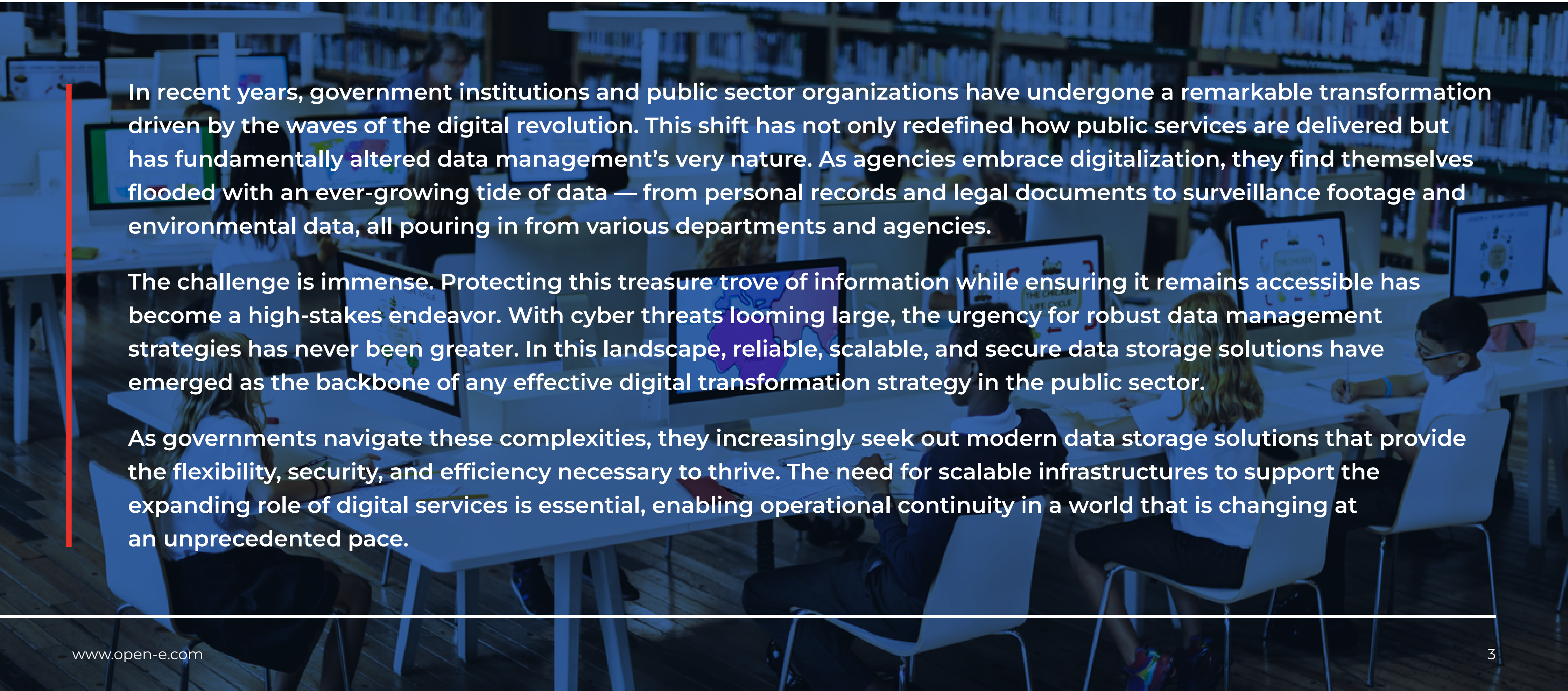
DATA STORAGE FOR GOVERNMENT & PUBLIC SECTOR with Open-E JovianDSS

Table of Contents

Digital Transformation **in Government & Public Sector**



In recent years, government institutions and public sector organizations have undergone a remarkable transformation driven by the waves of the digital revolution. This shift has not only redefined how public services are delivered but has fundamentally altered data management's very nature. As agencies embrace digitalization, they find themselves flooded with an ever-growing tide of data — from personal records and legal documents to surveillance footage and environmental data, all pouring in from various departments and agencies.

The challenge is immense. Protecting this treasure trove of information while ensuring it remains accessible has become a high-stakes endeavor. With cyber threats looming large, the urgency for robust data management strategies has never been greater. In this landscape, reliable, scalable, and secure data storage solutions have emerged as the backbone of any effective digital transformation strategy in the public sector.

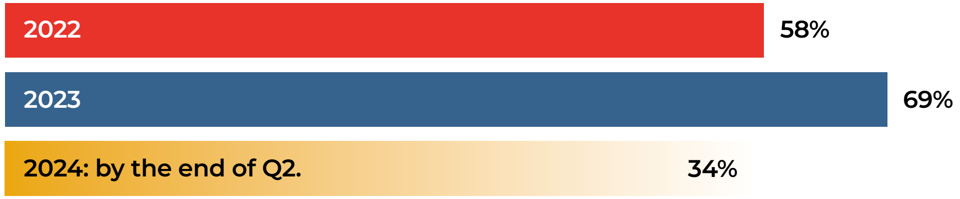
As governments navigate these complexities, they increasingly seek out modern data storage solutions that provide the flexibility, security, and efficiency necessary to thrive. The need for scalable infrastructures to support the expanding role of digital services is essential, enabling operational continuity in a world that is changing at an unprecedented pace.

Data Storage Statistics in Government & Public Sector

Here are some statistics about digitalization issues and data storage usage by the government & public:

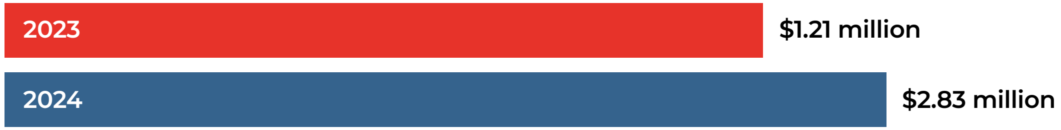
Ransomware Attack Rates in the US

State and local government organizations hit by ransomware



Recovery Costs Worldwide

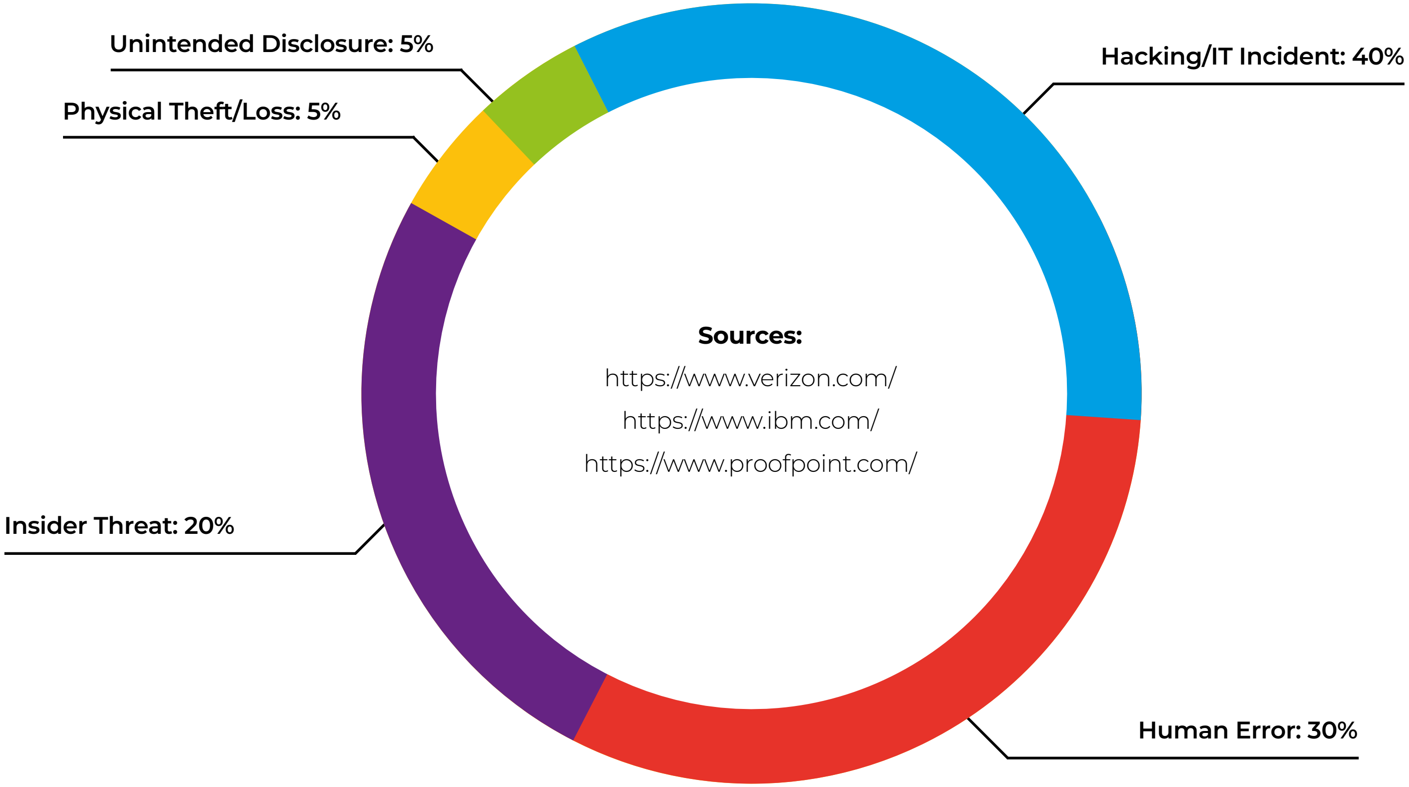
The mean cost to recover from a ransomware attack



Public Sector Cyber Threats

- **2023:** 15% of all successful attacks on organizations related to the public sector. Malware, including remote access trojans and spyware, was the most common method.
- **2024:** 68% of successful attacks on government institutions in the first half of 2024 were made by malware. The use of advanced threats like APT groups and credential-compromising methods also persists.

Data Storage Incident Types



Sources:
https://www.verizon.com/
https://www.ibm.com/
https://www.proofpoint.com/

Rise of Digitalization in Government & Public Sector

As the world rapidly embraces digital technology, government and public sector organizations find themselves at a crossroads. The urgent transformation to digitized environments not only highlights the necessity for modern IT infrastructure but also underscores the critical need for efficient data management and robust security measures. In this evolving landscape, digitalization is not just a trend; it's the key to enhancing service delivery and fostering transparency in public engagement.

Increasing Demand for Online Services

Citizens and businesses now expect fast, seamless, and secure online access to government services. From tax filings and public records to healthcare services and legal processes, digital platforms have become essential for efficient public service delivery. This demand for accessible, always-on services has required governments to modernize their IT infrastructure, ensuring that data is readily available, secure, and efficiently managed.

Pandemic-Driven Changes

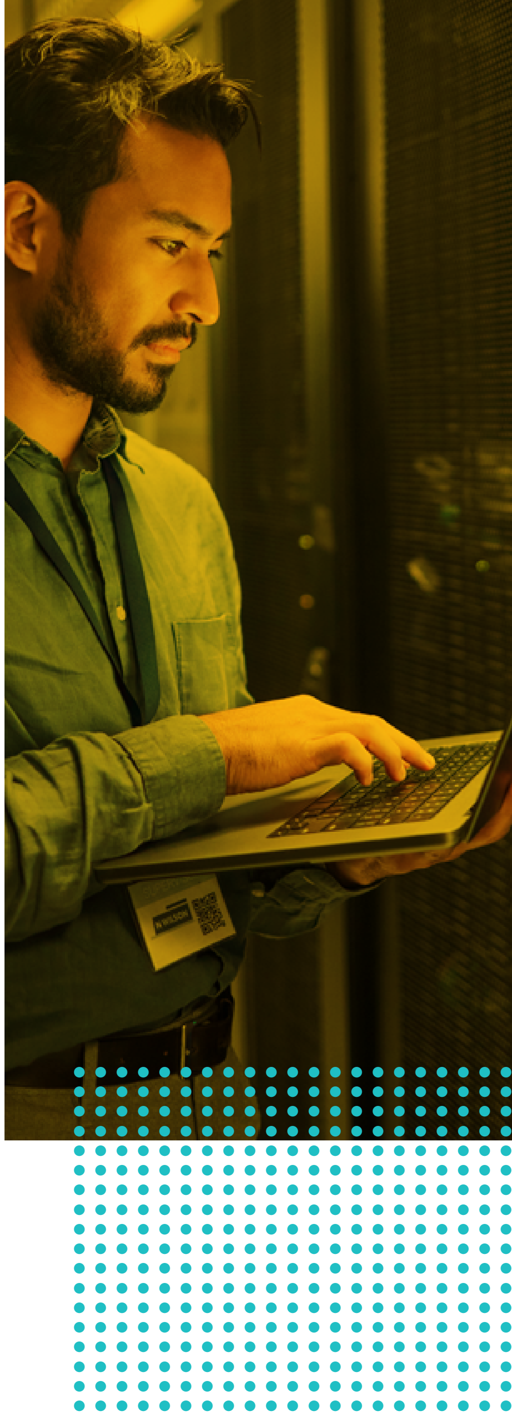
The COVID-19 pandemic catalyzed digital transformation across all sectors, including government. Lockdowns and social distancing measures made it impossible to rely solely on physical, in-person services. Governments around the world were forced to rapidly shift to online models, enabling employees to work remotely and citizens to access services digitally. This shift dramatically increased the volume of data being created, shared, and stored, making robust and scalable data storage solutions more critical than ever.

The Need for Modern Infrastructure

As digitalization continues to expand, legacy systems can no longer keep up with the demands of modern data management. Older data storage solutions are often inefficient, difficult to scale, and lack the robust security measures needed to protect against today's cyber threats. Modernizing infrastructure—particularly around data storage—has become a priority for governments looking to enhance their operational efficiency, reduce costs, and improve the quality of public services.

The Impact of Digitalization on the Public Sector

Digitalization has revolutionized how government institutions and public sector organizations operate. By replacing paper-based processes with electronic systems, digitalization has greatly improved workflow, made data more accessible, and enhanced transparency in public services.



Improved Workflow

Digitalization streamlines complex government processes that previously relied on manual paperwork and in-person interactions. With digital systems in place, tasks such as processing applications, managing citizen records, or issuing licenses are automated, significantly reducing the time and effort required. This results in faster service delivery, fewer errors, and more efficient resource allocation.

Enhanced Accessibility

Citizens now can access public services online anytime, from anywhere. Whether it's paying taxes, renewing a driver's license, applying for permits, or accessing healthcare services, digital platforms have made government services more accessible to the public. This increased accessibility is particularly beneficial for individuals in remote areas or those with limited mobility, ensuring everyone can engage with government services without physical barriers.

Increased Transparency

Digitalization also improves transparency by allowing citizens to track the progress of their requests, access public data, and engage in government processes more easily. Digital records and databases provide clear audit trails, ensuring accountability and reducing opportunities for corruption or errors. This fosters greater trust between governments and their constituents.

Enhanced Laws, Regulations, and Safety

Well-structured and accessible data storage supports regulatory compliance and public safety by preserving evidence and documentation. Analysis of stored data can help identify areas where new laws are needed or where existing laws should be revised. For instance, data from public safety, transportation, and emergency response sectors can guide updates in safety regulations, contributing to community well-being and security.

Data Analysis

With robust data storage solutions, institutions can efficiently collect and retain vast amounts of historical and real-time data, facilitating deep analysis of trends, patterns, and correlations. It enables making informed, data-driven decisions across areas like public health, crime prevention, and resource allocation, using insights derived from crime reports, healthcare records, and economic indicators. Access to well-organized, up-to-date data allows governments to quickly respond to challenges, from setting public health policies to optimizing disaster response, ultimately improving services and aligning resources to meet citizens' needs better.

Improved Insights into Social Problems

Reliable and scalable data storage facilitates the accumulation of large datasets from multiple sources, including law enforcement, healthcare, education, and public services. Analyzing these datasets helps governments understand complex social issues, such as poverty, crime, and education gaps. With better insights into the root causes and dynamics of these issues, governments can design and implement more effective policies and interventions.

Key Data Storage Challenges in Government & Public Sector

As governments and public sector organizations embark on their digital transformation journeys, they encounter a series of tremendous data storage challenges that threaten their ability to deliver essential services. Picture a bustling agency juggling an overwhelming volume of data—from personal records to vital public information—while grappling with the need to protect sensitive information against ever-evolving cyber threats. In this high-stakes environment, the quest for cost-efficiency and operational continuity becomes paramount. Without robust, scalable, and secure storage solutions, these institutions risk falling short of their mission. Successfully navigating these challenges is not just about improving efficiency; it's about earning public trust and ensuring compliance with rigorous regulatory standards.

Protection Against Attacks on Voting Processes

To protect the voting process from attacks, storage systems incorporate disaster recovery and data replication. During ransomware or DDoS attacks, these systems minimize downtime, allowing rapid recovery from secure backups to keep operations running. Replicating data across multiple locations ensures that election-related data remains accessible even if a primary data center is compromised, supporting continuous voting operations in critical scenarios. Moreover, compliance with security standards like FISMA and FedRAMP provides an additional layer of defense against cyber threats.

Countering Misinformation

Effective data storage also helps counter misinformation in government and public sectors. Solutions with robust metadata tracking verify data sources, which supports the authenticity of information shared within agencies and helps reduce the spread of misinformation. Advanced storage systems equipped with AI-driven analytics can monitor data patterns to detect and mitigate abnormal content associated with misinformation campaigns. Additionally, stringent data security protocols and structured silos protect sensitive information from unauthorized access, reducing the likelihood of leaks or distortions that might fuel misinformation.

Enhanced Transparency and Public Trust

Finally, secure data storage enhances transparency and public trust. Storage solutions that support public data-sharing platforms allow real-time access to accurate information, like verified election results, which limits the effectiveness of deceptive narratives. Blockchain-based or immutable storage methods add further transparency by maintaining a tamper-resistant history of all data interactions, promoting public confidence in the authenticity of government records. Together, these storage measures fortify data reliability, security, and accessibility, essential for protecting against external influence and misinformation in public sectors.

Storing Vast Amounts of Data

Government and public sector organizations must manage vast amounts of data, including citizen records, legal documents, and digital services, with scalable storage solutions that support growth and regulatory compliance. At the same time, they must protect sensitive information like personal data and classified documents from cyber threats and breaches, making robust encryption, access controls, and continuous security monitoring essential. Rising ransomware risks and the demand for secure data sovereignty further heighten these challenges.

Achieving Cost-Efficiency

Public sector organizations often operate within constrained budgets, necessitating data storage solutions that balance affordability with high performance, security, and scalability. Cost efficiency must be achieved through technologies like data deduplication, compression, and flexible hardware choices that reduce overall expenses without sacrificing reliability.

Ensuring Continuity and Disaster Recovery

Government services require continuous uptime and reliable access to data, meaning that any disruptions - whether from cyberattacks, natural disasters, or system failures - can have widespread, critical impacts. Ensuring continuity demands advanced disaster recovery plans, high availability configurations, and automated, regular backups to minimize downtime and guarantee rapid data recovery when needed.

Data Storage Management in Government & Public Sector

Data storage security transcends mere compliance in government and public sector institutions; it is a cornerstone of public trust. These organizations are custodians of a vast array of sensitive information, including personal records, health data, and national security details. The responsibility of safeguarding this data weighs heavily on those in charge, as their decisions must not only ensure its protection but also align with an intricate framework of national and international regulations.

As we explore the critical security requirements and legislative measures that govern data storage in the public sector, we reveal the essential actions these institutions undertake to maintain transparency and accountability in their data management practices.

Relevant Legislation Governing Data Storage

As data privacy concerns intensify, government and public sector organizations face the challenge of navigating a complex array of data protection regulations. These laws are crucial for safeguarding personal and sensitive information and establishing stringent standards for data collection, storage, and processing. Compliance with these regulations is not just a legal obligation; it is essential for maintaining public trust and ensuring the responsible management of data. Understanding the relevant legislation, including prominent regulations such as the General Data Protection Regulation (GDPR) and the Health Insurance Portability and Accountability Act (HIPAA), is vital for public entities as they work to protect data and avoid the significant repercussions of non-compliance.

§ General Data Protection Regulation (GDPR) - European Union

GDPR is one of the most comprehensive data protection laws globally governing how personal data is collected, stored, and processed. Public sector organizations in the EU must comply with GDPR requirements, which include ensuring the secure storage of personal data, using encryption, and reporting breaches within strict timeframes. Non-compliance can lead to severe fines.

§ Health Insurance Portability and Accountability Act (HIPAA) - United States

While HIPAA primarily governs healthcare organizations, it is also relevant for public health departments and government agencies involved in healthcare services. HIPAA mandates strict security measures to protect sensitive health information, including secure storage, encryption, access control, and regular auditing of data handling practices.

§ Federal Information Security Management Act (FISMA) - United States

FISMA requires U.S. federal agencies to implement comprehensive data security programs to protect government information systems. This includes implementing security controls such as data encryption, intrusion detection, continuous monitoring, and regular risk assessments to ensure compliance with federal standards like NIST’s SP 800-53 guidelines.

§ Public Services Network (PSN) Compliance - United Kingdom

The PSN is a government network that enables secure data exchange between UK public sector organizations. To use the PSN, organizations must comply with stringent security protocols, including the secure storage of data, encryption, and robust access control measures. Annual compliance checks are mandatory to ensure continued security adherence.

§ Cloud Act - United States

The CLOUD (Clarifying Lawful Overseas Use of Data) Act requires U.S. technology companies to provide data stored on their servers to law enforcement agencies, even if it is stored overseas. This legislation affects how data storage services handle requests for government data, particularly in cloud environments. Government agencies must consider where their data is stored and how it might be affected by international laws.

§ Local Data Protection Laws and National Security Requirements

Many countries have their own data protection laws and national security regulations that dictate how government data must be stored and protected. For instance, the Germany’s Federal Data Protection Act (BDSG) and France’s CNIL regulations enforce strict rules on the handling of personal data by public sector organizations. These laws often impose requirements related to encryption, data retention, and breach notification.

§ Network and Information Systems (NIS-2) Directive - European Union

The NIS-2 Directive enhances cybersecurity standards across key sectors, including government and public services, to ensure data system resilience. It requires risk management measures, rapid incident reporting within 24 hours, and secure data storage protocols like encryption and access control. The directive broadens its reach to cover more entities, with strict compliance and heavy penalties for breaches, underscoring the need for robust cybersecurity practices.

Key Data Storage Security Requirements

In government and public sector institutions, data storage security is essential for maintaining public trust. These organizations handle sensitive information, including personal records, health data, and national security details, making secure management critical. They must not only protect this data but also comply with complex regulations. As we explore key security measures and legal frameworks, we see how these institutions ensure transparency and accountability while safeguarding valuable information.

→ Access Control and Identity Management

Strict access control mechanisms are crucial to ensuring that only authorized personnel can access sensitive data. Role-based access control (RBAC) and multi-factor authentication (MFA) help limit access to confidential information. Detailed logging and monitoring of access activity are also required for auditing purposes and tracking potential security breaches.

→ Data Integrity

Ensuring data integrity is critical, as corruption or tampering with records can lead to catastrophic results in governance. Technologies like data checksumming, error detection, and automatic data repair mechanisms (such as those found in ZFS-based systems like Open-E JovianDSS) help prevent data corruption.

→ Backup and Disaster Recovery

Government institutions must have comprehensive backup strategies and disaster recovery plans in place. This includes regular, automated backups of data both on-site and off-site to mitigate the effects of data loss due to cyberattacks, natural disasters, or human error. Government standards often require that data can be quickly restored in the event of a disaster.

→ Data Encryption

Encryption is a fundamental requirement for protecting sensitive government data, both at rest and in transit. This ensures that even if unauthorized access occurs, the data remains unreadable and unusable without the correct decryption keys. Government agencies are often required to use strong encryption standards to safeguard information.

→ Ransomware Protection

Governments are frequently targeted by ransomware attacks, which can disrupt essential services and compromise sensitive data. Ransomware protection strategies include creating immutable backups, regularly updating software to close vulnerabilities, and employing intrusion detection systems that alert administrators to suspicious activities.

Secure Government & Public Sector Data Storage with Open-E JovianDSS!

The Trusted Solution for 2025 and Beyond

open-e JovianDSS

Trusted Solution for 2025 and Beyond

Secure your government and public sector data with Open-E JovianDSS. This cutting-edge storage technology meets strict regulatory requirements, delivering optimized, scalable, and protected data management — without vendor lock-in and at a lower cost.

Safeguard National and Public Data Integrity

Protect mission-critical information across government, judicial, and defense sectors. Open-E JovianDSS ensures secure, seamless scalability and prepares your infrastructure for the future.

Why Government and Public Sector Leaders Choose Open-E JovianDSS:

→ **Compliance-Ready Encryption**
With Self-Encrypting Drives (SEDs), Open-E JovianDSS protects sensitive government data, maintaining strict compliance with data storage protection standards.

→ **Reliable Business Continuity & Disaster Recovery**
Government institutions can't afford downtime. Open-E JovianDSS offers High-Availability Clusters and On- & Off-site Data Protection, ensuring data accessibility even during cyber attacks or system failures.

→ **Seamless Scalability for Growing Public Data Storage Needs**
Open-E JovianDSS's hardware- and hypervisor-agnostic technologies expand your infrastructure as demands increase, providing unmatched flexibility and performance.

→ **Snapshot Technology to Guard Against Cyber Attack Consequences**
Instantly capture and secure your data storage with snapshots. In case of a ransomware attack, simply roll back to a clean state. No ransom, no downtime.

→ **Budget-Friendly Storage Optimization**
Open-E JovianDSS allows for cutting costs without sacrificing performance or security. Take advantage of storage efficiency features like deduplication and customizable retention plans.

Extension licence
open-e JovianDSS
#1 Software for Data Storag
Backup & Business Continu
Product key
open-e JovianDSS
#1 Software for Data Storage, Backup & Business Continuity

Discover how Open-E JovianDSS **enhances your government data security and resilience**!

Scan the QR code or visit open-e.com to learn more and schedule a demo.

Secure your infrastructure with the trusted choice in public sector data storage — Open-E JovianDSS!

Open-E Solutions Addressing Data Storage Challenges

As government and public sector organizations embrace digital transformation, they encounter increasing challenges in managing and securing vast amounts of data. The need for reliable and efficient data storage solutions has never been more critical as these entities strive to enhance service delivery, ensure compliance with regulatory standards, and protect sensitive information. With the growing demands for accessibility, scalability, and security, these organizations must adopt modern data management strategies to support their evolving needs while maintaining operational continuity.

Here is how Open-E JovianDSS provides a robust response to these challenges by offering tailored storage solutions that prioritize data integrity and accessibility, enabling government institutions to navigate the complexities of digital data management effectively. By implementing such solutions, public sector organizations can not only safeguard sensitive data but also streamline workflows, ultimately enhancing their responsiveness to constituents' needs.

Compliance and Data Sovereignty

Open-E JovianDSS ensures compliance with global and national regulations regarding data protection. The system supports disk encryption, access control, and secure data replication, allowing institutions to meet data sovereignty requirements by ensuring sensitive data is stored within national borders or specific geographic locations.

✓ **Example of Use in Government & Public Sector**

A national government agency uses Open-E JovianDSS to store classified information on a private cloud infrastructure located within national borders, ensuring compliance with data sovereignty regulations.

Cost Efficiency

Open-E JovianDSS is designed to be a cost-effective storage solution for government and public sector organizations that optimizes resource usage and reduces overall operational costs. Key elements contributing to its cost efficiency include:

- **Virtualization:** By supporting various virtualization platforms (e.g., VMware, Microsoft Hyper-V, Proxmox), Open-E JovianDSS allows organizations to consolidate their IT infrastructure. This means multiple virtual machines can run on a single physical server, reducing the need for extensive hardware investments. Virtualization also simplifies resource allocation, enabling organizations to scale their infrastructure dynamically based on demand without incurring significant additional costs.

- **Hypervisor-Agnosticism:** Open-E JovianDSS is hypervisor-agnostic, meaning it can seamlessly integrate with any virtualization platform. This flexibility allows organizations to choose the hypervisor that best meets their specific needs without being locked into a single vendor's ecosystem. By eliminating hypervisor constraints, organizations can leverage their existing investments in virtualization technology, ensuring optimal resource utilization and cost savings.

- **Hardware Agnosticism:** The software's hardware-agnostic nature allows it to work with a wide range of hardware configurations, from standard x86 servers to specialized storage appliances. This flexibility means organizations can utilize their existing hardware or choose cost-effective options tailored to their budgets. By avoiding proprietary hardware requirements, organizations can benefit from competitive pricing and longer lifecycle management of their assets.

✓ **Example of Use in Government & Public Sector**

A city government could use Open-E JovianDSS to create a virtualized data center, reducing hardware costs and energy expenses. Its hypervisor- and hardware-agnostic features enable infrastructure adaptability, maximizing existing resources and avoiding vendor lock-in.

Scalability

Open-E JovianDSS uses the ZFS file system, designed for large-scale data management. It offers near-unlimited scalability, allowing institutions to store massive datasets without performance degradation. The system can easily expand data storage capacity by adding new disks without downtime, making it ideal for organizations dealing with increasing data volumes over time.

✓ **Example of Use in Government & Public Sector**

A national archive can manage decades of records, from birth certificates and tax filings to environmental data, ensuring quick access and real-time updates without the need for constant infrastructure upgrades.

Data Security and Integrity

Open-E JovianDSS is built to deliver comprehensive, enterprise-grade protection for sensitive and mission-critical information. It addresses the complex demands of data security and integrity in the government and public sector by offering a scalable and resilient storage solution. Designed to meet strict compliance and regulatory requirements, Open-E JovianDSS enables organizations to safeguard vast amounts of critical data while ensuring restricted but continuous access and great performance.

- **SEDs:** Supporting self-encrypting disks ensures data is secured at rest, meeting stringent regulatory standards.
- **ZFS Technology:** The system incorporates end-to-end checksumming to automatically detect and correct data corruption, preserving the integrity of critical records.
- **RBAC:** Role-based access control restricts access to authorized personnel, while comprehensive logging enhances security monitoring and accountability.
- **Open-E High-Availability Clusters and Open-E On- & Off-Site Data Protection:** With these features, public sector organizations can maintain continuous access to vital information and implement reliable recovery solutions, reinforcing their commitment to data security in a dynamic digital landscape.

✓ **Example of Use in Government & Public Sector**

Health departments store and manage sensitive medical records with encryption, ensuring that patient data remains secure and uncorrupted, thus complying with data protection regulations like HIPAA.

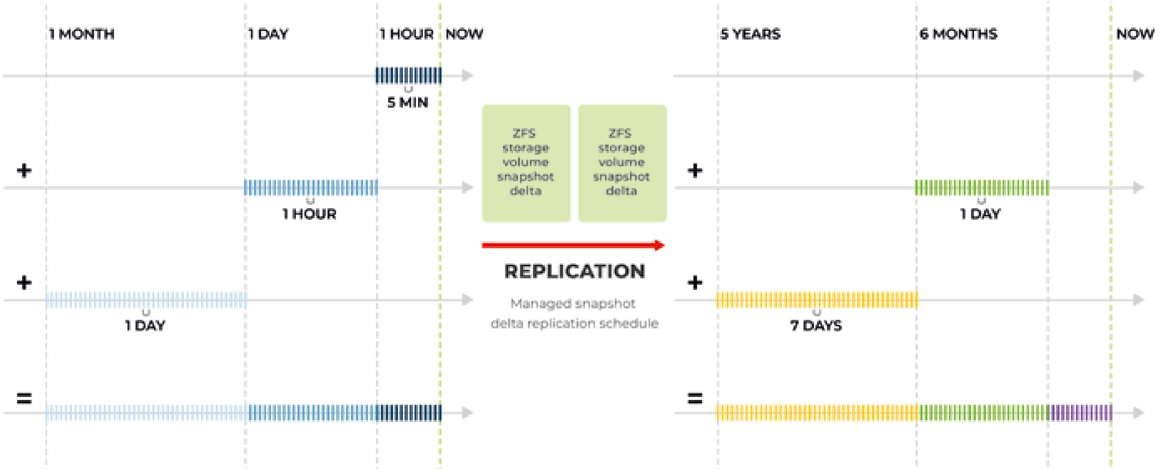
Snapshots and Retention Plans

- **Snapshots:** Snapshots in ZFS are read-only copies of the file system at a specific point in time. They are created quickly and efficiently, allowing users to capture the current state of data without requiring significant additional storage space. This capability enables organizations to recover quickly from accidental deletions, data corruption, ransomware attacks, or other issues by reverting to a previous system state from a snapshot.
- **Retention plans:** Retention plans leverage snapshots to manage the lifecycle of data by defining how long snapshots should be kept before they are automatically deleted. This allows organizations to maintain a structured approach to data retention, ensuring that necessary data is available for compliance, audits, or recovery while efficiently managing storage resources. By setting clear retention policies, organizations can balance data accessibility with storage efficiency, mitigating risks associated with data loss and regulatory compliance.

✓ **Example of Use in Government & Public Sector**

The department can create read-only copies of sensitive patient records at regular intervals by utilizing snapshots. If an error such as a data entry mistake or a cyberattack occurs, the department can quickly revert to the last known good snapshot, ensuring minimal service disruption and safeguarding sensitive information.

A public sector agency responsible for environmental monitoring implements retention plans to manage the lifecycle of their data. By establishing policies that dictate how long snapshots of environmental data should be retained, the agency ensures compliance with regulatory requirements. For instance, they might keep snapshots for five years to align with audit protocols while automatically deleting older versions. This structured approach not only helps maintain essential data for compliance and research purposes but also optimizes storage costs by managing space effectively.

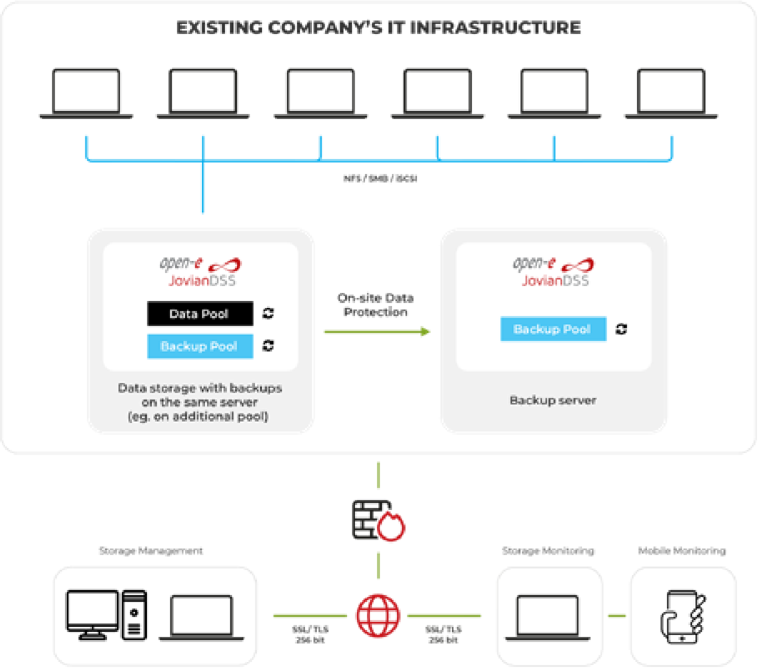

1 MONTH
1 DAY
1 HOUR
NOW
5 MIN
+
1 HOUR
+
1 DAY
=
ZFS storage volume snapshot delta
ZFS storage volume snapshot delta
REPLICATION
Managed snapshot delta replication schedule
5 YEARS
6 MONTHS
NOW
+
1 DAY
+
7 DAYS
=

High-Availability Cluster

Open-E JovianDSS offers high availability (HA) cluster configurations, where multiple storage nodes work together to provide continuous data access. If one node experiences a failure, the other node takes over seamlessly, eliminating single points of failure. This ensures constant uptime and service availability, making HA crucial for mission-critical public sector operations where any downtime could impact essential services.

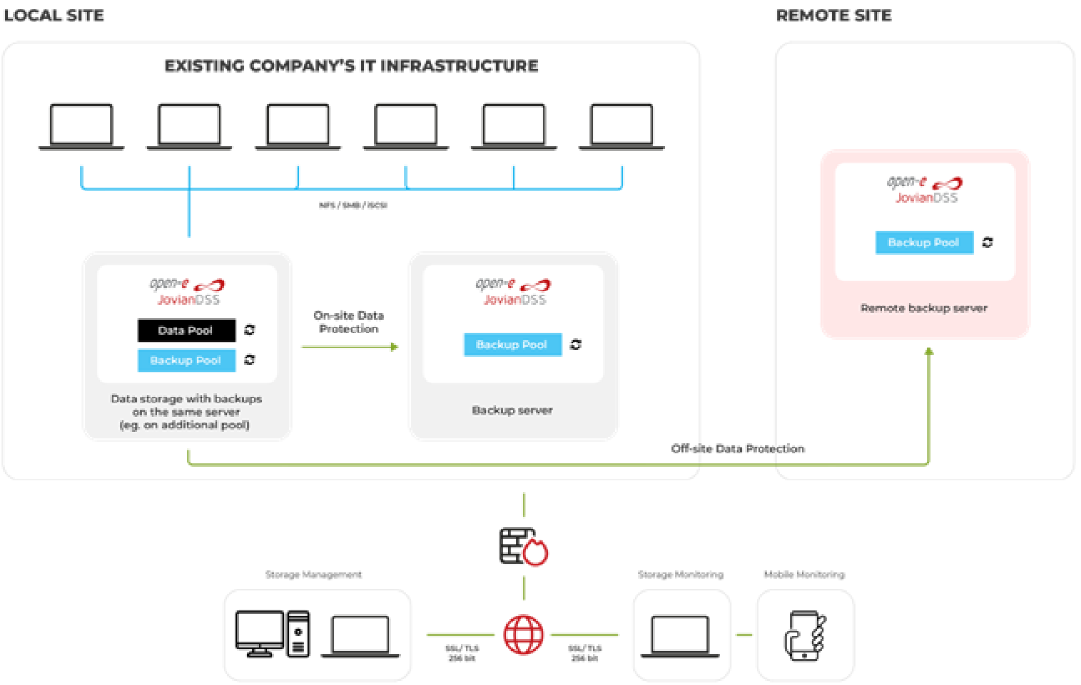
✓ **Example of Use in Government & Public Sector**

City emergency services use an HA cluster to ensure their critical communication systems and databases remain operational 24/7, even during server hardware failures or maintenance periods.



On-Site and Off-Site Data Protection

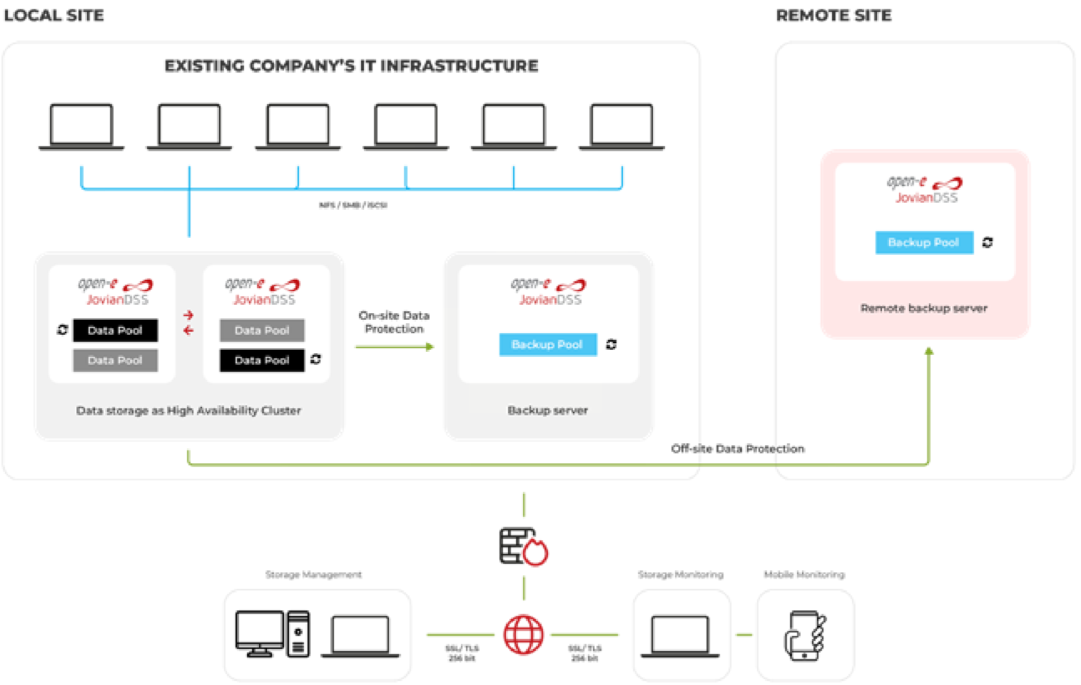
Open-E JovianDSS supports both on-site and off-site data backups, providing robust disaster recovery solutions. Institutions can schedule regular, local backups for instant access and fast restoration, as well as use off-site replication to protect against localized disasters like fires, floods, or cyberattacks. This guarantees critical data remains intact and accessible, even if the primary data center is compromised.



- ✓ **Example of Use in Government & Public Sector**
  A transportation agency replicates operational data to an off-site location, ensuring that in the event of a disaster, the organization can recover essential information from the remote site, preventing prolonged service disruption.

Maximum Data Protection

In government and public sector operations, data security and continuous availability are non-negotiable, especially when managing critical information like citizen records, sensitive patient data, public safety data, and national security files. Open-E JovianDSS meets these demands by integrating on- and off-site backup with high-availability clustering, ensuring seamless data protection without compromising uptime. This advanced setup combines local backups for quick recovery and remote replication to safeguard data against regional disasters, such as fires, floods, or cyberattacks, guaranteeing that essential data remains accessible even under extreme conditions.



✓ Example of Use in Government & Public Sector

Institutions like public health departments leverage the maximum data protection features of Open-E JovianDSS to manage sensitive patient data. By implementing regular integrity checks and creating frequent snapshots, the department can quickly restore data to a previous state in case of accidental deletions or ransomware incidents. This ensures compliance with data protection regulations while safeguarding critical health information against threats.

Reliable Surveillance Data Storage Solutions with Open-E JovianDSS!

Future-Proof Your CCTV Infrastructure

Surveillance and security data have never been more crucial. With Open-E JovianDSS, you can confidently manage your growing data storage demands, powered by a data storage solution designed to efficiently handle high-resolution video and continuous recording. Dive into our comprehensive guide to discover tailored strategies for secure and scalable CCTV data storage!

Explore Optimal Data Storage Strategies:

Whether you need on-premises, cloud, or hybrid data storage, our brochure lists the best approaches to meet your organization's unique surveillance needs. As video quality advances and file sizes increase, Open-E JovianDSS ensures you have the technology to keep pace.

- → **Reliable and Efficient Storage Management**
  Ensure every frame of critical footage is preserved without interruption. Open-E JovianDSS optimizes your data storage capacity, keeping your data accessible and secure.
- → **Seamless Scalability for Expanding Needs**
  Adapt your data storage infrastructure effortlessly as your surveillance requirements grow, with no vendor restrictions holding you back.
- → **Instant Data Recovery with Snapshot Technology**
  Minimize data loss and downtime. Quickly restore your video archives using point-in-time snapshots to recover from any incident.
- → **Hybrid Solutions for Enhanced Security**
  Combine the best of the on-premises and cloud data storage strategies for a comprehensive data protection strategy. Open-E JovianDSS makes it simple to balance accessibility and security.

open-e JovianDSS

Empower Your Surveillance System with Expert Knowledge
Scan the QR code or visit open-e.com for **your free download!**

Examples of Government & Public Organizations

with Open-E Systems Implementations

Throughout its extensive implementation across government and public sector institutions, Open-E JovianDSS has proven to meet and exceed tight legislative requirements, establishing itself as a reliable solution for secure and efficient data storage management. Designed with flexibility in mind, Open-E JovianDSS supports hardware and hypervisor agnosticism, allowing institutions to optimize their data infrastructure while reducing operational costs — a critical factor in budget-conscious public sectors.

The software offers robust tools for data storage protection, scalability, and seamless management, enabling government and public entities to maintain business continuity and adapt as their data storage needs evolve. Additionally, the platform's support for compliance standards and ease of integration streamlines IT operations, ensuring secure, high-performance data storage solutions across various government and public-sector environments, such as:

Government Ministries/Departments

Local Government/ City Administrations

Judicial Institutions

Law Enforcement Agencies

Military Units

Educational Institutions

Historical and Cultural Organizations

Research and Scientific Institutions

Public Utilities and Services

Consumer Protection Authorities

Founded in 1998, Open-E is a well-established developer of IP-based storage management software. Its flagship product, Open-E JovianDSS, is a robust, award-winning storage application that offers excellent compatibility with industry standards. It is also the easiest to use and manage. Additionally, it is one of the most stable solutions on the market and an undisputed price-performance leader.

Thanks to its reputation, experience, and business reliability, Open-E has become the technology partner of choice for industry-leading IT companies. Open-E accounts for over 40,000 installations worldwide.

+40,000 software implementations

+120 countries worldwide

+25 years of experience

+800 certified engineers and sales professionals

Open-E, Inc. | +1 (678) 666 2880 (US) | +49 (89) 800 777 0 (Europe) | info@open-e.com