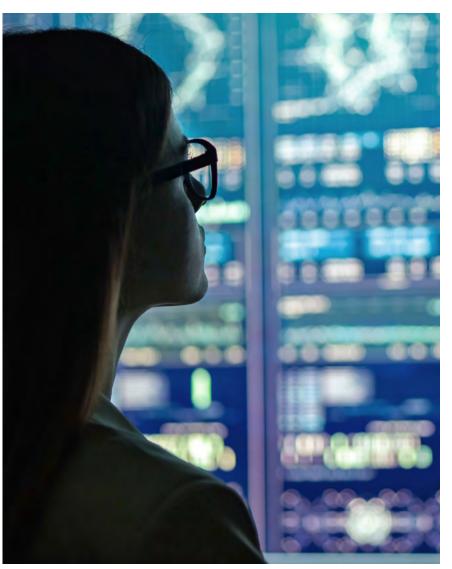![Microsoft](Microsoft logo)

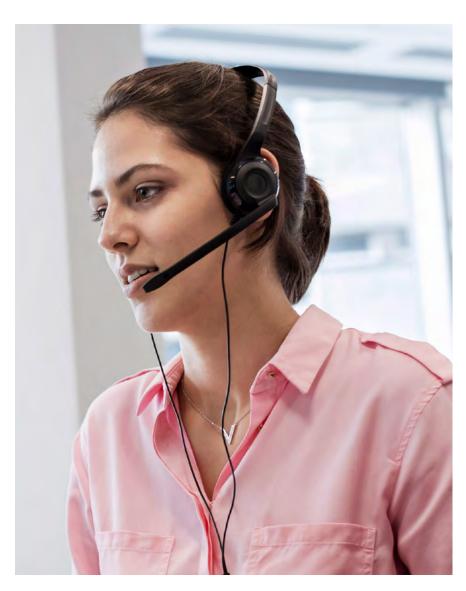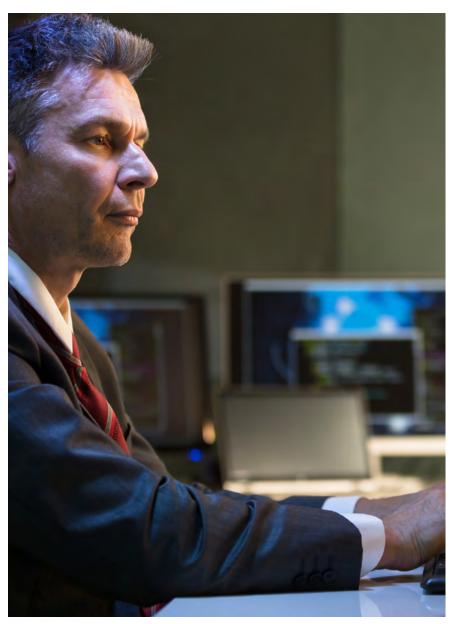# Building Trust with Secure Services

Modern datacenters

This information is for government leaders who:

- Recognize the pressure to provide more secure public services to residents and want to understand what this means for modern datacenters.

- Are planning a strategic digital transformation initiative and want to ensure all aspects are considered.
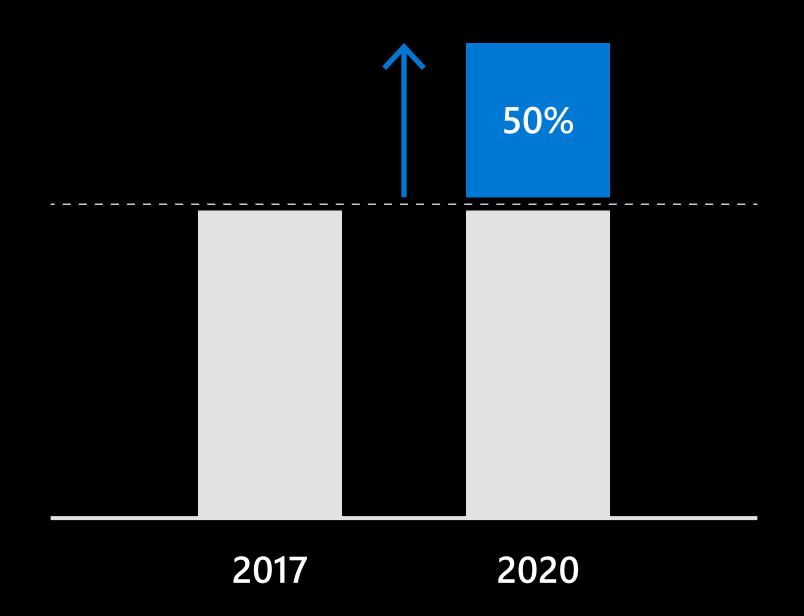
Rebuilding trust

As technologies evolve and people encounter more and more innovation in their everyday lives, they begin to expect more from government services as well. Yes, they want services to be easily accessible. But they also expect privacy and security on all levels, from basic data like name and address, to tax records or health information. And because governments handle extremely sensitive personal information such as tax filings, expectations for privacy in the context of government services is often higher than those for the private sector.
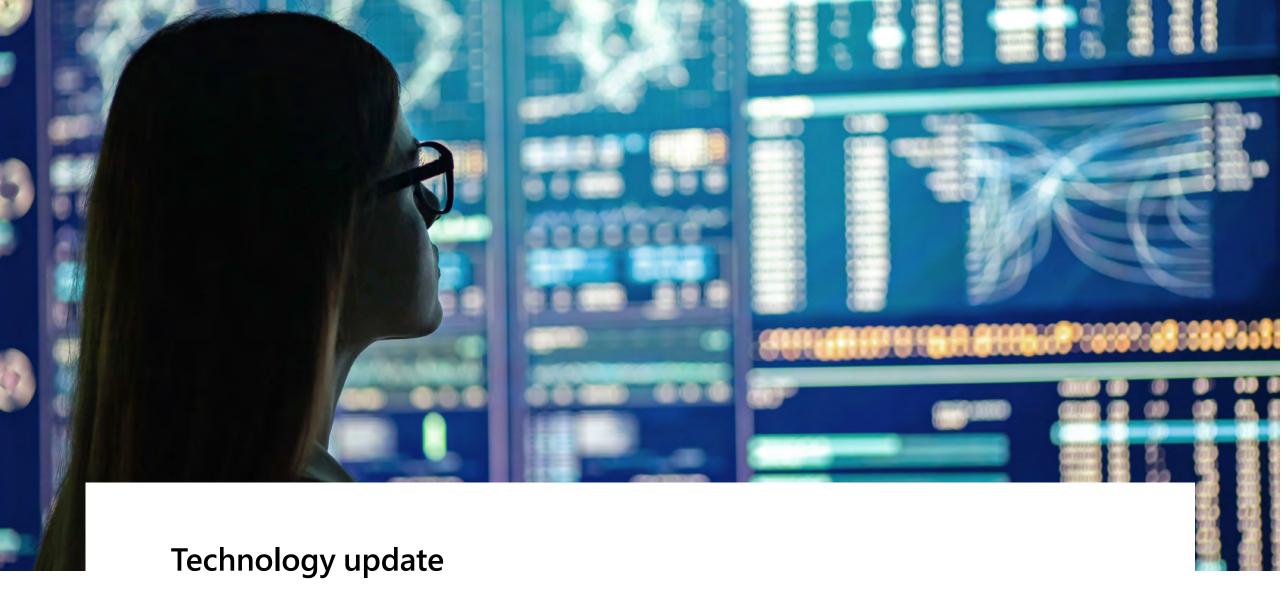
Meeting that expectation gives governments an opportunity to deliver trusted and secure services even as they face an increase in cybersecurity threats. Governments have an opportunity to transform systems and processes to meet the needs of their communities while combating cybercrime.

In this e-book we'll identify six specific technology updates with the most potential to deliver trusted and secure services.[1]

50%

2017   2020

Cyberattacks on state, local, tribal, and territorial governments increased 50% from 2017 to 2020.[1]

[1] GCN, "Cyberattacks on state, local government up 50%," September 2020.

Technology update

Modern datacenters

Providing trusted and secure services for the public begins with consolidating data in modern datacenters. To run programs and provide services to people effectively, governments all over the world must maintain vast amounts of information. This data includes birth records, addresses, income levels, and much more. As storage capabilities have modernized, many governments have been unable to take advantage of more flexible, automated systems because of budget or process constraints. Using legacy systems for data storage limits the usefulness of the data because it's stored in a way that prevents easy visibility or integration with other systems.

Moving to a modern datacenter in the cloud gives governments the infrastructure for a flexible digital environment with better security, protection, and compliance—wherever they are in the process of digital transformation.

| 65% of global GDP will be digitalized by 2022.[2]

Modern datacenters help governments deliver trusted and secure services by:

✅ **Laying the foundation**

Digital transformation is a multiphase, multistep process, but it starts with a strategic plan to create flexibility for technology growth and expansion. This accommodates the unpredictable nature of budgeting and planning around unforeseeable events, while continuing to lay the foundation for digital transformation. New business models in tandem with key technology solutions give governments scalability, flexibility, and extensibility for the future. Near-term planning for modern datacenters might mean being able to connect data sources for services such as transportation, utilities, and public safety for better monitoring and more efficiency. In the long-term, moving government services to the cloud, with public-friendly interfaces, can transform how they operate and help serve people more effectively.

✅ **Reducing complexity**

Aging infrastructure contains critical systems but working with those systems often involves challenging processes that are also time-consuming to manage. With a modern datacenter, governments can move to a hybrid system where old and new live side by side, aligning technology and processes for more efficiency. Modern datacenters also relieve a significant amount of the burden for compliance with security and privacy laws through automation, and their self-service capabilities put less demand on IT teams.

---

[2] IDC, "2021 Worldwide Digital Transformation Predictions," October 2020.
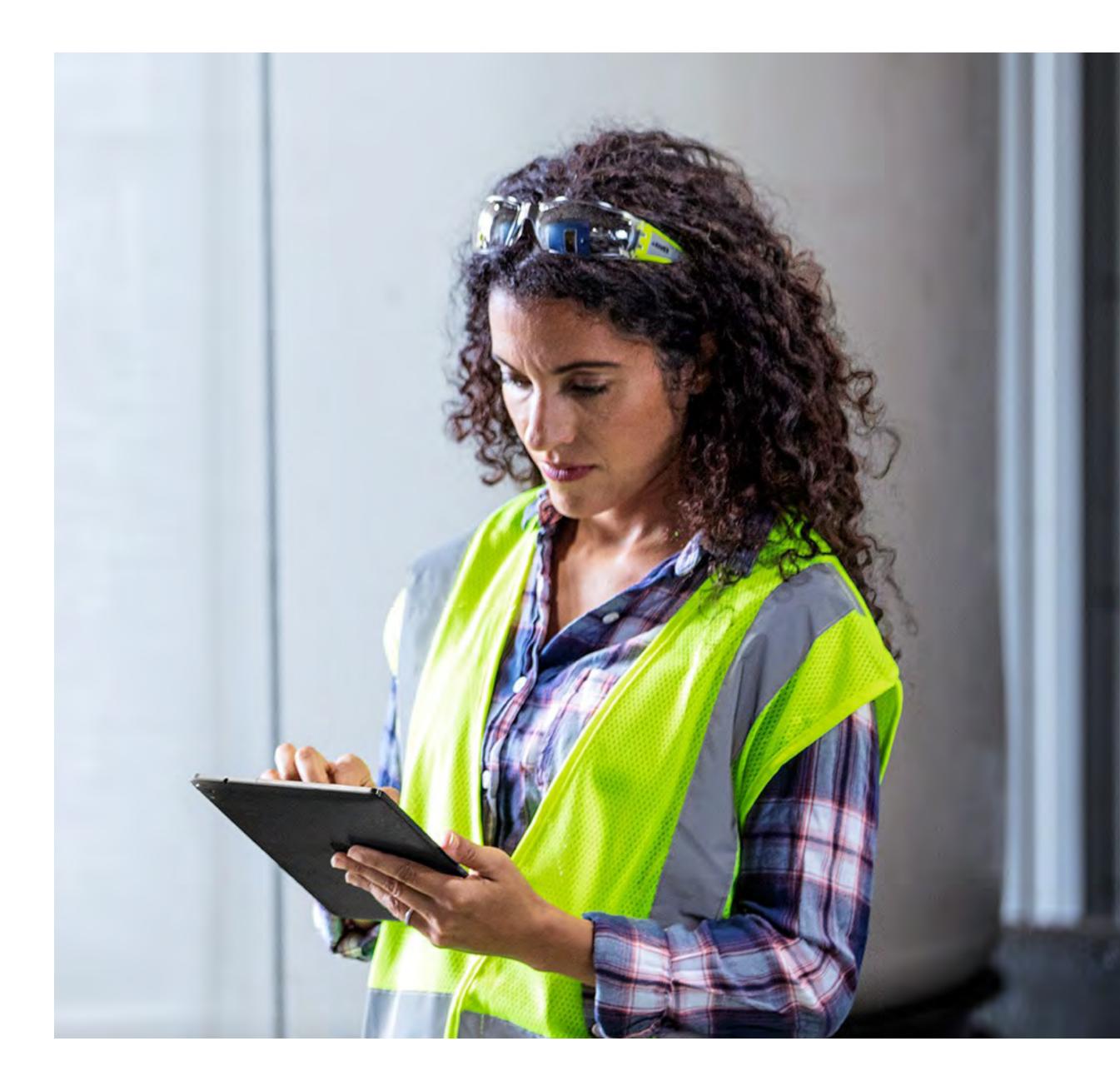
Customer story

DC Water cuts costs, streamlines processes, improves customer support with tech implementation

Spurred by the pandemic, DC Water in Washington, DC, continued to migrate most of its applications and workforce systems to the cloud, even as the agency adjusted to working remotely while fulfilling utility customer requests. The agency now runs nearly 100 percent of its apps and IT systems in the cloud, minimizing the need for paper tracking, in-person interaction, and managing multiple inflexible technology systems. In addition, the utility is using Microsoft's cloud and artificial intelligence technologies to conduct predictive analytics on the water distribution system, fast becoming a "digital utility." DC Water has saved USD 1.2 million in software costs and expects to save over USD 1 million in its capital budget from 2019 to 2023—all as a result of their Microsoft partnership.

> The implementation of Azure Sentinel as well as other Microsoft security products, such as Defender Advanced Threat Detection, Identity Protection, and Cloud App Security provide the cyber team the ability to monitor, analyze, detect, and respond to cyber events of interest."

Nelson Sims
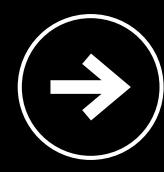Senior Advisor of Information Security,
DC Water

Getting started

What it means to deliver trusted and secure public services is changing. Technology is accelerating expectations for the public, while increasing cyber risk. A shift to trusted and secure services built on a foundation of Microsoft solutions, starting with modern datacenters, will move government transformation initiatives forward.

With a global partner ecosystem, Microsoft stands ready to help governments everywhere modernize legacy systems, enhance cyber-resilience, and create a secure and compliant foundation for the future.

Get the full e-book >

Learn more >

Microsoft