# Don’t Forget to Secure Your Linux Devices

Protect your Linux endpoints from a wide range of threats with KACE solutions

Ransomware and other cyberattacks are growing exponentially. When one third of security breaches are caused by unpatched vulnerabilities, are you neglecting to update your Linux servers, desktops and your growing number of IoT devices? If you don’t keep up with the Linux security updates, you are leaving your organization open to a heightened level of risk.

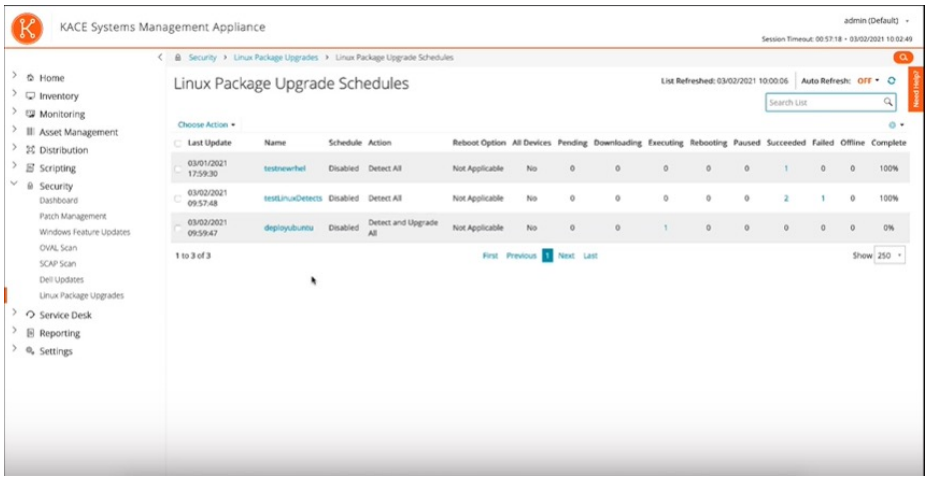
With one of the largest update libraries in the industry, our KACE® endpoint security solutions can not only patch Windows OS devices, but they also give you the power to automate the installation of security update packages for the most used Linux distros, including Red Hat, Ubuntu, Suse, CentOS and Raspbian.

In addition, KACE provides vulnerability scanning for Linux as well as Mac and Windows, which means you don’t need to purchase, train and maintain separate, disparate management systems to both isolate and remediate at risk computers. With OVAL scanning, you can quickly uncover vulnerabilities and prevent malware infection or data theft by ensuring that every Linux desktop, mobile and Internet of Things (IoT) device in your organization, as well as every Linux server, desktop and IoT device, has the proper endpoint protections in place.

## FEATURES

**Linux package updates —** The KACE Systems Management Appliance (SMA) and the KACE Unified Endpoint Manager (UEM) now allow you to automate the process of installing and managing Linux package updates that keeps the Linux OS security updates up to date on your managed Linux RedHat, SUSE, Ubuntu CentOS, and Raspbian devices. These updates improve the overall performance of your managed Linux devices and protect them from potential vulnerabilities.

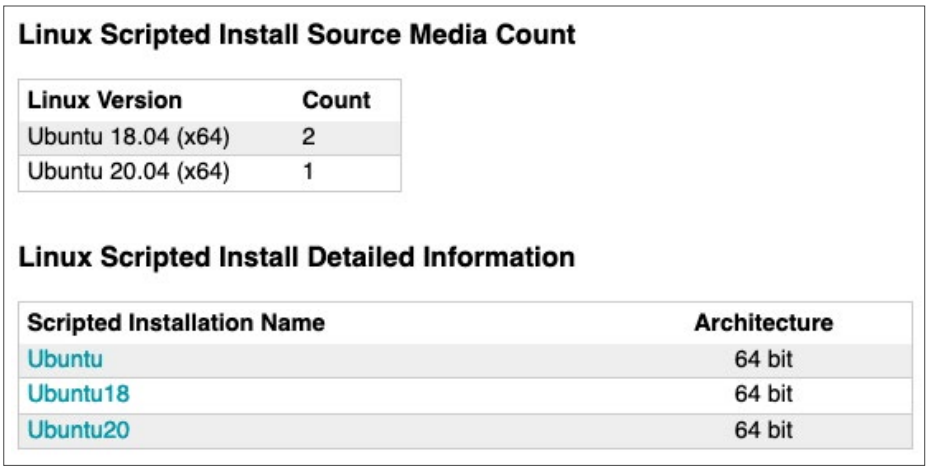
Linux package updates use a process very similar to device patching. You can create update schedules which allow you to either detect package updates, or both detect and update all applicable packages. You can review the list of the available package updates after a detect-only schedule action, for each Linux flavor.




*The KACE Systems Management Appliance automates Linux security package updates.*

## BENEFITS:

- Automate the deployment of security updates for the most popular Linux distros to your Linux RedHat, SUSE, Ubuntu CentOS, and Raspbian devices.
- Perform OVAL scanning to uncover vulnerabilities in Linux servers, desktops and IoT devices.
- Automatically image and reimage Red Hat, CentOS and Ubuntu machines.



**Linux Scripted Install Source Media Count**

| Linux Version | Count |
|---|---|
| Ubuntu 18.04 (x64) | 2 |
| Ubuntu 20.04 (x64) | 1 |

**Linux Scripted Install Detailed Information**

| Scripted Installation Name | Architecture |
|---|---|
| Ubuntu | 64 bit |
| Ubuntu18 | 64 bit |
| Ubuntu20 | 64 bit |

*The KACE Systems Deployment Appliance automatically images and reimages Red Hat, CentOS and Ubuntu machines.*

The update process relies on the assumption that your managed Linux devices point to the appropriate package repositories. Only the packages that include security updates are identified. The appliance does not attempt to detect or update all packages, or to the entire OS to the latest version.

NOTE: The Linux Raspbian does not make a distinction between regular and security updates. Detecting and upgrading packages for managed Raspbian devices results in all updated packages being installed on those devices.

**Linux OVAL scanning —** The U.S. government regularly publishes a standardized list of all publicly known cybersecurity vulnerabilities – the Common Vulnerabilities and Exposures (CVEs). OVAL security scanning for computers running the Windows operating systems has been available on the KACE SMA for years. In May 2021, Mac and Linux scanning were added to the KACE Systems Management Appliance and Unified Endpoint Manager products.

Simply load the latest set of vulnerabilities from the CVE list, then schedule and run assessment reports of endpoint systems against the available list of CVEs. This greatly reduces risk associated with data breaches and privacy violations. So, now you have access to a database of all known Linux CVEs from the most trusted source in the world and can regularly schedule scans to automatically isolate and remediate non-compliant, vulnerable comput-ers/servers/IoT devices that you can update using Linux package updates.

**Automatic Linux imaging and reimaging —** Using the KACE Systems Deployment Appliance (SDA) you can automatically image and reimage Red Hat, CentOS and Ubuntu machines. In an ever-increasing remote management world, this is becoming a must have for Linux Administrators.

## ABOUT QUEST

Quest creates software solutions that make the benefits of new technology real in an increasingly complex IT landscape. From database and systems management, to Active Directory and Office 365 management, and cyber security resilience, Quest helps customers solve their next IT challenge now. Quest Software. Where next meets now.

Quest
4 Polaris Way, Aliso Viejo, CA 92656 | www.quest.com
If you are located outside North America, you can find local office information on our Web site.

Quest and the Quest logo are trademarks and registered trademarks of Quest Software Inc. For a complete list of Quest marks, visit www.quest.com/legal/trademark-information.aspx. All other trademarks are property of their respective owners.

© 2021 Quest Software Inc. ALL RIGHTS RESERVED.

Datasheet-KaceLinux-LP-67763#