ONAPSIS

The Threat Landscape is Transforming: Understand The Importance of Protecting Your SAP Applications

Krunal Gala & Thierry Tailhardat | July 29th, 2022

Onapsis: The Market Leader in Business Application Security

Founded

2009

Headquarters in Boston, MA. Global Offices in Argentina, Germany, and Singapore

#1

Market Category Leader

20% FORTUNE 100

of the Fortune 100 Rely on Onapsis for Business-Critical SAP Security

17

Patents for Our Unique Technology

62

Global NPS: “Excellent”

94%

CSAT Customer Support

Trusted by the World’s Leading Brands

AMERICA'S NAVY
Disney
DOW
BMW
ALDI SÜD
gm
UNDER ARMOUR
THE HOME DEPOT
Bloomberg
PEPSICO
Colgate
Google
3M
Pfizer
Cargill
Kimberly-Clark

Deloitte. Technology Fast500

AMERICA'S FASTEST-GROWING PRIVATE COMPANIES Inc. 5000

THE CHANNEL CO. CRN SECURITY 100 2022

GLOBAL INFOSEC AWARDS WINNER CYBER DEFENSE MAGAZINE 2022

CYBERSECURITY BREAKTHROUGH AWARD 2021

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

6

US DHS critical alerts based on our research

17

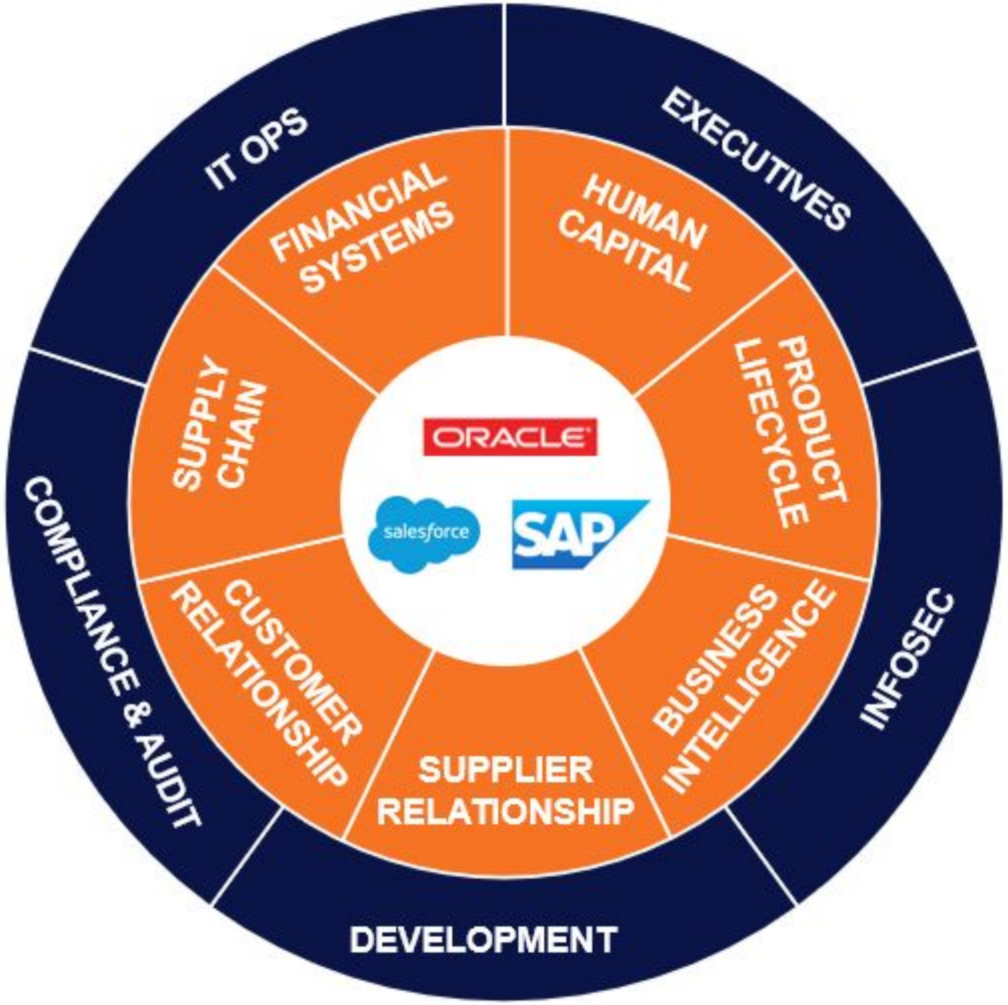
Patents, 8 issued & 9 pending

Knowledgebase of

10,000+

vulnerabilities and attacks on business applications

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]

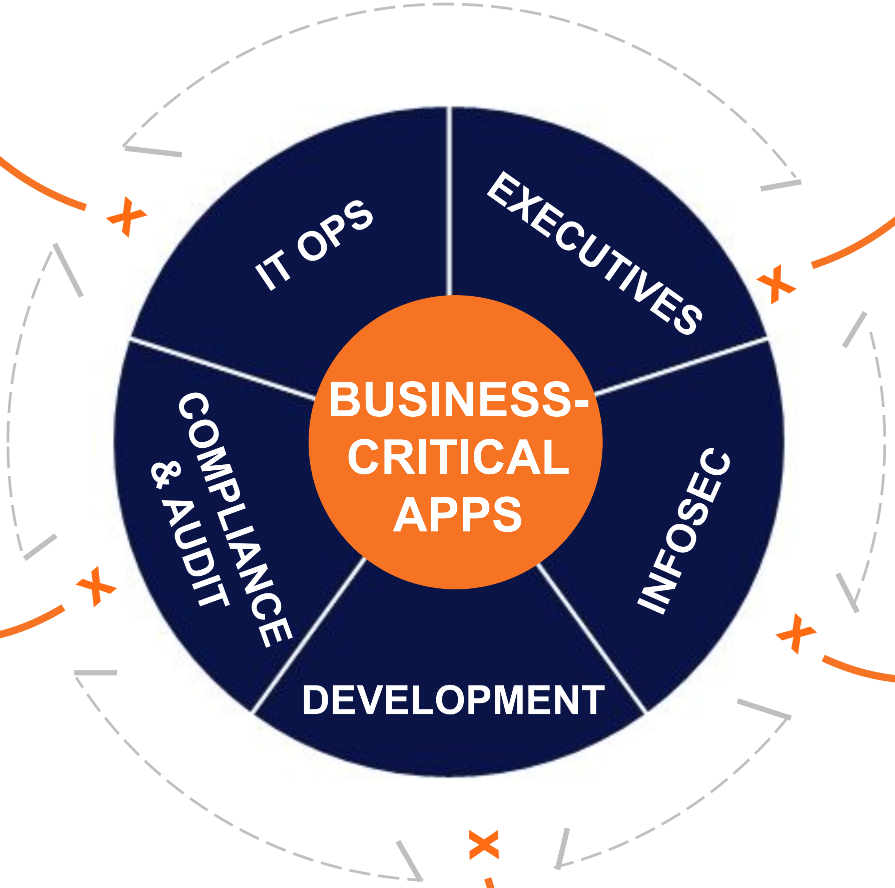
BUT, WE'RE FACING A PERFECT STORM OF COMPLEXITY

Cloud

IS EVAPORATING THE PERIMETER

Digital Transformation

FORCING VELOCITY NOT SECURITY



BUSINESS-CRITICAL APPS

IT OPS

EXECUTIVES

INFOSEC

DEVELOPMENT

COMPLIANCE & AUDIT

Compliance

DRIVING STRICTER AND AUTOMATED CONTROLS

Cyberattackers

EVOLVED TO TARGET THE CORE

Constant Change

ERRORS CAN DISRUPT BUSINESS OPERATIONS

AND ATTACKS ON BUSINESS-CRITICAL APPLICATIONS ARE INCREASING

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

IDC ANALYZE THE FUTURE

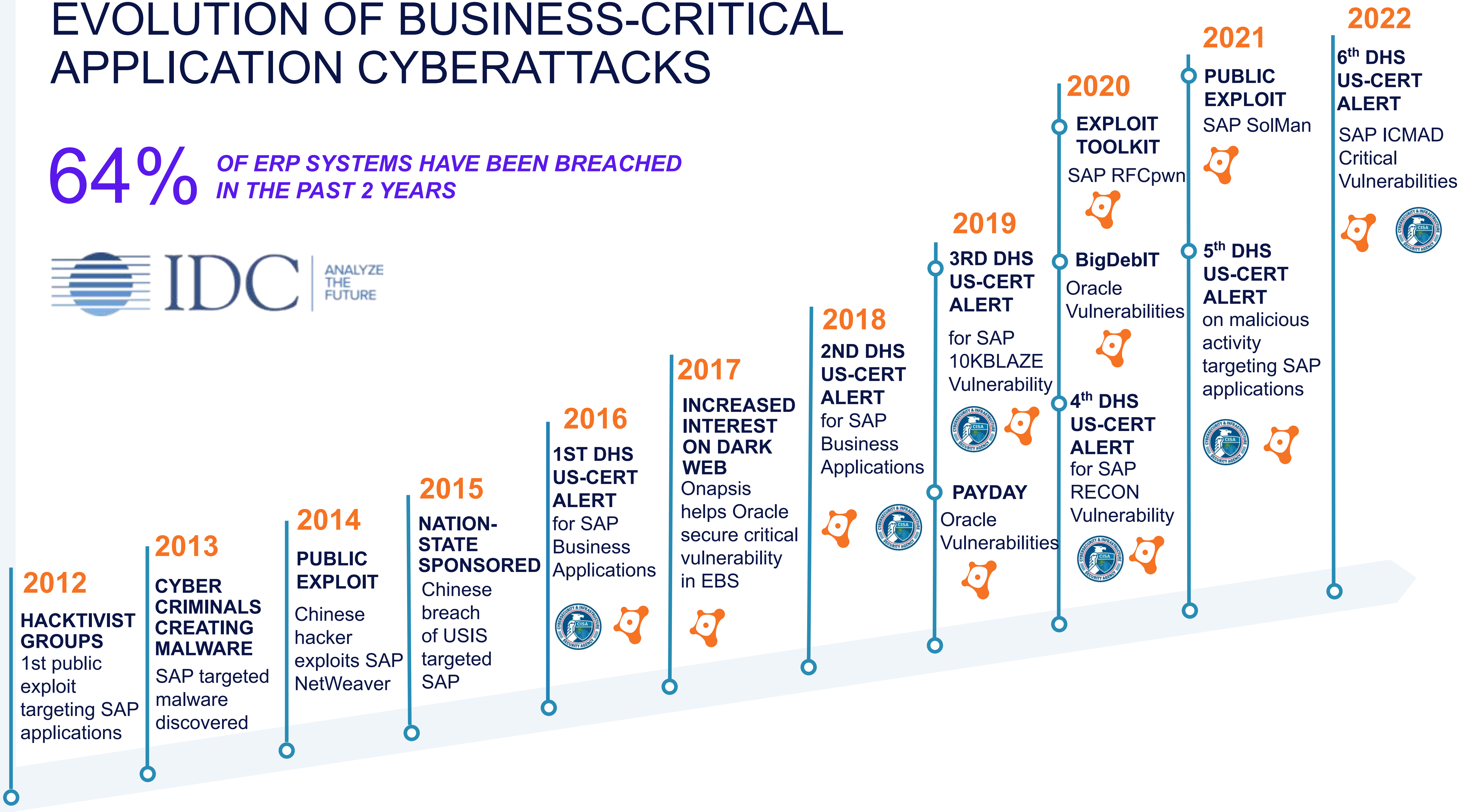
6 ALERTS IN 6 YEARS **ON MALICIOUS CYBERACTIVITY OR VULNERABILITIES IN BUSINESS CRITICAL APPLICATIONS**

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

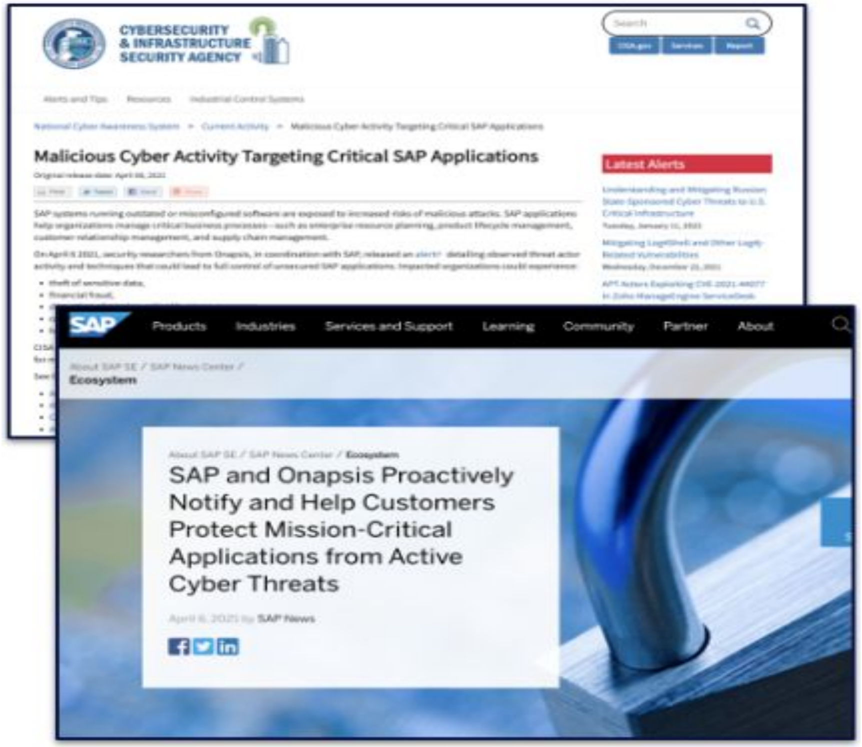
2021
PUBLIC EXPLOIT
SAP SolMan

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

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

ONAPSIS Threat Intelligence from Onapsis and SAP

THREAT ACTORS ARE BECOMING MORE SOPHISTICATED...



CYBERSECURITY & INFRASTRUCTURE SECURITY AGENCY

Search

Alerts and Tips | Resources | Industrial Control Systems

National Cyber Awareness System > Current Activity > Malicious Cyber Activity Targeting Critical SAP Applications

Malicious Cyber Activity Targeting Critical SAP Applications

Original release date: April 06, 2021

SAP systems running outdated or misconfigured software are exposed to increased risks of malicious attacks. SAP applications help organizations manage critical business processes – such as enterprise resource planning, product lifecycle management, customer relationship management, and supply chain management.

On April 6 2021, security researchers from Onapsis, in coordination with SAP, released an alert detailing observed threat actor activity and techniques that could lead to full control of unsecured SAP applications. Impacted organizations could experience:

- theft of sensitive data,
- financial fraud,

Latest Alerts

Understanding and Mitigating Russian State-Sponsored Cyber Threats to U.S. Critical Infrastructure
Tuesday, January 11, 2022

Mitigating Log4Shell and Other Log4j-Related Vulnerabilities
Wednesday, December 22, 2021

APT Actors Exploiting CVE-2021-44077 in Zoho ManageEngine ServiceDesk

SAP | Products | Industries | Services and Support | Learning | Community | Partner | About

About SAP SE / SAP News Center /
Ecosystem

About SAP SE / SAP News Center / Ecosystem

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

April 6, 2021 by SAP News

...AND THE WINDOW TO DEFEND IS SHRINKING

400+
CONFIRMED EXPLOITATIONS

107+
HANDS-ON ATTACKS

18
UNIQUE COUNTRIES
* may include VPS / TOR

<72hrs
SAP PATCH RELEASE TO EXPLOITATION

<3hrs
NEW SYSTEM ONLINE TO BEING EXPLOITED

<24hrs
LOG4J PUBLIC DISCLOSURE TO OBSERVED EXPLOITATION

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.

ICMAD Vulnerabilities: What Was Discovered? Why Is This Important?

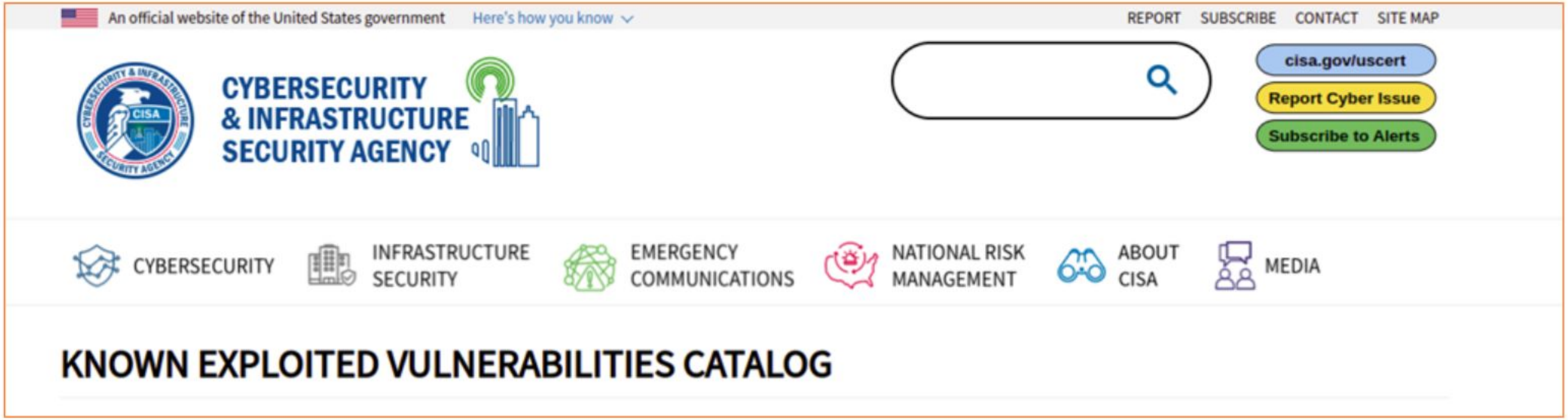
The ICMAD *("Internet Communication Manager Advanced Desync")* vulnerabilities are critical, network-exploitable vulnerabilities affecting the SAP Internet Communication Manager, the component that enables HTTP(S) communications in SAP systems.

- **CVE-2022-22536 - CVSSv3 10.0** Affected: NetWeaver ABAP/Java; Web Dispatcher
- **CVE-2022-22532 - CVSSv3 8.1** Affected: NetWeaver Java
- **CVE-2022-22533 - CVSSv3 7.5** Affected: NetWeaver Java

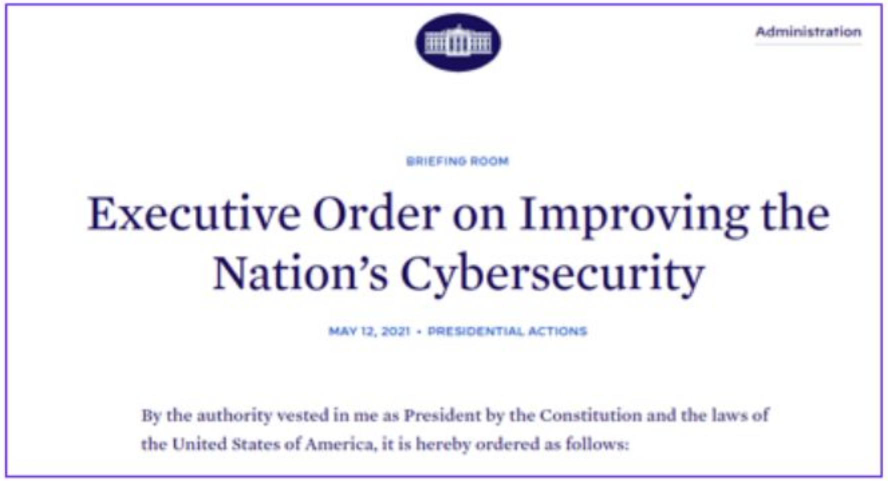
Important to Note: Issues could be exploited over the Internet **with no authentication**, bypassing common MFA controls.

SAP and Onapsis are not currently aware of known breaches directly related to these vulnerabilities but strongly recommend patching as soon as possible.

The Catalog of Known Exploited Vulnerabilities



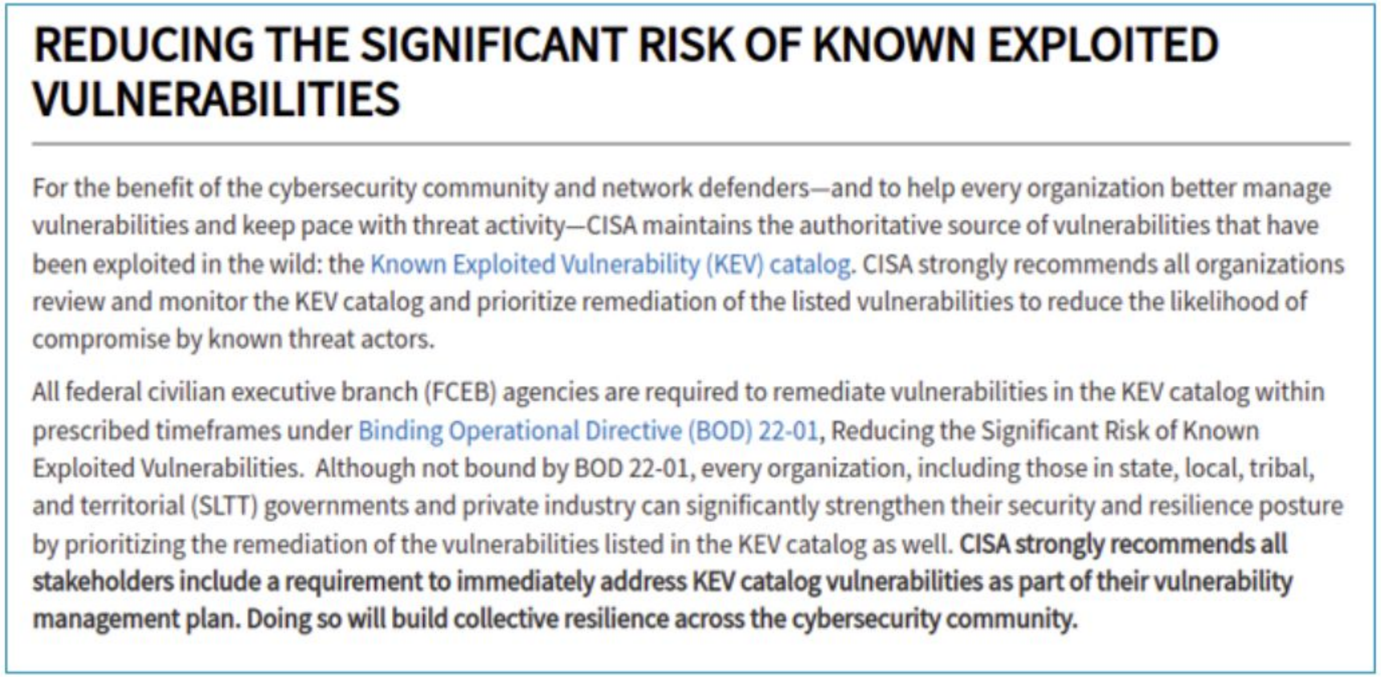
KNOWN EXPLOITED VULNERABILITIES CATALOG



Executive Order on Improving the Nation's Cybersecurity

MAY 12, 2021 • PRESIDENTIAL ACTIONS

By the authority vested in me as President by the Constitution and the laws of the United States of America, it is hereby ordered as follows:

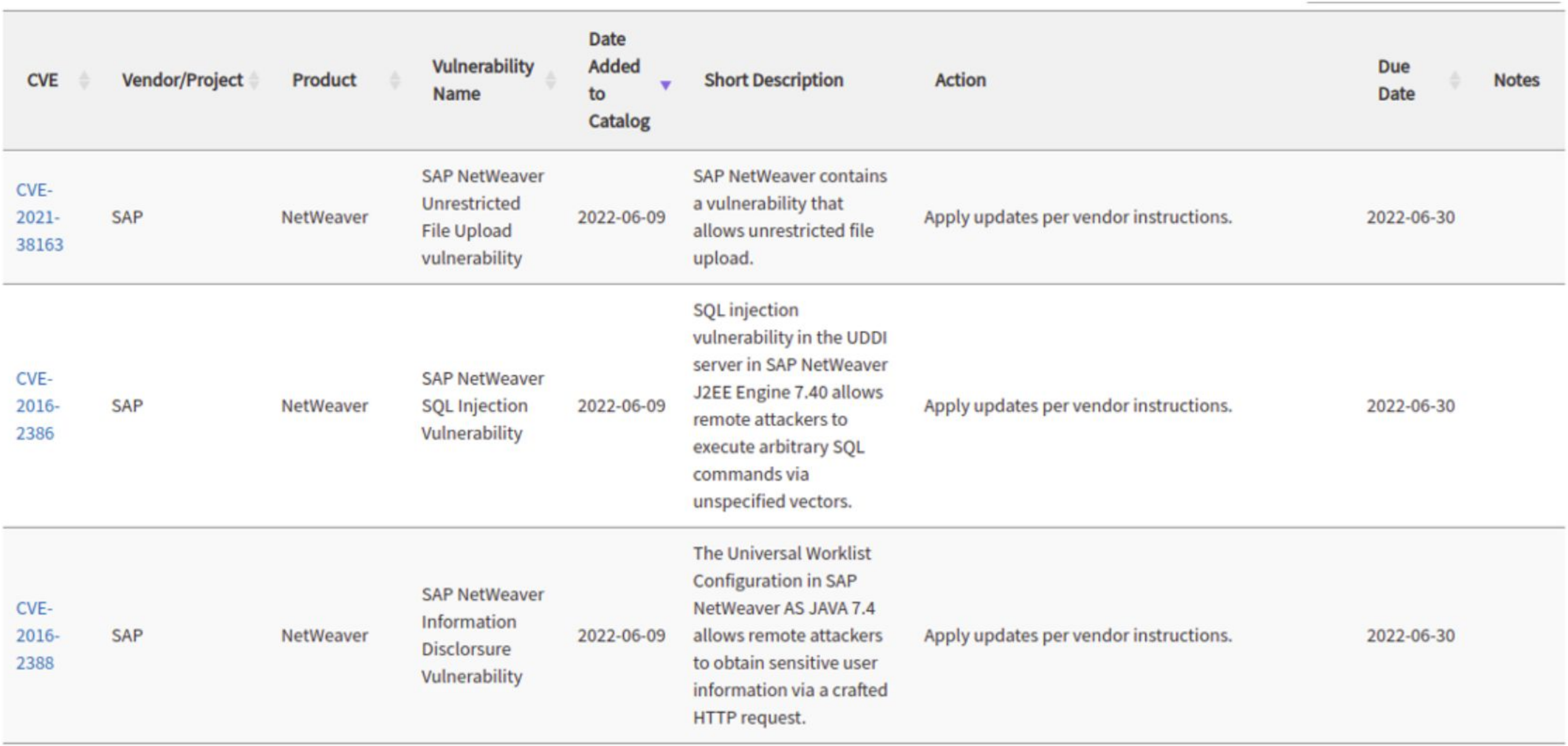


REDUCING THE SIGNIFICANT RISK OF KNOWN EXPLOITED VULNERABILITIES

For the benefit of the cybersecurity community and network defenders—and to help every organization better manage vulnerabilities and keep pace with threat activity—CISA maintains the authoritative source of vulnerabilities that have been exploited in the wild: the Known Exploited Vulnerability (KEV) catalog. CISA strongly recommends all organizations review and monitor the KEV catalog and prioritize remediation of the listed vulnerabilities to reduce the likelihood of compromise by known threat actors.

All federal civilian executive branch (FCEB) agencies are required to remediate vulnerabilities in the KEV catalog within prescribed timeframes under Binding Operational Directive (BOD) 22-01, Reducing the Significant Risk of Known Exploited Vulnerabilities. Although not bound by BOD 22-01, every organization, including those in state, local, tribal, and territorial (SLTT) governments and private industry can significantly strengthen their security and resilience posture by prioritizing the remediation of the vulnerabilities listed in the KEV catalog as well. **CISA strongly recommends all stakeholders include a requirement to immediately address KEV catalog vulnerabilities as part of their vulnerability management plan. Doing so will build collective resilience across the cybersecurity community.**

Update on Jun 09 - 2022



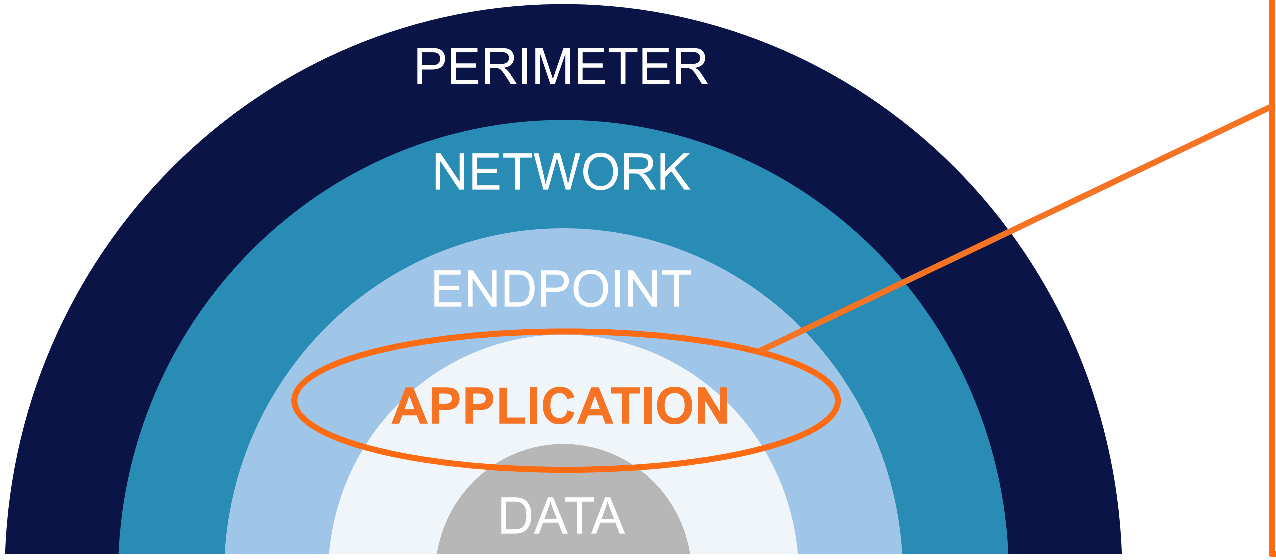
CVE	Vendor/Project	Product	Vulnerability Name	Date Added to Catalog	Short Description	Action	Due Date	Notes
CVE-2021-38163	SAP	NetWeaver	SAP NetWeaver Unrestricted File Upload vulnerability	2022-06-09	SAP NetWeaver contains a vulnerability that allows unrestricted file upload.	Apply updates per vendor instructions.	2022-06-30	
CVE-2016-2386	SAP	NetWeaver	SAP NetWeaver SQL Injection Vulnerability	2022-06-09	SQL injection vulnerability in the UDDI server in SAP NetWeaver J2EE Engine 7.40 allows remote attackers to execute arbitrary SQL commands via unspecified vectors.	Apply updates per vendor instructions.	2022-06-30	
CVE-2016-2388	SAP	NetWeaver	SAP NetWeaver Information Disclorsure Vulnerability	2022-06-09	The Universal Worklist Configuration in SAP NetWeaver AS JAVA 7.4 allows remote attackers to obtain sensitive user information via a crafted HTTP request.	Apply updates per vendor instructions.	2022-06-30	

Actions to Take Now

- Ensure none of the vulnerabilities highlighted in the Catalog of Known Exploited Vulnerabilities are present in your landscape
- This is critically important for Internet-Facing SAP Systems
- Start with the latest added to the Catalog
    - **CVE-2021-38163 - SAP Security Note 3084487** - Unrestricted File Upload vulnerability in SAP NetWeaver (Visual Composer 7.0 RT). This vulnerability has a CVSS Base Score of 9.9 and allows an attacker to upload a webshell on the target SAP System.
    - **CVE-2016-2386 - SAP Security Note 2101079** - SAP Netweaver Application Server Java UDDI SQLI. This has a CVSS Base Score of 9.8 and allows an attacker to execute arbitrary commands on the database
    - **CVE-2016-2388 - SAP Security Note 2256846** - SAP Netweaver AS JAVA Information Disclosure. This has a CVSS Base Score: 5.3 and allows an attacker to list valid users of the system
- Remember these are just a few of the vulnerabilities and risks that could be affecting SAP Applications

WHY AREN'T TYPICAL SECURITY EFFORTS EFFECTIVE HERE?

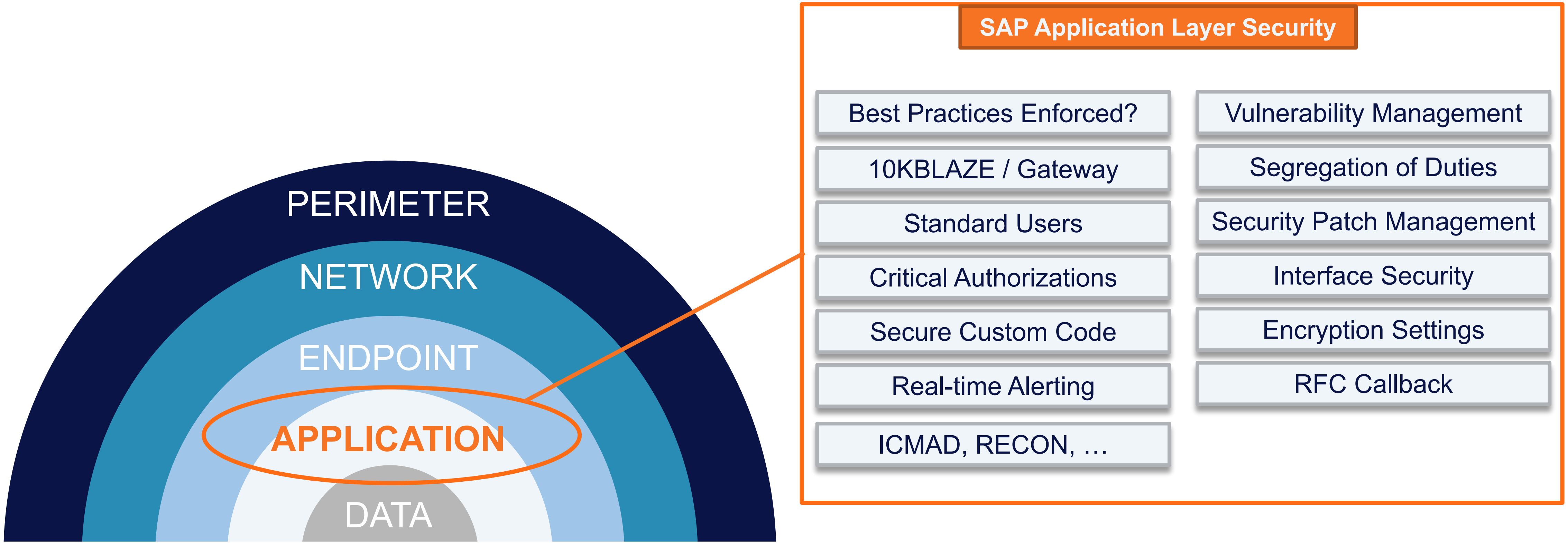
Defense-in-Depth Models Surround but Ultimately Neglect That Critical Application Layer.



- **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

WHY AREN’T TYPICAL SECURITY EFFORTS EFFECTIVE HERE?

Defense-in-Depth Models Surround but Ultimately Neglect That Critical Application Layer.



SAP Application Layer Security

- Best Practices Enforced?
- 10KBLAZE / Gateway
- Standard Users
- Critical Authorizations
- Secure Custom Code
- Real-time Alerting
- ICMAD, RECON, …
- Vulnerability Management
- Segregation of Duties
- Security Patch Management
- Interface Security
- Encryption Settings
- RFC Callback

What holes do organizations have in their 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

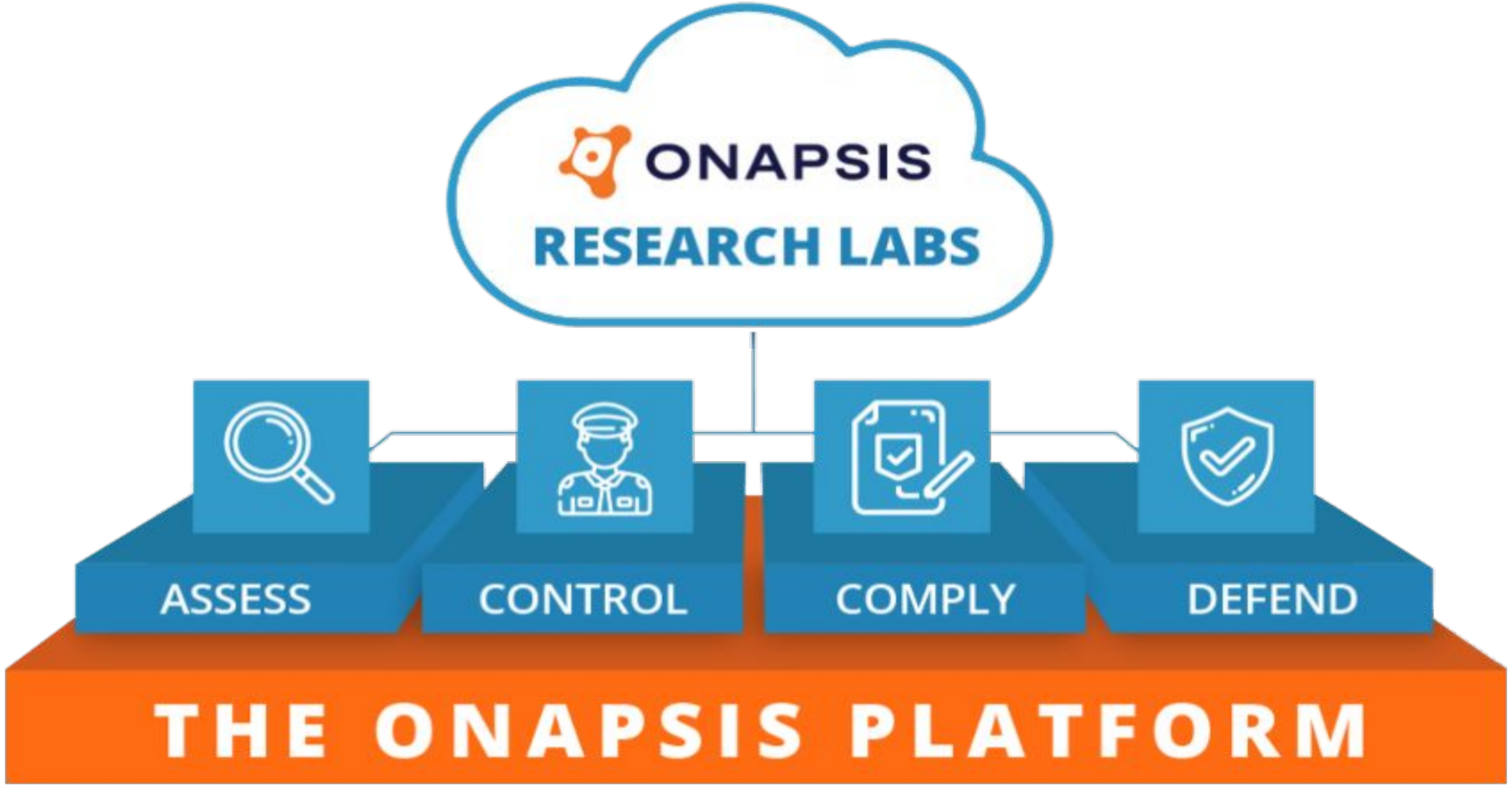
7.3% Average decrease in stock price following a security breach[7]

[1] Centrify
[2] DarkReading
[3] Fortinet
[4] Onapsis

[5] Ascent
[6] TechRepublic
[7] Forbes

Support from The Onapsis Platform

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



ONAPSIS

RESEARCH LABS

ASSESS

CONTROL

COMPLY

DEFEND

THE ONAPSIS PLATFORM

“Prior to using Onapsis, 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.” - *F100 Biotech*

“Saves time identifying, prioritizing, and remediating security vulnerabilities. **Enables security generalists** to ensure Basis is properly maintaining SAP systems.” – *F100 Tech Manufacturer*

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

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

MANAGEMENT FUNCTIONALITY

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

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.