ONAPSIS

RISE with SAP Cyber-Resilience

Managing SAP Application Risk: Before, During and After SAP Migrations

Jordan Thompson | Account Manager

6/9/2023

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]

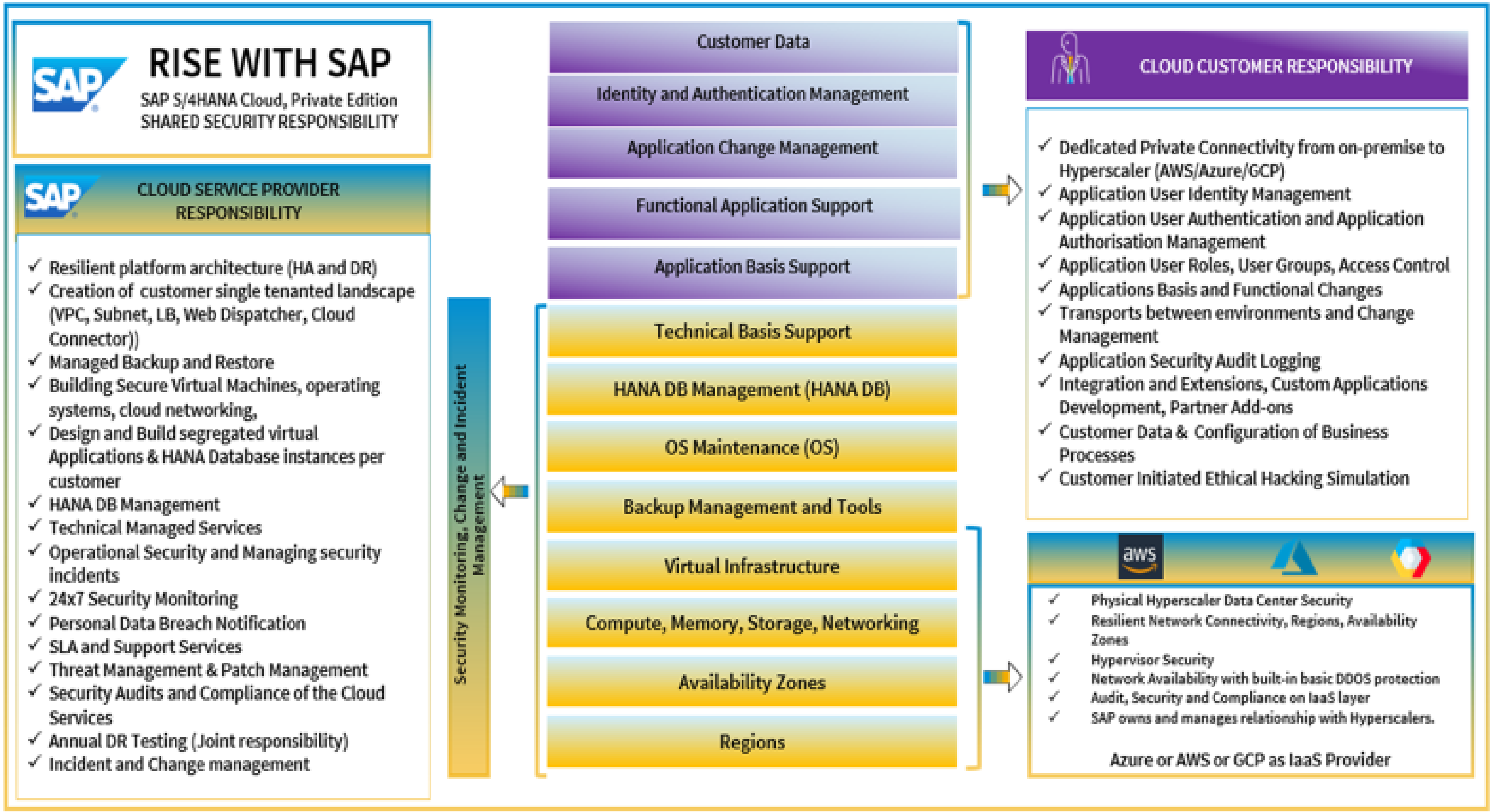
Financial Ramifications

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

Understand Your Security Responsibilities and Obligations

- ECC to S/4HANA Cloud Migrations - Your responsibility to clean the code before you migrate
- Your third-party providers and developers are also your responsibility with their access, AAA, and custom code
- SAP only automatically applies the most critical security notes; you own the responsibility of requesting the application of other security notes.
- Proven research from SAP and Onapsis demonstrated that SAP-knowledgeable threat actors can **exploit a new, vulnerable system <3 hours after coming online**
- Neglecting to “build in security” for your RISE migration can create expensive delays due to security concerns

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

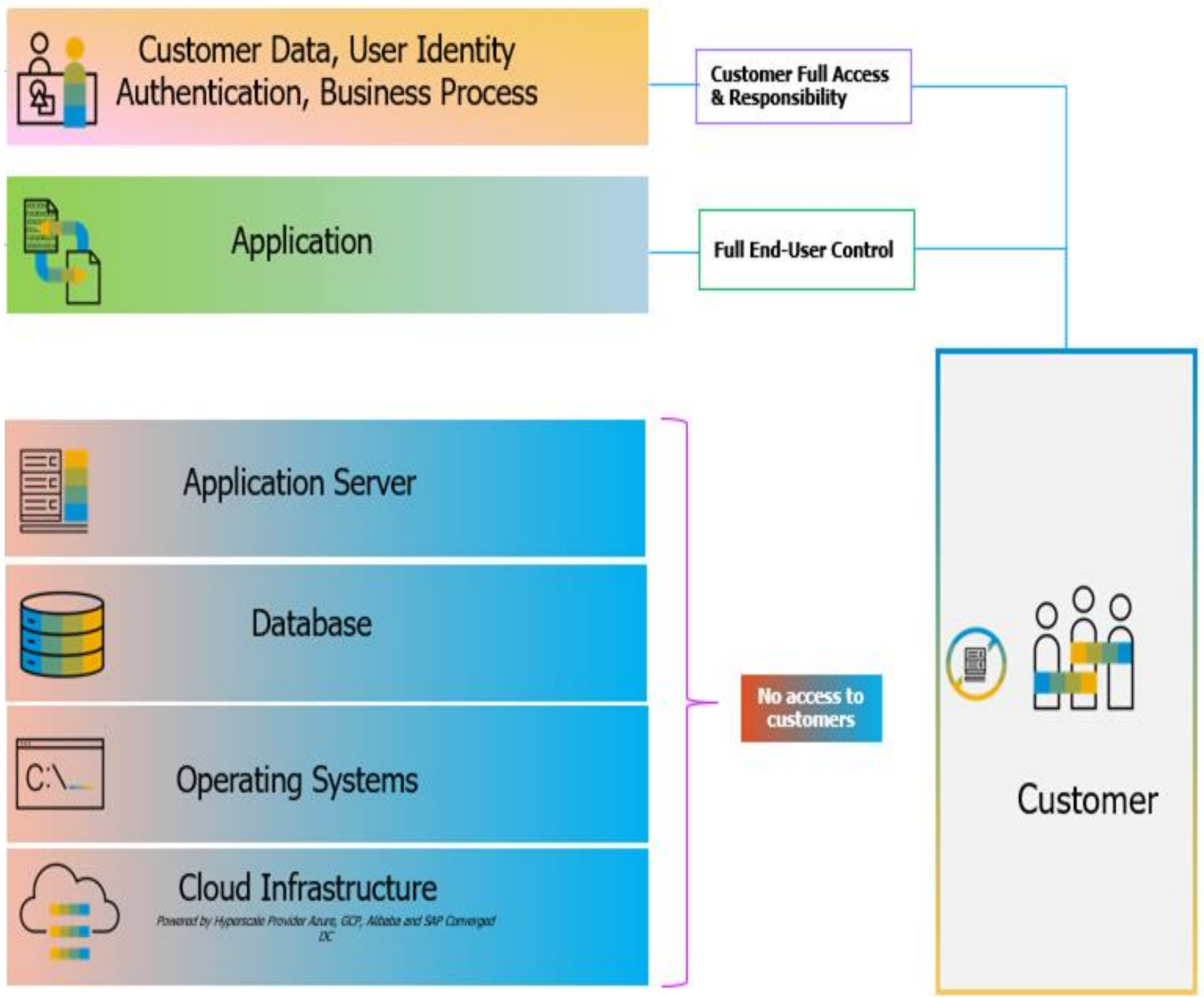
CLOUD CUSTOMER RESPONSIBILITY

- ✓ 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

- ✓ 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

Onapsis Simplifies Customer Security Responsibilities…



Customer Data, User Identity Authentication, Business Process

Customer Full Access & Responsibility

Application

Full End-User Control

Application Server

Database

Operating Systems

Cloud Infrastructure

Powered by Hyperscale Provider Azure, GCP, Alibaba and SAP Converged DC

No access to customers

Customer

Image courtesy of SAP

ONAPSIS

- **Control** ensures your custom app code is clean prior to migration
- **Assess** scans for misconfigurations, misauthorizations, as well as errors in custom code in production
- **Assess** UEBA and ML helps prioritize important Security Notes that are ***not*** automatically applied by SAP (high, medium, low)
- **Defend** monitors for zero-day threats to your landscape
- **Comply** automates SAP compliance and integrates with SAP PC (GRC)

ONAPSIS

RISE and S/4HANA Cloud: Build In Security. Don’t Bolt On.

$4.12M is the Average Cost of a Failed, Delayed, or Scaled Back Digital Transformation Project

Planning

Common Challenges at This Stage

92% of organizations consider existing customizations as a problem on their path to S/4

35% of organizations expect to face security challenges during their transformation

Overcome Them with Onapsis

- Identify problems in legacy systems and custom code before migrating
- Inventory and baseline all your systems prior to migration
- Make testing as efficient as possible during the project

Implementation

Common Challenges at This Stage

71% of organizations are concerned that the skills deficit will slow down migration

New systems deployed in IaaS environments are exploited in as little as **3 hours**

Overcome Them with Onapsis

- Secure areas of customer responsibility under RISE with SAP
- Validate the custom code work of contractors and SI from QA to Prod
- Monitor for threats in real-time while you build and migrate securely

Post-Deployment

Common Challenges at This Stage

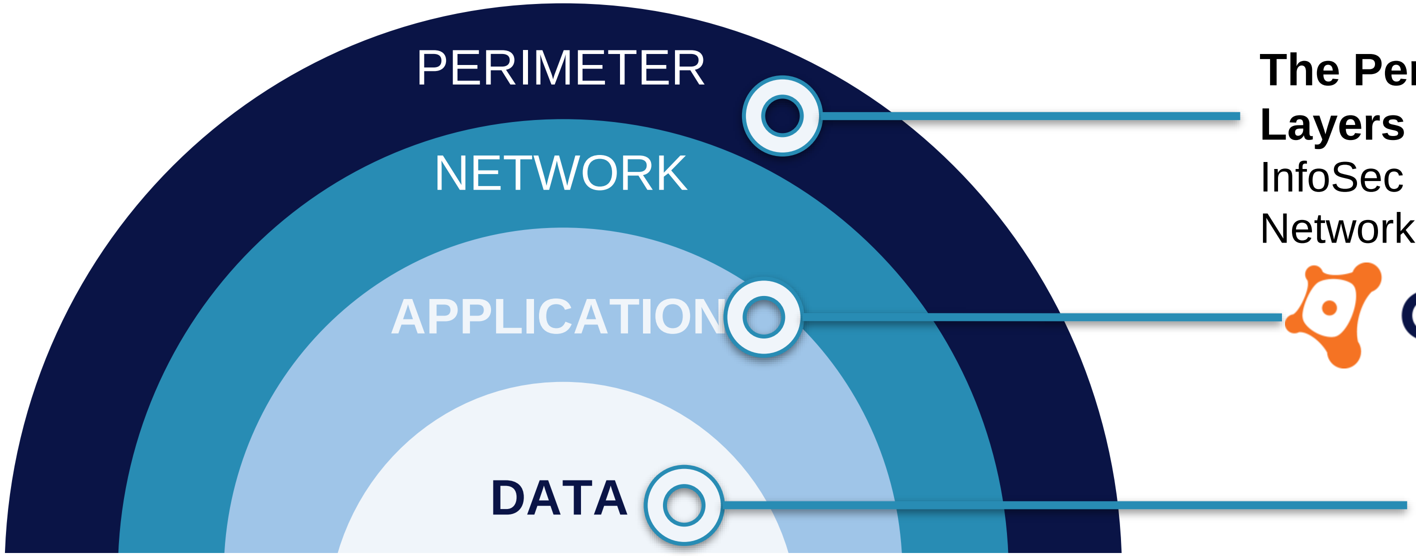
Exploit activity is observed in as little as **72 hours** after a patch is released

$5M: The average annual cost of business disruption due to non-compliance

Overcome Them with Onapsis

- Accurately measure & communicate risk facing new systems over time
- Stay protected against new SAP threats with Onapsis Research Labs
- Stay compliant with automated ITGC testing + SAP PC integration

Where Does Onapsis Fit



The Perimeter and Network Security Layers
InfoSec Defense-in-Depth Models Secure the Network and Traffic But Not the Applications.

ONAPSIS Risk-Driven Security at the Application Layer

The Data Layer SAP
SAP Primarily Focuses Here on Controls That Provide for Segregation of Duties, Authentication, and Business Logic Monitoring…But Ignore Securing the Application Itself.

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

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

Futureproof Your SAP Security Investment with Onapsis

TODAY

- Full Onapsis Platform Support for ABAP and HANA systems on SAP S/4HANA PCE (as well as onPrem)
- Control for Code for HANA supports development in SAP (BTP) Business Application Studio
- Control for Code for ABAP supports scanning ABAP code within SAP-approved code repositories, such as Jenkins and Piper

TOMORROW

- Enhancements to the Control product line in FY23, delivering more direct support for BTP-related use cases, such as development, migration, and code movement
- Exploring both internal and SAP-joint opportunities to extend the supported capabilities of the Onapsis Platform for RISE and BTP

OUR VISION

- Onapsis is the premier expert and market leader on SAP application security and compliance.
- Onapsis is committed to supporting our customers' SAP journeys, wherever they take them, and we are actively taking steps to enhance and expand our portfolio with more comprehensive support for the broader RISE with SAP program.
- We focus on areas where we can apply our deep security knowledge, threat research capabilities, and SAP expertise.

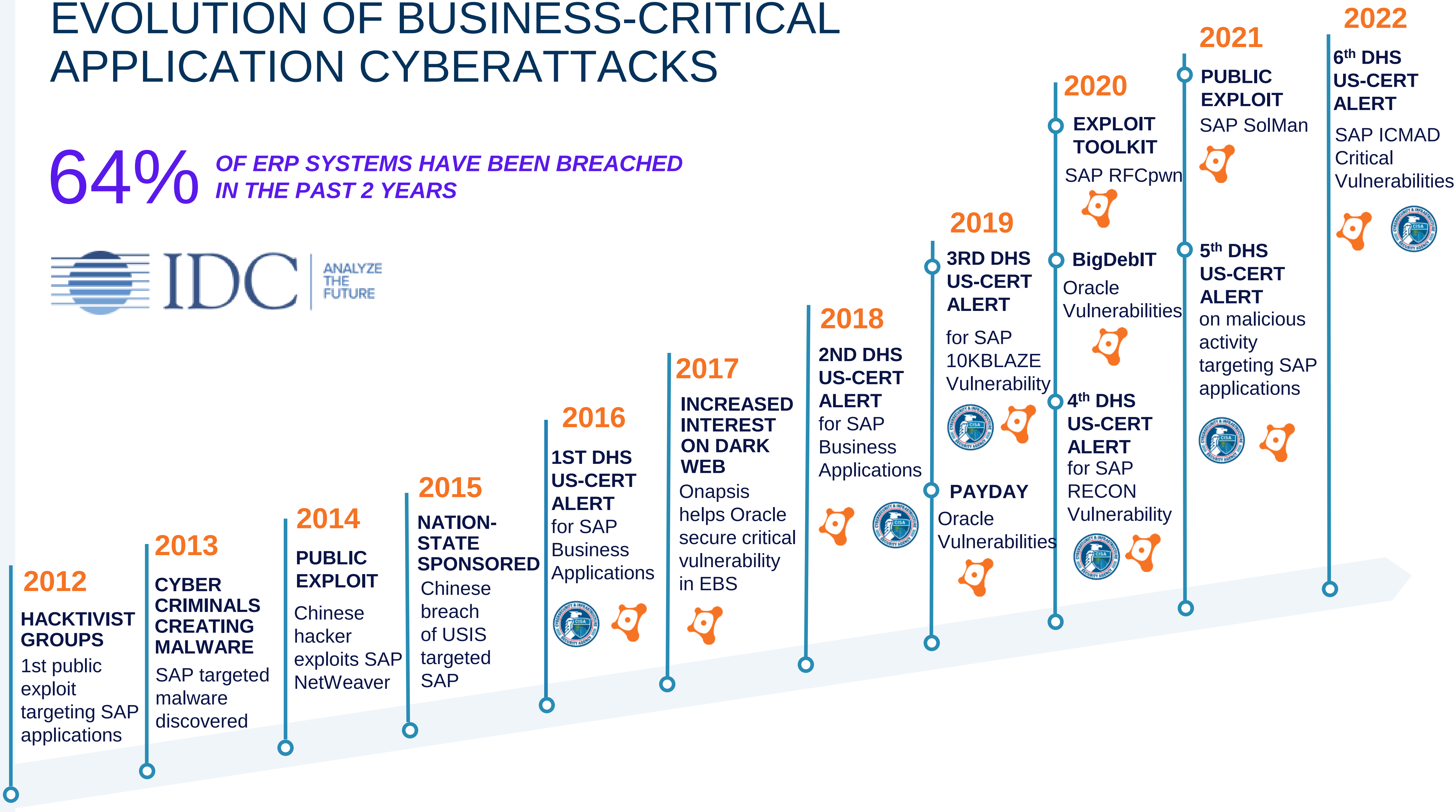
Confidential & Proprietary Information of Onapsis

The following information is being shared in order to outline some of Onapsis' current product plans, but it is important to understand that it is being shared for informational purposes only, and not as a binding commitment. Please do not rely on this information in making purchasing decisions because Onapsis makes no representations about future functionality, and ultimately, the development, release, and timing of any products, features or functionality remains at the sole discretion of Onapsis and is subject to change.

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

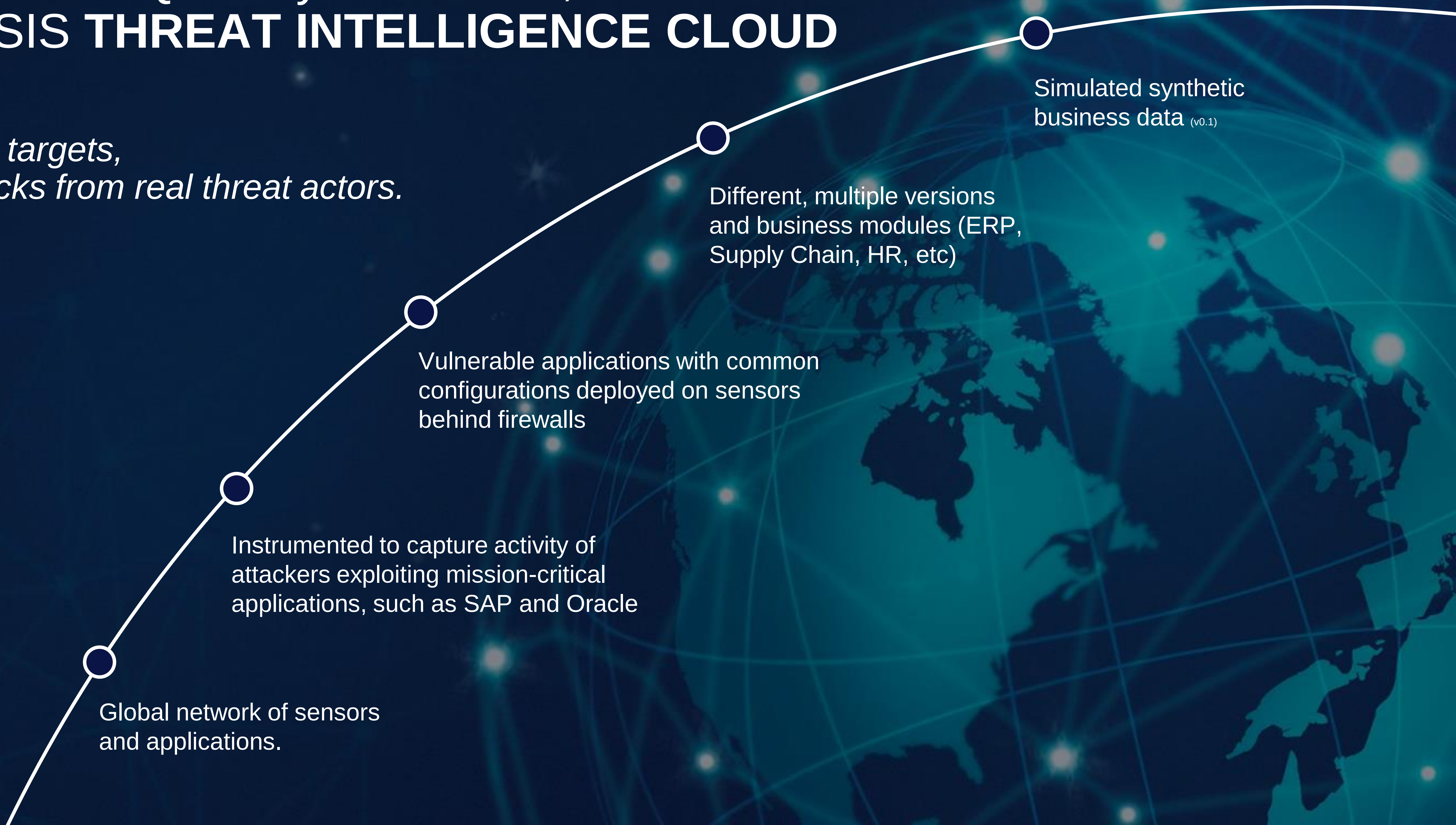
2021
PUBLIC EXPLOIT
SAP SolMan

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

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

How Did We Quantify This? Well, We Built the ONAPSIS **THREAT INTELLIGENCE CLOUD**

Synthetic targets,
Real attacks from real threat actors.



Global network of sensors and applications.

Instrumented to capture activity of attackers exploiting mission-critical applications, such as SAP and Oracle

Vulnerable applications with common configurations deployed on sensors behind firewalls

Different, multiple versions and business modules (ERP, Supply Chain, HR, etc)

Simulated synthetic business data (v0.1)

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

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

Thank You!

@onapsis

linkedin.com/company/onapsis

ONAPSIS.COM