



Managing Updates to Keep Devices at Optimal Operation
and Safety

The Evolution of Endpoint Management

Part 3: Dell Trusted Update Experience

August 2023

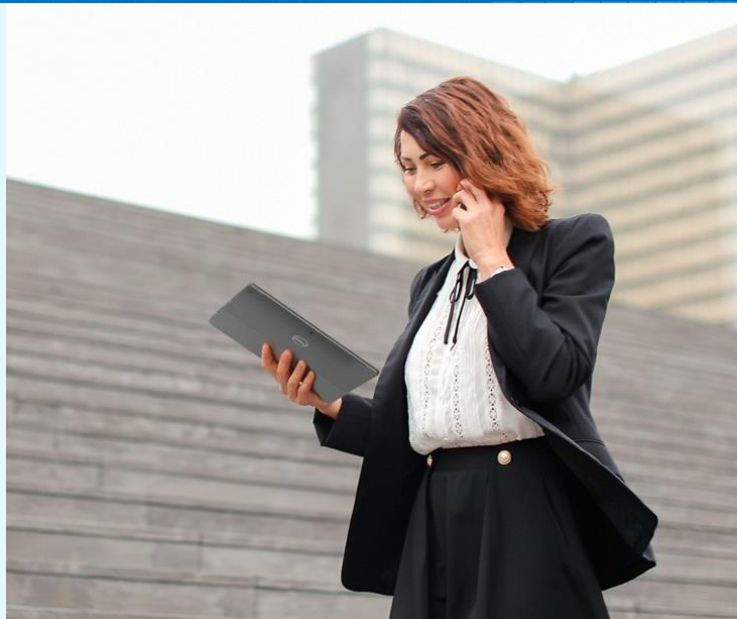


Market Context & Challenges	3
Traditional Methods for Updates & Dell's Approach	4
Value of Dell Trusted Update Experience	5
Cutting-Edge Security	5
Optimize Performance	6
Seamless Experience	7
How It Works	8
Next Steps	9

Market Context

Keeping devices updated is rarely a top priority for most workers

For office workers who rely on their laptops to get work done—but who can't wait to close their devices at the end of the day—it's not always natural to see the importance of updating your devices. If it's not broken, why fix it? And if updates are going to take up valuable space in the workday, when will there be a good time?



26% Percent of new vulnerabilities have known exploits that may have been mitigated with patching¹

But failing to update puts both workers and their businesses at risk

Often, users may not even notice the differences updates make. However, delaying or neglecting the latest updates can lead to performance degradation, increased susceptibility to security breaches, and compatibility issues with newer software and hardware.

Device updates are essential for ensuring optimal operation and safety in today's technology-driven world. Regular updates provide functional improvements, crucial bug fixes, and security patches that address vulnerabilities and enhance device performance. Updates help protect devices against evolving cyber threats, ensuring that systems remain resilient against malicious attacks. Updates also often introduce new features and capabilities that keep devices in line with the latest technological advancements.

At Dell, we understand better than most that device updates are often perceived as burdensome or time-consuming. That's why we've worked tirelessly to streamline the process, leveraging advanced technologies and intelligent systems to optimize every step. We believe that device updates should be more than just a necessary task. We strive to make it a great experience, optimized for your convenience and secure to protect what matters most. Our commitment goes beyond delivering cutting-edge technology; we want to empower you with seamless device updates that enhance your productivity and keep you ahead of the curve.

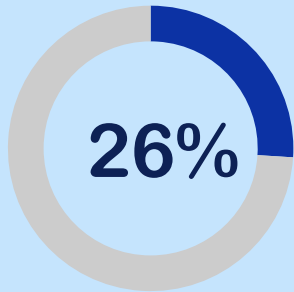
[1. IBM, 2023.](#)

We can improve how we manage updates

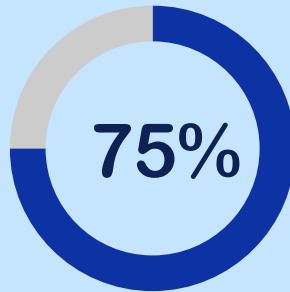
Traditional device update methods are often unpredictable and can create compatibility issues, leading to delays for workers. In addition, these methods often fail to provide real-time visibility and comprehensive security patch management.

Manually managing updates is a time-intensive process that can take hours or even days depending on the size of the company. Often a company may not have enough resources allocated to this level of work.

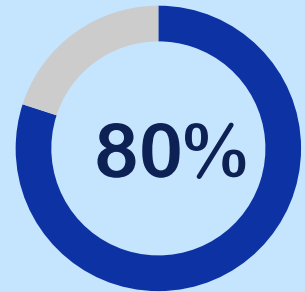
Traditional methods for updating devices can be slow and burdensome



increase in known vulnerabilities between 2016 and 2021¹



of attacks in 2021 were launched through vulnerabilities that were exposed in or before 2017²



of security incidents are driven by the exploitation of unpatched vulnerabilities³

A better way is possible.

Introducing Dell Trusted Update Experience

Thankfully, a better way is possible—a process for automating updates that is minimally intrusive to employees' workdays, requires little if any manual intervention from IT, and is delivered through familiar tools to every device in your fleet.

Dell has developed an experience to provide efficient and streamlined updates that are validated against hardware models, aligned with industry release dates, and can be configured to receive automatic updates with minimal interruption, ensuring support every step of the way.

[1. Vida Ahmadi Mehri, Patrik Arlos, and Emiliano Casalicchio, 2022.](#) [2. Check Point, 2021.](#)

[3. Arctic Wolf, 2022.](#)

Value of Dell Trusted Update Experience



By ensuring your devices are automatically equipped with the latest drivers, BIOS, and firmware versions, users in your organization can maintain cutting edge security and optimize their system performance—all through a seamless experience that's minimally intrusive to both IT and the users they serve. Organizations that regularly update endpoints have noted several significant benefits, including improved security, performance, and user experience.

1. Maintain Best Device Security

Businesses and their IT organizations have a responsibility to protect both their own and their customers' data and privacy. A critical element of this responsibility is ensuring devices are secure and up-to-date to minimize the risk of data breaches and cyber attacks, all while maintaining compliance.

This has never been more critical, as new and emerging cyberthreats continue to develop alongside increasingly stringent regulations that require your devices to continuously evolve.

From a security standpoint, there has never been more risk in failing to secure your workers' devices. Bad actors are always searching for softer targets, with hardware and firmware increasingly making their list. A study conducted in 2021 found that **83% of businesses had experienced at least one firmware attack in the past two years.**¹

83%
of businesses surveyed in
2021 had experienced at
least one firmware attack in
the past two years¹

238%
increase in cyberattack
frequency with the rise of
remote and hybrid work²

With the rise of remote and hybrid work, **cyberattack frequency has increased by 238%.**² Since hybrid work isn't going anywhere, and hardware-level and BIOS attacks are on the rise, it's critical that known vulnerabilities are patched and addressed quickly and regularly to keep devices safe from attacks.

Dell Trusted Update Experience helps ensure regular security and functional updates are applied—including BIOS updates—to keep pace with emerging threats and ensure workers' devices run smoothly. In addition, IT can configure these updates to go out automatically if they so choose, to counteract bad updating habits within the workforce.

These updates also help businesses keep pace with evolving regulations, particularly those related to data security, helping organizations avoid legal consequences while maintaining a superior security posture. All of this is delivered through regular, timely, and frictionless updates available for delivery through multiple, familiar toolsets

[1. Microsoft, 2021.](#) [2. Alliance Virtual Offices, 2023.](#)

Value of Dell Trusted Update Experience

2. Optimize Performance

Users expect their devices to be fast, reliable, and efficient. The last thing any employee wants is for the tools they need to do their jobs to let them down. And downtime due to device issues doesn't only impact the employee experience—it costs businesses money and taxes support teams.

Dell Trusted Update Experience (DTUE) solves these challenges to deliver a better employee experience with less manual intervention required from IT admins and support desks. Ultimately, implementing DTUE can reduce support costs, improve system performance, and minimize downtime for both IT admins and their users.

By checking compatibility between updates and users' existing software and hardware configurations, DTUE helps you stay ahead of issues that can overload helpdesks and halt productivity. For instance, **75% of blue screens are caused by faulty drivers**,¹ so this is particularly critical. In addition, these updates can reduce costs for organizations, as expensive hardware fixes are often requested for issues that could have been resolved through driver updates.

Downtime is extremely costly; **\$300,000 is the cost per hour of IT downtime across a majority of mid-sized and large enterprise**²

This means that it is not only essential to proactively address issues that create downtime for your workers, but to do so in a manner that is itself minimally disruptive. By delivering updates on a predictable, monthly schedule, DTUE helps minimize downtime while keeping devices working and IT in control.

\$300,000

per hour of IT downtime across a majority of mid-sized and large enterprise²

But Dell's perspective is that updates are meant to do more than maintain the status quo. To improve system performance, DTUE leverages telemetry from devices to track update metrics including platform update penetration and measure its impact to device health. All to ensure employees are not only able to work, but able to work productively with the experience they expect.

[1. Microsoft, 2023.](#) [2. ITIC, 2022.](#)

Value of Dell Trusted Update Experience

3. Seamless Experience

None of the benefits we've discussed matter if employee behavior around device updates doesn't change. A survey conducted by Kaspersky in 2021 found that **50% of respondents postpone installing updates**, with 63% seeing no harm in this delay.¹

50%
of workers postpone the installation of updates¹

Users expect seamless and hassle-free updates that keep their OS and hardware up-to-date with the latest features, security patches, and bug fixes. They expect these services to be easy to use, fast, reliable, and secure. Most importantly, they don't want updates to be disruptive—they simply want to know their devices are up-to-date, secure, and available as they work while also being in sync with how their IT organization operates.

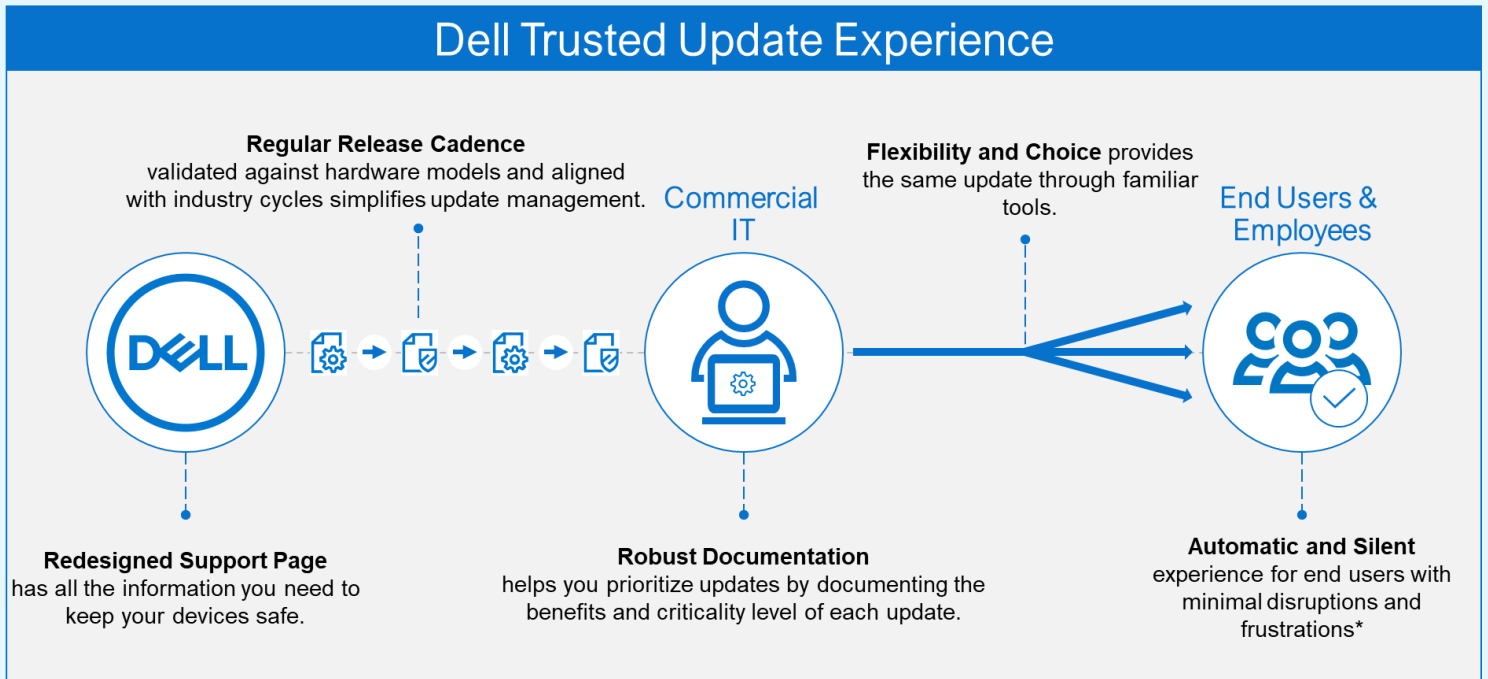
Failing to meet these expectations drives user behavior, leading to users actively hammering the snooze button and delaying critical updates. DTUE delivers reliable and trustworthy updates that are consistent and simple, so IT organizations and users are minimally disrupted. We do this on a monthly release cadence that alternates between functional and security releases on a proactive basis, all pushed out through familiar Dell Tools or Windows Update. DTUE also ensures updates are effectively supported as they're rolled out, with robust documentation available.

We've also invested in improving the end-user experience, having recently revamped our support page to make drivers and downloads even easier to find—along with the previously discussed changes meant to minimize interruption and make updates easy to plan around when needed.



[1. Kaspersky, 2021.](#)

What is Dell Trusted Update Experience?



*IT has the flexibility to decide how updates are delivered



How does it all work?

Dell Trusted Update Experience is a simplified way of updating that provides the latest fixes and updates validated against your hardware models.

Updates are aligned with industry release dates and can be configured to install automatically with minimal interruption for users, with support every step of the way.

Dell Trusted Update Experience is available through all of our update tools, including the following:

- Dell Command | Update
- Dell Update
- SupportAssist
- Alienware Update
- dell.com/Support
- Dell Command Driver Packages
- Dell Business Client Catalog
- Update Catalogs in TechDirect
- Windows Update



Next Steps

1 Identify gaps and pain points in your updates process

- How frequent are your updates? What causes the most issues in the updates process? How would making updates more predictable improve your process?
- How long does updating take, and how many resources do you invest in keeping endpoints updated? Where do you want to save time and resources?
- Do you update BIOS and firmware regularly? If not, would reducing risk in this process make more regular updates possible?
- What are the gaps in your current update process that you wish you could fill?

2 Consider the age of your fleet

- What is the average age of your fleet?
- Have you checked your devices to see how many are approaching end of warranty / end of life?
- How much time and resources do you dedicate to hardware that's more than 4 years old?
- How does the age of your endpoints and peripherals impact your updates process? How would the increase in security and decrease in update difficulties help justify the purchase of newer hardware?

3 Reach out to Dell

Contact your Sales Rep