

# Introducing BIG-IP Next SSL Orchestrator

BIG-IP Next SSL Orchestrator provides modernized, next-generation encrypted traffic visibility and orchestration services that enterprises depend on for the security of their apps and organization.



## Key Benefits

### Accelerate time-to-value

Enable greater agility and automation for encrypted threat protection via declarative APIs and configuration templates.

### Lower operational complexity

Centralize all management and lifecycle tasks for BIG-IP Next SSL Orchestrator and your entire BIG-IP Next portfolio within a single console.

### Simply deploy the latest protections

Maintain a state-of-the-art security posture with accelerated software release cycles.

### Apply fast, consistent policy updates

Write a security policy once, deploy it to multiple instances, and freely migrate across platforms—regardless of policy complexity.

### Make rapid software upgrades

Perform major upgrades in minutes, shortening or entirely removing the need for maintenance windows and app downtime.

**To support an increasingly automated and DevSecOps-driven business environment, encrypted threat protection must be automated and agile—from policy implementation to the underlying software platform.**

# Apps Are Changing—So Is the Way We Secure Them From Encrypted Threats

**Applications, their deployment environments, and the security measures needed to protect them from encrypted threats are evolving at a record pace.** Look no further than today's modern business landscape as a testament to this transformation. Businesses are progressively embracing automation. They're relying on DevSecOps practices to achieve greater code quality, faster time-to-market, and heightened security. The typical application portfolio comprises a hybrid mix of modern, SaaS-based, legacy and custom apps, with the supporting platforms just as diverse—from on-premises data centers and private clouds to various public clouds and remote edge locations.

While these trends pave the way for greater business innovation and adaptability, they also fundamentally shift what's required to protect your organization, users, and applications from the ever-growing volume of risks and threats hidden within encrypted traffic. Attackers exploit encrypted traffic to bypass many security devices that double as inspection devices, serving as a Trojan Horse, delivering malware inside your network and exfiltrating sensitive data without detection.

Encrypted threat protection has become integral to app security—and SSL/TLS orchestration the gold standard approach. The ability to bridge the gap between applications that employ legacy and modern encryption protocols—to enable dynamic traffic steering across your security stack for each application—is key to enhancing visibility into, and protection against, encrypted threats. This also simplifies the intricacies of managing multiple points of control for encrypted traffic handling. Perhaps equally significant is the ability to reduce the overhead and complexity linked to security architecture itself. To align with the demands of an increasingly automated and DevSecOps-driven business environment, encrypted threat protection must be automated and agile—from policy implementation to the underlying software platform.

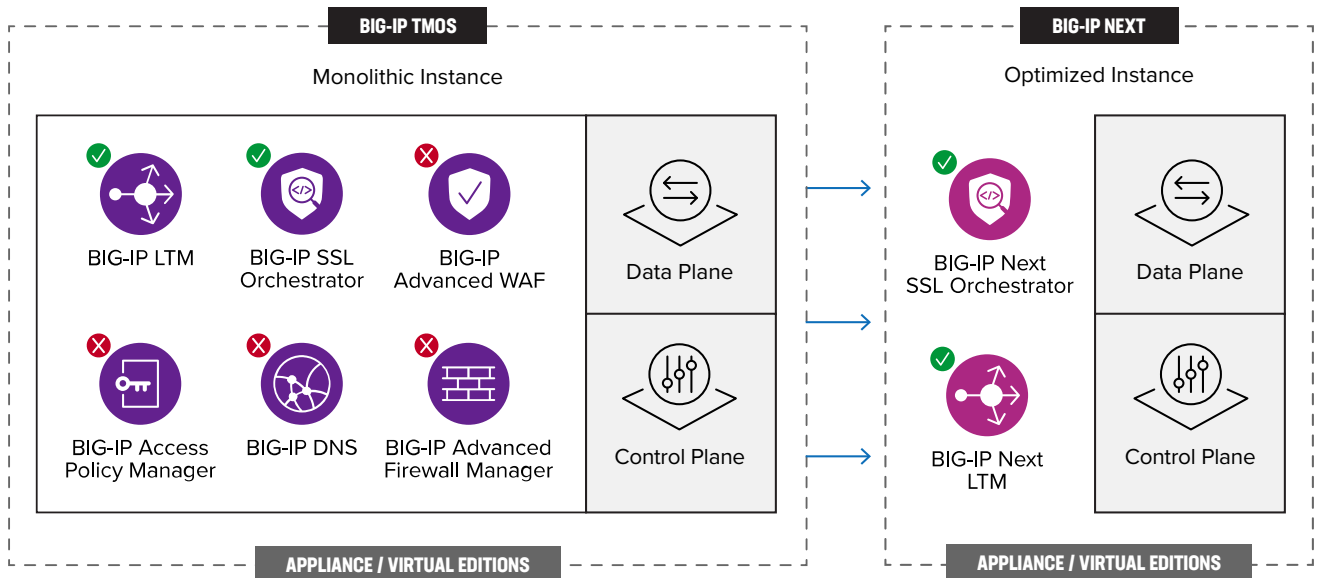
## BIG-IP Next: The Next-Generation BIG-IP Software

F5® BIG-IP® Next™ represents the cutting edge in F5® BIG-IP® software, designed to reduce operational complexity, improve performance, strengthen security, and enhance observability. This next-generation software harnesses a modern, highly scalable, and easily automatable architecture. It empowers you to capitalize on all the innovation happening with applications and the cloud while addressing security challenges inherent in hybrid apps and platforms.

Divided into container-based software modules, BIG-IP Next accelerates application delivery with app services that can be deployed and managed wherever they're needed. These services are supported by programmatic interfaces that are declarative and backward compatible. Its architecture enables quicker setup as well as more frequent and simpler upgrading and updating. It streamlines security management, eases purchasing and managing licenses, and robustly protects any app, anywhere.

BIG-IP Next introduces an automation-friendly framework that transitions away from imperative APIs, such as iControl REST, where you have to painstakingly sequence individual commands just to automate even the most basic of tasks. BIG-IP Next embraces declarative APIs (Application Services Extension (AS3)) and configuration templates (F5 Application Services Template (FAST)). AS3 and FAST are fully integrated with BIG-IP Next software and enable reuse of declarations and templates, plus comprehensive instance control, dramatically accelerating the app provisioning process from hours to mere minutes.

The lighter weight and adaptable architecture of BIG-IP Next not only simplifies operations and drives down costs but also delivers the flexibility and scalability essential for supporting even the most configuration-intensive applications.



**Figure 1:** Container-based BIG-IP Next has a lighter weight footprint and enables you to deploy only the desired product modules.

## Key Features

### Protect any app, anywhere against encrypted threats

Automate efficient decryption, re-encryption, and orchestration of inbound and outbound SSL/TLS traffic—all from a single control plane that's built for extreme scale.

### Deploy encrypted threat protection-as-code

Write to or embed APIs into your CI/CD pipeline, locking down SSL/TLS traffic inspection across your existing security solutions early in the dev cycle.

### Intelligently manage encrypted traffic

Centralize SSL/TLS decryption and route traffic across your security stack using advanced context-based classification and logical security service chains.

### Simplify cloud deployment

Leverage the API-first architecture to simply deploy cloud-based encrypted threat protection.

## BIG-IP Next Central Manager: Centralized Control and Visibility Across All Your BIG-IP Next Instances

At the core of every BIG-IP Next module is F5® BIG-IP® Next™ Central Manager—an intuitive user interface designed to streamline critical tasks and workloads, reducing complexity and saving time. Serving as a single source of truth, BIG-IP Next Central Manager ensures consistency and enforces compliance. Now, you can more cost-effectively and efficiently manage all your BIG-IP Next estate with:

- Full instance lifecycle management
- Policy and compliance management and security enforcement
- GUI, CLI, and API driven service provisioning and troubleshooting
- Comprehensive visibility and analytics
- Automation capabilities leveraging AS3 and FAST

## BIG-IP Next SSL Orchestrator: Modular, API-First, App-Centric Encrypted Threat Protection

F5® BIG-IP® Next™ SSL Orchestrator® is the modernized, next-generation evolution of F5® BIG-IP® SSL Orchestrator®, enabling enhanced automation, scalability, and overall ease of use. Designed to provide more agile encrypted traffic visibility and orchestration services, BIG-IP Next SSL Orchestrator empowers you to shift encrypted traffic decryption, inspection, re-encryption, and dynamic security orchestration left in your application development cycle and reduce operational complexity and costs by delegating encrypted threat protection to a hardened solution.

Leveraging an API-first, encrypted threat protection-as-code platform, BIG-IP Next SSL Orchestrator makes it possible for you to bring modern dynamic traffic steering to every application in your portfolio. You can achieve this effortlessly by either writing to an API or embedding APIs directly into your app development CI/CD pipeline.

With a completely re-architected software layer that leverages a container-based framework, you can flexibly migrate encrypted traffic handling policies across platforms\* while gaining significantly improved control plane scale. This means you can allocate dedicated compute resources as needed, adjusting to changing demands and updating configurations in real-time to prevent overload and maintain optimal performance. Plus, the streamlined upgrade and update process lets you independently select only the necessary modules that require upgrading or updating, accelerating the entire procedure.

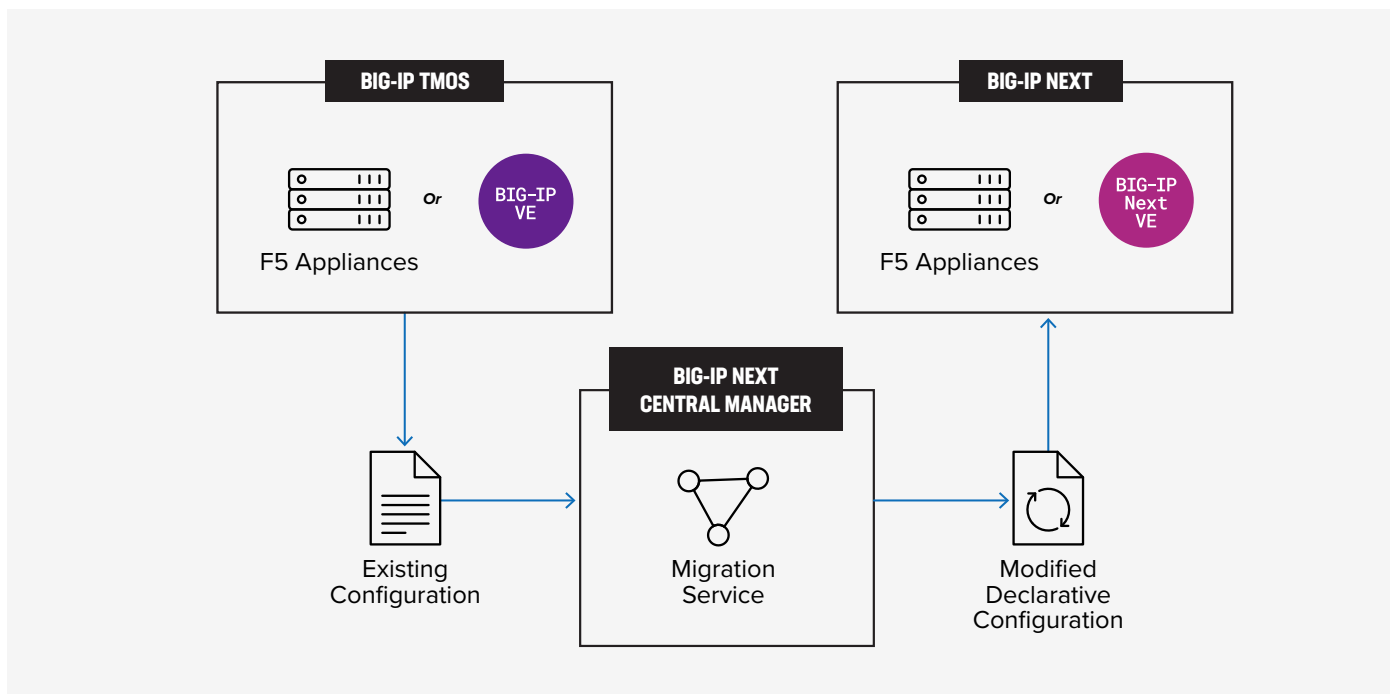
**BIG-IP Next SSL Orchestrator not only streamlines but revolutionizes the deployment of encrypted threat protection for your applications, offering unparalleled ease and speed –which is especially crucial for apps distributed across diverse cloud locations.**

As a result, BIG-IP Next SSL Orchestrator not only streamlines but revolutionizes the deployment of encrypted threat protection for your applications, offering unparalleled ease and speed. This is especially crucial for apps distributed across diverse cloud locations. Moreover, BIG-IP Next SSL Orchestrator enables you to focus on what’s crucial to your apps—building features—while ensuring that your security measures are tested and encrypted traffic visibility and orchestration services extend across your entire application portfolio.

\*F5® rSeries, F5® VELOS® platform, and F5® BIG-IP® Virtual Edition (VE)

## **BIG-IP Next Central Manager Migration Service: Complementary, Seamless Migrations to BIG-IP Next From Existing BIG-IP Configurations**

[BIG-IP Next Central Manager Migration Service](#) makes it effortless to transition your BIG-IP TMOS configurations, including what you’ve set up for BIG-IP SSL Orchestrator, to BIG-IP Next. Using AS3 as the basis for this process, BIG-IP Next Central Manager Migration Service transforms BIG-IP TMOS User Configuration Set (UCS) files or AS3 declarations into AS3 or FAST declarations that replicate configurations onto BIG-IP Next. With it, you have the ultimate flexibility to perform the migration process for entire BIG-IP instances or on a per-app basis, allowing you to migrate at your own pace.



**Figure 2:** Effortlessly transition to BIG-IP Next using the BIG-IP Next Central Manager Migration Service.

**BIG-IP Next SSL Orchestrator supports a range of deployment options that should satisfy the requirements of any app deployment.**

## Flexible Deployment and Licensing Options

BIG-IP Next SSL Orchestrator supports a range of deployment options that should satisfy the requirements of any application deployment—from cloud to edge and on-premises.

- **rSeries:** High-performance, fully automatable appliance for traditional and emerging apps
- **VELOS:** Powerful next-generation chassis and blade system with the agility and scale of a modern architecture
- **F5 BIG-IP VE:** Cloud optimized virtual instance for public or private cloud environments

Choose the licensing model that best meets your needs.

- **Flexible consumption program:** 3-year enterprise agreement empowering self-service licensing for maximum architectural flexibility
- **Subscription:** 1- to 3-year renewable subscriptions affording upfront savings plus access to F5 premium support
- **Term-limited subscription:** 5-year, one-time CapEx investment plus annual OpEx fees for F5 support
- **Utility:** Pay-as-you-go model with no long-term commitments plus access to F5 premium support

## Next Steps

Want to learn more about BIG-IP Next SSL Orchestrator? Or see how it works with a free trial? Contact your F5 account manager or [F5 Sales](#) today.

