Benchmarking a Risk-Driven Approach to SAP Application Security

David D'Aprile | Vice President, Product Marketing
Onapsis

Anitha Meruga | Director, Information Security
HD Supply

Las Vegas

2024

SAPinsider

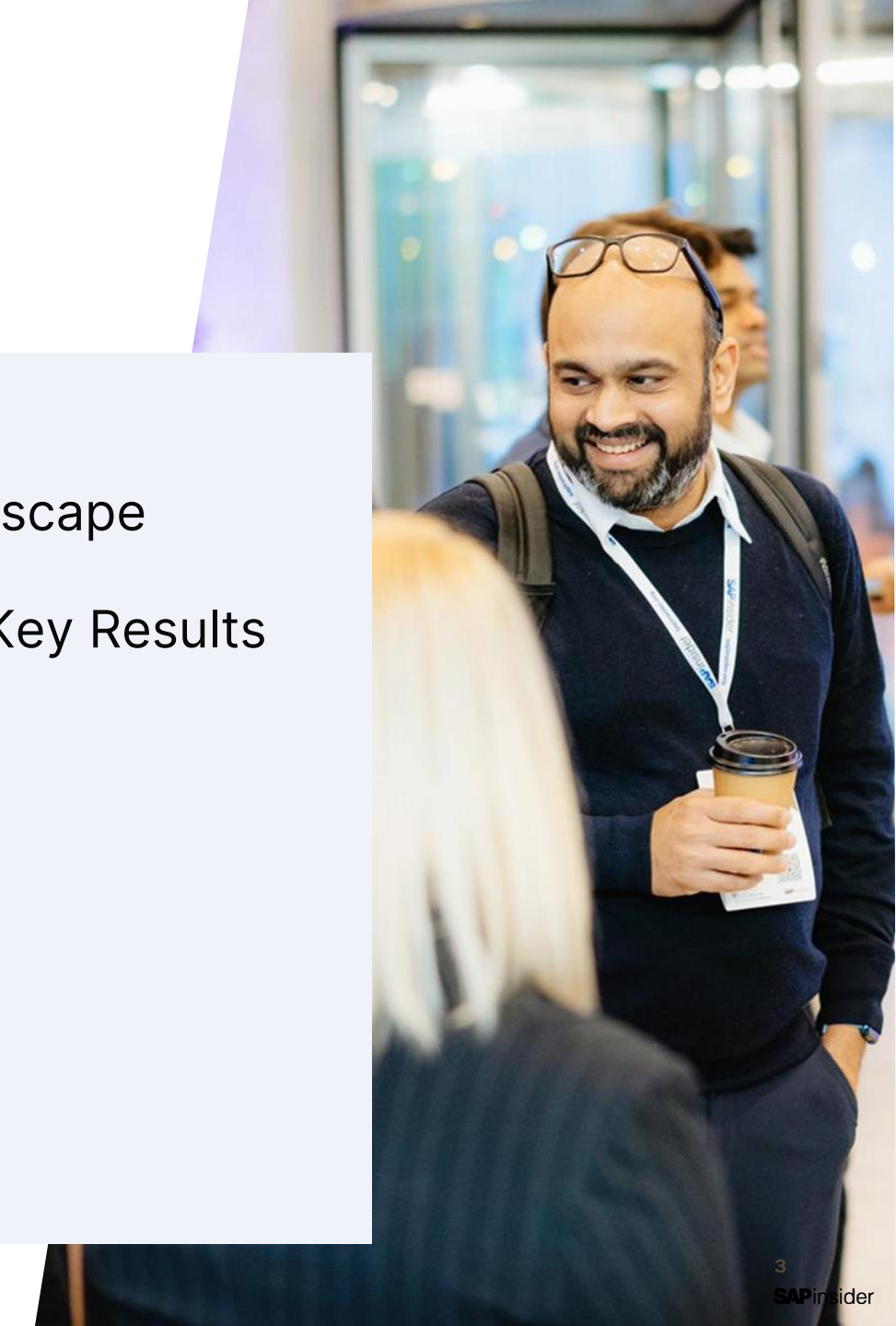
In This Session

SAP landscapes have exploded in scale and complexity. It's more challenging than ever before for organizations to understand where they should be focusing their security efforts for the best results.

Adoption of **a more risk-driven approach** to SAP security drives greater success. We'll take a closer look into how HD Supply Group is adopting this risk-driven approach to SAP security to better optimize how and where they focus their efforts for maximum impact.

What We'll Cover

- Challenges in Securing an SAP Landscape
- Partnering for Success and Driving Key Results
- Wrap Up



Securing A Complex SAP Landscape Isn't Easy

Huge Blindspots

into the attack surface of broad SAP landscapes

Targeted SAP Attacks

are on the rise, threatening your critical systems

Misaligned Teams

for InfoSec & SAP create larger security issues

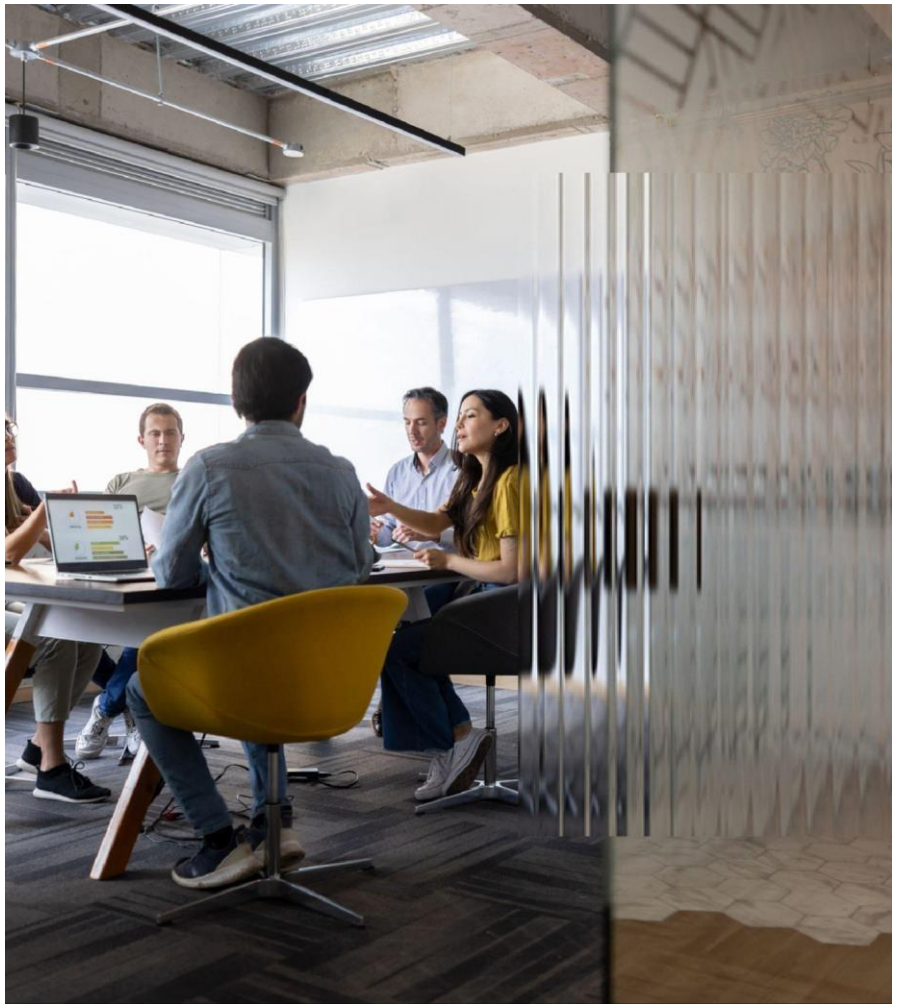
Compliance Obligations

are trickier and more cumbersome than ever before

If downtime for critical SAP Systems can be measured in minutes and dollars,
what is the cost to **YOUR** company if there's a **material incident, loss of integrity, or breach?**

Some of the Challenges My Team Faced

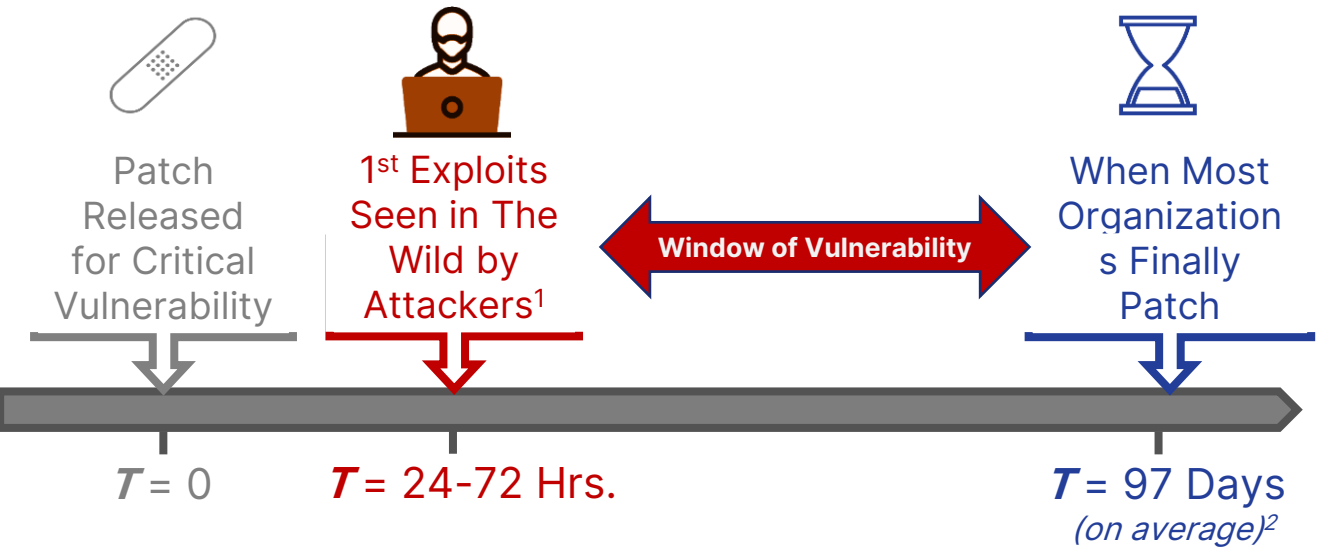
- Irregular **patch management** schedule
- Absence of **risk management** framework
- **Slower turnaround time** in patching our SAP systems
- **Huge backlog** of security patches to apply to our landscape
- **Absence of prioritization** on the remediation of the risks
- Absence of **robust alert management** for privileged accounts



Our Previous Status Quo Wasn't Good Enough Anymore

- Limited knowledge on the **risks present** in our landscape
- Absence of robust processes to **identify and contain risks**
- Adopting a **"reactionary" approach** to remediate the risks

The SAP Threat Landscape Isn't Getting Any Better...



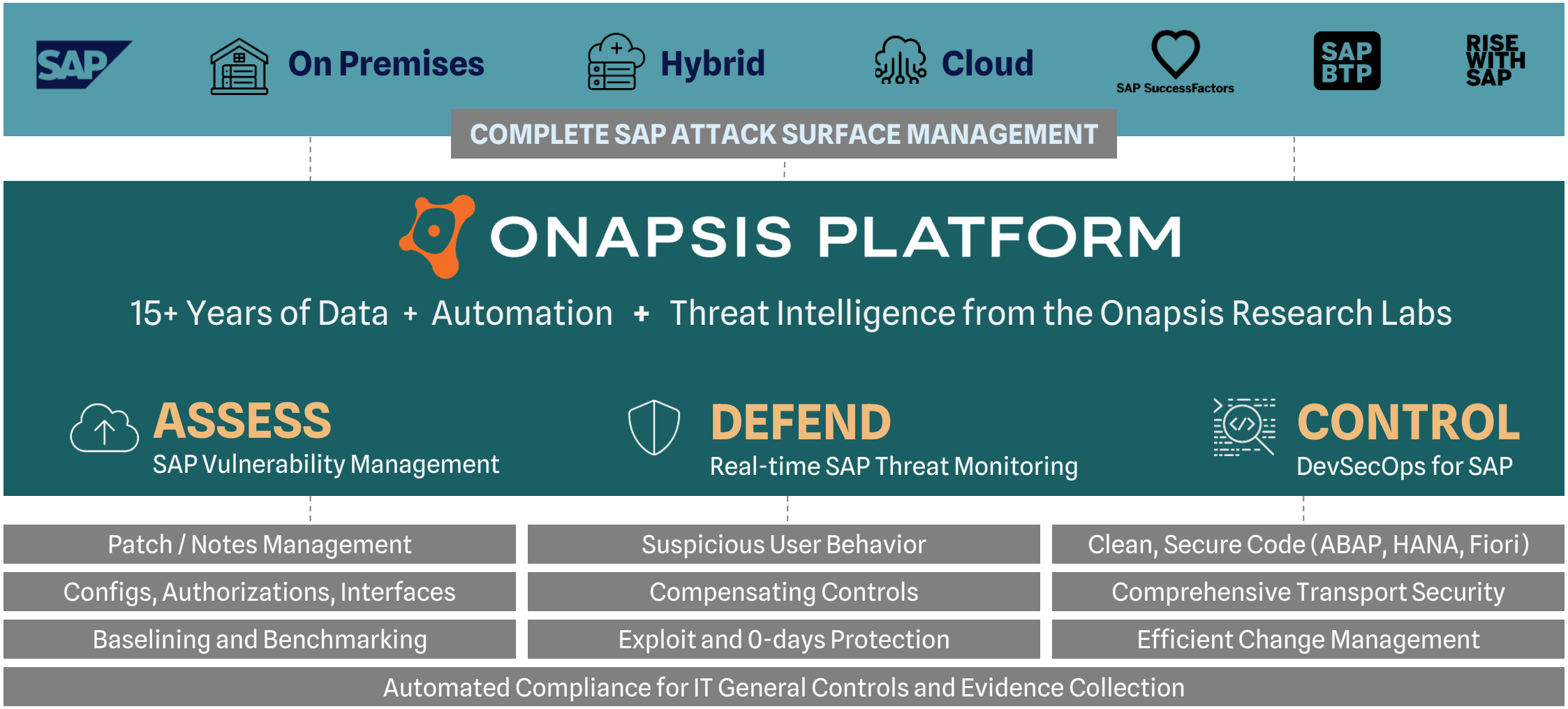
A Sampling of 2023 SAP Threats
(Courtesy of the Onapsis Research Labs)

- **Q1 2023:** **P4CHAINS** Vulnerability Family
- **April 2023:** BlackCat/ALPHV **published data of SAP applications** from a large org affected by ransomware
- **June 2023:** TTALeaks SAP **User Credential Dump**
- **August 2023:** Five Eyes added SAP vuln to the **Top Routinely Exploited Vulnerability List** for the First Time
- **Sept 2023:** ORL Data Demonstrates **Time-to-Exploit Is Decreasing** for SAP Vulnerabilities

[1] **Active Cyberattacks on Mission-Critical SAP Applications** Onapsis Threat Intelligence Report April 2021

[2] **The Third Annual Study on the State of Endpoint Security Risk** Ponemon Institute LLC Publication Date: January 2020

Onapsis: Risk-Driven Security for SAP

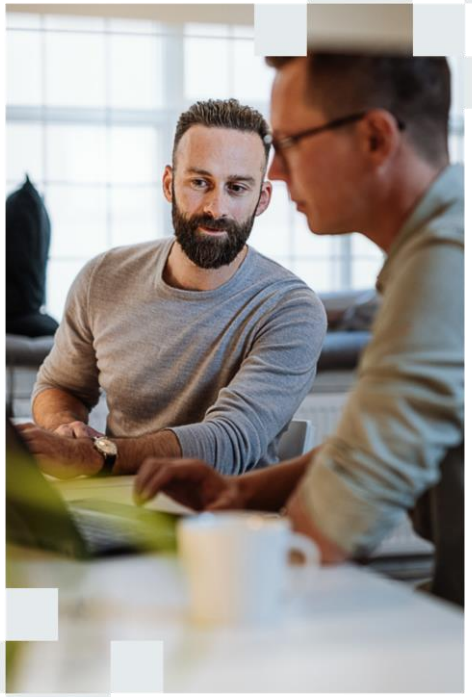


Security Priorities and Execution for Key Results

- Revamp the existing risk framework and **adopt a risk-based approach**
- Leverage **CVSS scoring model** to identify critical, high and low risks and set SLA timelines to achieve the remediation
- Adopt a **"Preventative" approach in establishing a patch management process** on a monthly cadence
- Socialize identified critical risks to stakeholders to **achieve awareness and operational priority for risk remediation**
- Establish **monitoring and detection controls** for risk identification

Our Journey with Onapsis

- Started leveraging Onapsis to **identify all the vulnerabilities and gaps** in our SAP environment
- Leveraged Assess and Defend capabilities from Onapsis, which helped us **set up monitoring and alerts** for our privileged accounts, elevated access monitoring
- Leveraged Assess to **perform full system scans monthly** to identify critical and high vulnerabilities
- This delivered to us a **360 degree overview of all the risks present in our landscape** and gave us a ***pathway*** towards the remediation plan



Celebrating Our Successes

- Established a **robust patch management cadence** that helped bring our SAP landscape to the current patch levels
- Implemented a **risk-based approach with rigid SLA timelines** to ensure risks are remediated in a time–bound manner
- Deployed **robust monitoring of our SAP privileged accounts and elevated access** on a 24/7 schedule
- Invested in **bringing our entire SAP landscape into Onapsis Platform** to continuously monitor for any vulnerabilities
- **Invested in future initiatives of Onapsis** in system health checks, etc.

Where to Find More Information

https://onapsis.com/event/meet-with-onapsis-at-sapinsider-2024

- Schedule a Meeting with the SAP application security leader at SAPinsider. Or stop by Booth #120 to talk to an expert!

https://onapsis.com/platform/assess

- **Complete ERP Attack Surface Management** – Discover vulnerabilities and get risk-based guidance to better prioritize and respond to the greatest threats to your business.

https://onapsis.com/platform/defend

- **SAP Threat Monitoring & Pre-Patch Protection** – Get real-time threat intel and gain an early warning system for sensitive data access, user behavior anomalies, unauthorized changes, misuse, or cyberattacks targeting critical SAP applications.

https://onapsis.com/platform/control

- **SAP DevSecOps** – Secure your SAP software development lifecycle from DEV to PRD. Use automation to clean your code and transports. Recognized three years in a row in the Gartner® Magic Quadrant™ for Application Security Testing.

Key Points to Take Home

- **Threats *to* and Attacks *on* SAP Are Growing Exponentially**, Especially with Complex, Cloud-Connected Landscapes.
- Securing SAP Can Be a Complex Undertaking …But It **Doesn't Have to Be Complicated.**
- **Rethink Your SAP Security Approach**; Adopt a More Risk-Based Framework with Well-Executed Fundamentals.
- **Back to Basics:** Timely Patching and Ongoing Maintenance Are More Critical than Ever Before
- The Best Vulnerability Management Programs Have **Both Point-in-Time Scanning and Continuous Monitoring** Paired with the Right Processes and SLAs.

Thank You! Any Questions?

David D'Aprile
VP, Product Marketing

david.daprile@onapsis.com
Linkedin.com/in/davedaprile

Anitha Meruga
Director, Information Security

anitha.meruga@hdsupply.com

Please remember to complete your session evaluation.

SAPinsider

SAPinsider.org

PO Box 982Hampstead, NH 03841

SAPinsider comprises the largest and fastest growing SAP membership group with more than 800,000 members worldwide.