Harbor solutions and Druva

Achieving Australian cyber resilience and meeting Australian signals directorate's (ASCS) Essential Eight.

The Essential 8 imperative

The core aim of the Australian Signals Directorate's (ACSC) Essential Eight is to significantly improve the cyber resilience of Australian businesses. These mitigation strategies are grouped into three primary areas:

Prevent Attacks
Limit Attack Impact
Data Availability

The eight mitigation strategies include regular backups, multi-factor authentication, patching systems and applications, restricting office macros and restricting administrative privilege.

Achieving compliance with the Essential 8

The joint solution directly addresses multiple Essential 8 controls across all maturity levels, providing comprehensive coverage.

- Regular Backups (Data Availability): Druva's resilient cloud infrastructure ensures operational continuity and immutability
- Multi-factor Authentication (Limit Attack Impact): Druva supports MFA out-of-the-box, integrating with existing SSO providers or enforcing mandatory MFA for local accounts
- Restrict Administrative Privileges (Limit Attack Impact): Druva's Role-Based Access Control (RBAC) allows for granular permissions
- Patching and Application Control (Prevent Attacks): As a 100% SaaS service, Druva takes away the responsibility of patching and maintaining the underlying infrastructure and applications

IRAP-assessed (protected)

- Completed IRAP assessment at the PROTECTED level for Druva Data Security Cloud
- Administered by ACSC, IRAP enables Australian Government customers to validate that proper security controls are in place
- Helps customers determine the appropriate responsibility model for addressing the requirements of the Australian Government Information Security Manual (ISM)
- Druva's Data Security Cloud has been assessed under IRAP for all workloads

The joint solution: managed resilience

ZERO INFRASTRUCTURE
- Harbor manages the entire backend, so clients have no hardware to buy, manage, or maintain
- 100% SaaS platform, hosted and fully managed by Druva

RANSOMWARE RECOVERY
- 24/7/365 protection and recovery support with financially backed SLAs
- Air-gapped, immutable backups with automated recovery testing and clean data on-demand

COMPLIANCE & SECURITY
- Expertise in highly regulated environments (finance, legal) and local data sovereignty requirements.
- Secure-by-design platform with end-to-end encryption, continuous monitoring, and FedRAMP/HIPAA/GDPR compliance

SCALABILITY
- Onboard new users and workloads with ease, scaling dynamically based on business needs
- Unlimited, dynamic scale across global regions

Data security cloud

RAPID RESPONSE
- 24/7 continuous monitoring and Safe Mode
- Additional eyes and proactive notification
- Sensitive data governance

AUTONOMOUS PROTECTION
- Monitoring of critical data events
- Complement EDR tools with data alerts
- Advanced threat hunting
- Ransomware recovery playbook

GUARANTEED RECOVERY
- Always on recovery
- Clean data, on-demand
- Automated recovery testing
- Industry-leading SLAs
- Druva Data Resiliency Guarantee

WHY HARBOR?
TRUSTED. PROVEN.

The Global Cyber Recovery MSP | **100+** PB of data under management | **ISO 27001** Certified | **97%+** Customer Retention | **24x7x365** global support [SLAs]

BACKUP AS A SERVICE
WHAT WE COVER & PRODUCT.

DATA CENTRE: Physical Machines | Virtual Machines | File / NAS | Database | CLOUD: Azure | AWS | SaaS: M365 | Entra ID | Dynamics | SFDC | Google Workspace

For more information contact **anz@harborsolutions.com**