



# Get Proactive! Secure Your SAP Applications from Ransomware

David D'Aprile | Vice President, Product Marketing  
8 November 2021





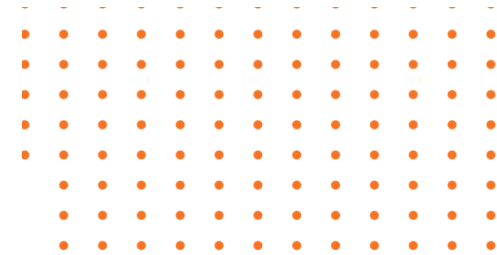
## Meet Our Presenter



### David D'Aprile

Vice President, Product Marketing

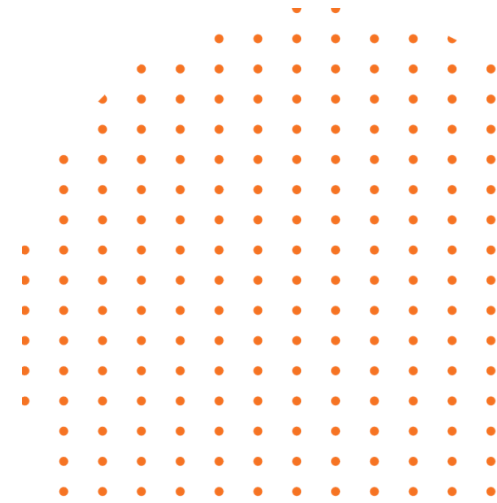
- 20 years experience in new product development, strategic alliances, marketing
- Owns global product marketing vision and strategy at Onapsis.
- Formerly, leadership roles at Cogito AI, Dell EMC, RSA, Cisco





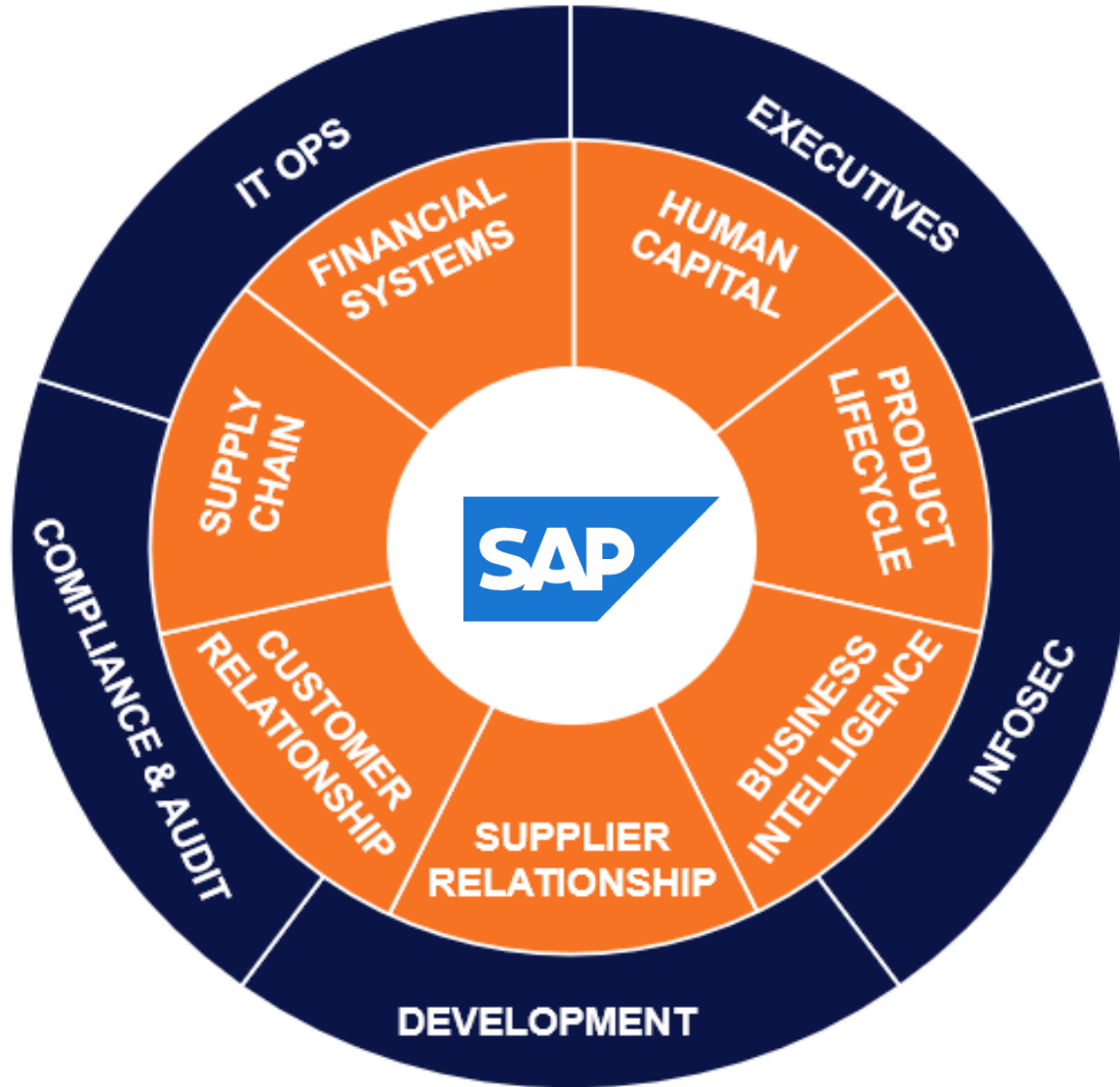
01.

# The **Perfect Storm** Putting Business-Critical SAP Applications at Risk





# SAP Applications Power Your Org...and The Global Economy



**92%** of the Global 2000 use SAP

**87%** of the world's revenue touches these systems

**94%** of the world's 500 largest companies use SAP



# But We've Seen Many Changes Over the Past Couple of Years

## Aggressive Technology Modernization

- Increased cloud adoption is **evaporating the perimeter**
- Accelerated digital transformation projects **favor expediency not security**

## Interconnected Risk Means Greater Exposure

- **Increasing interconnectivity** between on-prem and cloud environments, between internal and third-party systems
- More access from third parties (e.g., partners, contractors, SIs)

## More External Pressure for Enterprises

- **Greater regulation** (and regulation enforcement) around data privacy and protection
- Increasing frequency and costs of data breach



# “Cloudy” ...With A Chance of Compromised Security

## CFOs to defer capex spending but invest in digital transformation

Facilities/general capital expenditures



Operations



Workforce



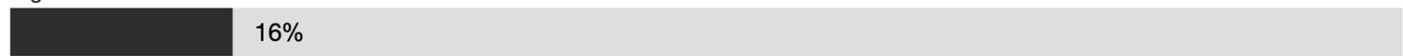
IT



R&D



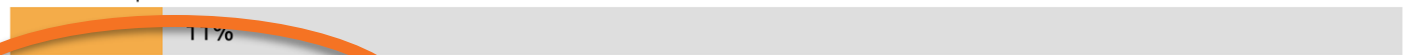
Digital transformation



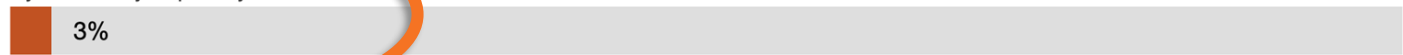
Environmental, social and governance activities



Customer experience



Cybersecurity or privacy



Q: You mentioned your company is considering deferring or cancelling planned investments as a result of COVID-19. Which of the following investment types are being considered in that regard? Source: PwC COVID-19 CFO Pulse Survey May 4, 2020

Cloud spending **rose 37%** in Q1 2020 alone.

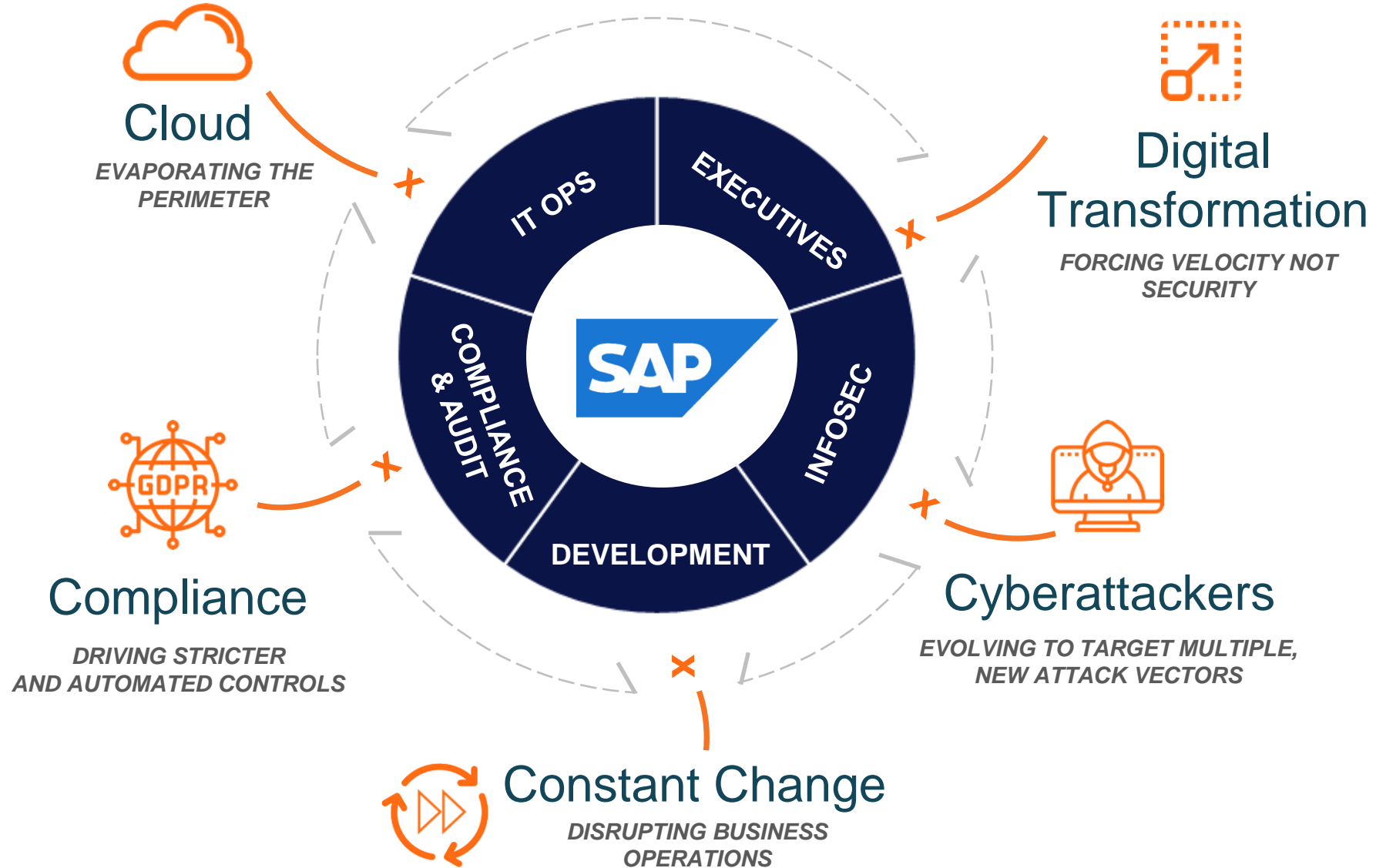
Cloud accounted for **20% growth in 2020**, compared to IT spend dropping by 8% overall.

**Security has taken a back seat to expediency.**

Rapid cloud deployments from the past couple years may cause future headaches...



# Ultimately, Enterprises Face a Perfect Storm of Complexity





# And Now...Add the Threat of Ransomware in the Mix

The Washington Post  
Democracy Dies in Darkness

Get one year for \$40 Sign

PowerPost • Analysis

## The Cybersecurity 202: Ransomware is wreaking havoc on U.S. cities

By Joseph Marks  
Anchor of The Cybersecurity 202 newsletter

September 7, 2021 at 7:05 a.m. EDT

with Aaron Schaffer

When hackers struck Collierville, Tenn. with a ransomware attack in 2019, the city's IT staff worked around the clock to recover.

WIRED  
BACKCHANNEL BUSINESS CULTURE GEAR IDEAS MORE SIGN IN SUBSCRIBE

LILY HAY NEWMAN SECURITY 06.05.2021 09:00 AM

## Security News This Week: FBI Head Compares Ransomware Threat to 9/11

Plus a Supreme Court decision on a controversial anti-hacking law, a WhatsApp CEO's top security news.

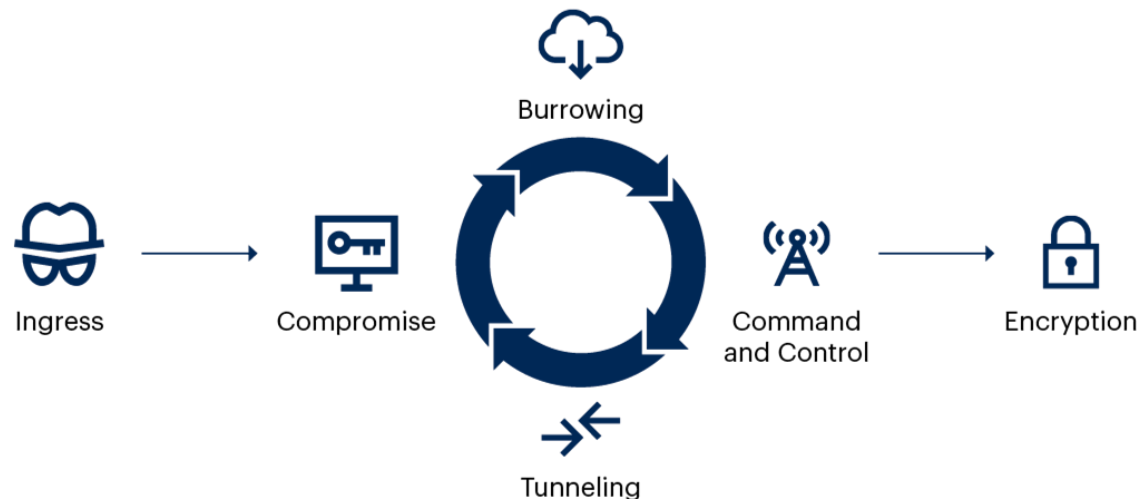
The New York Times

## *Hundreds of Businesses, From Sweden to U.S., Affected by Cyberattack*

In Sweden, a grocery chain temporarily closed its doors after the attack. Some companies have been asked for \$5 million in ransom.



# So, Let's Level-Set Here...What *IS* Ransomware?



Ransomware is a type of **malware** that prevents you from accessing your files, systems, or networks until a **ransom** is paid.

## How Does It Work?

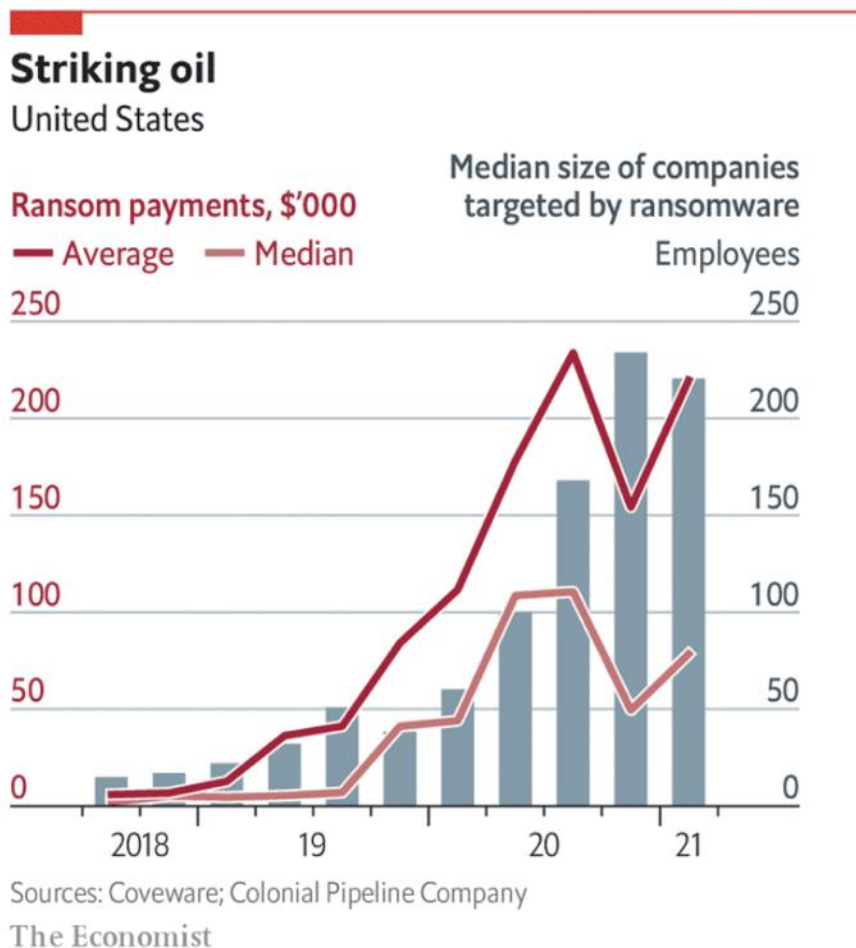
Ransomware identifies the drives on an infected system and encrypts the files within each drive. Once encrypted, it displays instructions on how to pay a ransom. When paid, the threat actor usually provides a key to unlock the files.

## What Are The Most Common Attack Vectors?

Phishing for valid credentials and exploiting software vulnerabilities.



# Sadly, The Ransomware Threat Will Only Get Worse...



- **More, More, More** - Threat actors are targeting larger organizations, demanding bigger payouts
- **Powerful Market Dynamics** – It's lucrative! The more people pay, the more this continues.
- **It's Evolving!** - Guess who else can pay? Your clients! Welcome to the new world of extortionware. (e.g., the Vaastamo cyberattack in Finland)



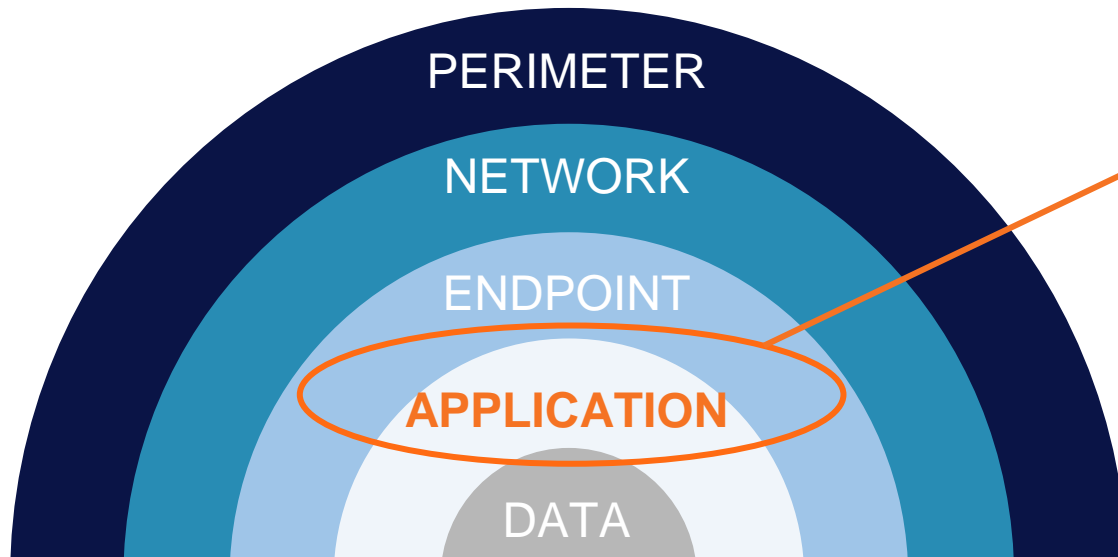
# How Do You Think Enterprises Commonly Respond?

**The Challenge:** When people hear “ransomware”, they think of endpoints, cyber education, network detection tools, and backups. And “how did this happen to us?”





# Why? Defense-in-Depth Models Surround But Frequently Neglect the 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

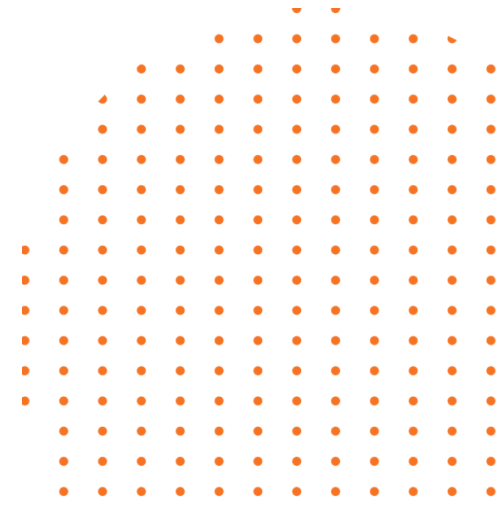
**Gartner**<sup>®</sup>

*“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.”*



# 02.

## **Onapsis Research Labs: Threat Actors Are Actively Targeting Business-Critical SAP Applications**



# Threats to Business-Critical Systems Are On the Rise...

**64%** of ERP systems have been **breached** in the past 2 years



**5** **US-CERT alerts** on malicious cybersecurity or vulnerabilities in **SAP over the past 5 years**



*“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.**”*

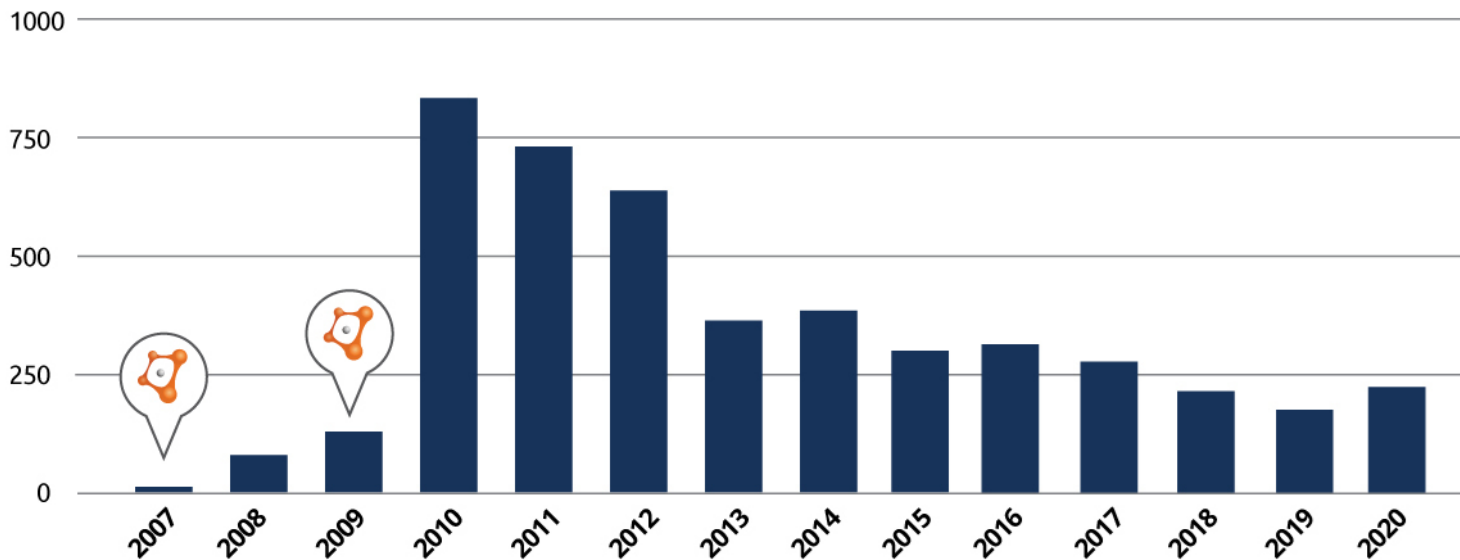




# Onapsis Research Labs: A Rich History of SAP Threat Expertise

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

SAP SECURITY NOTES



Onapsis founded

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

Onapsis & 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**

OOTB compliance policies for Onapsis, plus customization

Database of

**350+**

test cases for security and compliance issues in SAP code and transports

# The Onapsis Threat Intelligence Cloud Captures In-the-Wild Intel on Critical Attacks

*Synthetic targets, Real attacks from real threat actors.*

*Real threat intel and data for our clients.*

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)



# The Result? A Threat Intelligence Report Jointly Issued with SAP

Active Cyberattacks on Business-Critical SAP Applications

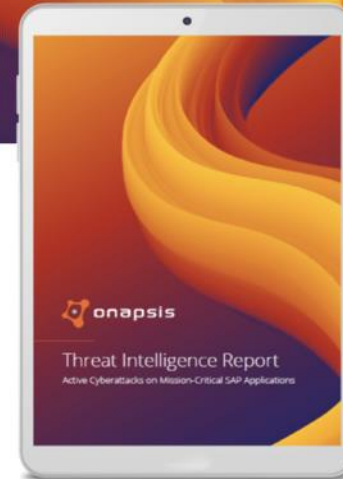
SAP Endorsed App  
Premium Certified

SAP and Onapsis partner to release new threat intelligence on active threats

## Defend your Business-Critical SAP Applications from Active Threats

On April 6, Onapsis and SAP released a new threat intelligence report to help SAP customers protect from active cyber threats seeking to specifically target, identify and compromise organizations running unprotected SAP applications, through a variety of cyberattack vectors. **SAP and Onapsis strongly advise organizations to take immediate action** including swift application of the relevant SAP security patches and a thorough review of security configurations of their SAP landscapes, as well as performing a compromise assessment and forensic investigation of at-risk environments.

The [U.S. Department of Homeland Security's CISA](#) and Germany's Federal Office for





# ...With Very Compelling Observed Results

**400+**

CONFIRMED  
EXPLOITATIONS

**107+**

HANDS-ON  
ATTACKS

**18**

UNIQUE  
COUNTRIES

\* may include VPS / TOR

**Active, Sophisticated Attacks** in the Wild...Often Using Known Exploits

**<72hrs**

SAP PATCH RELEASE  
TO EXPLOITATION

**<3hrs**

NEW SYSTEM ONLINE  
TO BEING EXPLOITED

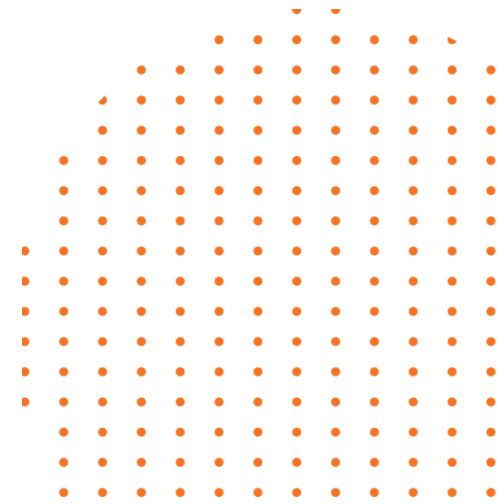
**An Increasingly Shrinking Window  
for Defense**

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.



# 03.

## What Organizations Can Do About This to Protect Their Business-Critical Applications





# The Status Quo Is a Recipe for Disaster



SAP and Other ERP Systems Are Critical Centerpieces...and Vulnerable to Attack

---

A Perfect Storm of Complexity

---

Threat Actors Are Actively Targeting Unpatched, Misconfigured Applications



# Which Means We Have Some Big Challenges



- Certain exploits have been known to give access directly to the operating system and are **easily exploitable without authentication.**

---
- Even with proper backups, **ransomware will create an outage with immeasurable costs** to the organization.

---
- Ongoing digital transformation **increases the number of potential entry points** for attackers exponentially. After a network has been breached, infections can spread more quickly when critical systems are connected.



# So We Need to Shift Our Attention to the Left...

**Goal:** Focus organizations on *proactive* measures they can take to directly secure the “crown jewels”.





# Stay Ahead of Ransomware. Get Back to Basics.

- 1 Security Hardening of Business-Critical Systems
- 2 Timely Patch Management
- 3 Point-in-Time Vulnerability Assessments
- 4 Continuous Monitoring of Vulnerabilities and Threats
- 5 Securing Your Custom Enterprise Code
- 6 Renewed Commitment to Control and Governance



# You're Not Alone. Onapsis Is Here to Help.

 **SAP** Endorsed App  
Premium Certified

 **ORACLE** Gold Partner



“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*





## In Conclusion...



- › Expediency over Security, Added Complexity, and Lacking Security at the Application Layer Puts Critical SAP Applications at High Risk
- › Bringing Business-Critical SAP Applications into Vulnerability Management Programs Is a Great First Step.
- › Even Better: Build Security Earlier into Your Custom Code Development with Automated SAP Application Security Testing.



*Implement a **risk-based vulnerability management** process that includes threat intelligence...*

***This should be a continuous process.***

*The risk associated with vulnerabilities **changes** as vulnerabilities are exploited by attackers.*

**Gartner**<sup>®</sup>





# Where to Find More Information

**Active Cyberattacks on Business-Critical SAP Applications**

**SAP and Onapsis partner to release new threat intelligence on active threats**

**Defend your Business-Critical SAP Applications from Active Threats**

On April 6, Onapsis and SAP released a new threat intelligence report to help SAP customers protect from active cyber threats seeking to specifically target, identify and compromise organizations running unprotected SAP applications, through a variety of cyberattack vectors. **SAP and Onapsis strongly advise organizations to take immediate action** including swift application of the relevant SAP security patches and a thorough review of security configurations of their SAP landscapes, as well as performing a compromise assessment and forensic investigation of at-risk environments.

The U.S. Department of Homeland Security's CISA and Germany's Federal Office for

**SAP Endorsed App**  
Premium Certified

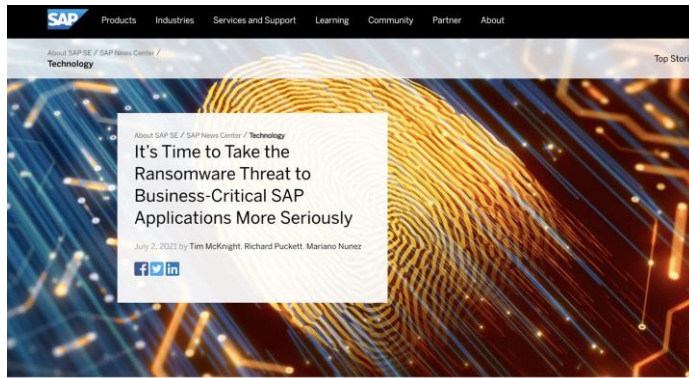


## SAP-Onapsis Joint Threat Intelligence Report

**It's Time to Take the Ransomware Threat to Business-Critical SAP Applications More Seriously**

July 2, 2023 by Tom McKnight, Richard Puckett, Mariano Nunez

Almost every day, we see yet another case of ransomware. While historically, companies of all sizes are targeted, recently it appears




## SAP-Onapsis Joint Blogpost on Ransomware

**GRC Tuesdays: Security and IT Risk Mitigation With Pre-Configured Automated Controls**

June 29, 2023 7 minute read

6 Likes 833 Views 0 Comments



A few months ago, I released a blog titled GRC Tuesdays: Integrating Cybersecurity and

## SAP Process Control + Onapsis Comply Integration

All Accessible from [Onapsis.com](https://www.onapsis.com)

THANK  
YOU

@onapsis

[linkedin.com/company/onapsis](https://www.linkedin.com/company/onapsis)

[www.onapsis.com](https://www.onapsis.com)

