Qualys.

LTS Secure

PM

# Patch Management

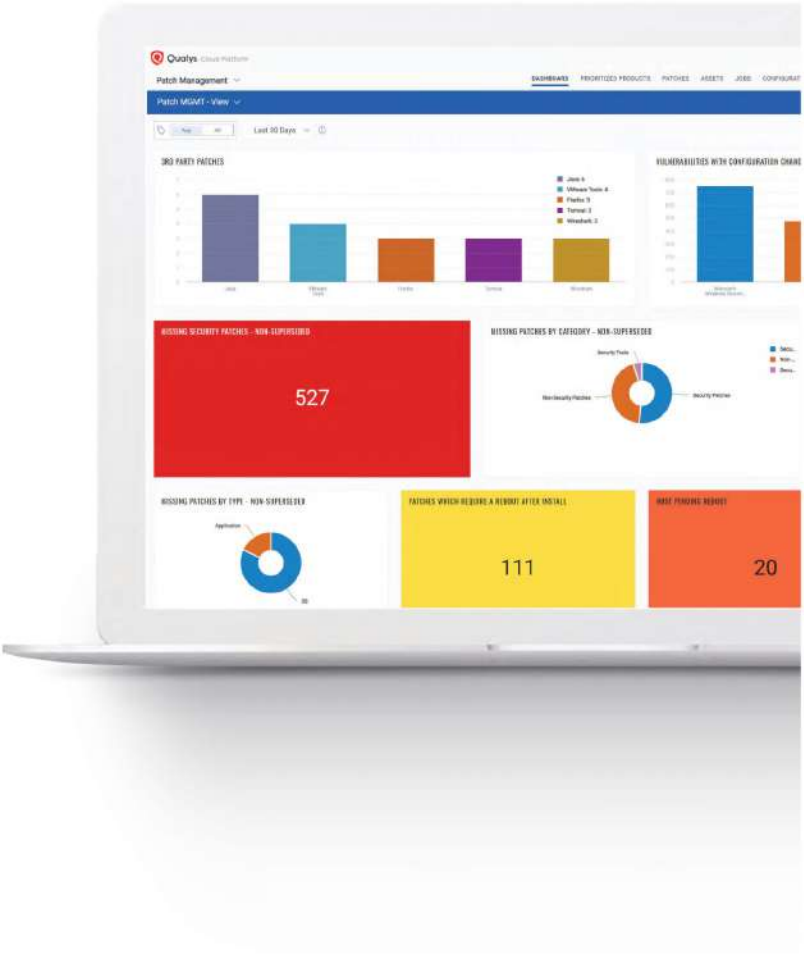
Streamline and accelerate vulnerability remediation for all your IT assets

---

Qualys Patch Management (PM) is a cloud service for IT and security teams to help quickly and efficiently remediate vulnerabilities and automatically patch systems – regardless of device location or operating system.

The solution provides workflow automation, unique prioritization capabilities, and accurate mapping of vulnerabilities detected to required patches and configuration changes. As an enterprise-grade patching solution, Qualys PM can patch Windows OS, Linux OS, macOS, and a large catalog of third-party applications.

Use Qualys PM to automatically reduce your attack surface and free up IT and cybersecurity resources to focus on more strategic areas. It's time to upgrade your current patch solution.



# Key Features

## A single solution to patch operating systems and third-party applications

Qualys Patch Management can be used to patch and apply post-patch configuration changes to operating systems and third-party applications from a large variety of vendors, all from a central dashboard. This capability means you don't have to manage patches in silos via multiple vendor-specific consoles. The solution manages reboots, honors maintenance windows, and ensures controlled deployment to servers and workstations to keep your enterprise IT and network environment secure and robust.

## Automated correlation of vulnerabilities and patches

Qualys Patch Management lets you automatically correlate vulnerabilities identified by Qualys VMDR with patches and required configuration changes to decrease MTTR. The solution efficiently maps vulnerabilities to patches and required configuration changes. It also provides ready-to-deploy patch jobs that can be scheduled and deployed automatically. Qualys Patch Management is the only patch solution to enable Cybersecurity and IT teams to define a single shared priority list of applications to patch regularly, based on historical per-application vulnerability data from VMDR. This fosters increased productivity and cooperation between these two teams.

## Zero-Touch Patching

Qualys Patch Management gives the flexibility to automate patching based on prioritized vulnerability data from Qualys VMDR. For example, this helps enterprises address the most critical threats like ransomware first. Teams can automatically apply routine patches where the risk of creating system instability is low, to reduce mean-time-to-remediation and free up critical IT and cybersecurity resources to focus on more strategic tasks. Zero-touch patching helps to automatically reduce the enterprise attack surface. Zero-touch also helps Cybersecurity and IT teams to meet SLAs and reduces manual remediation efforts and costs more easily.

## Cloud-based solution that is easy to deploy and use

No need to install software on-premises or configure open ports and VPNs. Any on-premises workstation and server, or work-from-home device with the Qualys Cloud Agent installed, can be immediately scanned for missing patches and patched automatically. Anywhere you can put the Qualys Cloud Agent, you can run Qualys Patch Management. When Qualys Patch Management is used with the Qualys Cloud Agent Gateway Service, you can significantly optimize bandwidth usage by caching patches locally on your network.

## Remote remediation for corporate and personal devices

With remote work now the norm, many organizations struggle to deliver patches to corporate and personal devices when users are working from home or otherwise infrequently connected to the network. Qualys Patch Management allows the patch team to automatically deliver patches, apply configuration changes, and even install/uninstall software via the cloud to these remote users while avoiding the use of limited VPN bandwidth.

## Unify discovery, prioritization, and remediation in one platform

Qualys Patch Management leverages the Qualys Cloud Platform and Cloud Agents to help IT and security teams quickly and efficiently remediate vulnerabilities and patch systems. The unified platform also includes services for asset inventory (including EOL/EOS data), vulnerability management, threat prioritization and response. These cloud services are all integrated and share the same data, console, and single cloud agent.

## Complements your existing Patch Management investments

Qualys Patch Management can complement the patch management tools your IT team already has, such as Microsoft System Center Configuration Manager (SCCM), should you choose to continue using it.

## One Platform | One Agent | One Data Model

As Patch Management leverages the same agent as VMDR, it can be turned on via simple one-click deployment, driving rapid time to value and total cost of ownership (TCO) benefits.

# Benefits

## FOR REMEDIATION / IT TEAMS

### Reduce patching time for a happier Cybersecurity team

- Automate patching where it makes sense
- Patch the right products and vulnerabilities at the right time on the right devices
- Create transparency for IT and Cybersecurity teams

### Close all your remediation gaps

- One unified solution to deploy patches and make configuration changes required by the Cybersecurity team to fix a vulnerability and uninstall or upgrade EOL/EOS software
- Largest out-of-the-box support for third-party applications, with no need to spend time packaging new patches

### Less maintenance, more patching

- One agent for all patching and vulnerability scans
- Simple patch deployment to servers and workstations
- No need to maintain VPN or network exceptions – patch any device in any location
- Cloud based, so easy-to-use access from anywhere with a browser

## FOR VM / CYBERSECURITY TEAMS

### Fix more vulnerabilities faster

- Accurately map prioritized vulnerabilities to patches and configuration changes required for remediation
- Simplify the integration between VM and IT assets to automate patch deployment based on different risk factors like vulnerability severity, ransomware, etc.
- Eliminate time researching if remediation requires applying both a configuration change and a patch – Qualys PM automatically does this for you

### Quickly respond to zero-day threats

- The same platform used to detect zero-day threats is used to initiate applying the right patches on the right devices
- Validate successful zero-day remediation by monitoring patches deployed and as well as vulnerabilities fixed – all from the same console

### Save costs while reducing your attack surface

- Detect, prioritize, and remediate vulnerabilities with the same platform and same agent – no need for multiple products
- Automated patch jobs target the right devices for the right vulnerabilities and reduce your attack surface more efficiently
- Focus on remediation of vulnerabilities, not just patch management

IDC

*"Qualys is uniquely positioned to leverage both vulnerability and threat intelligence insights in its patching solution. Cleverly, the Qualys approach of taking patch remediation a step further with the addition of zero-touch automation eliminates non-caustic threats like always patching Chrome or iTunes. It is a welcome addition that helps companies reduce their attack surface while also freeing up IT and Security resources to focus on more strategic areas."*

Christopher Kissel
Research Director, Security Products, IDC

# Results that Matter

60% faster remediation for critical vulnerabilities

Risk-focused Smart-Automation accelerates MTTR and addresses vulnerabilities causing the greatest risk to the organization

Fully integrated into Qualys VMDR, allowing customers to map findings to actionable remediation workflows

Better alignment across Cybersecurity and IT teams

Infosys®

*"Qualys Patch Management helps us quickly patch remote systems based on vulnerability-driven priorities. It has empowered our platform teams and improved our patch governance efforts. We chose Qualys PM as it is natively integrated into Qualys VMDR and allows cross-platform remediation."*

Surendra Nemani
**Head of Security Engineering, Infosys**

## Request a full trial (unlimited-scope) at qualys.com/trial

Qualys is easy to implement, easy to use, fully scalable–and requires NO infrastructure or software to maintain.