VNSG

VERBINDT. VERSTERKT.

FOCUS ONLINE

8 T/M 12 NOVEMBER 2021

Welkom

How to mitigate the Risk of Ransomware

Jonathan Cooper, Senior Sales Engineer – Onapsis

ONAPSIS

Agenda

SAP® Endorsed App
Premium Certified

Ransomware Challenges

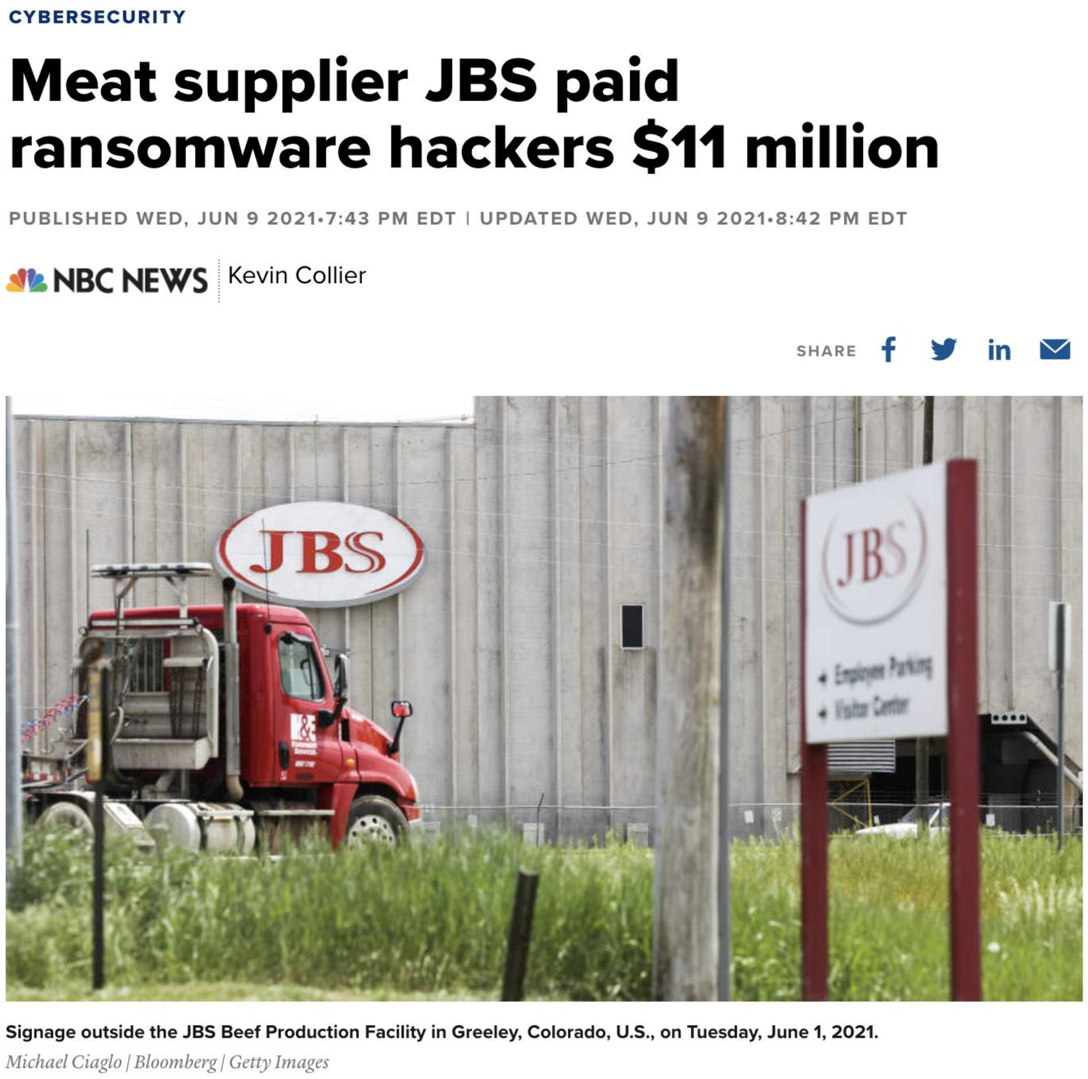
Recent Attacks

Why Onapsis

Demo

Key Takeaways

Ripped from the Headlines...



CYBERSECURITY

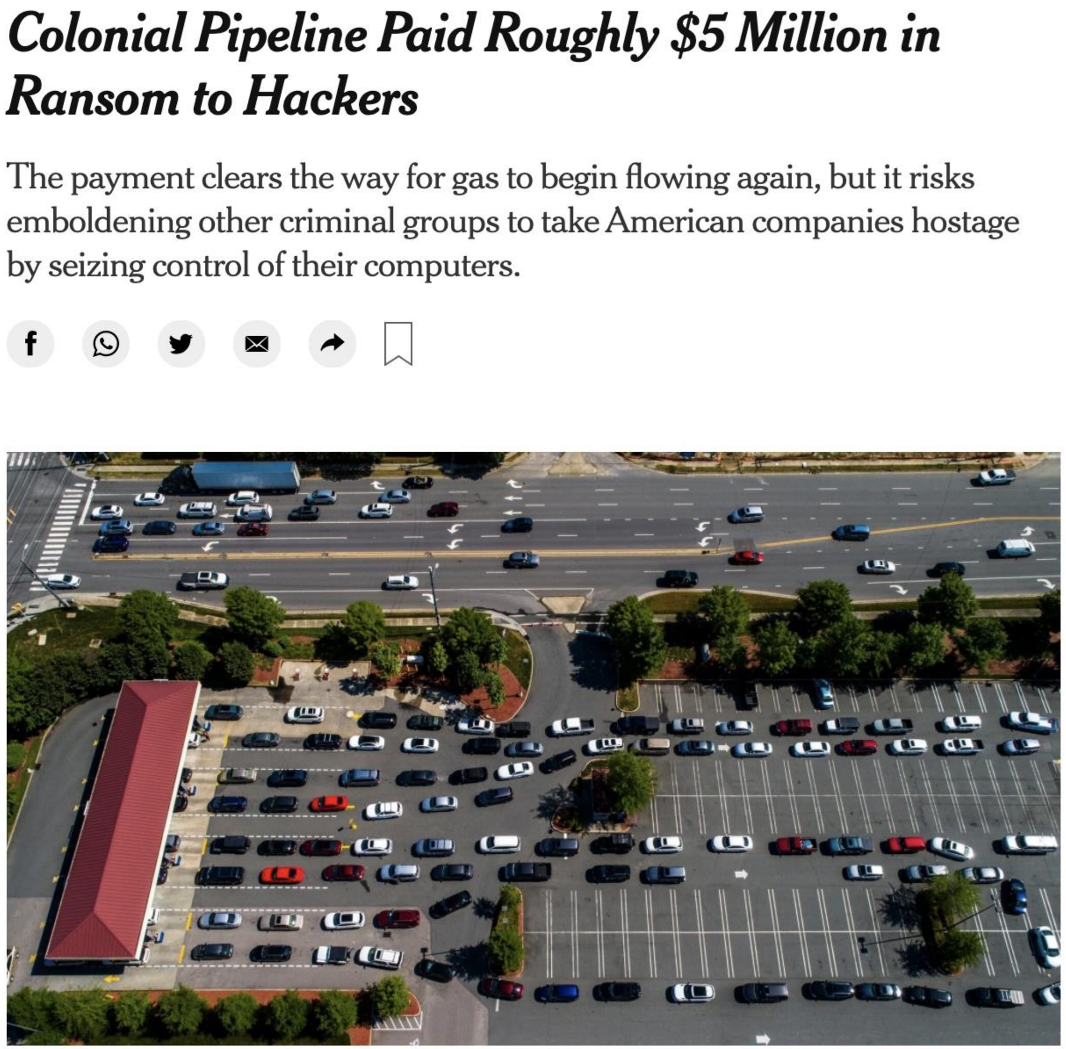
Meat supplier JBS paid ransomware hackers $11 million

PUBLISHED WED, JUN 9 2021•7:43 PM EDT | UPDATED WED, JUN 9 2021•8:42 PM EDT

NBC NEWS | Kevin Collier

Signage outside the JBS Beef Production Facility in Greeley, Colorado, U.S., on Tuesday, June 1, 2021.

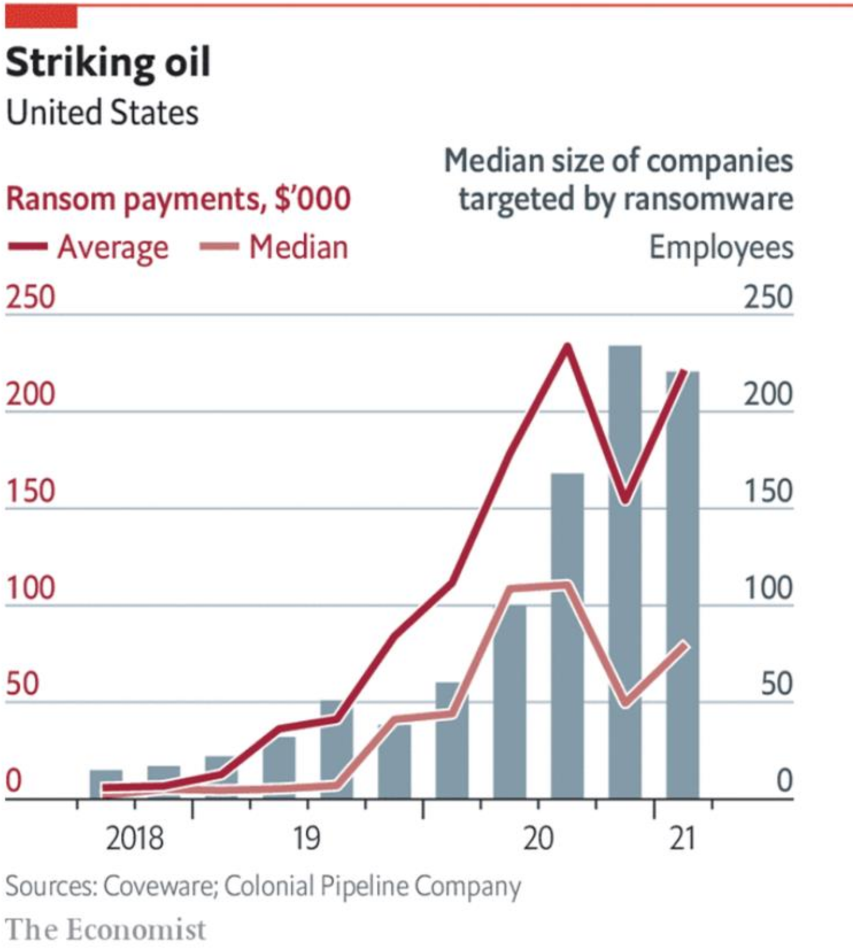
Michael Ciaglo | Bloomberg | Getty Images



Colonial Pipeline Paid Roughly $5 Million in Ransom to Hackers

The payment clears the way for gas to begin flowing again, but it risks emboldening other criminal groups to take American companies hostage by seizing control of their computers.

It’s Only Going to Get Worse...



More, More, More - Threat actor groups are targeting larger organizations and demanding bigger payouts

Powerful Market Dynamics - Ransomware is becoming very lucrative as people pay to get control over their data again. The more people are willing to pay ransoms, the more this continues.

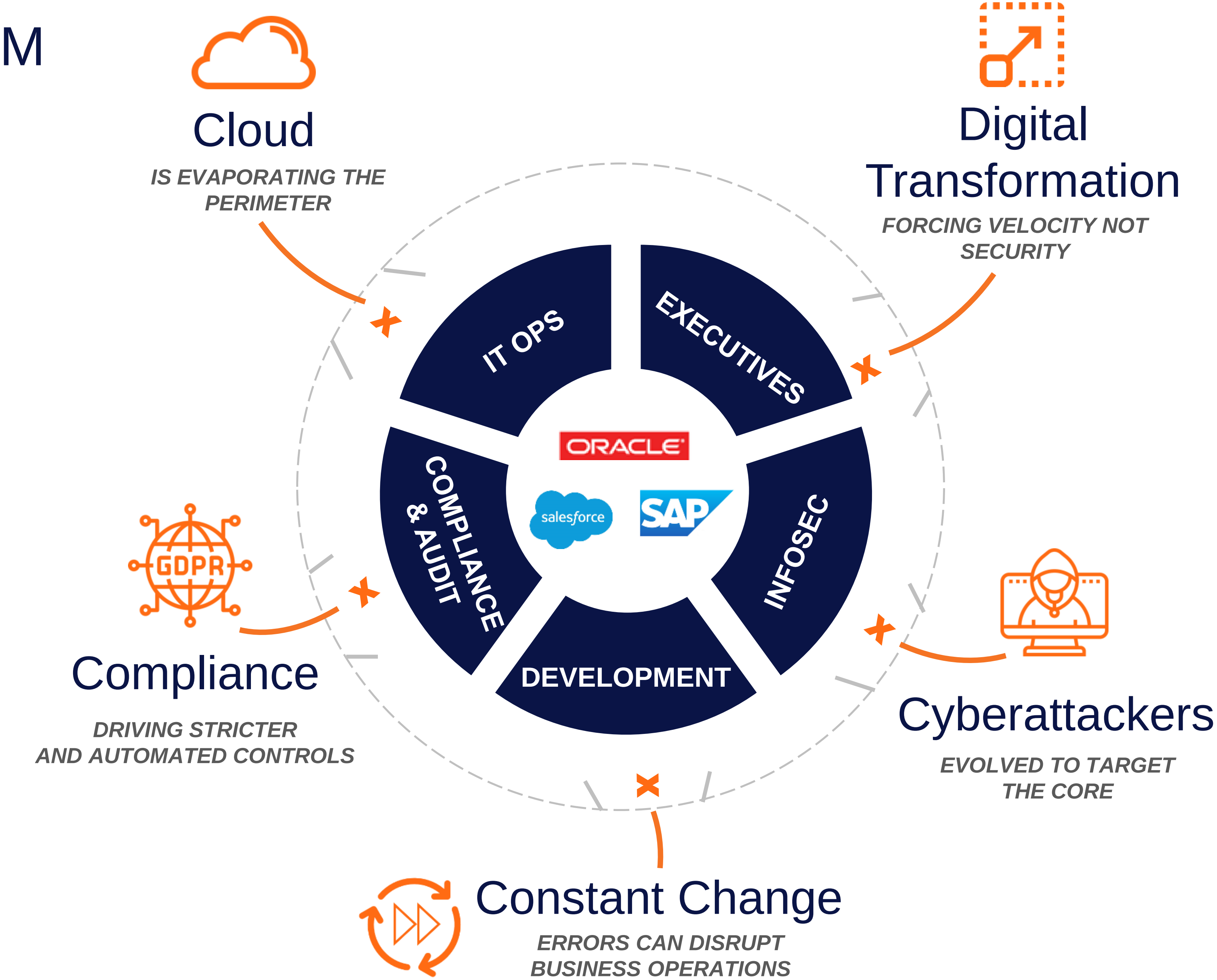
Environment’s Not Helping - The pandemic led to more WFH and accelerated companies’ digital transformation plans. It’s not easy managing and securing remote employees and data.

It’s Evolving! - Guess who else can pay? Organizations’ customers, executives, etc. Welcome to the new world of extortionware.

(e.g., Vaastamo cyberattack)

A PERFECT STORM

New Industry Dynamics and Emerging Cyber Threats Are Threatening Your Mission-Critical Applications



Cloud

IS EVAPORATING THE PERIMETER

Digital Transformation

FORCING VELOCITY NOT SECURITY

Compliance

DRIVING STRICTER AND AUTOMATED CONTROLS

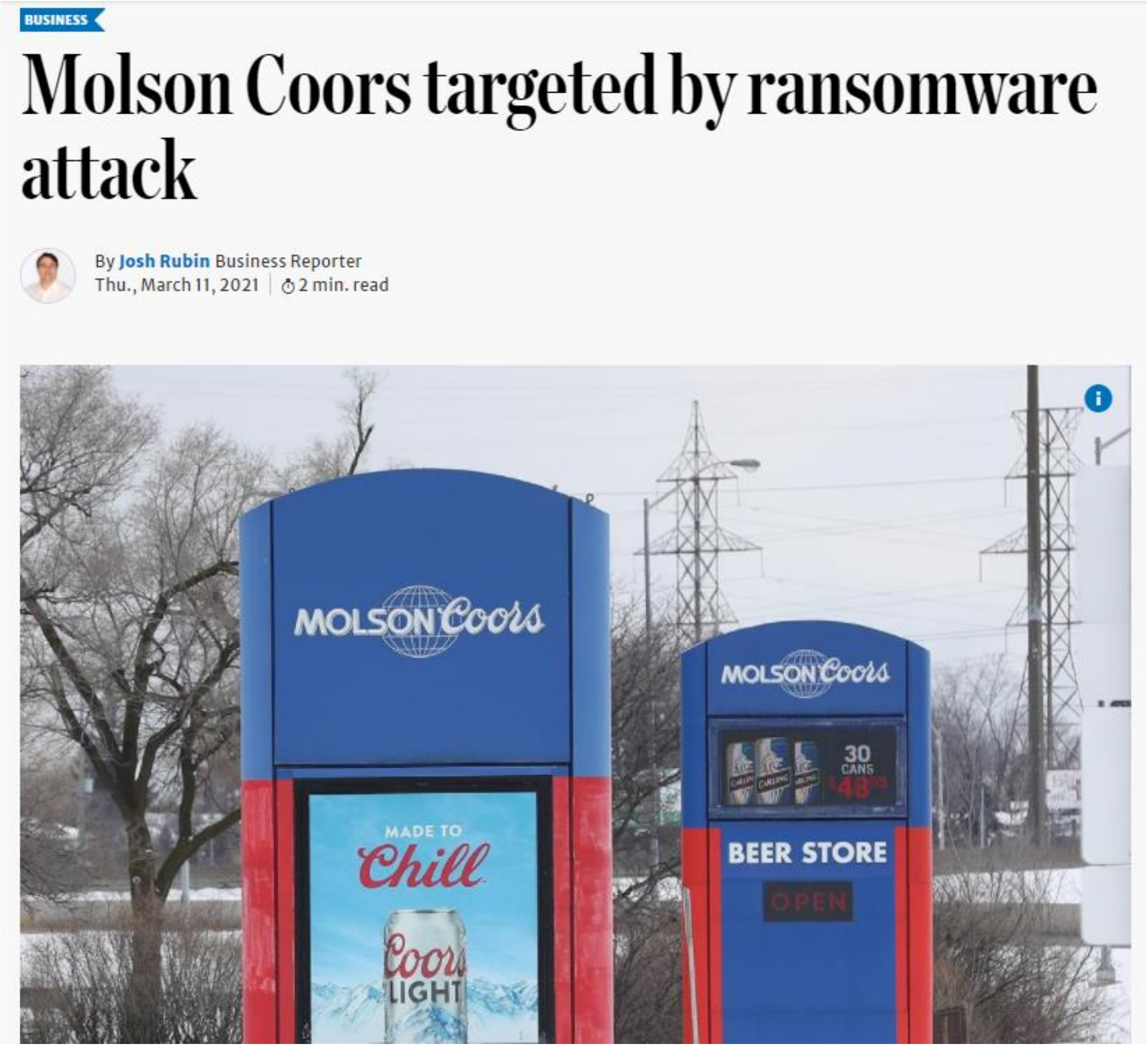
Cyberattackers

EVOLVED TO TARGET THE CORE

Constant Change

ERRORS CAN DISRUPT BUSINESS OPERATIONS

Let’s Walk Through a Recent Attack



BUSINESS

Molson Coors targeted by ransomware attack

By **Josh Rubin** Business Reporter
Thu., March 11, 2021 | 2 min. read

https://www.thestar.com/business/2021/03/11/molson-coors-targeted-by-ransomware-attack.html

- **March 11th, 2021:** Molson Coors Beverage Co. filed an 8-K report announcing brewery operations, production, and shipments **disruption due to cyberattack**.
- **March 11th, 2021:** Toronto Star newspaper “unofficially” reported it was a ransomware attack on business-critical software.
- **April 29th, 2021:** in the Q1 earnings call, the CEO shared more details about the business impact but no details about the attack - still an open investigation.

“It got into the software that makes all the different systems & hardware communicate with each other. They’re still able to do some things, but it’s running a lot slower.”
--Toronto Star Source, familiar with Molson Coors

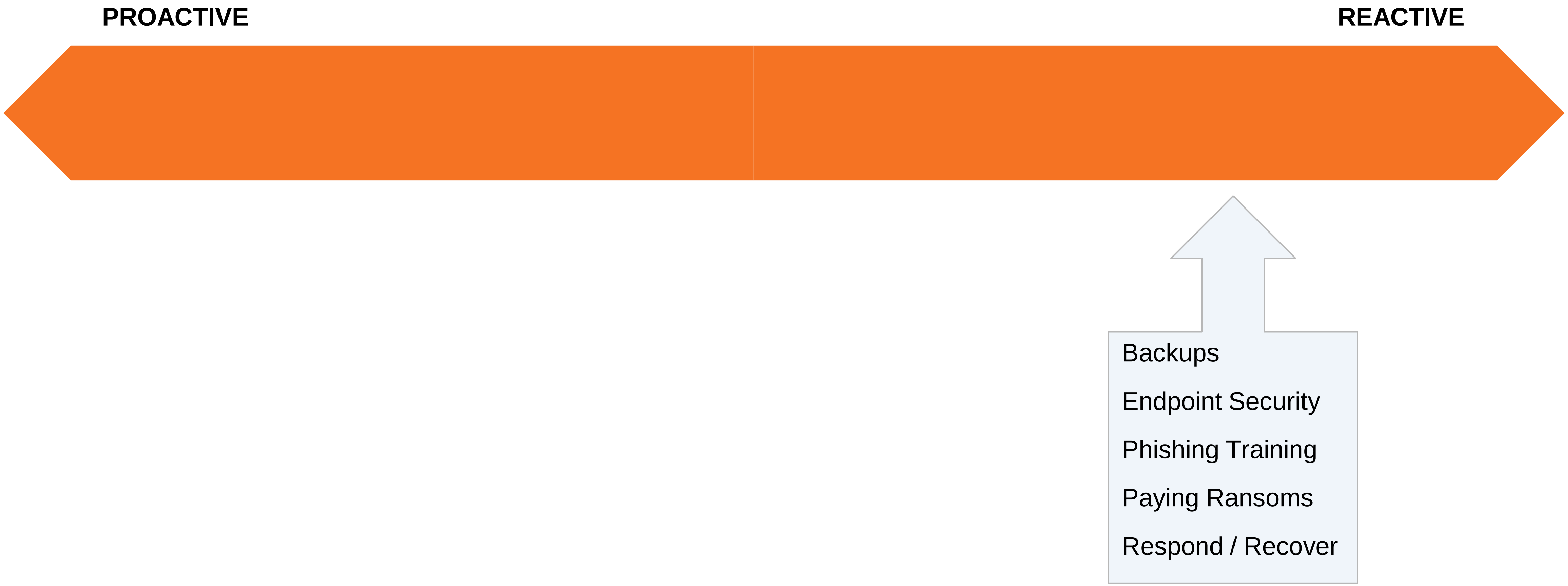
ONAPSIS - INTERNAL ONLY

The Impact from The Attack Was Widespread

- **Production Impact:**
  - *In* ***Q1 2021****, this F500 company was unable to produce and ship ~****1.8 and 2.0 million hectoliters*** *of product.*
  - *Production disruptions may mean increased run rates, production, work hours, etc., for the rest of the FY in order to achieve commits.*
- **Financial Impacts:**
  - *In* ***Q1 2021****, this F500 company had a shift between* ***$60M-70M of underlying EBITDA*** *(out of a total of $120M-140M) related to the cyber attack.*
  - *CyberSecurity Help: At least $2M being spent to conduct forensics and clean up the incident.*
  - *Ransom: Unknown if a ransom was paid on TOP of these other financial costs.*
- **Personnel Impacts:**
  - *Increased work hours for production-side employees*
  - *Increased work hours and decreased QoL/morale for Office of the CISO*

The Way Organizations Commonly Respond Isn’t Working...

Challenge: Commonly, people think of endpoints, cyber education, network detection tools, and backups when they hear the word “ransomware”. Lots of reacting...



Backups

Endpoint Security

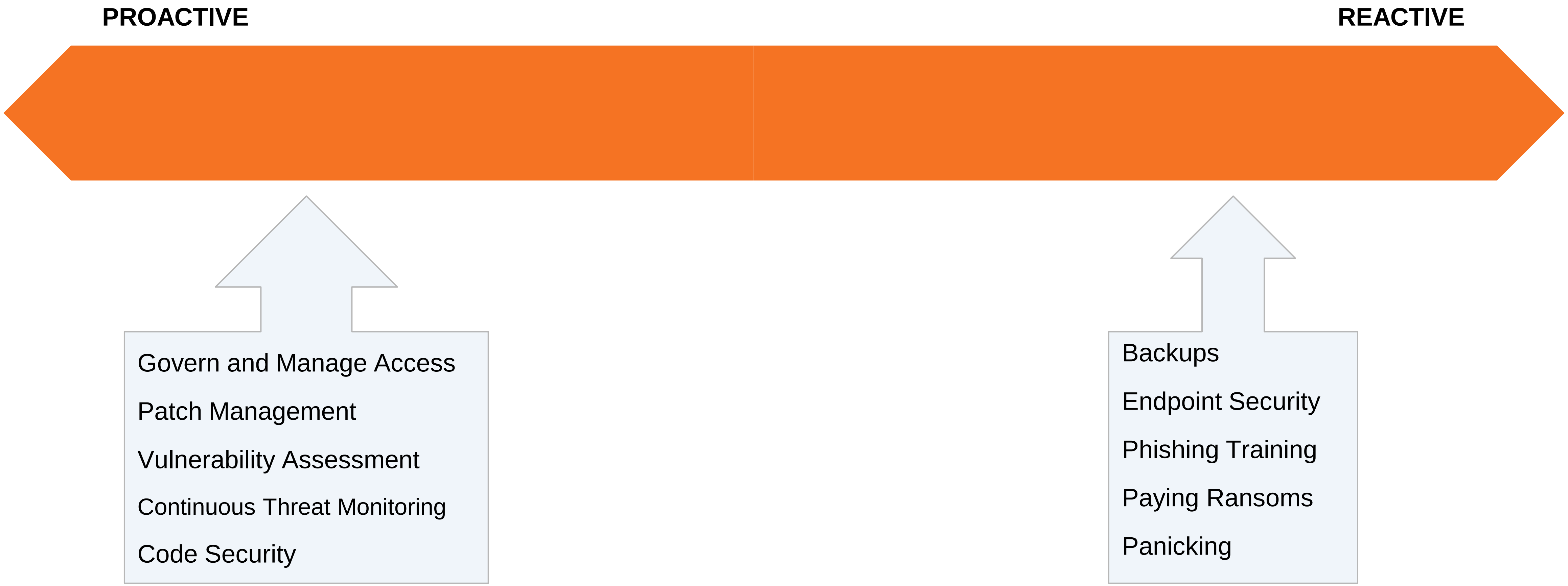
Phishing Training

Paying Ransoms

Respond / Recover

Where Do We Want Organizations Focusing?

Goal: Onapsis needs to help organizations focus on ***proactive*** measures to directly secure the "crown jewels". Onapsis needs to drive increased product awareness of how we can identify attack vectors and help mitigate disruptive attacks to business-critical applications.



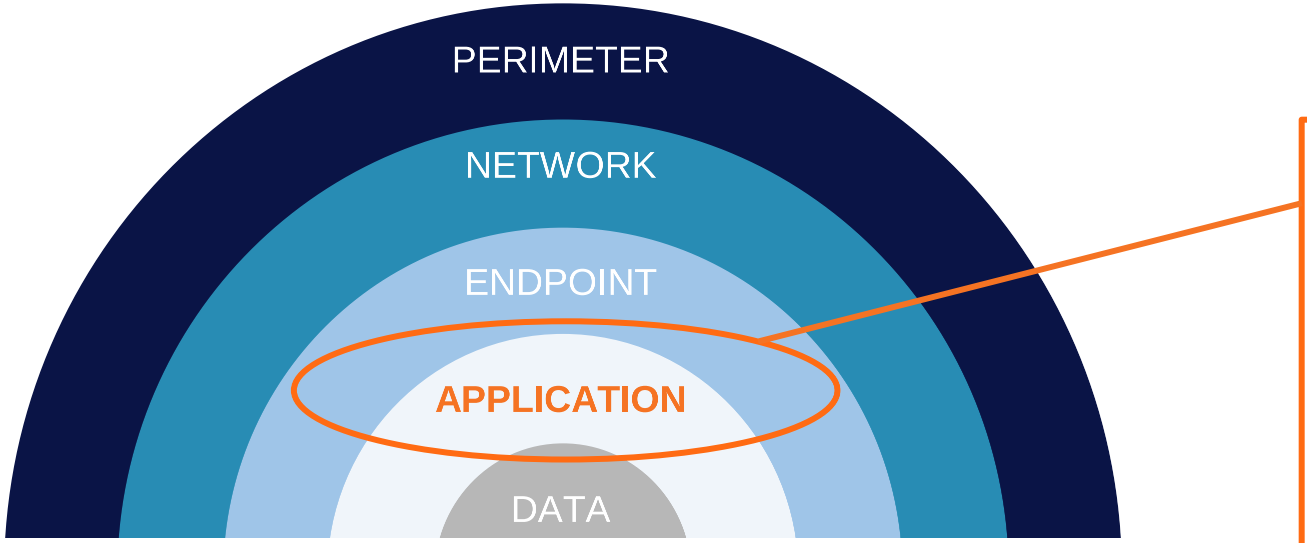
Ransomware for Mission Critical Applications

- Connected Applications Introduce More Weaknesses and Vulnerabilities.
- Getting Back to Basics Means Good Security Hygiene.
- Speed and Sophistication of attacks
- Surface area of attack has increased

“Implement a risk-based vulnerability management process that includes threat intelligence. ***Ransomware*** *often relies on unpatched systems to allow lateral movement.* ***This should be a continuous process. The risk associated with vulnerabilities changes as vulnerabilities are exploited by attackers.*** Gartner

Why Onapsis

"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." Gartner



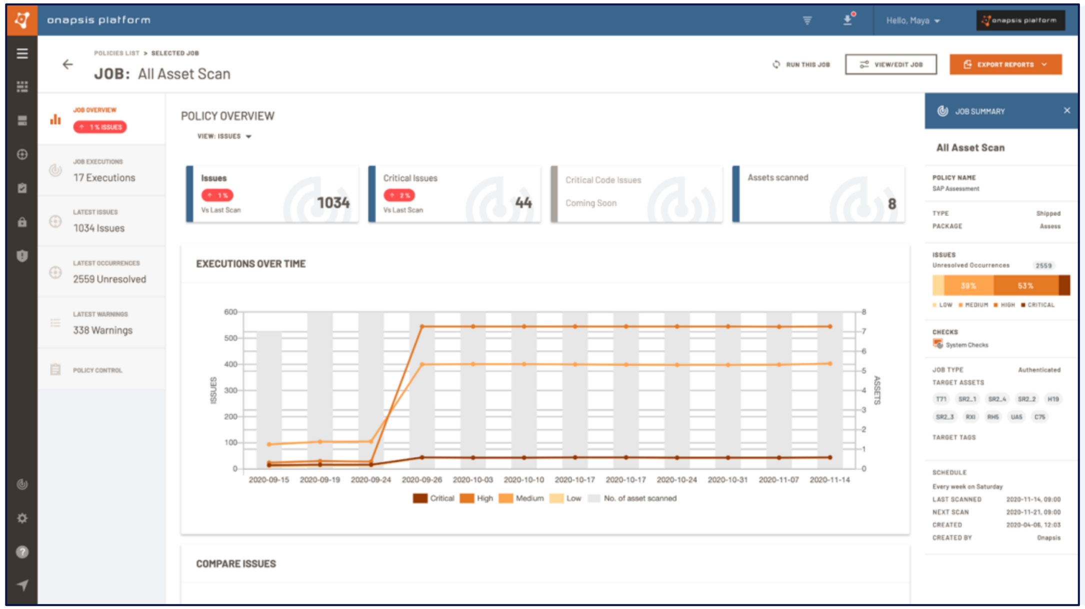
SAP Application Security

- Single Sign On, IDM, ID Access Governance/Service,
- Role Based Access Control, ABAC
- SolMan, Early Watch, Focused Run
- Code Vulnerability Analysis, Code Inspector, ATC
- SAP GRC AC, PC, RM, AM, BIS, UI Mask/Log, ETD

Traditional SAP controls can be bypassed by cyber attacks

Focused Vulnerability Management for Business-Critical SAP Applications

Powered by the Onapsis Research Labs research and insights, **Onapsis Assess** uniquely provides the specific SAP visibility and context both InfoSec and IT teams need to quickly act on vulnerabilities that ultimately pose the greatest risk to the business.



POLICIES LIST > SELECTED JOB

JOB: All Asset Scan

JOB OVERVIEW

↑ 1% ISSUES

JOB EXECUTIONS
17 Executions

LATEST ISSUES
1034 Issues

LATEST OCCURRENCES
2559 Unresolved

LATEST WARNINGS
338 Warnings

POLICY CONTROL

POLICY OVERVIEW

VIEW: ISSUES

Issues ↑ 1% Vs Last Scan 1034

Critical Issues ↑ 2% Vs Last Scan 44

Critical Code Issues Coming Soon

Assets scanned 8

EXECUTIONS OVER TIME

COMPARE ISSUES

JOB SUMMARY

All Asset Scan

POLICY NAME
SAP Assessment

TYPE Shipped
PACKAGE Assess

ISSUES
Unresolved Occurrences 2559

CHECKS
System Checks

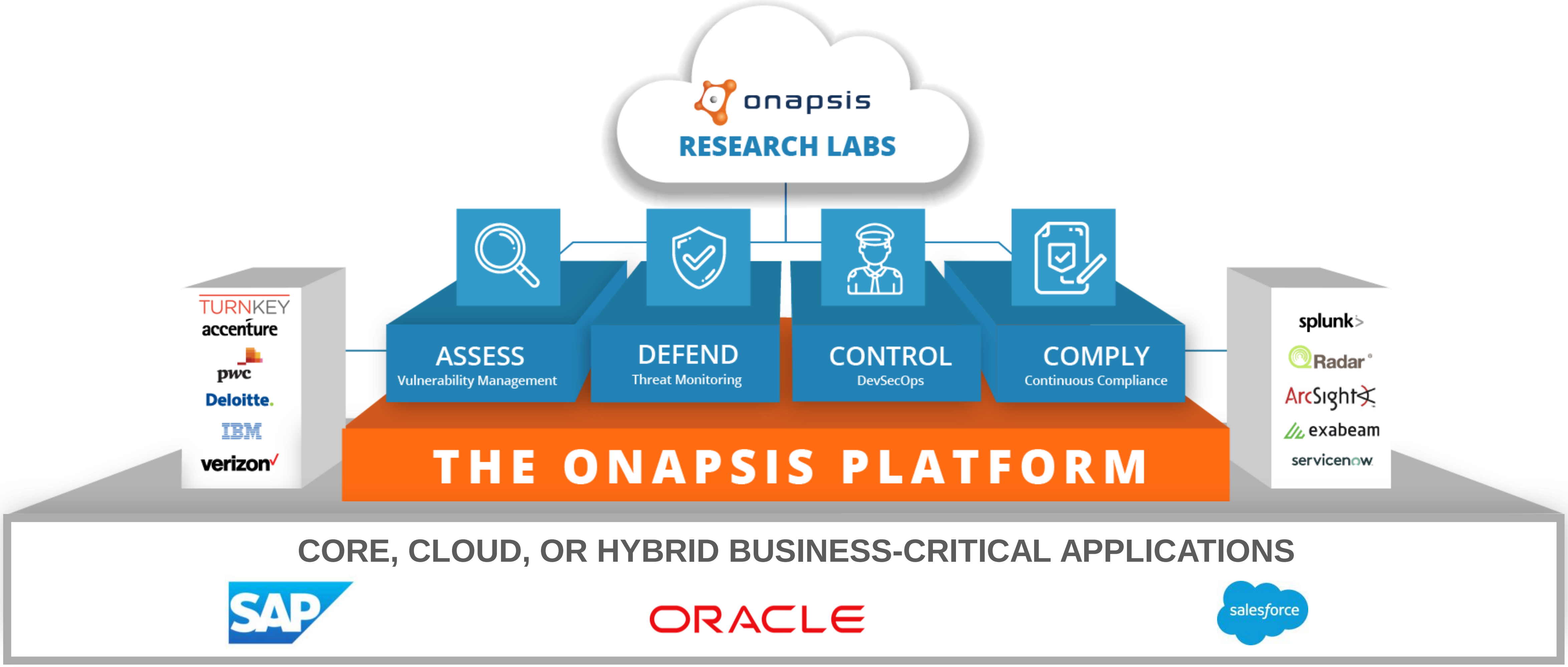
JOB TYPE Authenticated
TARGET ASSETS
T71 SR2_1 SR2_4 SR2_2 H19
SR2_3 RXI RH5 UA5 C75
TARGET TAGS

SCHEDULE
Every week on Saturday
LAST SCANNED 2020-11-14, 09:00
NEXT SCAN 2020-11-21, 09:00
CREATED 2020-04-06, 12:03
CREATED BY Onapsis

1. Provides Visibility of Critical Assets
2. Explains Risk and Context
3. Facilitates Remediation
4. Reports on Risk More Easily and Accurately

ONAPSIS BRINGS BUSINESS-CRITICAL APPLICATIONS INTO SCOPE

Unprecedented visibility into business-critical applications across your enterprise



Demonstration

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 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

MANAGEMENT FUNCTIONALITY

Reporting & Analysis

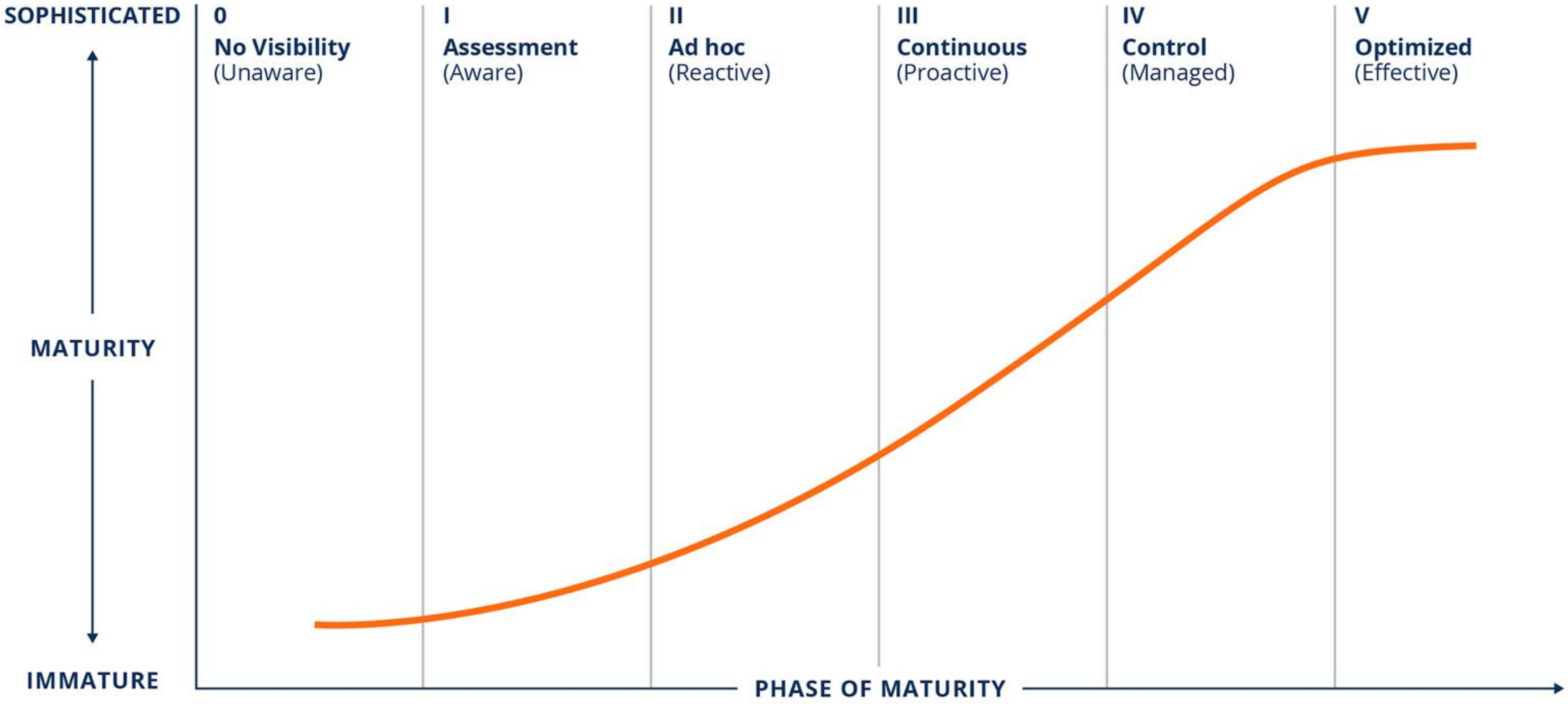
Ticketing/SOC Integration

Scheduling & Workflows

Asset Discovery

Users & Role Management

SAP CyberSecurity Maturity



ONAPSIS RESEARCH LABS

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

- 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

14
Out-of-the-box compliance policies, plus ability to customize

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

VNSG

VERBINDT. VERSTERKT.

FOCUS ONLINE

8 T/M 12 NOVEMBER 2021

Bedankt voor je deelname

Bekijk op www.VNSGFocusOnline.nl welke sessies er nog meer zijn!

Jonathan.cooper@onapsis
linkedin.com/company/onapsis

ONAPSIS