SUSE

5 MARCH 2024

Solving the Paradox of Patching
A path to a more secure SAP system

Agenda

In This Session

- Challenges
- The paradox of patching
- The need for a Day-1 patching policy
- Enforcing a dual patching policy
- Wrap up

Challenges

Threats and Challenges

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

5 of top 10

Top SAP Cybersecurity Threats

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

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.

Solving the paradox of patching

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

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 solution is a dual patching policy

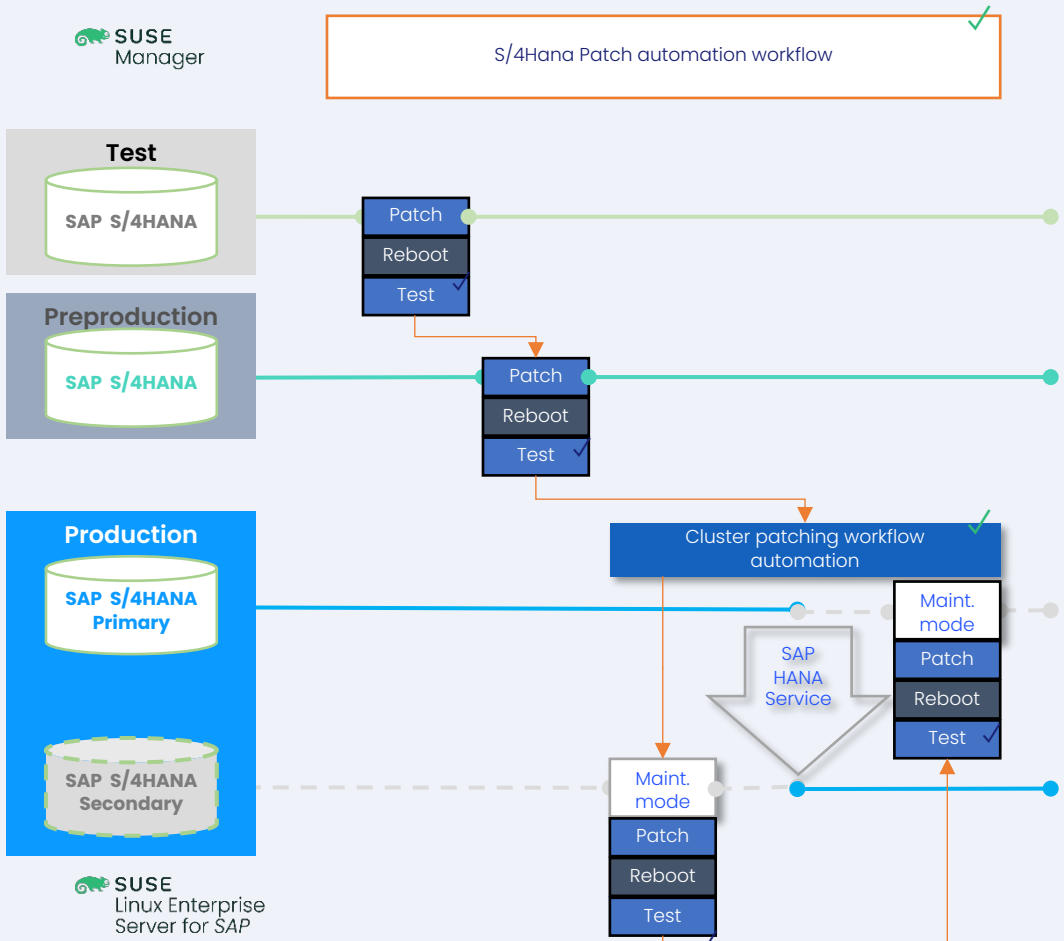
As soon as a vulnerability is known, the threat grows exponentially. Day-1 remediation is defined to fix this hole.

- **Regular maintenance, including patching**
  - All needed patches
  - Automate the patch application, including the clusters, to avoid disruption
  - Reboot needed

- **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

SAP S/4HANA periodic cluster patching staging and automation

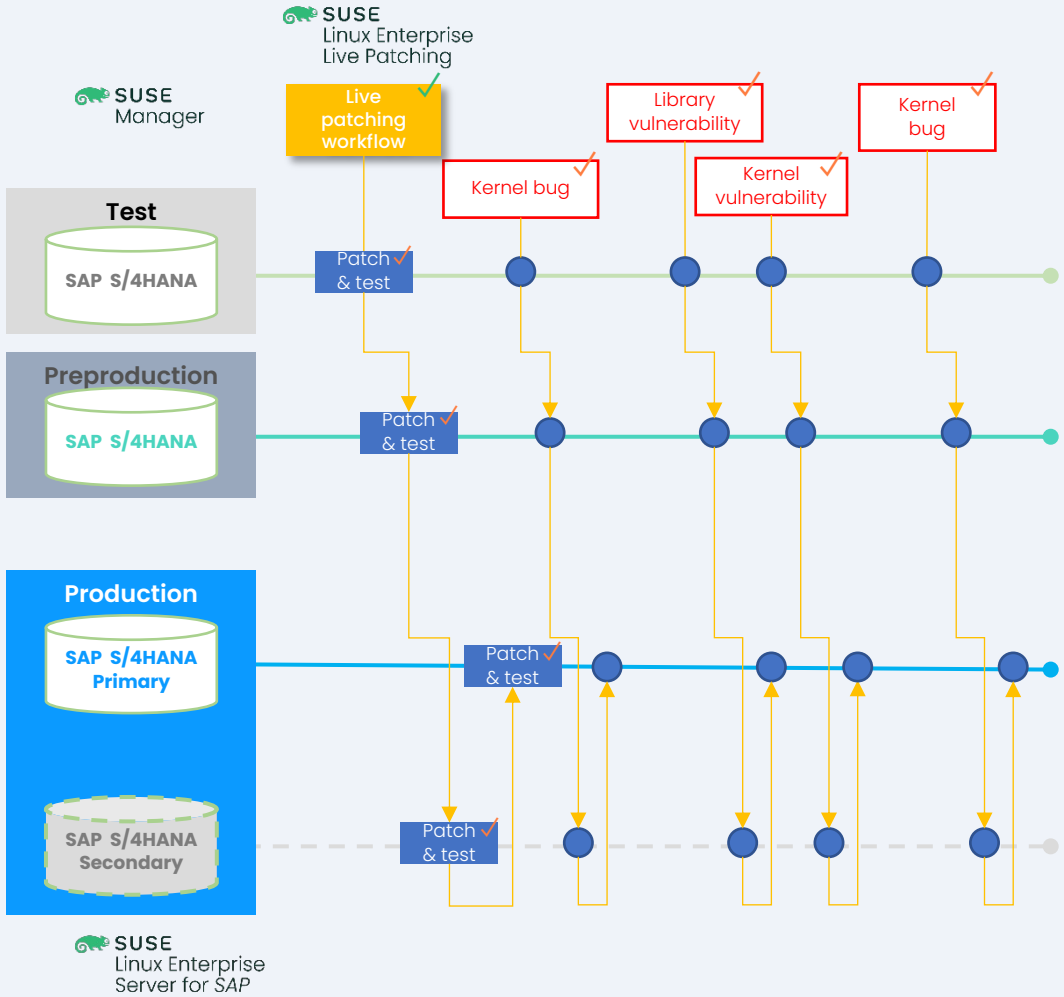
- A baseline and staging ensure patches tests
- Cluster patch automation avoids error-prone operations
- Test checks running processes and applied patches
- Vulnerability scanner checks it
- However, it can require reboot and impact SAP availability



A workflow including Staging, Automation and Test means less risk

Live patching and staging

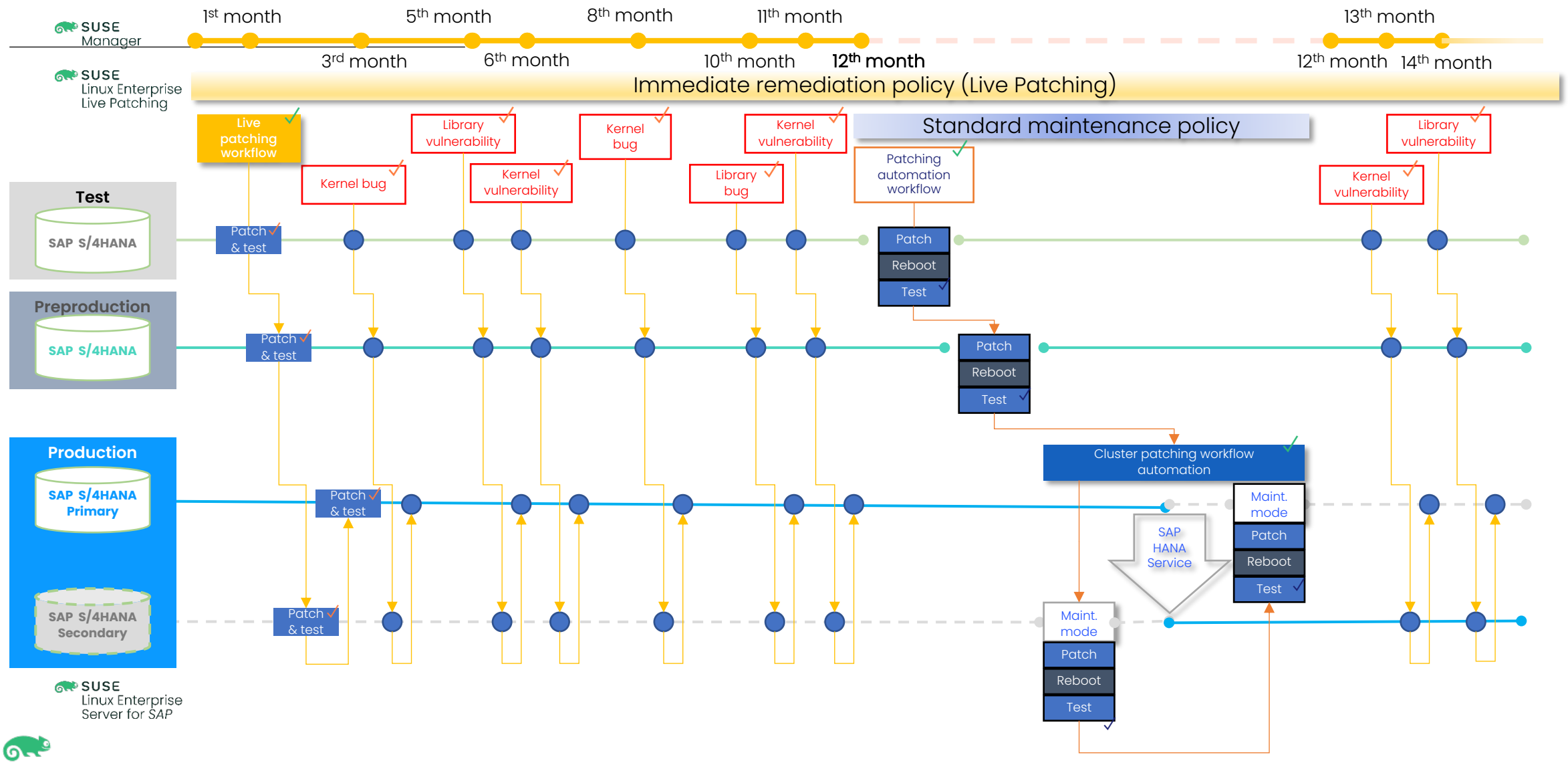
- Day-1 patching without Service downtime
- Staging ensures patches test.
- Include user space libraries too.
- Avoid crashes and data loss by fixing critical bugs
- Test checks running processes and applied patches
- Vulnerability scanner checks it



No service downtime means no need to patch outside working hours

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.

Thank you

For more information, contact SUSE at:

+1 800 796 3700 (U.S./Canada)

Maxfeldstrasse 5

90409 Nuremberg

www.suse.com