ONAPSIS | ASUG

SAP CYBER SECURITY AND HOW THE SAP THREAT LANDSCAPE HAS TRANSFORMED IN 2022

SAP AND ONAPSIS

SAP Vision and Mission

SAP is the market leader in **enterprise application software**, helping companies of all sizes and in all industries run at their best.

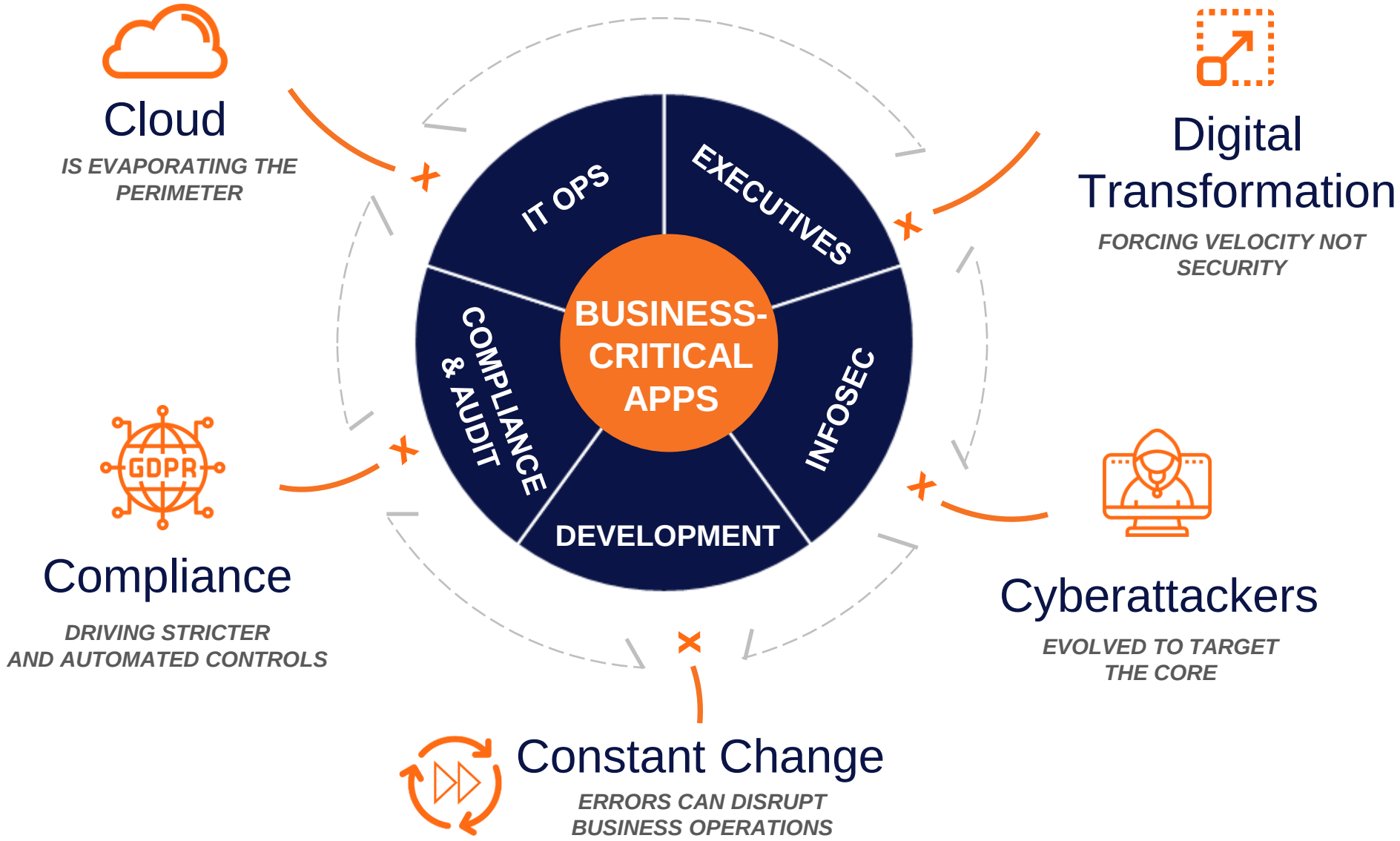
SAP provides the tools to harness the power of data flowing through our customers' systems. Our vision for the intelligent enterprise is an event-driven, real-time business powered by intelligent applications and platforms.

Onapsis Vision and Mission

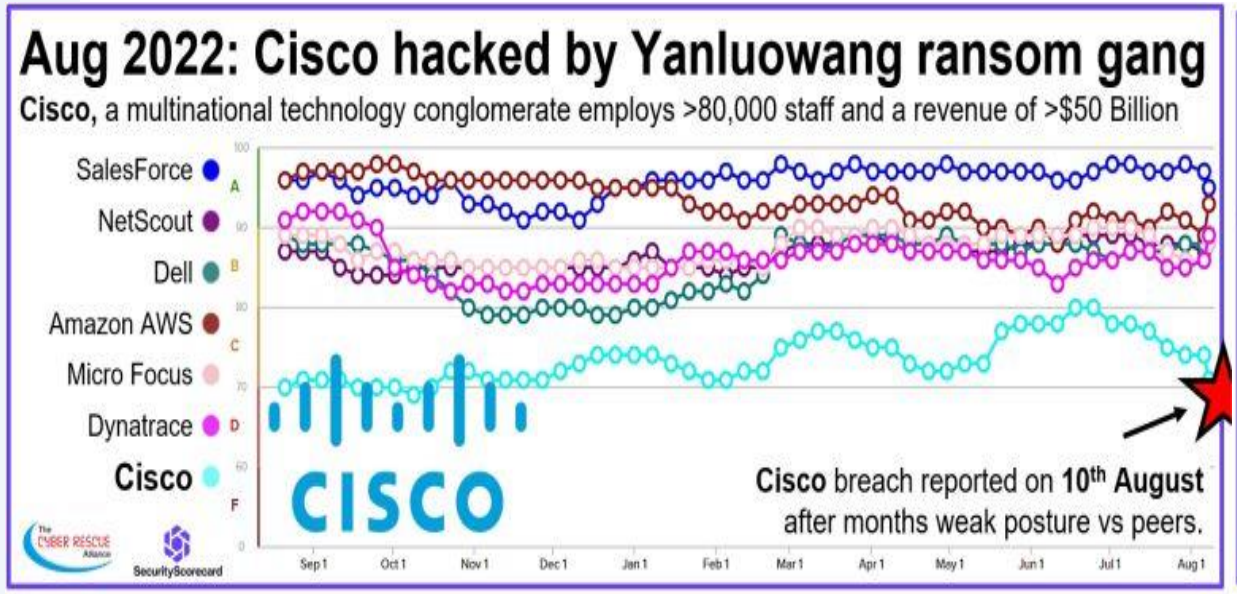
Onapsis is the market leader in **SAP application security.** We provide our customers with confidence that their business-critical applications are secure.

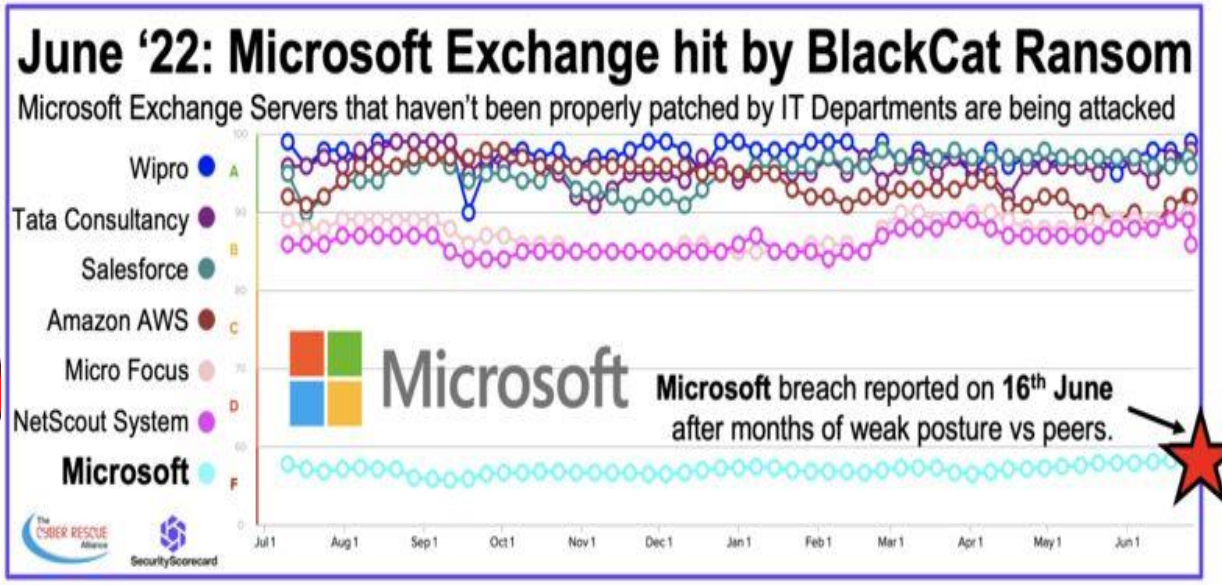
By safeguarding your company at its core, the applications you depend on each and every day will be secure, compliant and available.

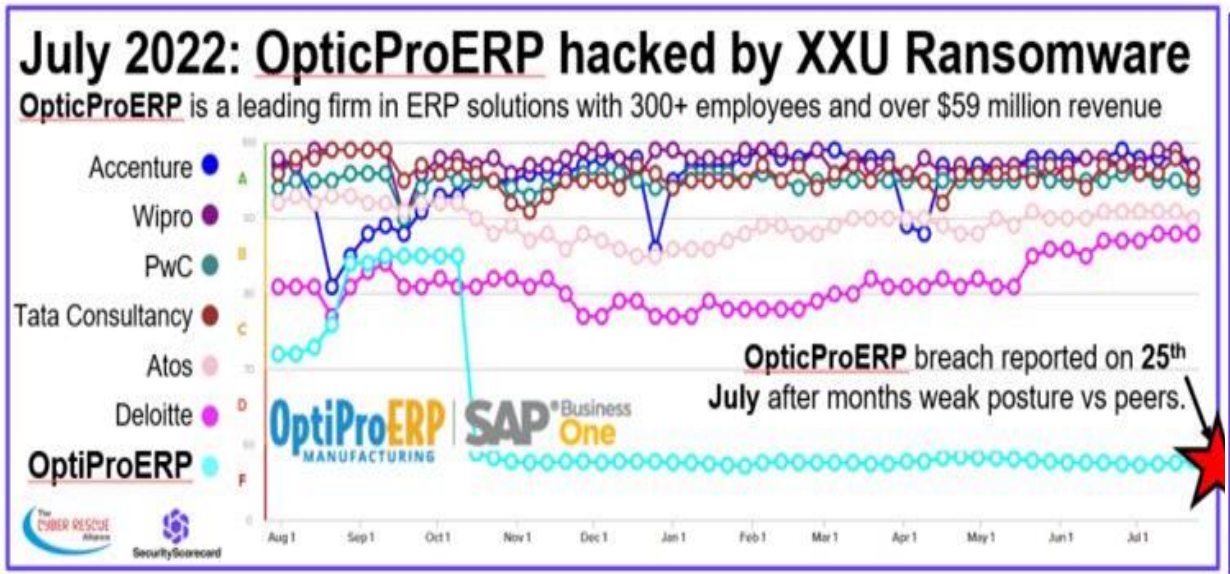
WHY CYBER SECURITY IS IMPORTANT IN 2022?

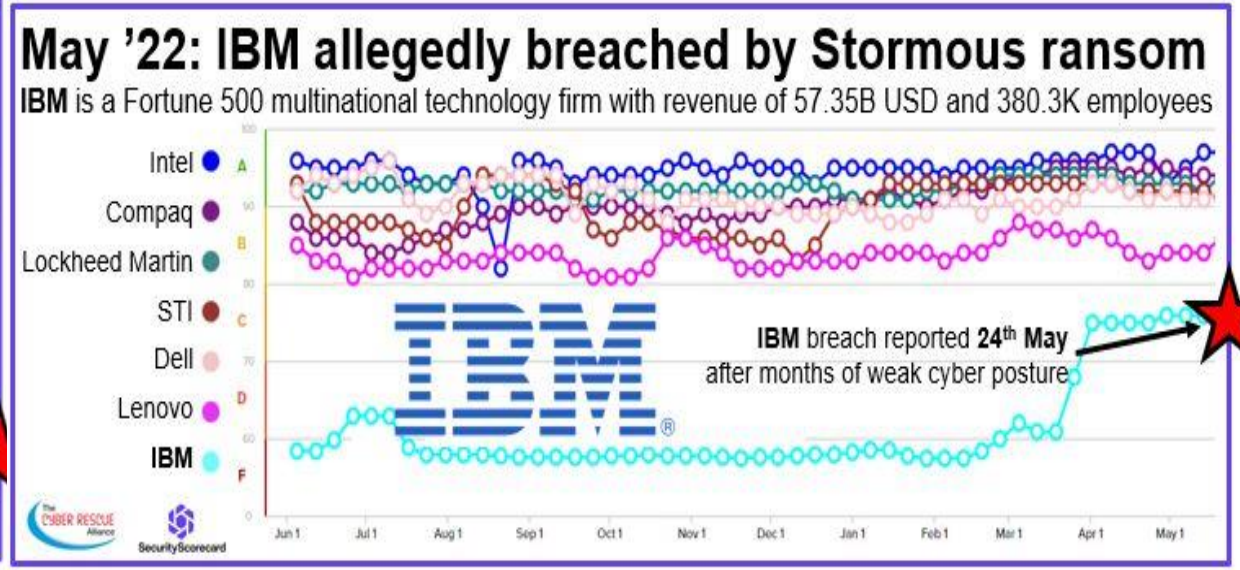


SO WHAT









ATTACKS ON BUSINESS-CRITICAL APPLICATIONS ARE INCREASING

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

IDC ANALYZE THE FUTURE

6 ALERTS IN 6 YEARS **ON MALICIOUS CYBERACTIVITY 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

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

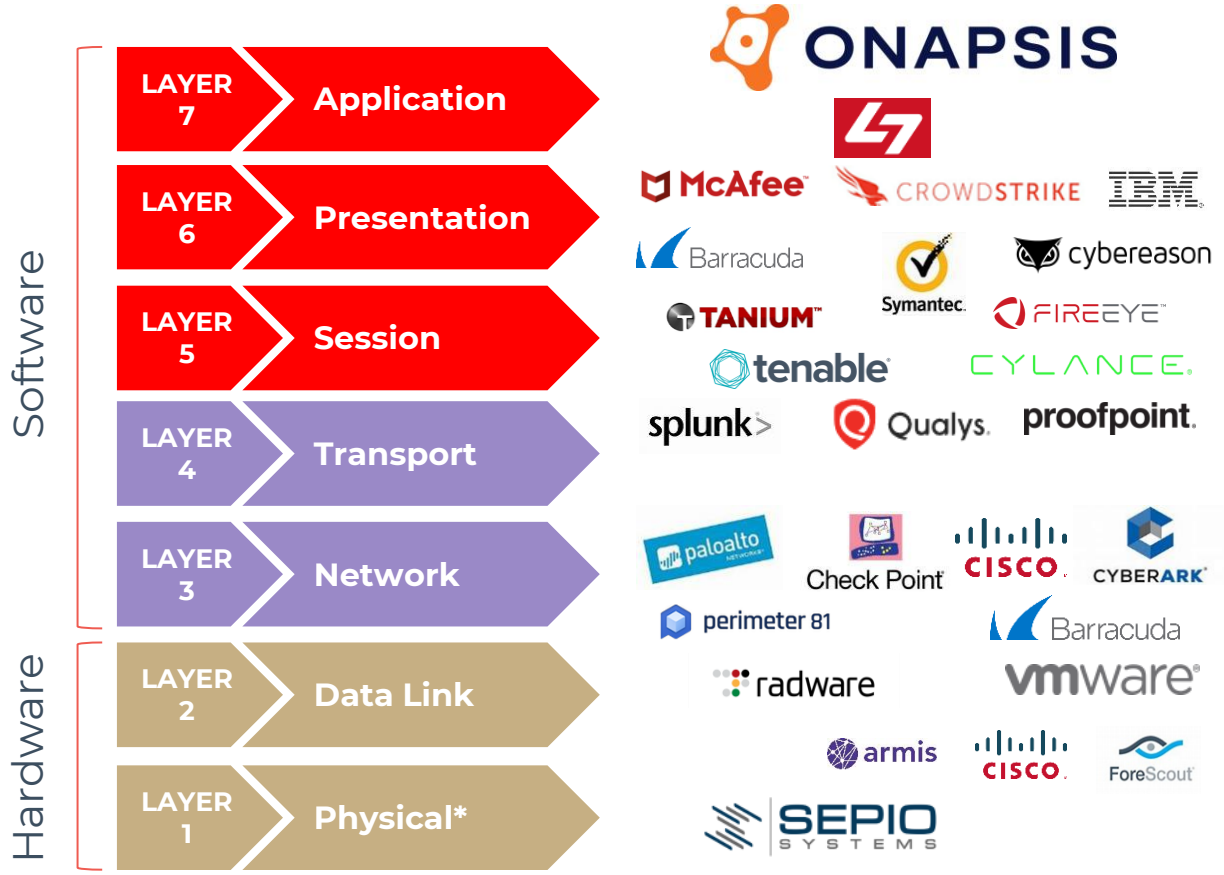
<72hrs
SAP PATCH RELEASE TO EXPLOITATION

<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.

Security In Depth – Protect the Application Layer

- All the solutions listed are in place to protect the **APPLICATION LAYER!**
  - Data is the Prize!
- Most cybersecurity solutions do not provide a ROI
  - Cost of doing business
- Onapsis IS “The First & Last Line of Defense” for Bus. Critical Apps



Application Layer ➔ Largest Surface Area for Attacks to Occur

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/

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]

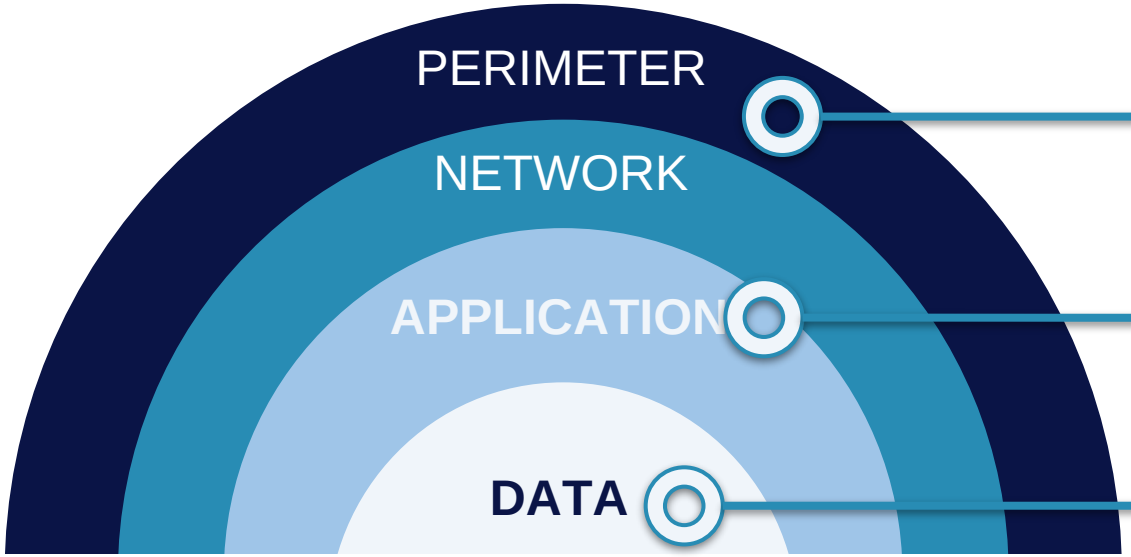
APPLICATION SECURITY TESTING

- 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/

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

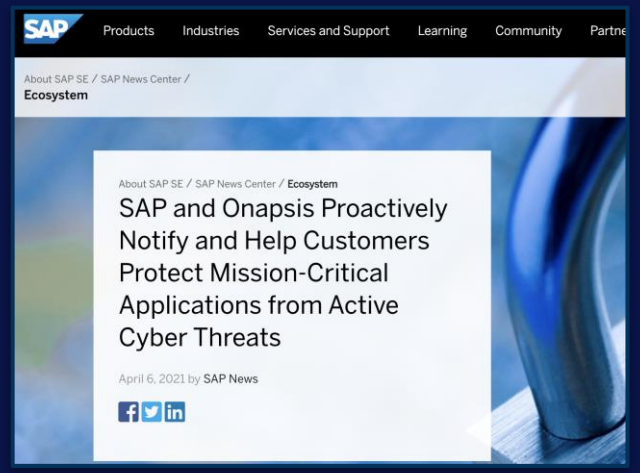
ONAPSIS RESEARCH LABS

The World's Leading Threat Research Group for SAP Application Security

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

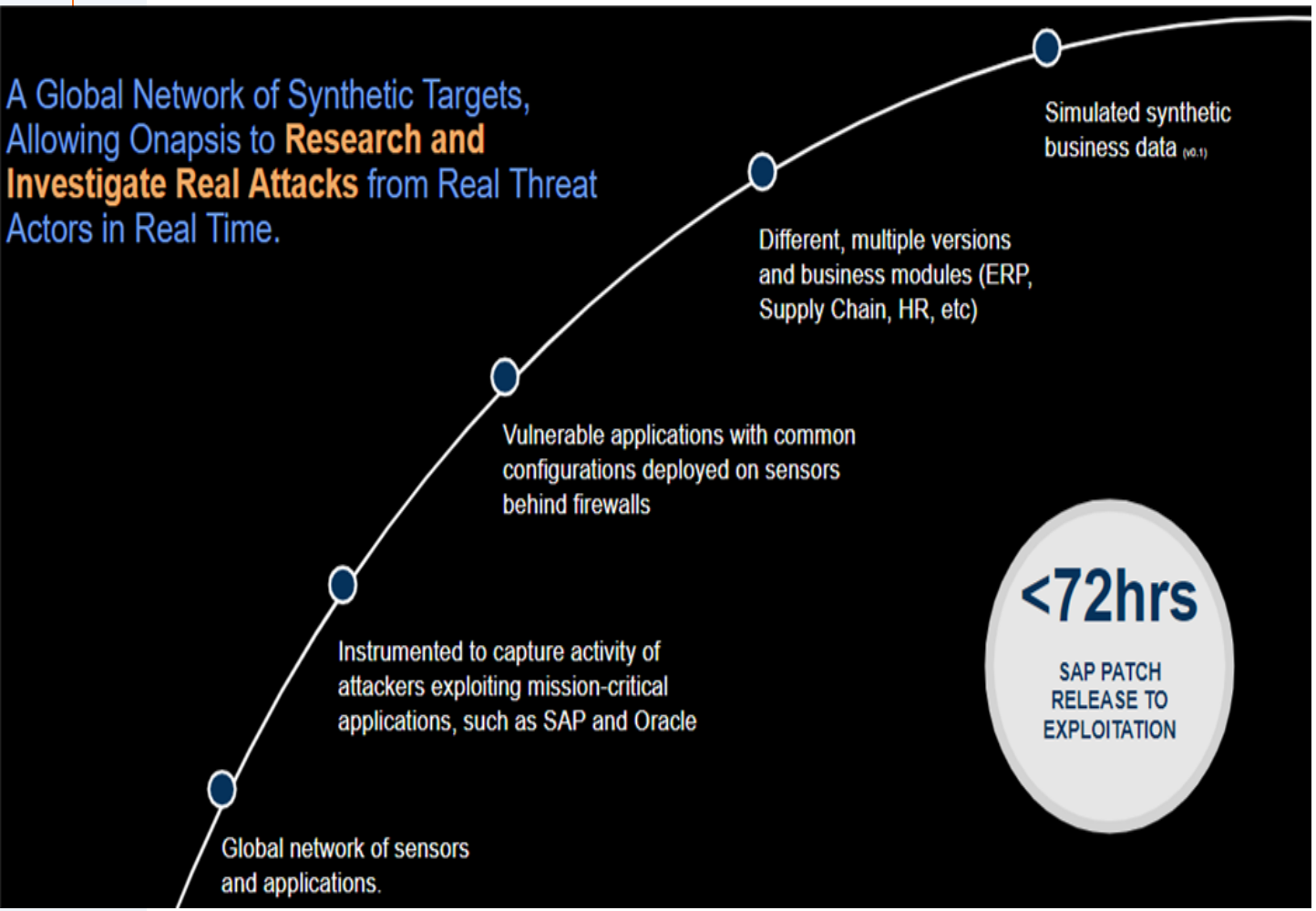
6
US DHS critical alerts based on our research

Knowledgebase of
10,000+
vulnerabilities and attacks on business-critical applications



Featured In: REUTERS FORTUNE CNBC WSJ Forbes

ONAPSIS, SAP, AND DHS: DIRECT ATTACKS ON SAP BUSINESS APPLICATIONS ARE INCREASING IN FREQUENCY AND SEVERITY



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

THE ONAPSIS PLATFORM - Protecting SAP at the Application Level

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

Integrations with compliance automation solutions:

SAP Process Control

Onapsis Research Labs

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

Realize Positive Business Impact from Onapsis Assess

83%

Reduced issue remediation time

AMGEN

95%

Of time saved, validating patches correctly applied

Pfizer

33%

Faster migration to the cloud

IPG

2 FTE

Saved replacing manual work

ATB Financial · BNSF Railway · deluxe · FOSSIL · lyondellbasell · Levi's

Lilly

*"Prior to using Onapsis Assess, 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."*

NuStar

"Happy Customer. It would be almost impossible to manage patches, configuration, and overall managing vulnerabilities manually."

NVIDIA

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

The Walt Disney Company

"Onapsis is integral to security management, saving considerable time and providing comfort that issues are addressed."

THANK YOU

steven.schliem@onapsis

linkedin.com/company/onapsis

ONAPSIS.COM

ASUG

ONAPSIS

Don’t Wait. Automate

Reduce risk and avoid security roadblocks on your journey to SAP S/4HANA with the Onapsis solution

70% faster
code reviews

95% faster
patch validation

83% faster
vulnerability remediation

92% automation
of controls testing

Why is SAP Cybersecurity a Blind Spot?

Organizations can’t patch quickly enough due to lacking prioritization tools and a massive backlog

- New patches released every month, SAP landscapes are large, and the patching process is complex.
- Enterprises could throw bodies at the problem or patch what is easiest to “make progress”.

Lack knowledge or understanding of other problems that exist, leading to unaddressed risk and open attack vectors

- Some organizations believe that their defense-in-depth model protects them, but we know that threat actors are attacking the application layer with brute-force approaches targeting default roles, highly privileged users
- Organizations don’t have an easy way to validate if they are following configuration best practices

Challenged with doing more with less, so they may skip patches or rush manual security reviews

- SAP, while critical, is only one part of an increasingly large portfolio of applications and systems
- Many budgets are stagnant or trimmed as a result of the pandemic or to support digital transformation or cloud migration projects.