SOLUTION OVERVIEW

# BIG-IQ Centralized Management

F5 BIG-IQ Centralized Management provides a unified, easy-to-use set of management tools, helping organizations ensure the performance, security, and availability of applications, wherever they live.

KEY BENEFITS

**Enhanced operational efficiency**
Increase operational efficiency among cross-functional teams.

**Improved security efficacy**
Simplify the auditing of security policies.

**Fewer configuration errors**
Reduce manual configuration errors.

**Better consistency and compliance**
Ensure consistency and compliance across BIG-IP devices.

**Increased automation**
Automate lifecycle management of encryption certificates on F5 BIG-IP devices.

KEY FEATURES

**Device and security management**
Easily manage devices and security services.

**Easy scalability**
Scale device management up to 1,200 devices.

**Detailed visibility and control**
Increase the security level with granular visibility and control.

**Advanced bot mitigation**
Manage unified bot defense with real-time visibility.

# The Need for a Centralized Approach to Application Security

As enterprises continue to expand their web applications portfolio, the demand for a centralized approach to app security visibility and management has increased. Defining and maintaining a consistent security level across platforms is often difficult given the heterogeneous mix of application architectures in a typical organization's portfolio.

Management of ever-expanding application portfolios and the additional services needed to support them have become even more challenging. The State of Application Strategy report shows complexity rises as modernization increases and found that modern and mobile applications are slowly replacing traditional applications. Addressing this complexity comes down to driving consistency across environments and ensuring that teams ranging from network operations to application developers have access to a unified, easy-to-use set of security management and visibility tools.

F5 BIG-IQ Centralized Management enables users to manage the F5 BIG-IP virtual and physical device lifecycle from a single console. BIG-IQ provides the holistic management of F5 Advanced Web Application Firewall (WAF), BIG-IP Access Policy Manager (APM), F5 SSL Orchestrator, and BIG-IP Advanced Firewall Manager (AFM). BIG-IQ is also API-driven. Administrators can glean all of the information available from the BIG-IQ user interface from its REST API, which can be used with third-party tools such as security incident and event management and security orchestration, automation, and response.

F5 BIG-IQ empowers network teams to take complete control of their F5 investments. They can assign resources and permissions with role-based access control, and application owners can quickly and easily add, modify, and manage security policies for their apps.

# Take Control of App Security with BIG-IQ Centralized Management

### F5 BIG-IP Access Policy Manager (APM)

As organizations shift to a "work from anywhere" workforce, their need for secure remote application access has become paramount. BIG-IQ Centralized Management simplifies the management of BIG-IP APM through its ability to create, control, and configure extensive collections of application access and security policies from a single portal. F5 BIG-IQ delivers deep visibility into application access and usage. It also enables security operations (SecOps) to centrally create, manage, and deploy access policies across their BIG-IP APM deployments. With BIG-IQ, SecOps teams can easily use declarative APIs to create secure assertion markup language (SAML) service provider configurations for deployments to manage BIG-IP devices—leveraging an easy-to-navigate dashboard to authenticate and view all of the apps to which users have access.

BIG-IQ CENTRALIZED MANAGEMENT SIMPLIFIES THE MANAGEMENT OF BIG-IP APM THROUGH ITS ABILITY TO CREATE, CONTROL, AND CONFIGURE LARGE COLLECTIONS OF APPLICATION ACCESS AND SECURITY POLICIES FROM A SINGLE PORTAL."

### F5 Advanced Web Application Firewall (WAF)

With F5 Advanced WAF, BIG-IQ Centralized Management enables fast and programmatic policy creation, deployment, and administration for organizations managing web application firewalls. It provides a central point of control for Advanced WAF on BIG-IP Virtual Editions and BIG-IP hardware in any environment—all from a role-specific, unified, app-centric dashboard that improves security management and visibility.

BIG-IQ can inject automation into Advanced WAF creation, provisioning, and ongoing management workflows with Application Services 3 (AS3) Extension templates. BIG-IQ and AS3—part of the F5 Automation Toolchain—are tightly integrated and enable the creation and deployment of Advanced WAF security services and deep visibility via app-centric dashboards. SecOps can achieve this automation and templating functionality from an intuitive graphical UI or via API.

BIG-IQ also provides SecOps teams with powerful tools to ensure compliance and deliver applications securely and effectively across multiple devices. SecOps teams can easily create WAF policies from pre-defined security templates, detect and mitigate cyber attacks, implement mitigations such as F5's Threat Campaigns, or manage security holistically using Advanced WAF features like bot detection, denial-of-service (DoS) configuration, and management. SecOps teams can also easily audit security policies with dashboards such as Configuration Analyzer to detect anomalies and vulnerabilities, understand policy effectiveness, and use proactive suggestions to improve policies quickly and easily to enhance application protection.

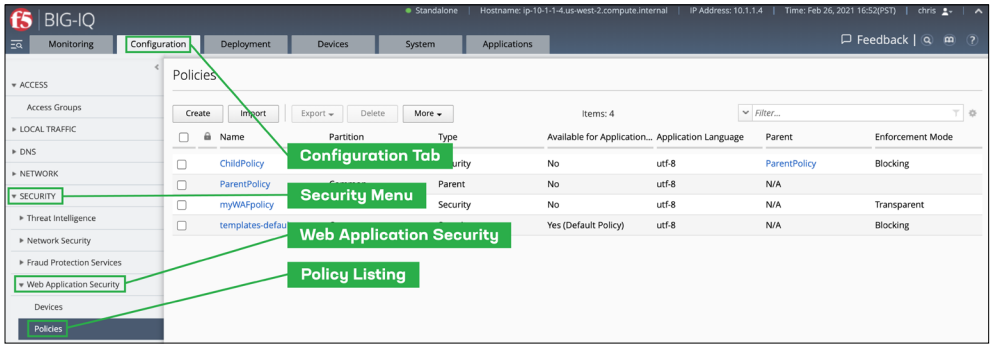


**Figure 1:** View many F5 Advanced WAF policies across deployments for immediate visibility and insight—and share in audits to simplify compliance.

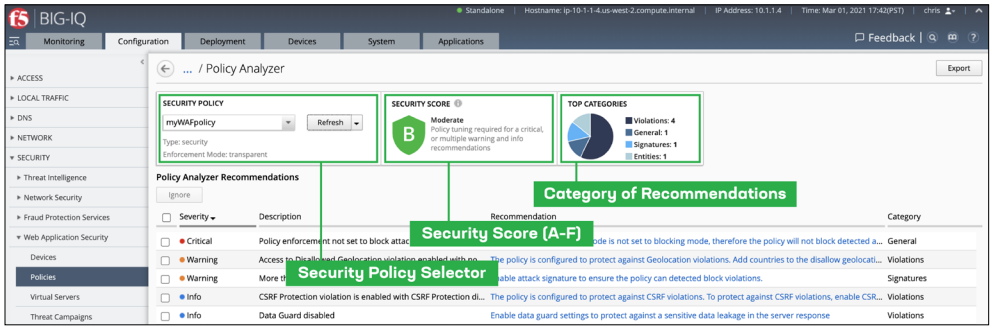


**Figure 2:** Use the BIG-IQ Centralized Management Configuration Analyzer to easily audit security policies, detect violations and anomalies, and enable strong application protection.

Security teams can ensure consistency and compliance across F5 security and application delivery solutions. They can easily compare WAF policies side-by-side in a table format. Policy comparison views enable SecOps teams to identify inefficiencies, redundancies, and weaknesses in different policies for quicker compliance.

### F5 SSL Orchestrator

Today, with the vast majority of web traffic encrypted, visibility is vital to mitigating encrypted threats and securing applications. Managing and orchestrating encrypted traffic at scale requires an advanced approach. BIG-IQ Centralized Management offers a dedicated dashboard to simplify and enhance management of the numerous topologies supported by F5 SSL Orchestrator for multi-site deployments. Administrators can easily configure and manage SSL Orchestrator to decrypt and re-encrypt traffic for multiple devices. SecOps teams can leverage a unified API to manage SSL Orchestrator configurations easily. Additionally, the SSL Orchestrator dashboard provides unified visibility and traffic control, monitoring the health of security products and services in their security stack across SSL Orchestrator topologies.

BIG-IQ also provides an integrated solution for Venafi management and Let's Encrypt certificates. Managing certificates through BIG-IQ allows organizations to discover and manage certificates on F5 devices, security solutions, and web and proxy servers. In addition to alerts management, it automates certificate renewals—pushing certificates to end devices, automating certificate lifecycle management, and helping to prevent costly certificate expirations and outages.

### F5 BIG-IP Advanced Firewall Manager (AFM)

Managing each BIG-IP device manually can become time-consuming. BIG-IQ Centralized Management enhances the manageability of F5 BIG-IP AFM. It provides enhanced troubleshooting, the ability to push updated configurations efficiently, and easy methods for maintenance and upgrades.

Managing each device can lead to human error and policy inconsistencies. BIG-IQ addresses these issues by letting users centrally apply existing sets of policies. Its enhanced scalability allows enterprises to oversee all F5 infrastructure with a single instance of BIG-IQ capable of managing up to 1,200 devices. BIG-IQ allows for easily configurable zones and reporting on unused objects to optimize performance. It enables better management and increased visibility of BIG-IP AFM, improving an organization's overall security posture.

## Conclusion

As organizations deploy applications in multiple clouds and architectures, it's becoming increasingly complex to manage security for all of these apps. F5 BIG-IQ Centralized Management enables enterprises to easily control all of their BIG-IP devices and services from a single, unified management platform—improving threat protection and their overall security posture.

**To learn more, visit the F5 BIG-IQ Centralized Management webpage and F5 Application Security webpage.**