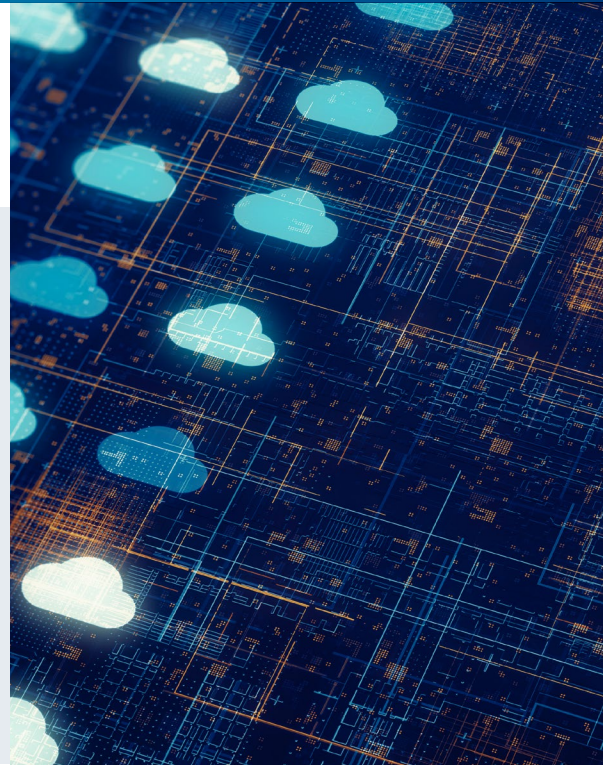


# Four Reasons to Leave Your Old Hardware Behind for Good

The idea of moving to a cloud application may seem daunting for a variety of reasons. However, as your technology needs grow more advanced, the benefits of leaving behind dated hardware and its maintenance becomes impossible to ignore.

The public sector can benefit from a move to a proven cloud environment that improves cost, security, support, productivity, and scalability. By moving to the cloud, your organization can feel confident it is delivering optimal value to your community.

Here are four benefits you can gain from moving to the cloud and leaving your on-premises servers and hardware behind.



## 1 Cost

Maintaining old hardware can be costly. Old systems may use replacement parts that are both expensive and hard to find. Unfortunately, if your organization is unable to procure these parts and decides to keep old systems running past their ideal retirement dates, you also risk not having access to the latest software and security safeguards.

Additionally, the costs of staff downtime for bug fixes and keeping outdated systems running can add up. Moving to the cloud eliminates the need for costly hardware purchases and maintenance, which frees up resources and reduces overtime spent on tasks.

Failures of hardware that you are responsible for can play havoc with tech budgets. Cloud deployments provide known costs, reducing the risk of unexpected expenses and improving budget planning in the process.

Reducing the burden on its IT department has been a key benefit for the city of Rancho Cordova, California.

“Using cloud technology frees up staff time in our IT department,” says Jessica Crone, management analyst for Rancho Cordova.

“That way, we can work on other items.”

## 2 Security

Moving away from in-house servers and hardware can also firm up your application security practices.

In 2021, the FBI’s Internet Crime Complaint Center (IC3) reported a “7% increase in cyber crimes from 2020,” with “potential losses exceeding \$6.9 billion.”<sup>1</sup>

However, despite this growing risk, a recent survey by McKinsey reported that “among 100 companies across various industries, only about 10% take aim at cyber risk reduction. Most — about 70% — are more reactionary, filling security gaps as they arise.”

Older on-premises hardware systems, like servers, networking equipment, and backup devices, can be viewed as part of the “security gaps” that departments need to be aware of. A vendor may announce that a product will reach the end of its support by a future date, providing enough time for you to migrate your applications to another environment. If you don’t migrate off these unsupported solutions, you will be responsible for administering a product that no longer receives security and non-security updates, bug fixes, or technical support.

Cyber-attacks have become extremely complex and sophisticated, and older hardware may not have the functionality to access new security features that could prevent an exploitation.

The city of Mobile, Alabama, points to the benefits of security on the cloud.

“The most pressing concern that I would have and the climate we’re in today is, security,” says Scott Kearney, chief technology officer for Mobile. “All those systems that we’re maintaining on-prem and trying to maintain them securely becomes a real struggle, and it’s hard. We still have some systems on-prem, but I couldn’t imagine having our full enterprise system on-prem. It would just be a bit overwhelming. I don’t think you have a choice now as a municipality, just for security reasons only. You have to (be on the cloud).”

### 3 Support and Productivity

It can be challenging to make sure you always have the latest software version on your on-prem servers. But not having the latest patches in place can put your data at risk.

A cloud environment reduces your team’s application administration responsibilities and streamlines the update process.

Applications that run on the cloud simplify the upgrade process, making it easier to make sure users have access to the latest version of software. The burden of performing backups, restoring software, and maintaining data shifts from the organization to the provider.

“The cloud has been phenomenal. We’ve not had to worry about the tech, the infrastructure, as far as upgrades, how we’re going to upgrade our servers, things of that nature,” says Daphne Cousson, Georgia’s Fayette County Board of Commissioners enterprise systems administrator. “It’s been nice to have that taken care of on the Tyler Technologies side.”

In addition, a cloud-based system provides peace of mind for data backup because a proven cloud solution offers the advantages of redundant systems and uptime reliability, which organizations such as Clermont County, Ohio, have taken advantage of.

“One of the biggest benefits of moving to the cloud is taking that burden off of your local staff to make sure that your backups are good – the whole disaster recovery situation,” says Cindy Hawk, deputy auditor, real estate operations, for Clermont County, Ohio. “In the old days of backup tapes, you just never knew if something was going to be good when you went to reload it. So that burden is completely removed from us.”

### 4 Scalability

To meet the growing expectations of today’s communities, the public sector must continuously improve its technological capabilities. To ensure your department is equipped to meet these challenges, your hardware must be able to scale to meet your evolving needs. Old hardware servers have limited capabilities and increasing capacity can mean making costly hardware purchases.

By moving to the cloud, you can ensure that your department’s technology is equipped to grow and change with you. The cloud’s inherent scalability provides valuable agility and flexibility. When the needs of your constituents change, so can your system.

---

**For more information, visit [tylertech.com/cloud](https://tylertech.com/cloud) or contact us at [info@tylertech.com](mailto:info@tylertech.com).**

<sup>1</sup> 2021 Internet Crime Report. Federal Bureau of Investigation Internet Crime Complaint Center (IC3). March 2022. [https://www.ic3.gov/Media/PDF/AnnualReport/2021\\_IC3Report.pdf](https://www.ic3.gov/Media/PDF/AnnualReport/2021_IC3Report.pdf)

<sup>2</sup> Organizational cyber maturity: A survey of industries. McKinsey & Company. August 4, 2021. <https://www.mckinsey.com/capabilities/risk-and-resilience/our-insights/organizational-cyber-maturity-a-survey-of-industries>