Kpatch to the rescue

RHUG Q3.2016

Marc Skinner
Principal Solutions Architect

9/21/2016

AGENDA

Can't we all just reboot?

What is Kpatch?

How does it work?

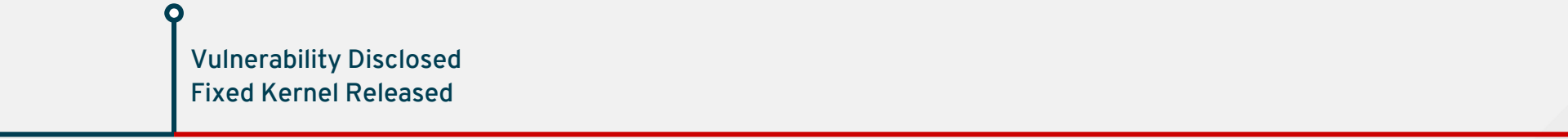
Support details

Kpatch + kGraft = livepatch!


Can't we all just reboot?

PROBLEM

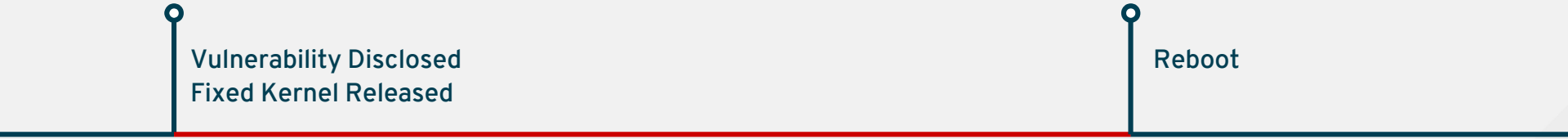
- Applying security fixes to software is a reality of modern IT



Exploit Window
(assuming not 0-day)

PROBLEM

- Security fixes to the kernel are particularly disruptive due to the need for a reboot in order to take effect



Exploit Window
(assuming not 0-day)

PROBLEM

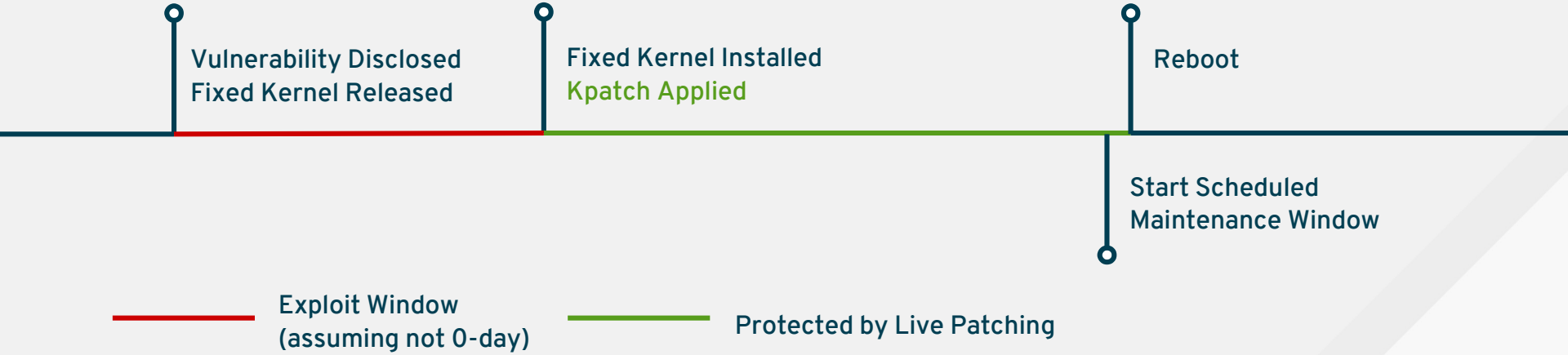
- Many systems can not be rebooted at arbitrary times, but require a maintenance window be scheduled

PROBLEM

- Until a reboot can be performed, the system continues to be vulnerable

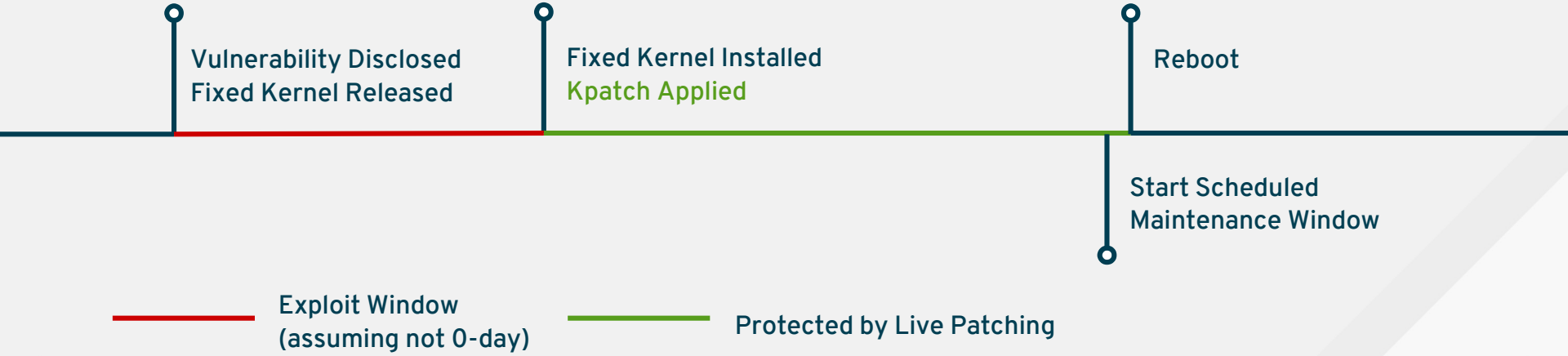
SOLUTION – LIVE PATCHING

- Kernel security and bug fixes applied while the system is running



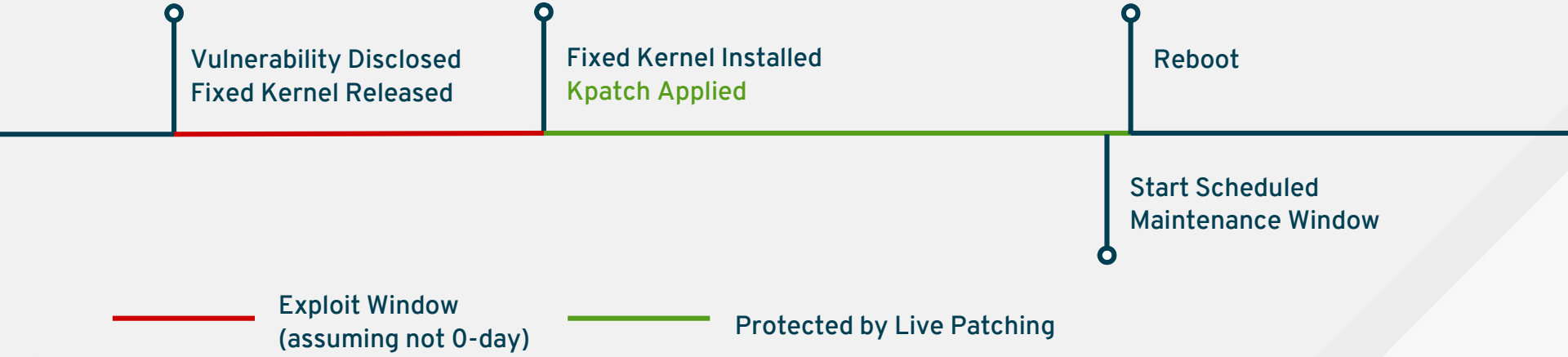
SOLUTION – LIVE PATCHING

- The update process is transparent to applications



SOLUTION – LIVE PATCHING

- Deployed using standard package management

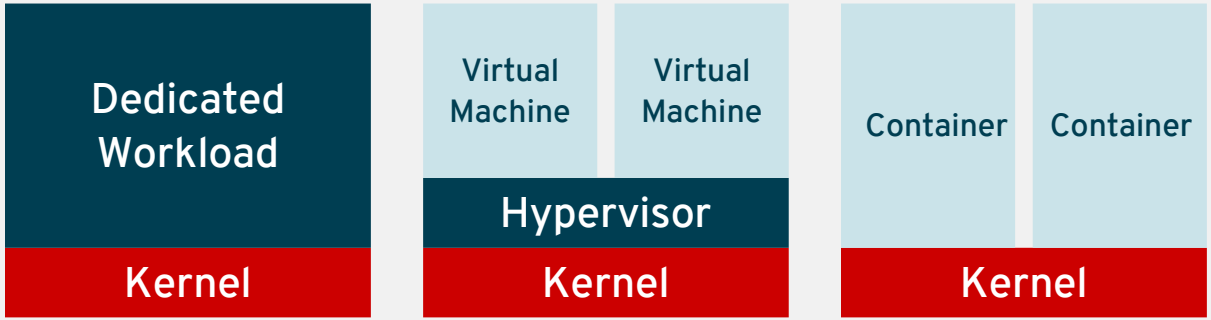


USE CASES

- Systems running dedicated workloads that can not be taken down in an incremental way

USE CASES

- Systems running dedicated workloads that can not be taken down in an incremental way
- Hypervisor or container host running tenant workloads




What is Kpatch?

What is Kpatch?

- Live kernel patching framework
- Patch a running kernel – with no reboot required
- No disruption to applications
- Used for security and stability fixes

What is Kpatch?

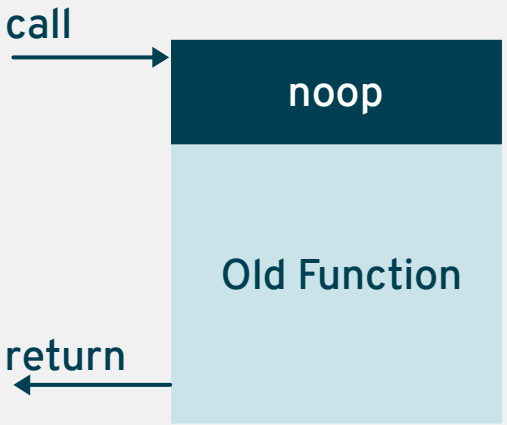
- Started as a Red Hat project
- Released to GitHub in February 2014
- GPLv2
- Introduced in RHEL 7.0 as Tech Preview
- Heavy feedback during testing and SIG
- Fully supported in RHEL 7.2


How does it work?

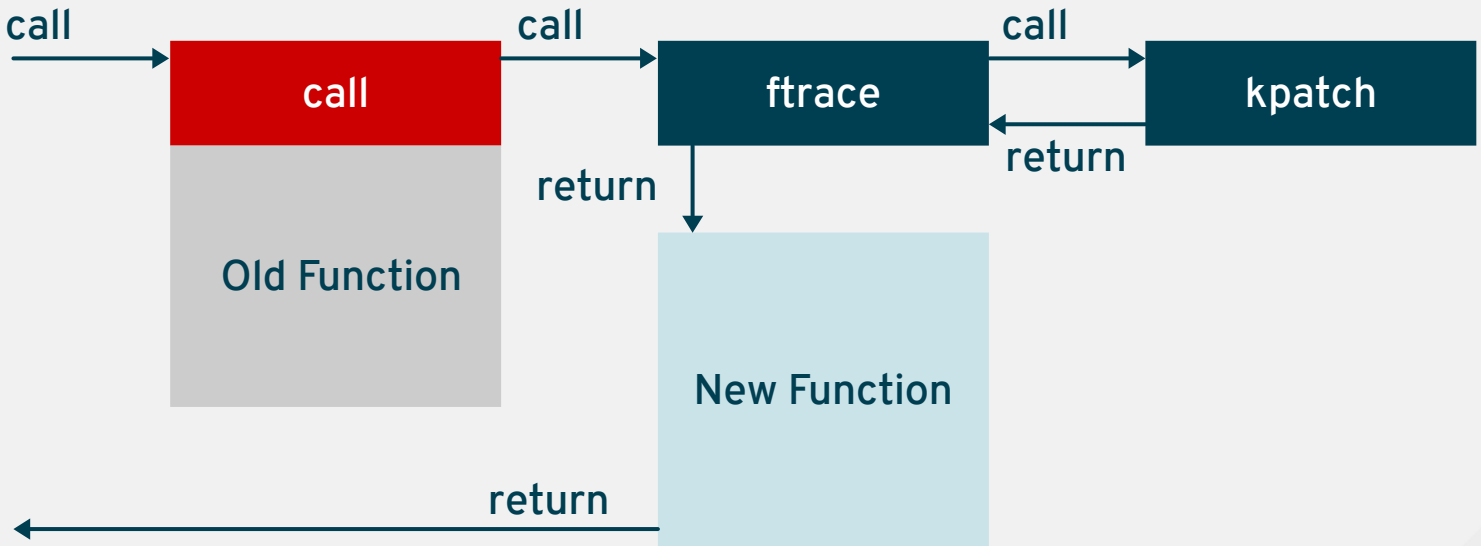
3 Steps to success

- Live patch is copied to /var/lib/kpatch and registered for re-application to the kernel via systemd on next boot
- Kpatch module is loaded into the running kernel and the new functions are registered to the ftrace mechanism with a pointer to the location in memory of the new code
- When the kernel accesses the patched function, it is redirected via the ftrace mechanism

FUNCTION CALL (BEFORE)



FUNCTION CALL (AFTER)



What are the Kpatch components?

- **kpatch-build:** tools to generate a hot patch module – compare a patched kernel to non-patched kernel
- **Live/Hot patch module:** kernel module (.ko file) which provides replacement function and metadata for kernel
- **kpatch core module:** kernel module (.ko file) which provides kernel interface to apply hot patch modules
- **kpatch utility:** userspace tool to manage collection of hot patch modules

Kpatch tooling : User Space

- Install user space tooling

  # yum -y install kpatch

  # systemctl start kpatch.service

Kpatch tooling : Install Patch

- Install Live/Hot patch

  # rpm -ivh kpatch-patch-7.2-1.el7.x86_64.rpm

  # kpatch list

  Loaded patch modules:

  kpatch_7_2_1_el7

  Installed patch modules:

  kpatch-7-2-1-el7.ko (3.10.0-327.36.1.el7.x86_64)

Kpatch tooling : Update/Remove Patch

- Update Live/Hot patch

  # yum update kpatch-patch-7.2-2.el7.x86_64.rpm

- Remove Live/Hot patch

  # kpatch unload kpatch_7_2_1_el7

  # kpatch uninstall kpatch_7_2_1_el7

Support details

Support Requirements

- Currently x86_64 architecture
- Requires Red Hat >= 7.2
- Specifically kernel-3.10.0-327 or later
- Requires RHEL Premium Support subscription
- Live kernel patching follows the active RHEL 7 aync errata phase – current Z stream
- Only one live kernel patch may be applied at any time
- Live patch will be supported 30 days after errata containing fix is released

Customer Process

- Install kpatch RPM
- Request live patch from Red Hat Support
- Install kpatch-patch RPM
- Upgrade to errata kernel < 30 days after published


Kpatch + kGraft = livepatch!

1 + 1 = 3!

- Red Hat Kpatch
- Suse kGraft
- True open source and community collaboration
- Merged upstream into Linux Kernel 4.0
- More users = better success!

redhat.

THANK YOU

plus.google.com/+RedHat

facebook.com/redhatinc

linkedin.com/company/red-hat

twitter.com/RedHatNews

youtube.com/user/RedHatVideos