RutterKey

WHITE PAPER

IFS CLOUD VS APPS 10

APRIL 2024

IFS INNOVATIVE PARTNER AWARD 2023

IFS SILVER SERVICES PARTNER

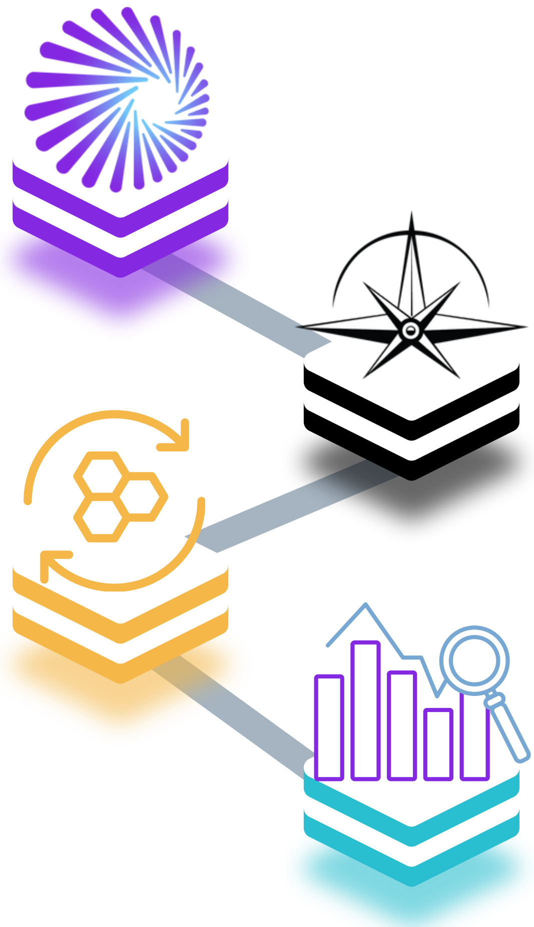
IFS PARTNER SUCCESS

Exploring the evolution of IFS, this white paper delineates the nuanced distinctions between IFS Cloud and IFS Apps 10, presenting their respective features, functionalities, and strategic advantages in driving organizational efficiency and innovation.

About RutterKey

At RutterKey, our diverse team of consultants brings expertise from various industries like Aerospace & Defense, Construction, and Manufacturing, allowing us to offer tailored solutions to our clients. We adopt a comprehensive approach to grasp our client's operations and culture, identifying challenges in alignment with enterprise-wide objectives.

IFS x RUTTERKEY SOLUTIONS



MOMENT OF SERVICE

We identify the Moment of Service for your business. A new invention? An improved production process? Everything starts with the intention to do something amazing for your customer.

RUTTERKEY IMPLEMENTATION

Our team of highly skilled consultants handle every facet of IFS functionality and oversee system setup, testing, and Go-Live activities.

CONTINUUM OF SERVICE

We work with you to ensure that you enhance your strengths and help you rise to the next level - even after implementation.

PREDICTIVE USE OF DATA

Our innovative approach allows system controls to initiate, track, and advance an IFS process, while moving data between parallel threads. Our solution enables customers to automate complex non-linear processes in IFS and help predict future challenges.

Through win-win strategies, we propose solutions that enhance efficiency while respecting existing processes, ensuring seamless transitions and improvements across all levels.

IFS Cloud Middle Tier Security Changes

- Kubernetes security layer in front of backend services.
- IAM client integration.
- Using KeyCloak as the security backend.
- Enhanced vulnerability scanning.
- Using Kubernetes Secrets instead of configuration files.

IEE vs Auerna

1. IEE security is checked once the request hits the database via Presentation Objects. The same http call is used to request data from different DB objects. The access granted to the DB methods controls the CRUD.
2. Aurena security is based on the Rest APIs. Rest API access controls the security. And controlled at the Projection CRUD level.

Even the network security can be setup for different URLs. With IEE this is not possible.

Summary

In summary, there are significant enhancements in middle-tier security, including the implementation of a Kubernetes security layer, integration of an IAM client, and the adoption of KeyCloak as the security backend. Additionally, enhanced vulnerability scanning and the use of Kubernetes for configuration management are highlighted. Another crucial aspect is the difference between IEE and Aurena regarding security enforcement. In IEE, security is controlled at the database level through Presentation Objects, while Aurena employs Rest APIs to manage security at the Projection CRUD level, facilitating network security configurations for various URLs.

The Facts

Cloud implementations are
30% QUICKER
BASED ON RECENT STUDIES

IFS Cloud can accommodate
UP TO 50% MORE
CONCURRENT USERS

Transitioning users reported
15% TO 25%
IN SAVINGS OVER A 5 YEAR PERIOD

CSP vs On-Prem Platforms and Networks

Homogeneous Architecture:

- Cloud architecture is consistent and standardized across all instances. Unlike traditional on-premises networks, which accumulate various security technologies over time, cloud providers build their data centers using a unified blueprint with built-in security capabilities. This results in a reduced attack footprint and a more secure environment.

Heavy Investment in Security:

- Public cloud providers invest heavily in security research and innovation. Since their entire business relies on the cloud platform, they prioritize both infrastructure and cloud services protection. Researchers frequently credit these providers for finding vulnerabilities, demonstrating their commitment to security.

Consistent Patching and Security Management:

- Enterprises often experience security breaches due to configuration errors and unpatched vulnerabilities. In traditional networks, patching and security management are challenging. However, cloud providers consistently apply patches and maintain security, reducing the risk of exploitation.

Ease of Security Architecture Changes:

- Cloud environments allow for flexible security architecture changes. Unlike on-premises stacks, where changing vendors or tools is complex, the cloud enables seamless adoption of new capabilities. This agility ensures that security remains up-to-date and adaptable.

Attracting Top Cybersecurity Talent:

- Cloud providers employ dedicated teams of experts focused solely on monitoring and securing cloud infrastructure. These experts stay abreast of the latest threats and best practices, enhancing overall security posture.

Cloud Hosting Applications vs On-Prem

When comparing a private cloud provided by a Cloud Solution Provider (CSP) to an on-premises solution, there are several compelling benefits from a cybersecurity perspective. Let’s explore each benefit in detail:

Enhanced Security and Isolation:

- Private clouds offer complete isolation from other organizations, reducing the risk of unauthorized access or data breaches.
- With a CSP-managed private cloud, security experts handle infrastructure protection, ensuring robust defenses against cyber threats.

Customized Security Policies:

- In a private cloud, you can tailor security policies to your organization’s specific needs.
- This flexibility allows you to enforce strict controls, such as access restrictions, encryption, and intrusion detection, without compromising performance.

Compliance and Data Sovereignty:

- Private clouds enable compliance with industry-specific regulations (e.g., GDPR, HIPAA) by keeping data within specific geographic boundaries.
- You maintain control over data residency, ensuring compliance with legal requirements.

Predictable Performance:

- On-premises solutions may suffer from resource constraints or bottlenecks.
- In a private cloud, you allocate dedicated resources, guaranteeing consistent performance for critical workloads.

Reduced Attack Surface:

- Private clouds minimize the attack surface by limiting external exposure.
- Unlike public clouds, where shared infrastructure poses risks, a private cloud focuses solely on your organization’s needs.

IFS INNOVATIVE PARTNER AWARD 2023

IFS SILVER SERVICES PARTNER

IFS PARTNER SUCCESS

Cloud Hosting Applications vs On-Prem cont.

Rapid Incident Response:

- CSP-managed private clouds benefit from 24/7 monitoring and incident response.
- Security teams promptly address threats, minimizing downtime and data loss.

Scalability with Security:

- As your organization grows, a private cloud scales seamlessly while maintaining security.
- You can add resources without compromising existing security controls.

Disaster Recovery and Business Continuity:

- Private clouds offer robust disaster recovery options.
- Regular backups, failover mechanisms, and geographically dispersed data centers ensure business continuity.

Cost-Effective Security:

- CSP-managed private clouds eliminate upfront capital expenses.
- You benefit from enterprise-grade security without investing in dedicated security hardware.

Access to Expertise:

- CSPs employ cybersecurity experts who specialize in securing cloud environments.
- Their knowledge and experience enhance your organization's overall security posture.

What does it mean for a Defence Business?

Enhanced Security and Compliance:

- SECRET-level cloud services offer robust security features, including encryption, access controls, and continuous monitoring. These services adhere to stringent compliance standards, ensuring data protection and regulatory alignment.
- Cloud providers invest heavily in security research and innovation, safeguarding against emerging threats. Their expertise helps maintain a secure environment for sensitive information.

Scalability and Agility:

- Cloud data centers provide elastic scalability. As your defense manufacturing business grows or faces fluctuating demands, you can easily scale up or down without significant upfront investments.
- Rapid provisioning and deployment allow you to respond swiftly to changing requirements, such as product development cycles or urgent defense needs.

Cost Efficiency:

- Cloud services operate on a pay-as-you-go model. You only pay for the resources you consume, eliminating the need for large capital expenditures.
- Traditional on-premises data centers involve substantial upfront costs for hardware, maintenance, and upgrades. Cloud services reduce these financial burdens.

Global Reach and Accessibility:

- Cloud data centers are distributed globally, enabling low-latency access from various locations. This is crucial for defense manufacturing, especially when collaborating with international partners or deploying products worldwide.
- Users can securely access cloud services from anywhere, promoting remote work and efficient collaboration.

IFS INNOVATIVE PARTNER AWARD 2023

IFS SILVER SERVICES PARTNER

IFS PARTNER SUCCESS

What does it mean for a Defence Business?

Disaster Recovery and Business Continuity:

- Cloud providers offer redundant data centers across different regions. In case of a disaster or outage, your data remains accessible.
- Automated backups, failover mechanisms, and disaster recovery plans ensure business continuity, even during critical situations.

Focus on Core Competencies:

- By leveraging cloud services, your defense manufacturing team can concentrate on core competencies—such as product design, innovation, and quality—rather than managing infrastructure.
- Outsourcing data center management allows your experts to focus on mission-critical tasks.

IFS INNOVATIVE PARTNER AWARD 2023

IFS SILVER SERVICES PARTNER

IFS PARTNER SUCCESS

IFS Cloud vs IFS Apps 10 Security Improvements

Enhanced Security Features:

- IFS Cloud offers enhanced security compared to IFS Applications 10. It includes a range of features such as:
    - Two-factor authentication: Adding an extra layer of security by requiring a second form of verification.
    - Data encryption: Protecting sensitive data during transmission and storage.
    - Access controls: Managing user permissions and restricting unauthorized access.
- These security measures help safeguard businesses' data and systems against cyber threats.

Built on Microsoft Azure:

- IFS Cloud is hosted in Microsoft Azure, a robust and secure cloud infrastructure.
- Customers access the service via the internet using TLS encryption over HTTPS.
- Being segregated from their own on-premise IT environment and with traffic restricted to necessary protocols, it provides additional protection against ransomware.

Modern Technologies and Capabilities:

- IFS Cloud is not merely an upgrade; it's a revolution. It offers a comprehensive, integrated suite of solutions tailored to meet the evolving needs of businesses in the digital age.
- It leverages cutting-edge technologies such as artificial intelligence (AI), machine learning, and advanced analytics.
- These technologies provide predictive insights, automate routine tasks, and enhance decision-making, contributing to a more secure environment.

Unified Platform and Streamlined User Experience:

- While IFS Applications 10 has been reliable, IFS Cloud takes it a step further.
- With a modern browser-based interface and mobile workforce capabilities, IFS Cloud provides a more streamlined and cohesive user experience.