

The Digital Fortress for your Business Critical Data

Application Resource Islands (ARI) from Atos

Trusted Partner for your digital journey

- ▶ Organizations are struggling to deal with the large volume of sophisticated and highly coordinated threats
- ▶ Highly sensitive data such as intellectual property are the prime target of attacks
- ▶ Theft or loss of privilege user credentials is often to blame for data theft
- ▶ ARI from Atos can help you to focus your security budget where it matters most
- ▶ ARI provides a high trust, fully managed environment for your most sensitive data, applications and supporting systems
- ▶ As well as fast detection and response to deliberate and inadvertent insider threats

Addressing your Key Business Challenges

- ▶ **Critical Business Infrastructure Secured** separate physical environment, indirect access for admin staff to data workloads via the ARI management zone that is controlled and monitored 24x7 with tight integration of security controls
- ▶ **Privileged User Management** and control, strict access enforcement using role base rights for authorized personnel only, privileged user access and changes to access rights verified by independent compliance team, administrator sessions are recording and behavior monitored
- ▶ **Measurement of Compliance** one point of entry for admin access, full audit access trail and reporting on who has access to what, when, which device; administrator sessions checked at random by the compliance team

“Providing a High Trust Environment for your sensitive data, through a strong integration of People , Process and Technology”

Single ARI specific delivery and governance organization. Full segregation of duties between system management, security operations and compliance teams.

CxO Benefits at a glance

Protect The Organizations Brand

- ▶ Strong focus and protection for business critical data and supporting systems
- ▶ Early detection and response to attacks, key to minimizing the resulting damage

Safeguard Corporate Assets

- ▶ Appropriate protection intellectual property, innovation, R&D topics
- ▶ Enhanced protection from malicious and inadvertent insider attacks, increasingly to blame for corporate data loss

Maintain Stakeholder Relationships

- ▶ Customer, partner and other sensitive data fully managed and monitored 24x7 within the trusted ARI environment

Management focus on Strategic Goals

- ▶ Instead of high media profile attacks

Security Policy Compliance

- ▶ Independent compliance team ensuring that in house and 3rd party policies and rules are consistently met

Full Segregation of Duties

- ▶ Between system operations,
- ▶ Security operations,
- ▶ Compliance and
- ▶ CSIRT security incident teams.

Security Compliance Teams

- ▶ Conduct and maintain security incident management processes
- ▶ Provide four eyes approval for the change execution in the enforcement system
- ▶ Supervise the governance & compliance processes for accreditation of admin staff

Enhanced Access Control and Monitoring

- ▶ Application aware firewall controls with intrusion prevention at the boundaries
- ▶ Strong (2 factor) access for admins
- ▶ Access to admin staff strictly enforced according to roles and rights
- ▶ Indirect access for admin staff to data workloads via the management zone
- ▶ Admin access to data workloads with one time passwords or hidden passwords
- ▶ Recorded and monitoring of admin access
- ▶ Encryption of data within the ARI zones
- ▶ 24/7 monitored security system with random checks of admin session logs
- ▶ Secure process for the transfer of content in / out of the ARI environment
- ▶ Data Loss Prevention at network, server and workload zone level
- ▶ Business systems reside within protected areas (workload zones) per landscape

Our unique value proposition

Providing a state-of-the-art security solution to meet your business needs

- ▶ Atos is the first to market with a high trust environment as a global standard offer
- ▶ We provide an ARI specific global delivery team to manage all operational towers
- ▶ ARI has a service specific global governance team to enable fast response to the threat environment
- ▶ The ARI service utilizes the same security operations teams that collectively manage events for the Olympic Games and government organizations, for a forward thinking proactive security approach
- ▶ ARI is already live and protecting hundreds of systems for one of the largest global manufacturers
- ▶ Your business critical data deserves special focus and attention
- ▶ This requires supplementary measures and control compared to standard security
- ▶ You can improve the security posture of your entire organization by focusing on highly sensitive data

Your Trusted Partner

ARI is a high trust, fully managed environment from Atos, a leader in European Data Center services and a major global provider of security offerings. We cover the full life-cycle from initial Assessment → Design/Build → Transform → Live Production.

Consulting Based Approach

- ▶ The starting point is a comprehensive audit of your environment, processes and procedures, the external threat profile
- ▶ We will help you establish whether your environment is "fit for sensitive data"
- ▶ Plus the gap analysis and effort to meet in-house and 3rd party compliance rules
- ▶ Once the gaps and ARI candidates are identified, we will work with you to develop a business case

Design & Build

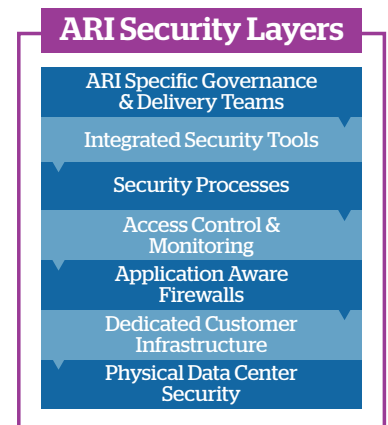
- ▶ A modular service based approach so that the service and options can be tailored to your specific requirements in the most cost effective manner

Transformation

- ▶ To the live environment using standard blueprints for popular customer scenarios
- ▶ Penetration testing to ensure the environment meets the objectives
- ▶ Independent security assessor signing off the implementation at key stages

Live Production

- ▶ Atos Tier2/3 managed data centers and operations
- ▶ Strictly Atos vetted and accredited staff performing system management and security operations



Key benefits:

| CEO | CIO | CFO |
|---|--|--|
| <ul style="list-style-type: none"> ▶ Protect the Organizations Brand ▶ Safeguard Corporate Assets ▶ Maintain Stakeholder Relationships ▶ Management Focus on Strategic Organizational Goals ▶ Security Policy Compliance | <ul style="list-style-type: none"> ▶ Enhanced protection for Business Critical Data and systems protected ▶ Advanced Defense against Sophisticated Attacks ▶ Security Policy Compliance ▶ Comprehensive Audit Access Log ▶ Focus Security Investments ▶ Strong Management of Privileged Users with enhanced rights | <ul style="list-style-type: none"> ▶ Safeguard Corporate Assets (R&D, Patents etc), long term profitability ▶ Reduce the risk of regulatory fines ▶ Protect Band Value ▶ Fill Gaps in Security Capabilities Cost Effectively |