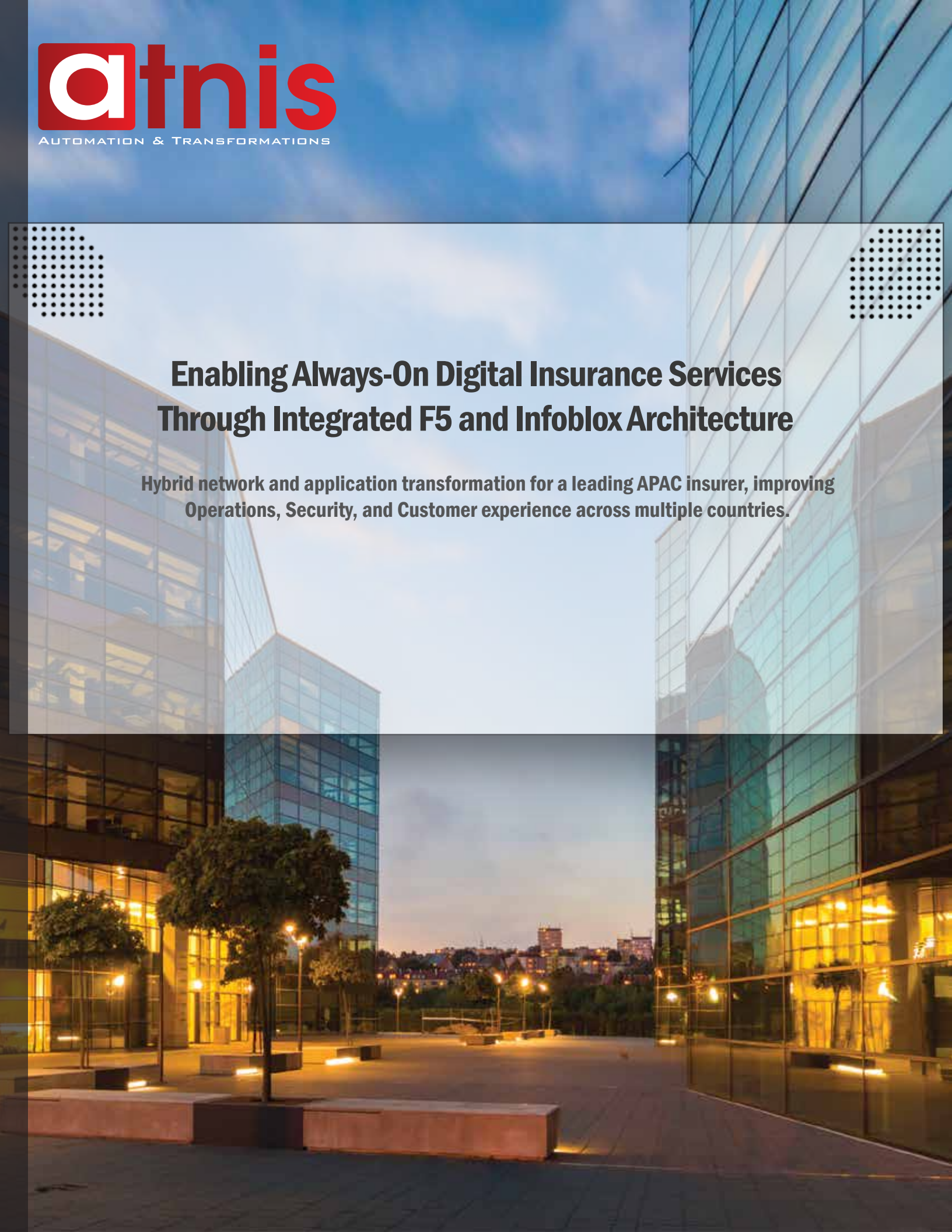
atnis
AUTOMATION & TRANSFORMATIONS

Enabling Always-On Digital Insurance Services Through Integrated F5 and Infoblox Architecture

Hybrid network and application transformation for a leading APAC insurer, improving Operations, Security, and Customer experience across multiple countries.



Executive Summary

A leading APAC insurance provider operating across Singapore, Hong Kong, and seven additional countries in the APAC region undertook a strategic modernization initiative to strengthen the foundation of its digital services, enhance customer experience, improve operational resilience, and reduce infrastructure complexity and operational costs.

By implementing Infoblox NIOS for network control automation and F5 BIG-IP for application delivery, traffic management, and security, the organization transformed its DNS and application delivery architecture into a scalable, resilient, and business-aligned platform capable of supporting secure, always-on digital services across the region.

Key Business Drivers

Infrastructure Modernisation

The organisation needed to modernise its legacy DNS, IP management, and application delivery infrastructure to support growing digital business demands. Existing systems were fragmented, difficult to scale, and heavily dependent on manual administration, resulting in operational inefficiencies and increased risk.

Improved Availability and User Experience

Business-critical applications required highly available and resilient delivery across multiple data centres and hybrid environments. The organisation needed intelligent traffic management, automated failover, and performance optimisation to ensure consistent user experience and minimise downtime across regions.

Security and Risk Reduction

The increasing frequency of DNS attacks, web application threats, and DDoS incidents created the need for stronger security controls across both the network and application layers. The organisation aimed to implement integrated protection mechanisms to improve cyber resilience and reduce operational risk.

Automation and Operational Efficiency

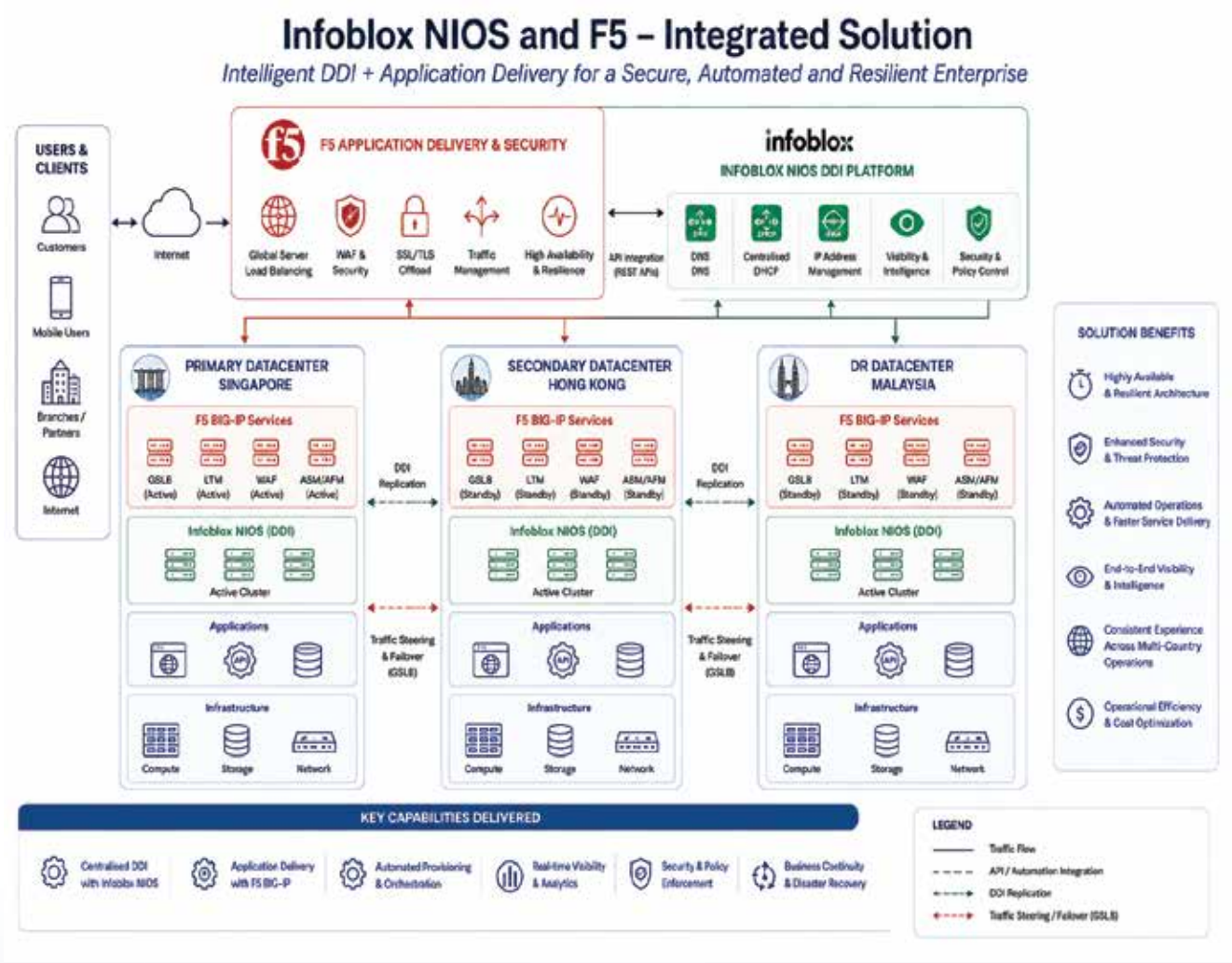
Manual provisioning of DNS records, IP allocations, certificates, and application services slowed deployment cycles and increased the likelihood of configuration errors. The organisation required an automation-driven architecture to accelerate service delivery, improve consistency, and reduce operational overhead.

Solution Details

ATNIS proposed a modern, highly resilient solution built on an integrated F5 BIG-IP and Infoblox NIOS architecture deployed across multiple data centers.

The design provides centralized DNS, IP address management, and application delivery capabilities, enabling intelligent traffic routing, automated failover, and consistent security enforcement across all impacted sites.

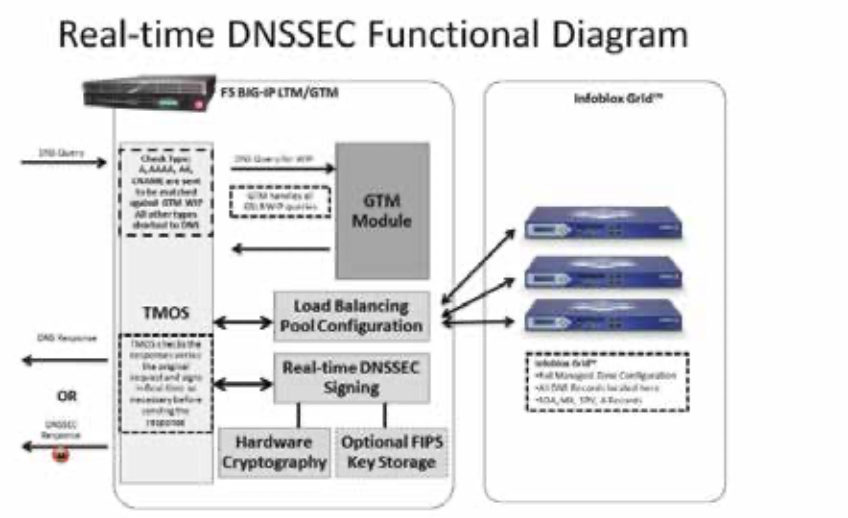
This multi data center architecture ensures high availability, improved performance, stronger security posture, and scalable support for hybrid and cloud-ready environments.



Key Business Challenges

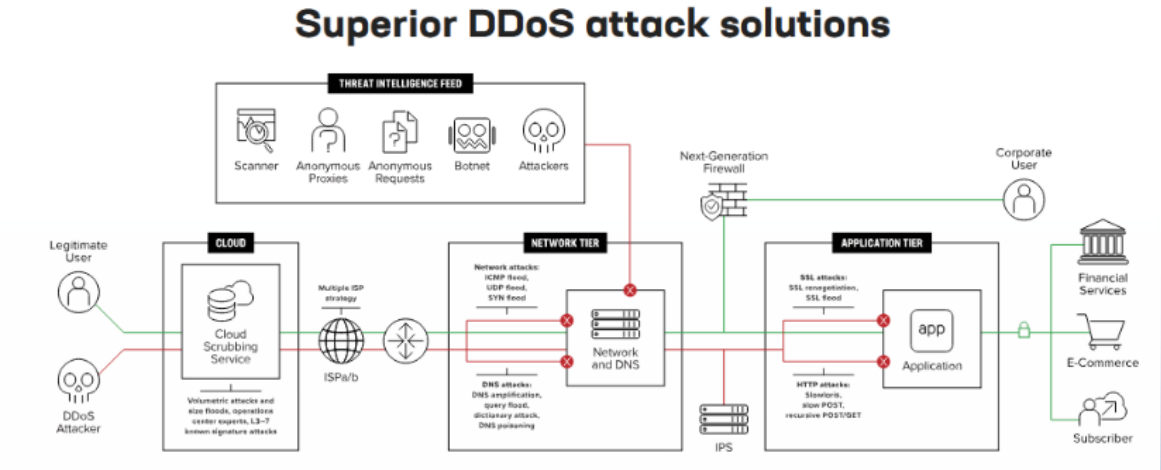
The enterprise deployed an integrated **F5 BIG-IP** architecture using key modules:

- **GTM (Global Traffic Management)**: Global DNS-based routing to the nearest or healthiest site.
- **LTM (Local Traffic Management)**: Local load balancing, health checks, and traffic optimisation.
- **WAF (Web Application Firewall)**: Protection from OWASP Top 10, bot, and API attacks.
- **DDoS Protection**: Mitigation of volumetric and application-layer attacks.
- **SSL/LS Management**: Centralized certificate handling and SSL offload for performance and security.



The organization implemented Infoblox NOS as its core DDI platform to support application delivery and network automation alongside F5.

- **Core DDI Services**: Centralized DNS, DHCP, and IPAM for consistent network control.
- **Automation & Orchestration**: API-driven provisioning integrated with F5 for faster, error-free service delivery.
- **Visibility & Intelligence**: Real-time insight into IP usage, DNS activity, and application dependencies.
- **Security & Policy Control**: Enhanced DNS security and policy consistency, reducing threats and misconfigurations.

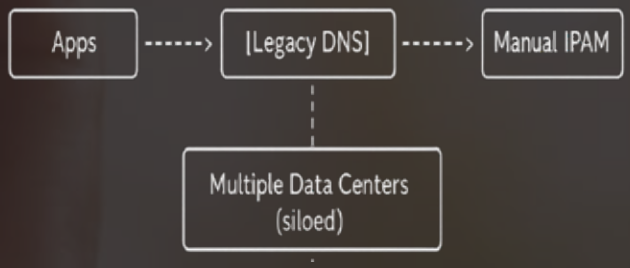


Implementation Phases

The proposed ATNIS solution, built on F5 BIG-IP and Infoblox NIOS across multiple data centers, was delivered in structured phases to ensure controlled rollout, minimal disruption, and operational stability.

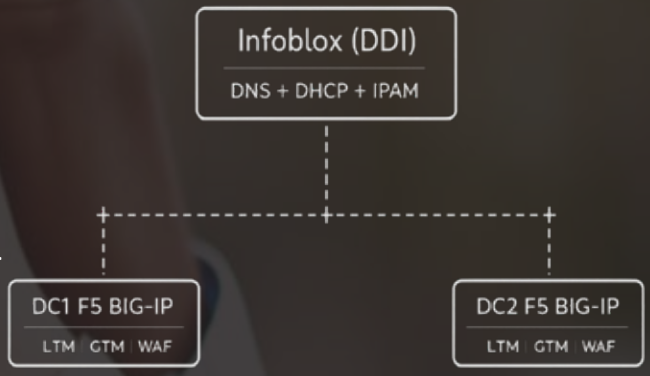
Phase 1 – Assessment & Discovery

- Review of existing DNS, IP, and application delivery environments.
- Identification of application dependencies and traffic flows.
- Baseline of current performance, availability, and security gaps.
- Infrastructure readiness and risk assessment.



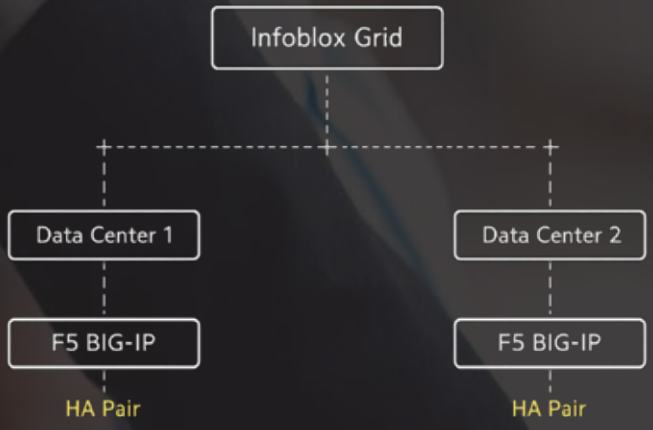
Phase 2 – Architecture Design

- Definition of multi–data center F5 and Infoblox architecture.
- Design of DNS, IPAM, and traffic management integration.
- High availability and disaster recovery design.
- Security architecture including WAF, DNS security, and SSL strategy.



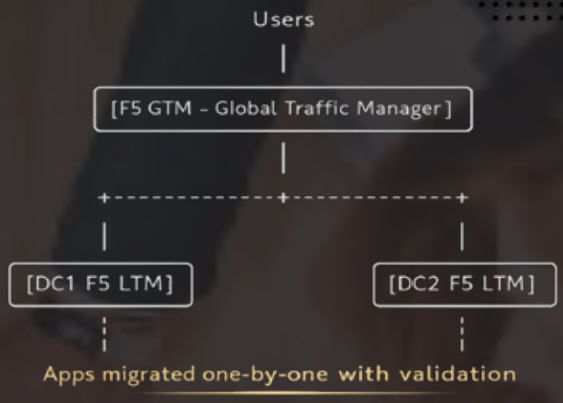
Phase 3 – Core Platform Deployment

- Deployment of Infoblox NIOS grid for centralized DDI services.
- Implementation of F5 BIG-IP clusters across data centers.
- Configuration of HA pairs and redundancy models.
- Establishment of baseline DNS and traffic management services.



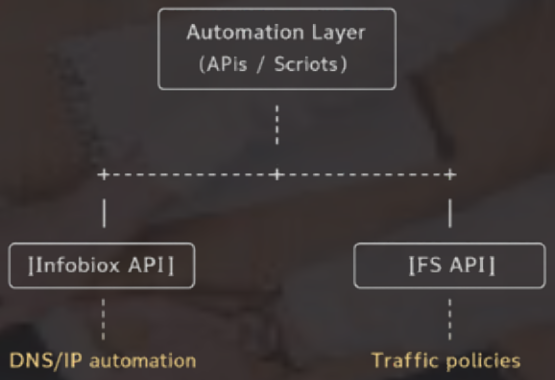
Phase 4–Application Onboarding & Migration

- Gradual migration of critical applications to F5 platform.
- Integration of DNS records into Infoblox-managed system.
- Configuration of load balancing and global traffic policies.
- Validation of failover, performance, and security controls.



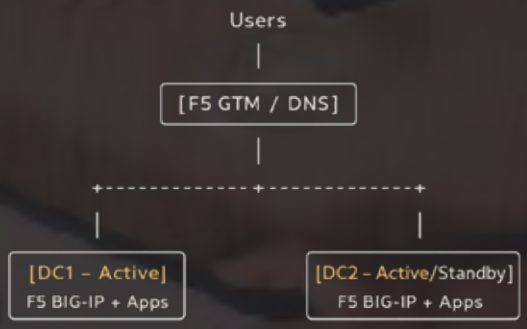
Phase 5–Automation & Optimization

- API-based automation for DNS, IP, and application provisioning.
- Optimization of traffic routing and performance tuning.
- Enhancement of monitoring, logging, and visibility.
- Operational handover and process stabilization.



Phase 6– Operational Enablement

- Knowledge transfer and runbook finalization.
- Establishment of monitoring and incident management processes.
- Ongoing tuning for performance, scalability, and security.
- Continuous improvement and hybrid-cloud readiness alignment.



Final Outcomes

The organization successfully established a modern, scalable, and resilient digital infrastructure platform capable of supporting current and future business requirements.

Key final outcomes included:

- Improved application availability through automated failover and multi-site resiliency.
- Faster service deployment using API-driven automation.
- Enhanced application performance and traffic optimization.
- Stronger protection against DNS and web-based threats.
- Reduced operational complexity and manual administration.
- Greater operational visibility and centralized governance.
- Scalable foundation for cloud and digital transformation initiatives.
- Improved business continuity and disaster recovery readiness.

The F5 and Infoblox integrated architecture now serves as a strategic digital foundation supporting the organization's long-term modernization and customer experience objectives. The organisation achieved a modernised, automated network and application delivery platform across multiple data centres (Singapore primary, Hong Kong secondary, Malaysia DR). This resulted in improved application availability, stronger DNS and application-layer security, faster service deployment through automation, and reduced operational complexity and cost.

ATNIS Australia

L 36, Gateway 1, Macquarie Street Sydney NSW 2000

enquiry_au@atnis.net

Direct Line : +61-57001300

ATNIS India

15A, 4th Floor, City Vista Fountain Road, Kharadi Pune Maharashtra 411014

enquiry_in@atnis.net

Direct Line: +91-99869 99094

ATNIS Singapore

2 Woodlands Square #13-79 Woods Square Tower 1 Singapore 737715

enquiry_sg@atnis.net

Direct Line : +65 6970 0179