Data Security for EMEA and APAC Public Sector Organizations

Helping government and education sectors across EMEA and APAC protect data and recover from cyber threats

The Challenge

Public sector organizations across EMEA and APAC face mounting challenges in securing critical data and modernizing infrastructure while adhering to strict data sovereignty laws. The region has seen a significant rise in ransomware and cyberattacks:

- Ransomware attacks targeting APAC's critical infrastructure increased by **200%** in the last two years (INTERPOL, 2024[1]).
- Europe faces heightened risks from state-sponsored attacks, with **government services being the most targeted sector** in recent ENISA reports (ENISA Threat Landscape 2024).

Budget constraints, outdated systems, and IT talent shortages make recovery from attacks slow and costly. Legacy infrastructure hinders operational agility and compliance, particularly as public agencies transition to digital services.

To navigate this evolving landscape, agencies require a data protection strategy that is secure, scalable, compliant, and cost-effective.

The Solution

Druva's cloud-native cyber resilience platform provides an ideal solution for government and public institutions across EMEA and APAC. Operating fully as SaaS with no hardware, Druva delivers:

- **Ransomware protection and rapid recovery** with ML-powered anomaly detection, rollback, and malware filtering.
- **Data sovereignty and compliance readiness** with support for GDPR, DORA (EU), PDPA (Singapore), APPI (Japan), IRAP (Australia), and ISO 27001.
- **Unified cloud management** for SaaS apps, data centers, and end-user environments.
- **Up to 40% reduction in TCO** by eliminating storage silos, hardware refreshes, and hidden licensing fees.
- **FIPS-compliant customizable reporting,** advanced filtering, and flexible subscription and attachment options to streamline delivery and decision-making.

SaaS Apps   Cloud   Data Center   Edge

druva
Data Security Cloud

Data Protection   Cyber Resiliency   Sensitive Data Governance   Legal Hold/ e-Discovery

---

[1] Source: CYFIRMA's report, The Changing Cyber Threat Landscape Asia-Pacific (APAC) Region – Volume 1

Key Benefits of Druva GovCloud

1. Enhanced Cybersecurity

- **Immutable, Air-Gapped Backups**: Protect against unauthorized access and ensure recovery integrity in the event of an attack.
- **Zero-Trust Architecture**: Features like encryption, role-based access control, and multi-factor authentication offer an extra layer of defense.
- **ML-Powered Anomaly Detection**: Detect suspicious activity, such as unexpected file deletions, access, or restoration attempts, in real time.

2. Simplicity at Scale

Legacy systems often require specialized skills and time-consuming maintenance. Druva's fully managed SaaS solution operates without the need for complex infrastructure, helping public sector organizations focus on missions instead of maintenance.

- **No Hardware, No Complexity**: 100% cloud-native architecture eliminates the challenges of managing on-premises solutions.
- **Unified Management**: Control and monitor all data protection tasks through a single, centralized dashboard.
- **Pre-built Compliance**: Leverage pre-built templates for DORA, GDPR, IRAP, and more
- **API Integrations**: Extend insights to your existing security stack easily and efficiently.

3. Unmatched Cost Efficiency

Taxpayer-funded organizations operate on tight budgets, often spending the majority of their IT budgets maintaining aging infrastructure.

- **TCO Savings of up to 40%**: Streamline operations by consolidating disjointed backup solutions into one platform.
- **Intelligent Deduplication**: Optimize data storage to reduce costs without compromising resiliency.
- **Eliminate Hardware Refreshes**: Say goodbye to expensive equipment upgrades and licensing fees.
- **Avoid Paying Ransoms**: With fast, clean data recovery, organizations can sidestep ransom payments and speed up operational recovery.

Regional Compliance and Data Sovereignty

Druva enables customers to **store data in-region**, supporting data sovereignty regulations across EMEA and APAC. With availability in multiple AWS regions, agencies can choose where their data is stored to comply with local laws.

Compliance frameworks supported include:

- **GDPR** (EU)
- **NIS2 Directive** (EU)
- **IRAP** (Australia)
- **DESC** (Dubai)
- **ISO 27001, SOC 2**
- **Cloud Security Alliance (CSA STAR Level 1 and Level 2)**
- **FedRAMP-Moderate, FIPS 140-2, StateRAMP** (USA)
- **HIPAA**

For more compliance and privacy specific details, please visit the Druva Trust Center www.security.druva.com

Regional Success Stories

- **City University of Hong Kong:** Protected M365 and Google Workspace data, improved governance, and accelerated recovery.
- **Policy Services (UK):** Maintained GDPR compliance, improved restore times by 95%, and eliminated backup complexity.

Solutions for Public Sector Leaders

- **Backup Admins / Cloud Infrastructure Teams**: Eliminate infrastructure, simplify backup policies, reduce operational overhead.
- **Security Administrators / CISOs**: Get real-time monitoring, ensure immutable backups, and orchestrate secure recovery.
- **CIOs and IT Directors**: Align IT with digital government goals, manage costs, and enforce data governance.

Learn more

Get the details at: **druva.com/use-cases/public-sector**