SOLUTION OVERVIEW

F5 Zero Trust Architecture Solutions

The F5 Application Delivery and Security Platform provides a holistic zero trust architecture that addresses the increasing sophistication and complexity of cybersecurity threats.

Key Benefits

Defend any strategic point in your environment
The F5 Application Delivery and Security Platform (ADSP) enables holistic zero trust architectures with context-aware access, deep traffic inspection, API protection, and dynamic policy enforcement across all applications including legacy, modern, and AI.

Secure and protect every app and API wherever deployed
F5 ADSP delivers zero trust protection as close to your apps and APIs as possible: on hardware, as software or SaaS, on DPUs for AI apps, or in containerized environments like Kubernetes—ensuring security wherever you deploy.

Ensure least privileged access and continuous monitoring
F5 ADSP integrates with most IDaaS providers, ensuring per-request access to applications and APIs in any environment, and continuously monitors to implement dynamic, context- and identity-based access policies that enforce least privilege.

Leverage existing investments
Enhance your trusted security solutions or established zero trust environment with additional capabilities from F5 ADSP to create an ultra-secure environment that extends critical security capabilities to every strategic point in your infrastructure.

Evolving threats, app infrastructures, and apps themselves drive the need for a new approach to security

Today's organizations face sophisticated attacks driven by bots and AI along with powerful new threats like ransomware-as-a-service. The changing nature of applications across highly distributed infrastructure add complexity and risk. Most organizations manage a mix of legacy, on-premises apps along with modern, SaaS-based, and AI-powered apps that are deployed across hybrid and multicloud environments. These factors make traditional perimeter network security obsolete, necessitating a new model for how apps are delivered and secured.

The emergence of a zero-trust model and supporting architectures

Traditional perimeter network defenses adhered to a "trust but verify" model. But any determined, sophisticated, and sometimes lucky cybercriminal could break those defenses and gain relatively easy access to everything on an internal network. Today, where users can be anywhere and apps and data are hosted across hybrid and multicloud environments, the threat landscape is vaster, providing numerous opportunities for attackers to exploit.

Zero trust has emerged as the necessary evolution in cybersecurity. Zero trust addresses the limitations in traditional perimeter approaches *and* adapts to the complexities of modern, interconnected IT environments. Zero trust is centered around the principles of "never trust, always verify." Effective enforcement of these principles requires a holistic approach—one where availability and security controls extend from the edge down to a container and workload level, ensuring least privileged access to resources and preventing lateral movement should an attacker already be lurking in your network. It's a zero trust *architecture*—the strategic combination of products and solutions—that allows you to put the "never trust, always verify" model into practice.

Key Capabilities

Complete security for every app
F5 ADSP's converged application delivery and security platform simplifies management for IT and security teams while ensuring availability and security for every app and API you use.

Deployable anywhere and in any form factor
F5 ADSP deploys and secures seamlessly across your diverse environments: from on-premises to public cloud, in containers and at the edge.

Single policy, unified management
F5 ADSP reduces time and improves efficiency with consistent security policy enforcement and unified management across all the environments where your apps and APIs are deployed.

Rich analytics and insights
Ensure your apps and APIs are available while strengthening their security with F5 ADSP's easy, comprehensive, and actionable AI-driven insights.

Secure third-party application access
Enable secure access for partners to specific apps through network segmentation and granular access policies with F5 on Equinix Network Edge.

F5 enables zero trust architectures that optimize your investments

A zero trust architecture must extend zero trust capabilities across your entire enterprise—users, devices, applications, workloads, data, and infrastructure—while seamlessly integrating with your existing investments. The F5 Application Delivery and Security Platform (ADSP) does exactly that. The F5 ADSP works with the existing portfolio of security solutions that create your zero trust architecture to extend zero trust security across every strategic point of your environment.

The F5 Application Delivery and Security Platform delivers consistent zero trust security across your entire portfolio

Employing a platform approach is key for ensuring consistent security measures across all apps, APIs, and app components. F5 ADSP delivers zero trust capabilities wherever they're needed, in any form factor or deployment model you require (e.g. hardware, software, SaaS, DPUs, or Kubernetes clusters), emphasizing the principals required in any zero trust architecture:

- **Explicit Verification:** Every user, device, and request must be authenticated and authorized using identity- and context-aware policies—not just network location.
- **Least Privilege Access:** Access is restricted to only authenticated and authorized users, and only to what's necessary for their work, minimizing the attack surface and potential breaches.
- **Continuous Monitoring:** Beyond initial verification, F5 emphasizes ongoing assessment of users, devices, and traffic to detect and respond to anomalies in real time.
- **Application-centric Security:** Given that applications and APIs are the primary targets in modern environments, F5 ADSP focuses on securing apps, APIs, and other application components wherever they reside—on-premises, in the cloud, or hybrid.

F5's leading industry solutions optimize any zero trust architecture

Application availability, application visibility, authentication, access control, and advanced threat protection are core to any zero trust architecture. F5 ADSP delivers industry-leading capabilities in each of these areas so you can deploy a layered security approach to ensure zero trust.

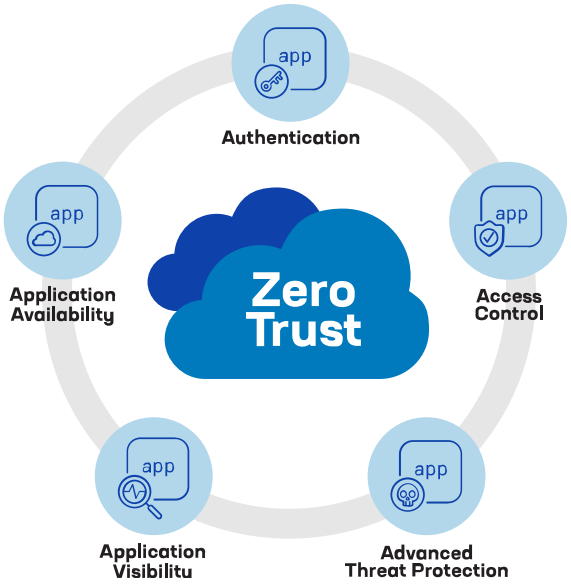

Figure: Components key to any zero trust architecture

Encrypted threat protection

Enhance zero trust security with high-performance decryption, re-encryption, and orchestration of encrypted traffic, enabling existing security tools to detect concealed threats, avoid unintended bypass, maintain compliance, and secure against hidden attacks like ransomware.

Zero trust app access

Extend zero trust access to any API and app—modern, classic, or custom—with authentication measures that include critical capabilities like MFA, SSO with support for SAML, OAuth and OIDC, behavioral risk analysis, and more.

Web app and API protection (WAAP)

Advance zero trust with layered protection for web apps and APIs—combining WAF, DDoS protection, bot defense, and API security to ensure app and API availability, enforce unified security policies, and block threats across all environments.

Zero trust for Kubernetes

Ensure all app and API communications in a Kubernetes environment are authenticated, authorized, encrypted, monitored, and secured with identity-based policies, least-privileged access controls, and WAF and DoS protection.

Data leakage prevention

Prevent sensitive data leaks with real-time, in-transit AI data classification, policy-driven enforcement, and continuous monitoring—all while eliminating risks from shadow AI.

Business partner application exchange

Ensure external partners can easily gain access to specific internal applications, services, and data. F5 and Equinix enhance security, reduce management complexity, and ensure compliance across global hybrid environments with network segmentation and granular service policy configuration.

Conclusion

No matter where you are in your zero trust journey, the F5 Application Delivery and Security Platform enables you to drive consistent, enhanced security across every app, API, and app component in your hybrid, multicloud environment. Gain visibility, enforcement, and intelligence where it matters most: the application layer. Leverage F5's zero trust capabilities to enhance security for users, apps, APIs, application components, and data through context-aware access, deep traffic inspection, and dynamic policy enforcement across legacy and modern environments.

Contact Us

Find out how you can employ F5 zero trust architecture solutions to achieve your goals. **Contact F5**