kyndryl

Navigating F5

A Kyndryl Guide to Modernization and Enhanced Security

The Challenge: A Two-Fold Risk to Your Infrastructure

The Inevitable: F5 End-of-Life is Approaching

Many widely deployed F5 BIG-IP hardware and software solutions are rapidly approaching their end-of-life (EoL) and end-of-support (EoS) dates throughout 2025 and 2026.

Running unsupported infrastructure introduces significant risks, including:

- **Increased Security Vulnerabilities:** Lack of security patches leaves your applications exposed.
- **Operational Instability:** Without vendor support, failures can lead to prolonged business disruptions.
- **Compliance Gaps:** Using unsupported technology can violate industry regulations.
- **Limited Capabilities:** Older technology hinders innovation and can't support modern application architectures.

The Immediate Threat: Source Code Breach and Undisclosed Vulnerabilities

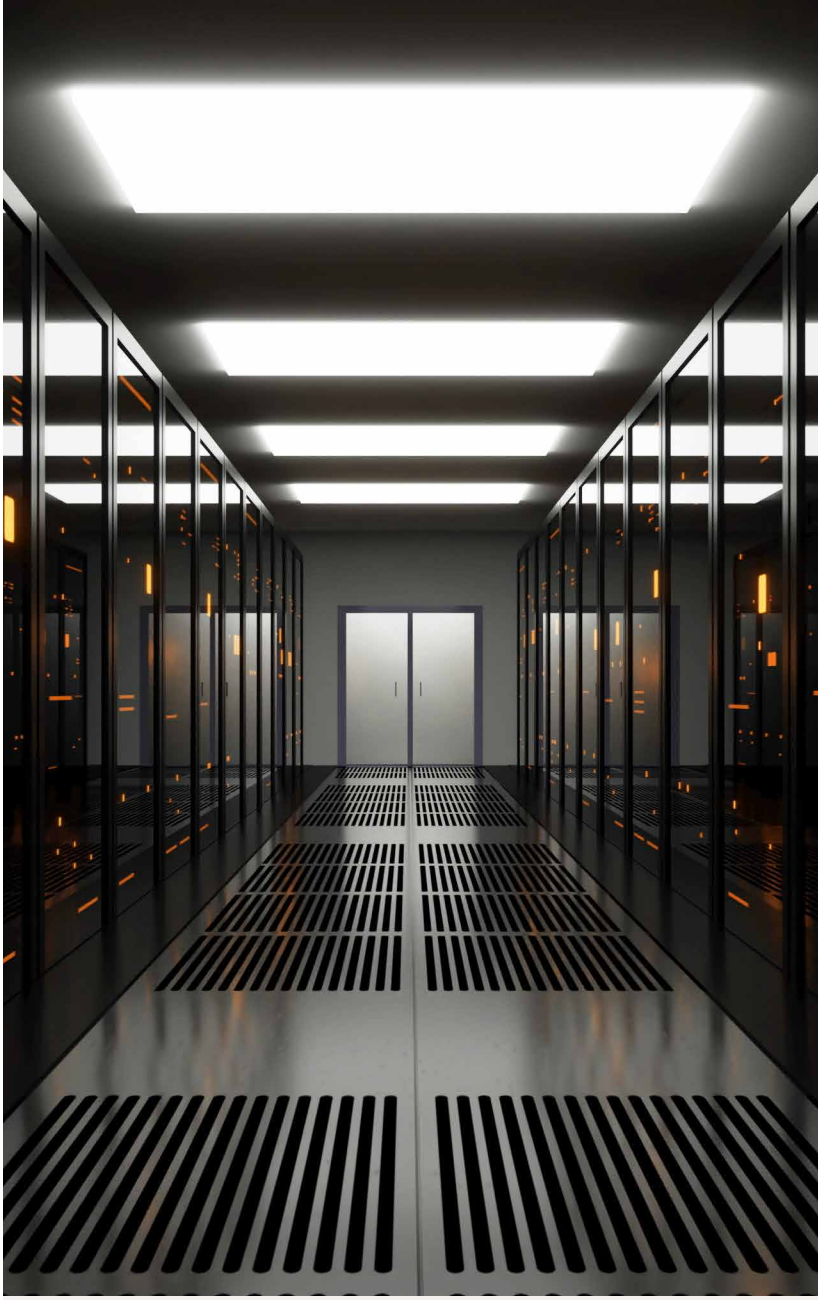
Beyond the planned end-of-life, the recent, highly concerning breach of F5's source code has fundamentally changed the threat landscape. This incident goes beyond typical vulnerabilities. When threat actors gain access to the very blueprint of the software, they can potentially insert malicious code, create hidden backdoors, and discover zero-day exploits that F5 itself may not be aware of. This means that even patched systems could harbor latent threats.

For older, unsupported devices, the risk is magnified significantly. They cannot receive any updates, leaving them permanently exposed to both known exploits and potential threats stemming from the compromised source code.

This raises critical questions:

- Is patching enough? With the source code compromised, can you be 100% certain that recent patches don't contain hidden vulnerabilities? For devices past their End of Software Development (EoSD) date, this is a moot point—they can't be patched at all.
- Can you trust your hardware's integrity? Without official vendor support and forensic tools, validating that your device hasn't been compromised by a sophisticated attack leveraging inside knowledge is nearly impossible. A compromise could persist undetected.
- Is your organization willing to risk a breach originating from a device whose core code was exposed?

Continuing to operate this equipment is no longer just a legacy issue; it's an active and potentially catastrophic security risk.



Key F5 Products to Address

Hardware:

- BIG-IP 5250V, 7000S, 7055s, 7200v SSL, and various iSeries models

Software:

- BIG-IP LTM, DNS, AWAF, and APM running on older, unsupported versions

The Kyndryl Solution: Your Partner in a Secure Transition

Kyndryl is here to help you navigate the dual complexities of the F5 end-of-life cycle and the current security landscape. We use our deep expertise across network security and mission-critical infrastructure technology services to create solutions that are designed to be sure, tackling both legacy and active threats. We don't just replace hardware; we build a more resilient and secure foundation for your critical applications.

Your Path Forward: A Suggested Approach with Kyndryl

We recognize that every organization's journey is different. Kyndryl offers two primary engagement models to help you secure your infrastructure:

Path 1: Secure and Modernize Your F5 Investment

For customers who want to retain their F5 equipment, the immediate priority is to mitigate risk. Kyndryl will engage in a multi-phased approach to secure your investment:

Phase 1: Comprehensive Assessment & Health Check

Kyndryl's experts will perform a thorough review of your F5 environment, including a configuration audit against best practices, a vulnerability assessment to identify known exploits, and a performance analysis to establish a healthy baseline.

Phase 2: Immediate Upgrade & Patch Management

We will develop a detailed plan to upgrade your BIG-IP hardware and software to a fully supported, long-term stability release so you can receive critical security patches and vendor support.

Phase 3: Advanced Security Hardening

Post-upgrade, we will implement critical security controls to reduce the attack surface. This includes implementing role-based access control (RBAC), configuring robust logging to your SIEM, disabling unused modules and services, and applying F5's security hardening guidelines.

Phase 4: Ongoing Proactive Management

Kyndryl can provide ongoing managed services for your F5 estate, offering 24/7 monitoring, proactive threat intelligence integration, and expert management to optimize your security environment.

Path 2: Strategic Assessment and Future-State Roadmap

For customers who are unsure of the best path forward, Kyndryl acts as your strategic partner to provide clarity and define a concrete plan.

This engagement is designed to analyze your current environment in the context of your business goals and risk tolerance, helping you decide whether to stay on F5, implement a hybrid solution, or migrate entirely.

We will perform a deep-dive analysis of your LTM, DNS, AWAF, and APM usage to deliver a tailored roadmap.

This roadmap will outline clear options, including like-for-like replacements, robust compensating controls, and long-term modernization strategies, allowing you to make an informed decision.

Below are some of the options we would explore with you.

Local Traffic Manager (LTM)

The Challenge:

Your core load balancing capabilities are at risk from both obsolescence and potential compromise.

Kyndryl's Recommended Options

- **Like-for-Like Modernization:** For customers seeking a direct, on-premises replacement, we recommend and manage leading Application Delivery Controllers (ADCs) from vendors such as **NetScaler**, **A10 Networks (Thunder ADC)**, and **Progress Kemp (LoadMaster)**. This approach provides a familiar architecture with modern performance and security.
- **Cloud-Native Integration:** Leverage the robust, continuously updated security of native load balancing services from **AWS (Elastic Load Balancing)**, **Azure (Application Gateway)**, and **Google Cloud**.
- **Strategic Compensating Controls:** If immediate migration isn't possible, we can create a defensible perimeter around the at-risk device. This includes enhanced network segmentation using firewalls from **Palo Alto Networks** or **Fortinet**, rigorous traffic monitoring with Network Detection and Response (NDR) tools like **Vectra AI**, and deploying a modern WAF from **Imperva** or **Akamai** in front of the LTM.

Global Traffic Manager (GTM) / DNS

The Challenge:

Your global application availability relies on a DNS infrastructure that may be outdated and vulnerable.

Kyndryl's Recommended Options

- **Like-for-Like Modernization:** To replace F5 GTM/DNS functionality, we can implement and manage on-premises or hybrid Global Server Load Balancing (GSLB) solutions from providers like **NetScaler** and **A10 Networks**. For a dedicated DNS platform, **IBM NS1 Connect** offers a powerful alternative.
- **Cloud-Native Integration:** Move to a cloud-native DNS and GSLB solution for superior security and reliability, using services like **AWS Route 53**, **Azure Traffic Manager**, or **Cloudflare DNS**.
- **Strategic Compensating Controls:** Mitigate risks by implementing a multi-layered DNS security strategy using protective DNS services like **Cisco Umbrella** or **Infoblox BloxOne Threat Defense**. Additionally, we can configure a Content Delivery Network (CDN) from providers such as **Akamai** or **Cloudflare** to reduce the direct attack surface.

Advanced Web Application Firewall (AWAF)

The Challenge:

Your web applications are exposed to sophisticated attacks, and your current WAF may not be sufficient or could itself be a point of weakness.

Kyndryl's Recommended Options

- **Like-for-Like Modernization:** Replace your F5 AWAF with a modern Web Application Firewall from industry leaders like **Imperva**, **Akamai (App & API Protector)**, **Fortinet (FortiWeb)**, or **Palo Alto Networks**. These provide advanced threat intelligence and API protection.
- **Cloud-Native Integration:** Deploy and manage powerful cloud-based WAFs such as **AWS WAF**, **Azure WAF**, or **Cloudflare WAF** for scalable and centrally managed application security.
- **Integrate WAF into your CI/CD Pipeline:** We can help you build security directly into your application development lifecycle (DevSecOps), reducing reliance on perimeter devices alone.
- **Strategic Compensating Controls:** If you cannot migrate immediately, we can help tune existing policies, implement a robust vulnerability management program using scanners from T**enable (Nessus)** or **Qualys**, and deploy an Intrusion Prevention System (IPS), often integrated within next-generation firewalls from **Palo Alto Networks** or **Fortinet.**

Access Policy Manager (APM)

The Challenge:

Your secure access and identity management solution is a prime target and, if compromised, could expose your entire application ecosystem.

Kyndryl's Recommended Options

- **Like-for-Like Modernization to Zero Trust:** The direct modern replacement for legacy VPN and access control is a Zero Trust Network Access (ZTNA) solution. We recommend and implement market-leading ZTNA platforms from **Zscaler (ZPA)**, **Palo Alto Networks (Prisma Access)**, and **Netskope (Private Access)**.
- **Cloud-Based Identity and Access Management (IAM):** Migrate to a comprehensive cloud-based IAM platform for modern single sign-on (SSO) and multi-factor authentication (MFA) from providers like **Microsoft Entra ID**, **Okta**, or **Ping Identity**.
- **Strategic Compensating Controls:** Immediately improve security by mandating MFA from providers like **Duo (Cisco)** or **Okta**. We can also implement advanced user behavior monitoring with SIEM platforms like **Splunk** or **Microsoft Sentinel** to detect and respond to suspicious access patterns.

Why Kyndryl?

Deep Security Expertise
Our certified professionals have decades of experience in secure infrastructure design, threat mitigation, and incident response.

Security-First Migrations
We don't just "lift and shift." We help you design and implement a new, secure architecture that is resilient against both legacy and modern threats.

Vendor-Neutral Approach
We partner with a wide range of leading technology vendors, allowing us to recommend the best and most secure solution for your specific needs.

Global Reach and Scale
With a presence in over 60 countries, we can support your secure F5 transition wherever you do business.

End-to-End Services
From security assessments and planning to secure migration and ongoing managed services, Kyndryl is your single partner for a successful transition.

Take the Next Step

Don't wait for an end-of-life deadline or a security incident to force your hand.

Contact Kyndryl experts today for a complimentary security and technology assessment of your F5 environment.

We'll help you understand your risks and develop a roadmap for a successful and secure transition.

kyndryl