Solving the Paradox of Patching
A path for a more secure SAP

Mark Gordon, SUSE

Las Vegas

2024

SAPinsider

In This Session

We will discuss how to resolve the conflict between system availability and security patching

We will show how Live Patching can enable a two-track process that combines periodic maintenance with a fast-path for high-impact vulnerabilities

What We'll Cover

- Challenges
- The Paradox of Patching
- The need for a Day-1 patching policy
- Solving the Paradox of Patching
- Wrap up

Challenges

- What are the threats?
- What organizational or technical challenges do these threats create?

Top SAP cybersecurity threats and challenges are closely related to the SAP platform

4 of 10

Top SAP Cybersecurity threats

- Unpatched systems
- Supply chain attacks
- Ransomware attacks
- Connections to other systems …

4 of top 4

Top SAP Cybersecurity challenges

- Detecting potential threats
- Keeping up with patches and updates
- Securing custom code
- Protecting data

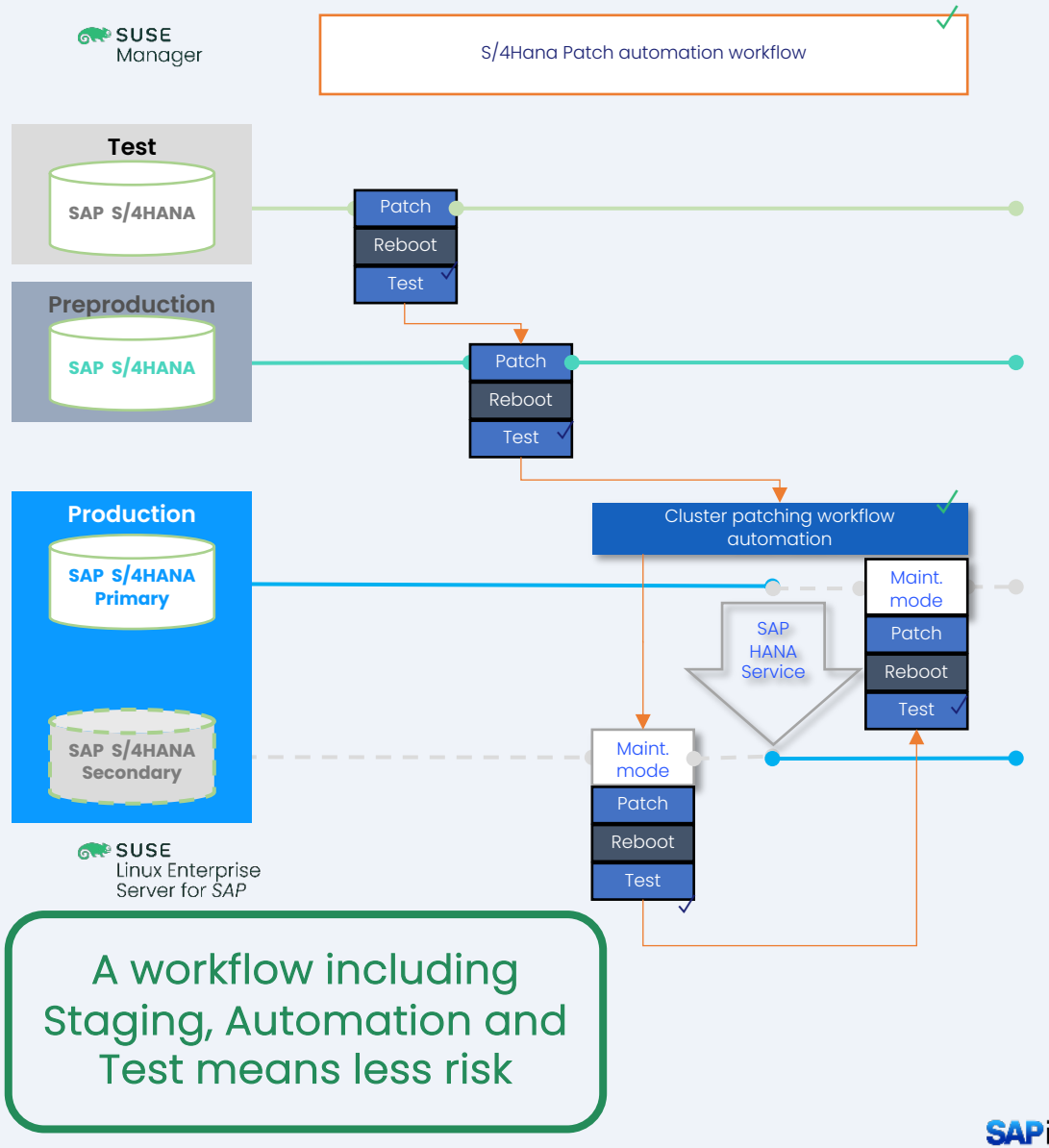
[1] "Cybersecurity Threats to SAP Systems" SAPInsider, March 2022. https://www.suse.com/c/cybersecurity-threats-to-sap-systems/

The Paradox of Patching

The more critical a system is and the more it needs to be available, the less likely it is to be patched to the latest state.

Example of S/4HANA patch process

- A baseline and staging ensure patches tests
- Cluster patch automation avoids error-prone operations
- Test checks running processes and applied patches
- Vulnerability scanner checks it



SAP Unpatched Systems Threat

SAP operating system vulnerabilities and critical bugs need to be fixed urgently

47%

SAP customers challenge to keep up with patches and updates

Day-1 vulnerabilities and critical bugs are a real threat !

- Complexity to **enforce security patching** policies
  - Inability to **negotiate maintenance windows** with service downtime
- Lack of vulnerability management tools

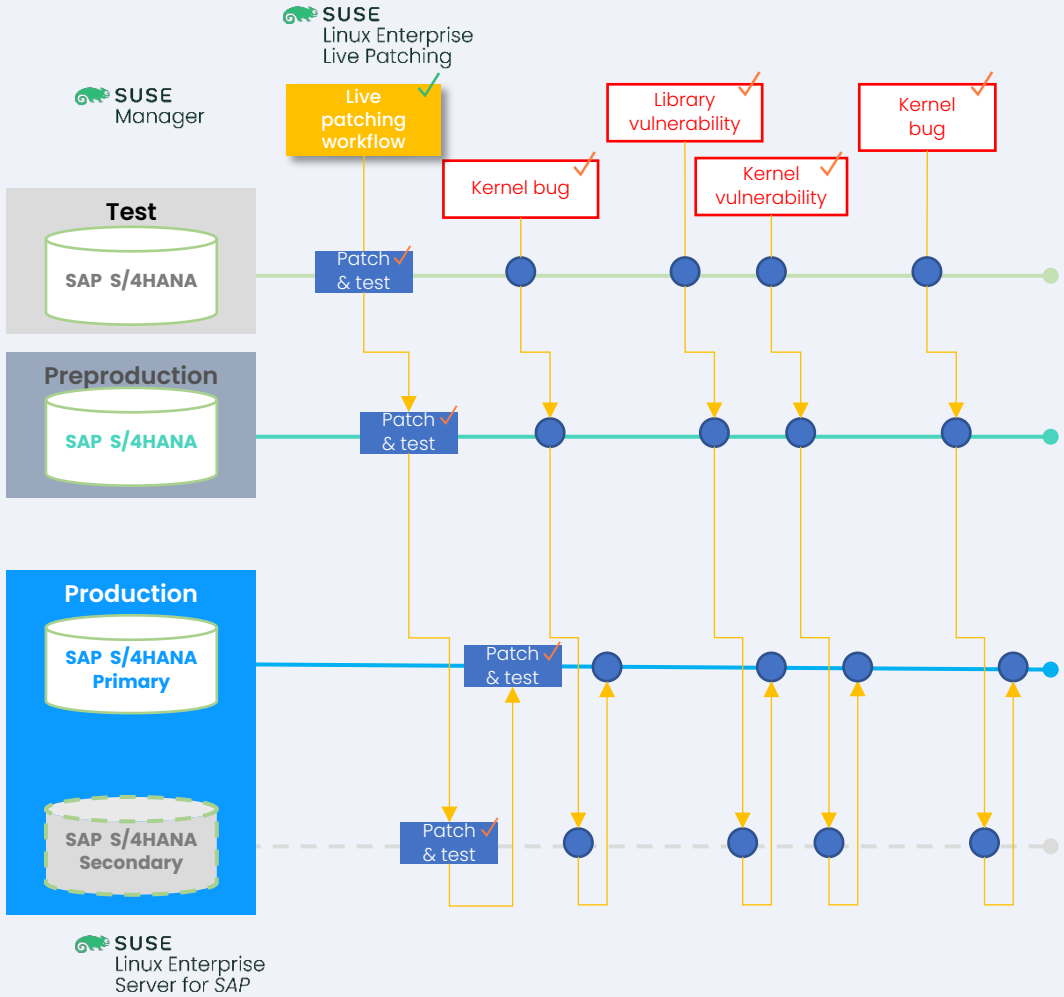
[1] "Cybersecurity Threats to SAP Systems" SAPInsider, March 2022. https://www.suse.com/c/cybersecurity-threats-to-sap-systems/

The need for a Day 1 patching policy

Once a *new* vulnerability is *known*,
how quickly can we prevent it?

Live patching without shutdowns

- Day-1 patching without Service downtime
- Staging ensures patch is tested.
- Include user space libraries too.
- Avoid crashes and data loss by fixing critical bugs
- Test checks running processes and applied patches
- Vulnerability scanner checks it



No service downtime means no need to patch outside working hours

Solving the Paradox of Patching

Enforcing a Day-1 patching policy on the SAP platform using SUSE Linux Enterprise Live Patching and SUSE Manager

The solution is a dual patching policy

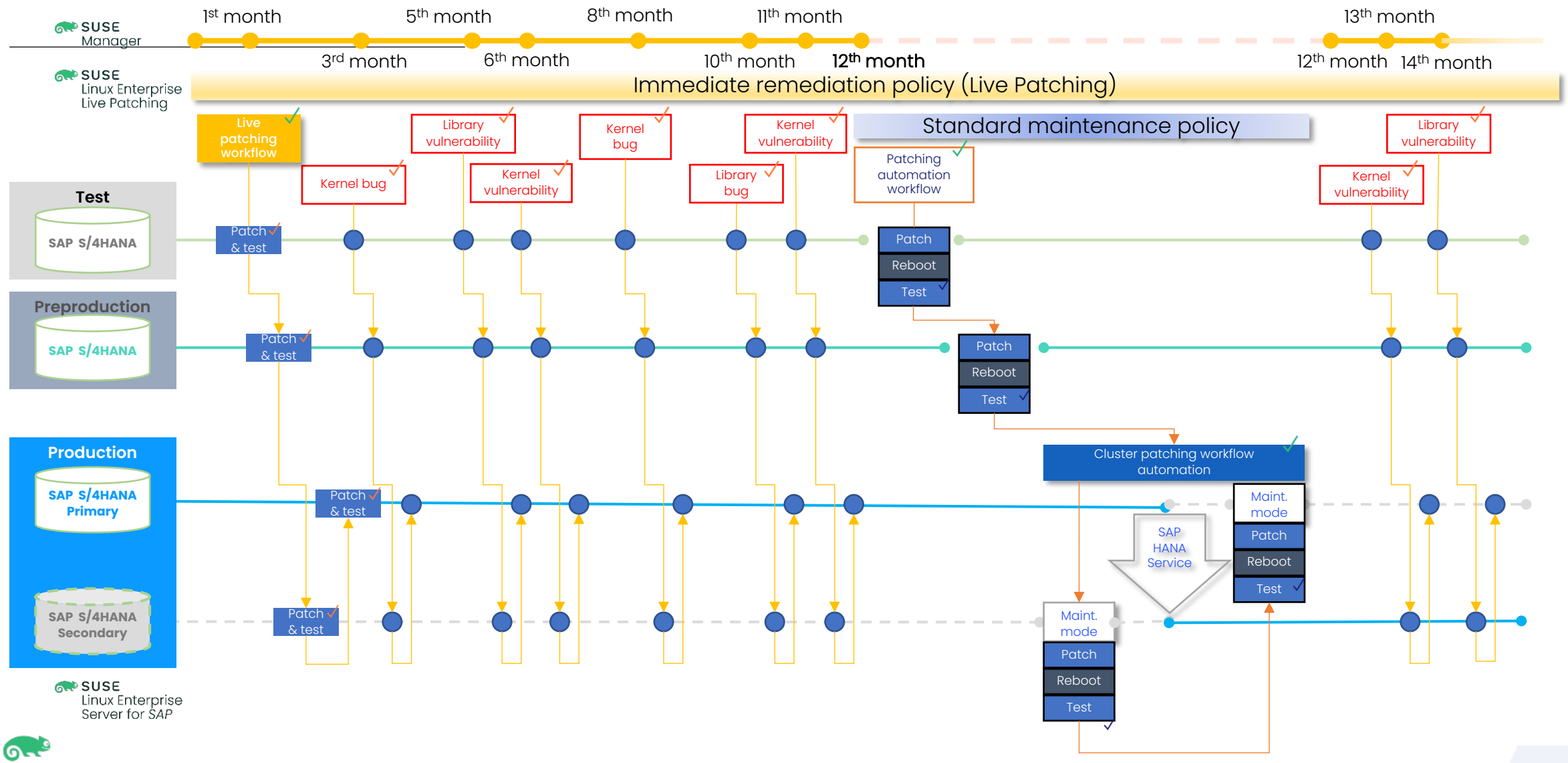
As soon as a vulnerability is known, the threat grows exponentially. Day-1 remediation addresses the gaps in periodic maintenance.

The day-1 patch is not optional Every day with a vulnerability is critical

- **Day-1 vulnerability remediation policy**
  - Vulnerabilities and bugs in OS Kernel and User Space libraries
  - **No downtime and no maintenance window**
  - Workflow, staging & test **ensure the system's reliability**.
  - Long-term **provider commitment** is needed
- **Regular maintenance, including patching**
  - All needed patches
  - Automate the patch application, including the clusters, to avoid disruption
  - Reboot needed

SUSE Linux Enterprise Server for SAP

SAP S/4HANA Dual patching policy with SUSE Live Patching and automation



Wrap up

- Secure your SAP platform by enforcing a day-1 vulnerability patching policy
- SUSE enables SAP customers to enforce a security patching policy to achieve a secure SAP platform that minimizes operational risk and cost.

SUSE Linux Enterprise Server for *SAP*

SAP® Endorsed App
Premium Certified

SLES for SAP applications is endorsed by SAP

SUSE Manager

SUSE Linux Enterprise Live Patching

Where to Find More Information

- SUSE web pages
  - https://www.suse.com/solutions/run-sap-solutions/
  - https://www.suse.com/products/suse-manager/
  - https://www.suse.com/products/sles-for-sap/
- Solving the patching paradox challenge
  - Blog post by Sebastian Martinez
- SAP Store
  - https://store.sap.com/dcp/en/search/SUSE
- Say Goodbye to Downtime
  - https://www.suse.com/goodbye-downtime/

Key Points to Take Home

- Vulnerabilities pose a significant risk to an organization's operations, and patching is crucial to maintain system security and stability
- Patching and updating software is always a top priority
- The patching paradox is one of the main security challenges that SAP environments face
- Organizations should define and implement a patching policy that outlines when to apply patches, factors to consider, and time windows for patching once a vulnerability is discovered
- The patching policy should address both Day-1 vulnerability patching and regularly scheduled updates
- A dual patching policy defines two patching workflows: An immediate remediation patching workflow and a regular maintenance patching workflow.

Mark Gordon

mark.gordon@suse.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 worldwide, with more than 750,000 global members.