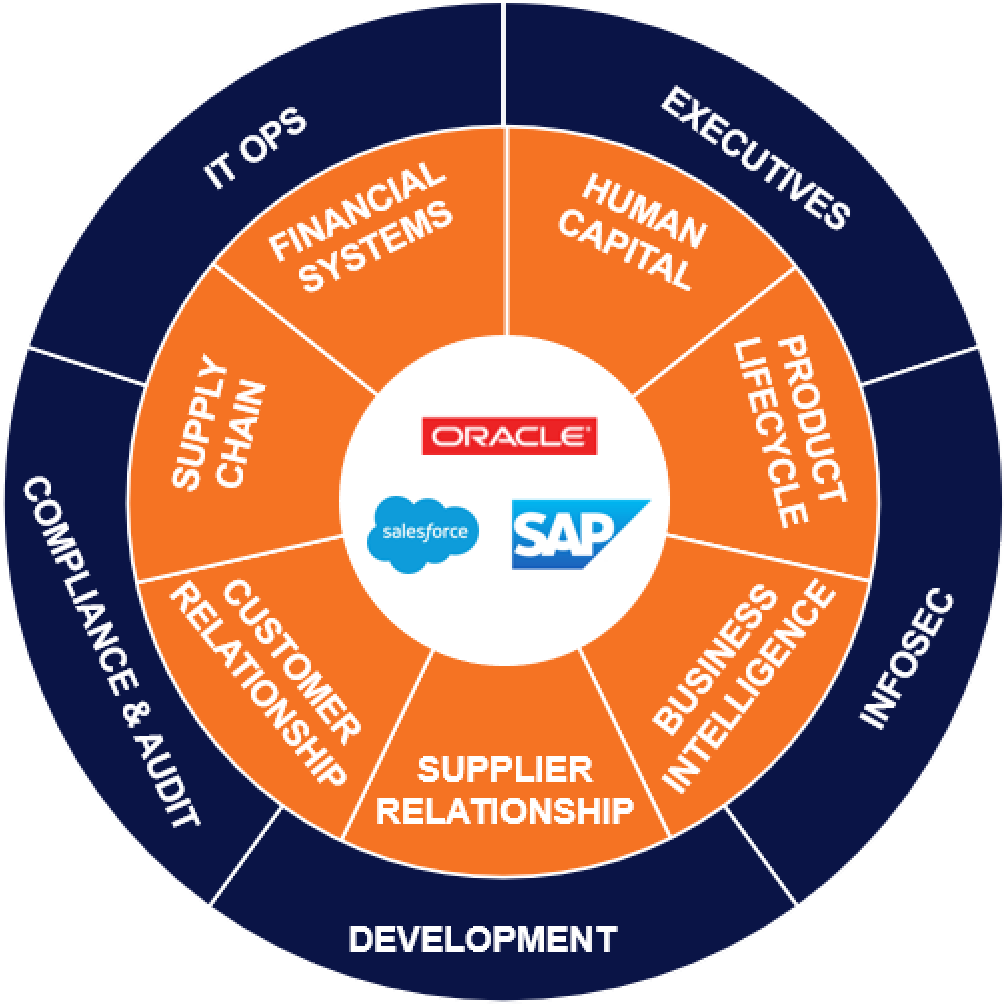
THE CHANNEL CO.
CRN
SECURITY
100
2022

AMERICA'S FASTEST-GROWING
Inc. 5000
PRIVATE COMPANIES

GLOBAL
INFOSEC AWARDS
WINNER
CYBER DEFENSE MAGAZINE
2022

CYBERSECURITY
BREAKTHROUGH
AWARD
2021

BUSINESS-CRITICAL APPLICATIONS POWER YOUR BUSINESS

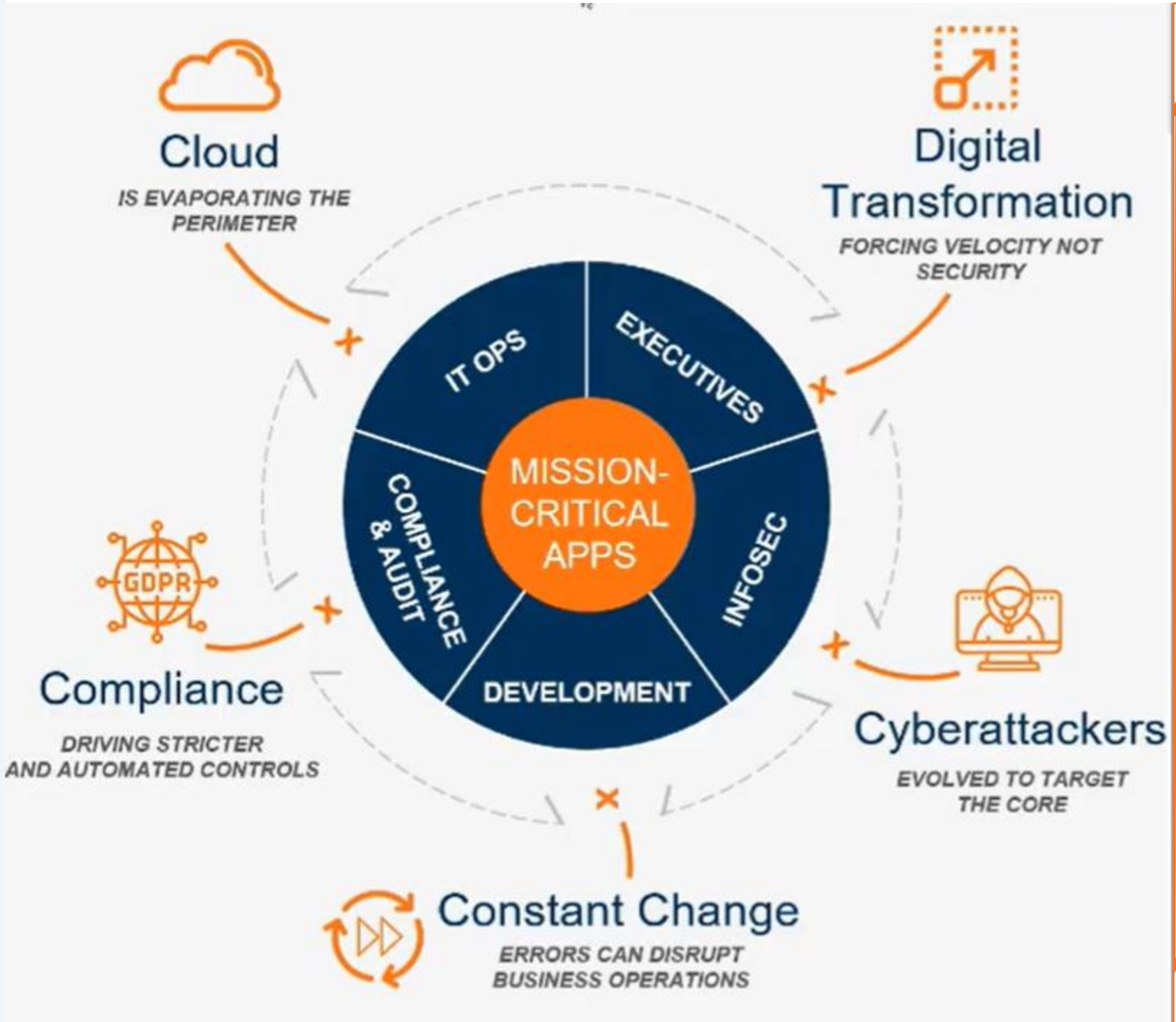


92% of the Global 2000 use SAP or Oracle[1]

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

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

THE CURRENT PROBLEM PROTECTING BUSINESS CRITICAL APPS


Cloud
IS EVAPORATING THE PERIMETER
Digital Transformation
FORCING VELOCITY NOT SECURITY
IT OPS
EXECUTIVES
MISSION-CRITICAL APPS
COMPLIANCE & AUDIT
INFOSEC
DEVELOPMENT
GDPR
Compliance
DRIVING STRICTER AND AUTOMATED CONTROLS
Cyberattackers
EVOLVED TO TARGET THE CORE
Constant Change
ERRORS CAN DISRUPT BUSINESS OPERATIONS

SAP DOMAIN

Blind Spot

GAP

Vulnerability Risks

- **Authorizations**
- **Configurations**
- **Interfaces**
- **Patching**
- **Best practice**

INTERNAL TEAMS ONLY INTERESTED IN IT RELATED ISSUES NOT SAP VULNERABILITIES

NO IMMEDIATE VISABILITY OF SAP THREATS TO CRITICAL SERVICES

IT CYBER-SECURITY DOMAIN

WHY ONAPSIS?

- Gain visibility into risk and business impact
- Monitor for internal and external threats
- Build security into app development lifecycle
- Maintain compliance and enforce baselines

PROTECT YOUR BUSINESS-CRITICAL APPS.
PROTECT YOUR BUSINESS.

AND ATTACKS ON BUSINESS-CRITICAL APPLICATIONS ARE INCREASING

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

IDC ANALYZE THE FUTURE

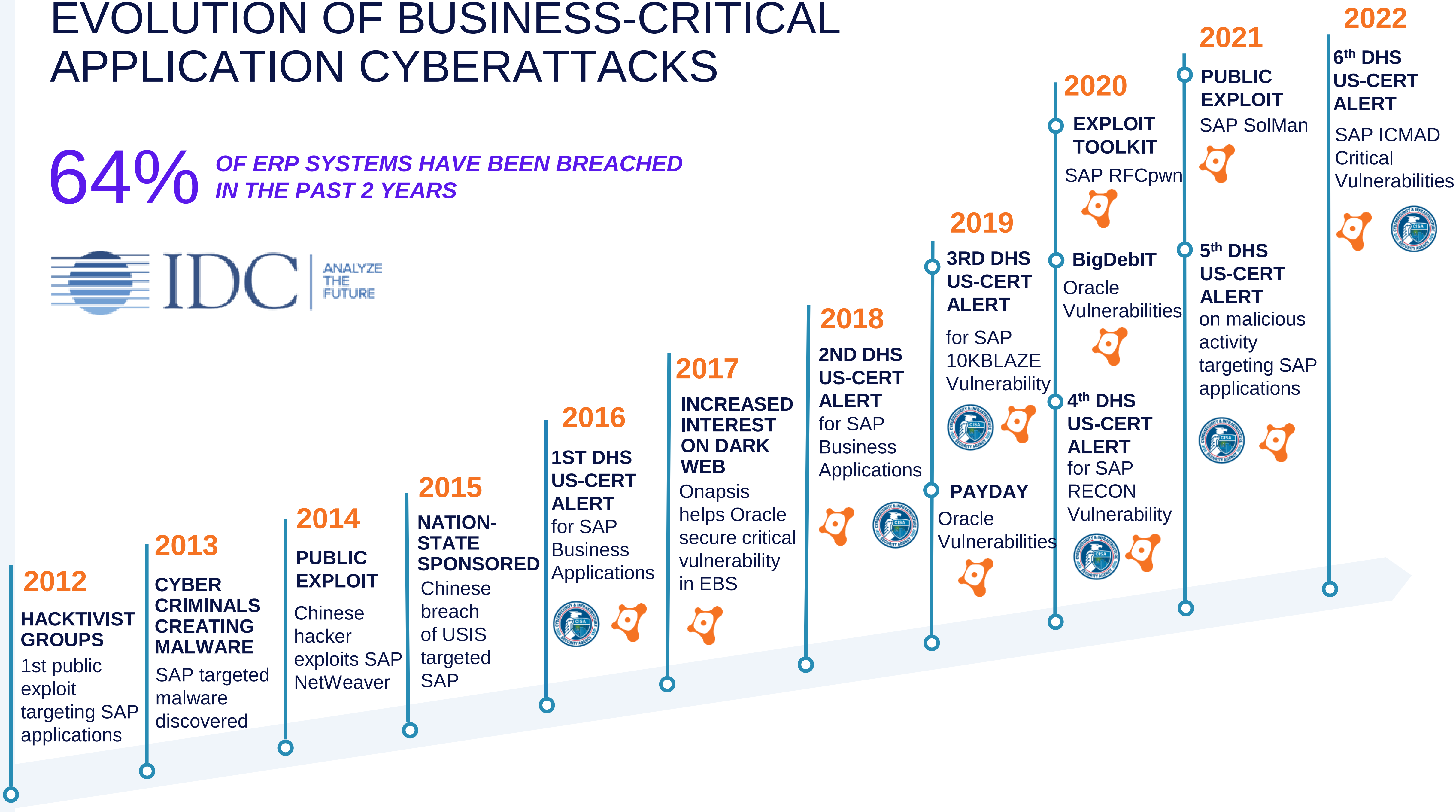
5 ALERTS IN 5 YEARS **ON MALICIOUS CYBER ACTIVITY OR VULNERABILITIES IN BUSINESS CRITICAL APPLICATIONS**

CYBERSECURITY & INFRASTRUCTURE SECURITY AGENCY

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

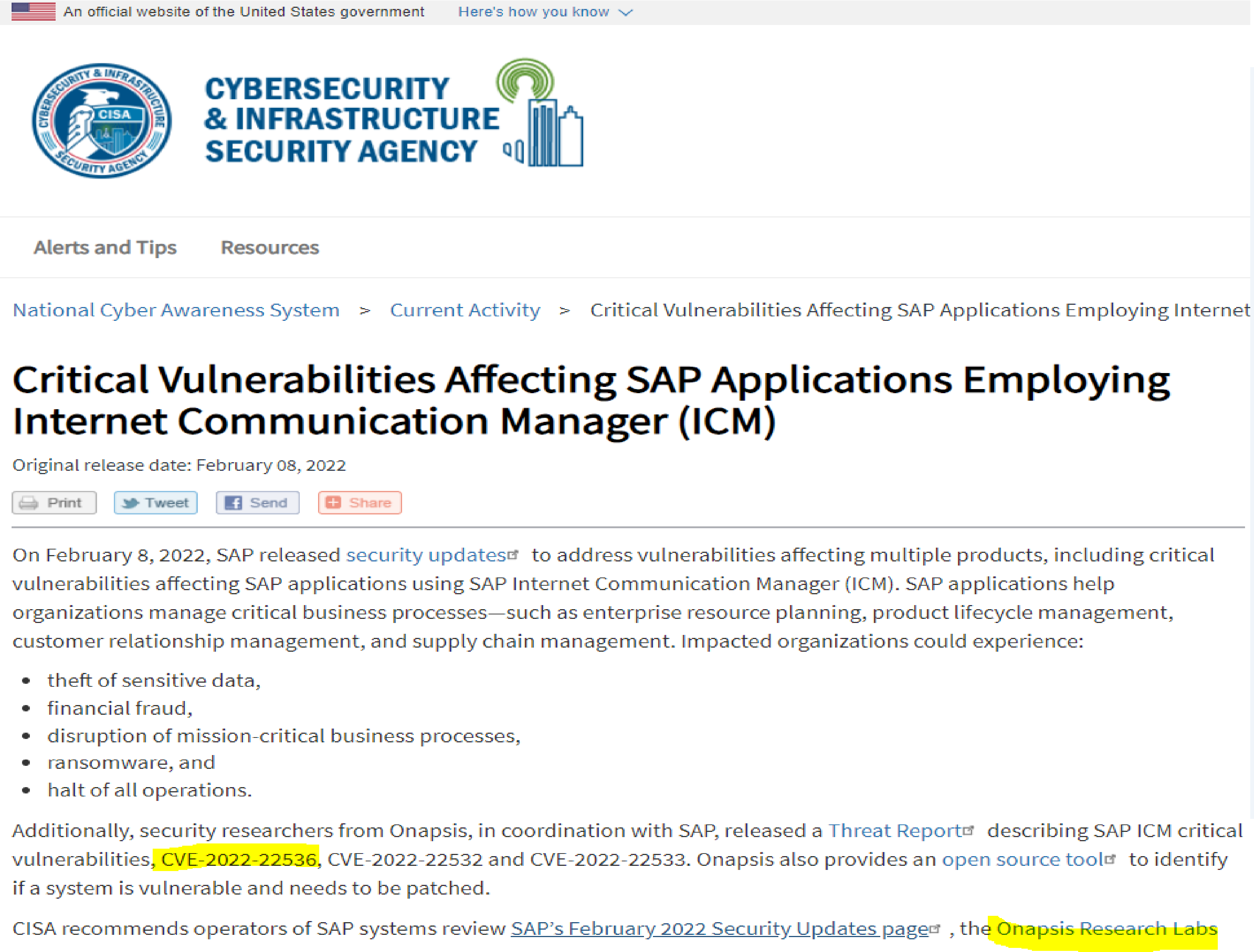
4th DHS US-CERT ALERT
for SAP RECON Vulnerability

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

CVE-2022-22536, CISA, Aug 2022, Joint CISA/Onapsis Webinar



An official website of the United States government
Here's how you know
CYBERSECURITY & INFRASTRUCTURE SECURITY AGENCY
Alerts and Tips
Resources
National Cyber Awareness System > Current Activity > Critical Vulnerabilities Affecting SAP Applications Employing Internet
Print
Tweet
Send
Share

Critical Vulnerabilities Affecting SAP Applications Employing Internet Communication Manager (ICM)

Original release date: February 08, 2022

On February 8, 2022, SAP released security updates to address vulnerabilities affecting multiple products, including critical vulnerabilities affecting SAP applications using SAP Internet Communication Manager (ICM). SAP applications help organizations manage critical business processes—such as enterprise resource planning, product lifecycle management, customer relationship management, and supply chain management. Impacted organizations could experience:

- theft of sensitive data,
- financial fraud,
- disruption of mission-critical business processes,
- ransomware, and
- halt of all operations.

Additionally, security researchers from Onapsis, in coordination with SAP, released a Threat Report describing SAP ICM critical vulnerabilities, CVE-2022-22536, CVE-2022-22532 and CVE-2022-22533. Onapsis also provides an open source tool to identify if a system is vulnerable and needs to be patched.

CISA recommends operators of SAP systems review SAP's February 2022 Security Updates page , the Onapsis Research Labs

Threat Intelligence from Onapsis and SAP

THREAT ACTORS ARE MORE SOPHISTICATED...

400+
CONFIRMED EXPLOITATIONS

107+
HANDS-ON ATTACKS

18
UNIQUE COUNTRIES
* may include VPS / TOR

...AND THE WINDOW TO DEFEND IS SHRINKING

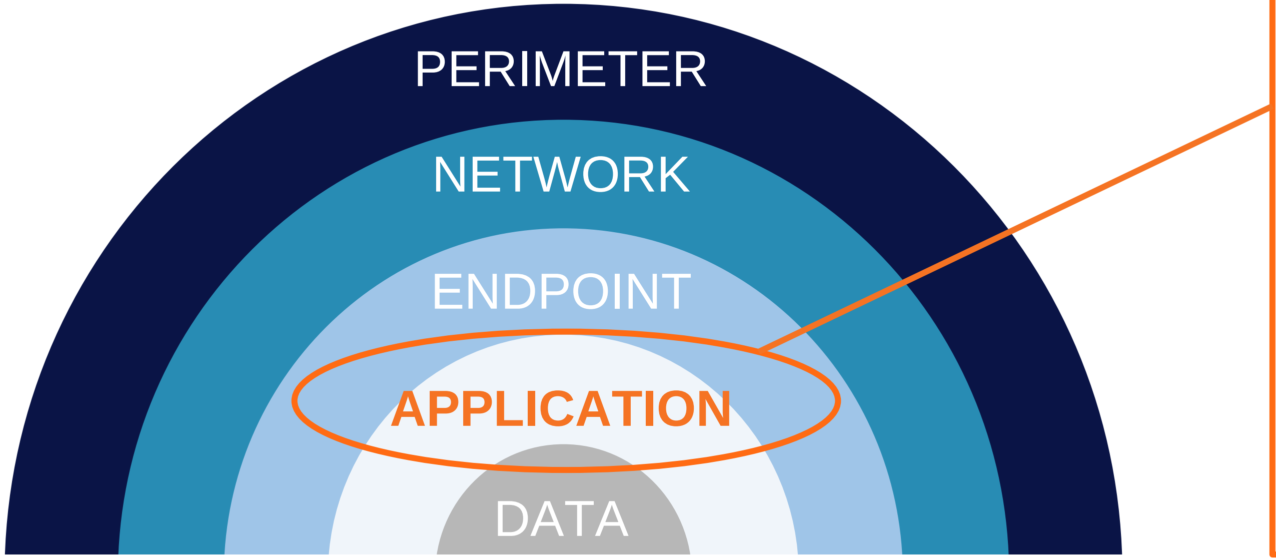
<72hrs
SAP PATCH RELEASE TO EXPLOITATION

<3hrs
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.

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

THIS MEANS BUSINESS-CRITICAL APPS ARE EXCLUDED FROM EXISTING CYBERSECURITY PROGRAMS

VULNERABILITY MANAGEMENT

- Systems managed by other teams, no visibility for InfoSec
- More processes moving to SaaS applications
- Increasing reliance on third-party developed apps

57% *Unable to quickly identify vulnerabilities at application level*[1]

54% *Unable to effectively monitor privileged access*[2]

THREAT DETECTION & RESPONSE

- No continuous monitoring, no visibility for SOC
- Reliance on manual log reviews to identify threat activity
- No ability to establish compensating controls

63% *Unable to monitor & prevent attacks at application level*[1]

APPLICATION SECURITY TESTING

- Reliance on manual code reviews
- Problems aren’t identified until they hit production
- Security is a final check, not built into DevOps process

79% *Do not build security features into app development*[1]

[1] https://www.cpomagazine.com/cyber-security/application-security-backsliding-over-70-of-organizations-say-their-portfolio-is-more-vulnerable/

[2] https://www.helpnetsecurity.com/2019/10/15/privileged-user-abuse/

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

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 CharRM, 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

Onapsis - Vulnerability Automation – SAP SuccessFactors

onapsis

SAP SuccessFactors

THE ONAPSIS PLATFORM FOR SUCCESSFACTORS HELPS YOU:

- Identify users with inappropriate rights and privileges, such as broad access to PII or the ability to impersonate other users
- Understand key security features and controls for the SuccessFactors application and how they should be used to reduce risk and comply with regulations
- Ensure that integrations with on-premises and other SaaS systems are properly implemented and configured according to best practices
- Validate that your team is minimizing the risk of configuration, access and authorization errors to improve security of both SuccessFactors and interconnected processes

THE ONAPSIS PLATFORM FOR SUCCESSFACTORS

There are multiple reasons to move your human resources business processes to the cloud with SAP SuccessFactors—from anywhere, anytime access to improved productivity, scalability and other benefits. However, extending business processes from on-premises to the cloud and back creates new security and compliance challenges, which could increase security, fraud and data privacy risks to your business.

While SAP SuccessFactors offers built-in security features, its native SaaS controls can be difficult to configure correctly, and do not give you the depth and breadth of insight you need to analyze and address risk across your interconnected business processes and applications—from the core to the cloud. In an interconnected application environment, one misconfigured system or security vulnerability can put your entire enterprise at risk.

Onapsis delivers the only platform purpose-built to protect organizations from cyber threats, streamline regulatory compliance and improve availability and performance of mission-critical applications across on-premises, cloud and SaaS apps. The Onapsis Platform for SAP SuccessFactors delivers actionable insight into your SaaS application and its interconnections so your IT operations, information security and audit and compliance teams can quickly and easily discover, assess, prioritize, and eliminate application misconfigurations and vulnerabilities.

Understand Your True Security and Compliance Risk

With Onapsis, you get a complete view into your most important applications whether they are

Onapsis - Vulnerability Automation – SAP SuccessFactors

THE ONAPSIS PLATFORM FOR SUCCESSFACTORS HELPS YOU:

- Identify **users** with inappropriate rights and privileges, such as broad access to PII or the ability to impersonate other users

- Understand key security features and controls for the SuccessFactors application and how they should be used to reduce risk and comply with regulations

- Ensure that integrations with on-premises and other SaaS systems are properly implemented and configured according to best practices

- Validate that your team is minimizing the risk of configuration, access and authorization errors to improve security of both SuccessFactors and interconnected processes

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

800+

zero-day vulnerabilities in business-critical apps

40%

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

5

US DHS critical alerts based on our research

17

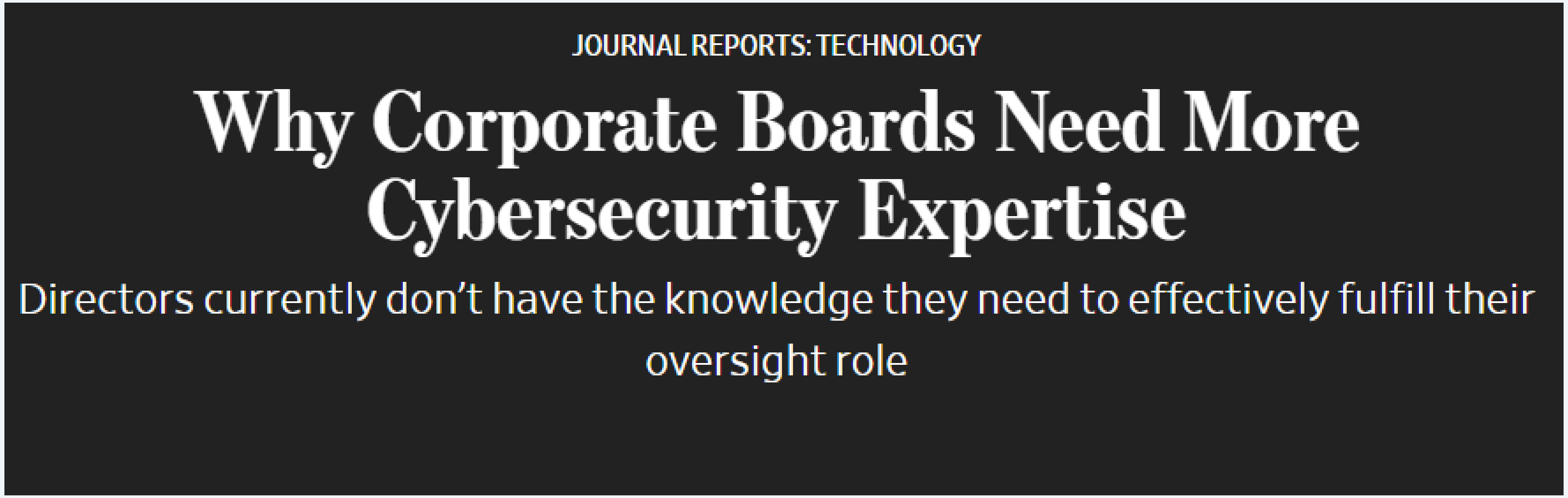
Patents, 8 issued & 9 pending

Knowledgebase of

10,000+

vulnerabilities and attacks on business applications

Compliance Audit and SAP Applications ---



JOURNAL REPORTS: TECHNOLOGY

Why Corporate Boards Need More Cybersecurity Expertise

Directors currently don’t have the knowledge they need to effectively fulfill their oversight role

WSJ Sep 9, 2022

https://www.sec.gov/files/33-11038-fact-sheet.pdf

Automate SAP system vulnerabilities reporting for compliance reporting and audits

Security Team - SAP Application vulnerability visibility
- Integration with ServiceNOW and other ticketing systems for

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

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

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

splunk> ArcSight Azure Sentinel

exabeam Radar

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 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

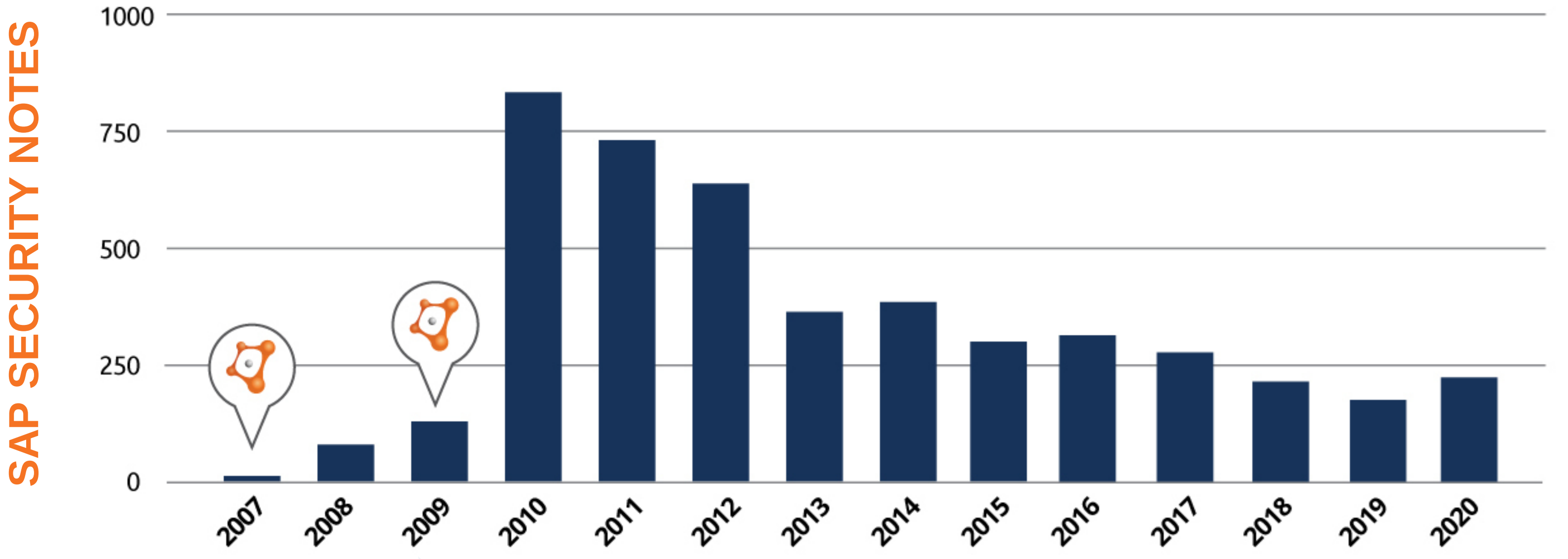
CONTROL FOR TRANSPORT | SAP TRANSPORT INSPECTION

- **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

ONAPSIS RESEARCH LABS

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



Onapsis founded

Onapsis researchers 1st to present on SAP security at Black Hat

Onapsis Influence on 2020 SAP Security Notes

40% of critical notes

18% of all notes

Discovered

800+

zero-day vulnerabilities in mission-critical applications

Mitigated

60%

of SAP HANA unpatched vulnerabilities

Created

14

out-of-the-box compliance policies for The Onapsis Platform, plus ability to customize

Database of

350+

test cases for performance, robustness, maintainability, security and compliance issues in SAP code and transports

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

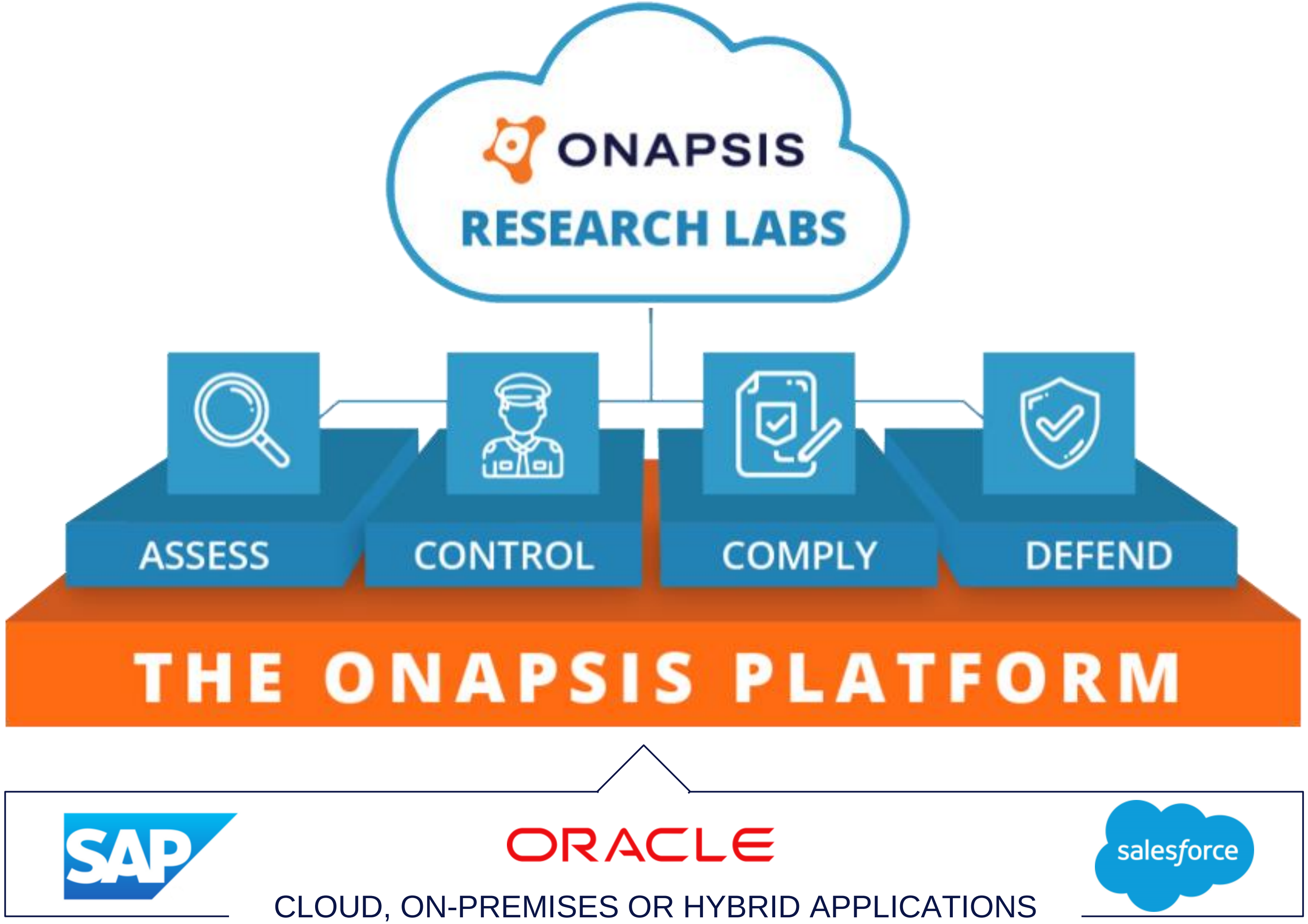
CLOUD PROVIDERS

- Microsoft Azure
- Google Cloud
- amazon web services
- SAP HANA
- ORACLE ERP Cloud

SYSTEM INTEGRATORS & MSSP

- IBM®
- Deloitte.
- pwc
- accenture
- Infosys® Navigate your next
- verizon✓

ONAPSIS GIVES YOU THE VISIBILITY AND TOOLS YOU NEED TO PROTECT YOUR BUSINESS-CRITICAL APPLICATIONS



CLOUD, ON-PREMISES OR HYBRID APPLICATIONS