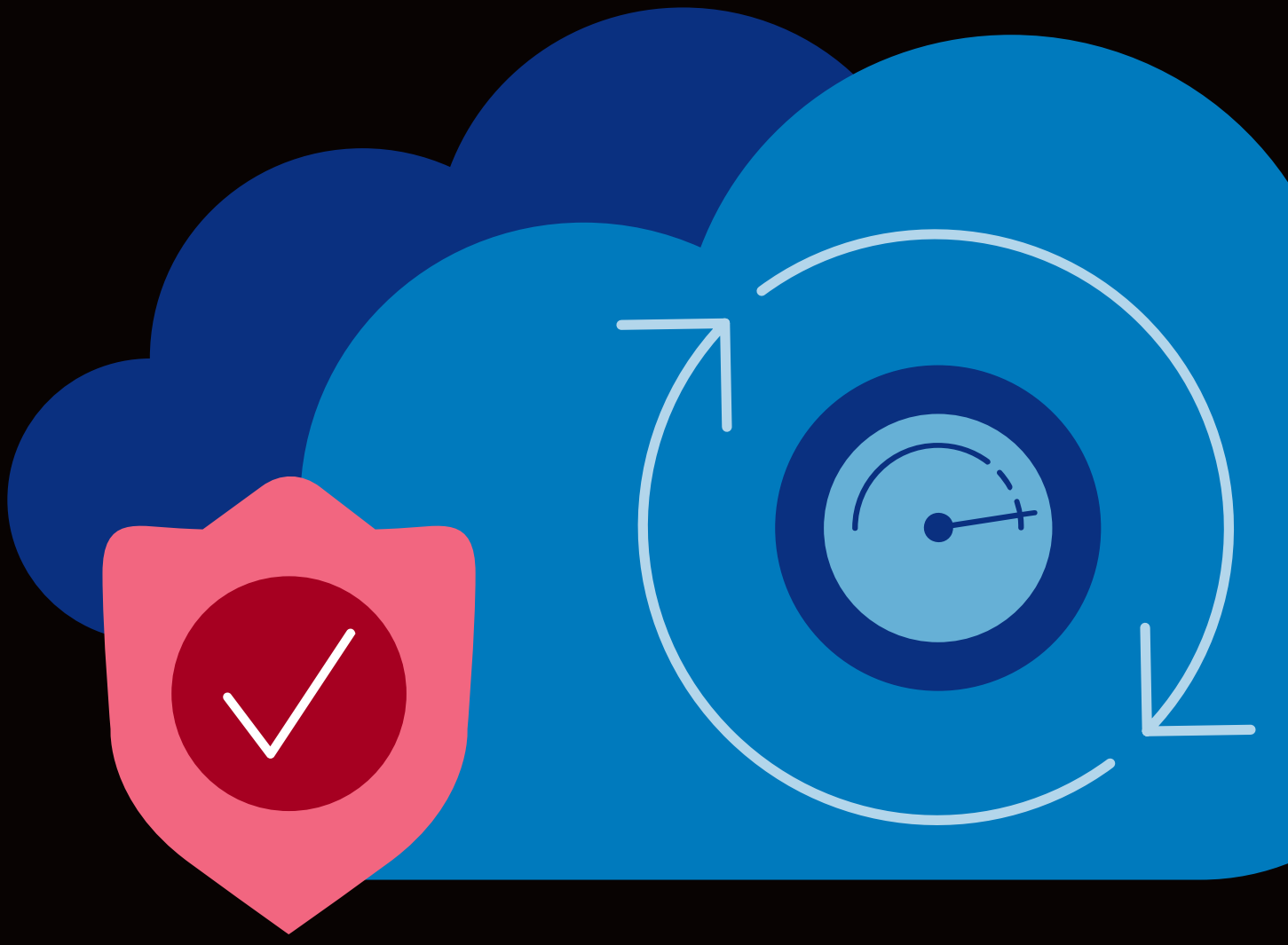
Solution Overview

F5 BIG-IQ Centralized Management

Ensure the performance, security, and availability of applications, wherever they live, with a unified, easy-to-use set of management tools.



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 Application Service Management
Easily manage devices and app delivery and security services.

Easy Scalability
Scale device management up to 1500 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 and continue to adopt hybrid, multicloud, and distributed application deployments, 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—what we call the "ball of fire."

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 that 88% of organizations operate multiple app deployment models, and the number of models in use is increasing. 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® BIG-IP® Advanced WAF®, BIG-IP® Access Policy Manager® (APM), BIG-IP® SSL Orchestrator®, and BIG-IP® Advanced Firewall Manager™ (AFM). BIG-IQ is also API driven, allowing administrators to access. 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 (SIEM) and security orchestration, automation, and response (SOAR).

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

BIG-IP APM

As organizations shift to a "work from anywhere" workforce, their need for secure remote application access has become paramount. BIG-IQ 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. BIG-IQ delivers deep visibility into application access and usage. It also enables security operations (SecOps) teams 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 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.

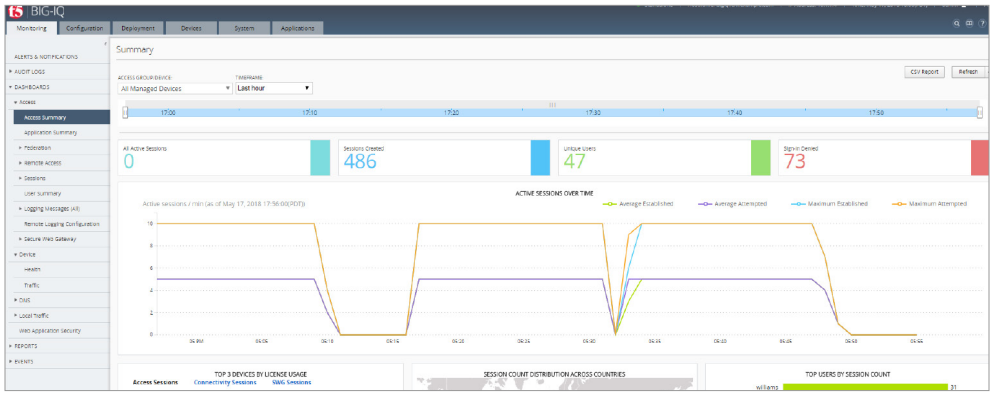


Figure 1: BIG-IQ provides flexible dashboards to help manage network access policies and events.

BIG-IP Advanced WAF

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

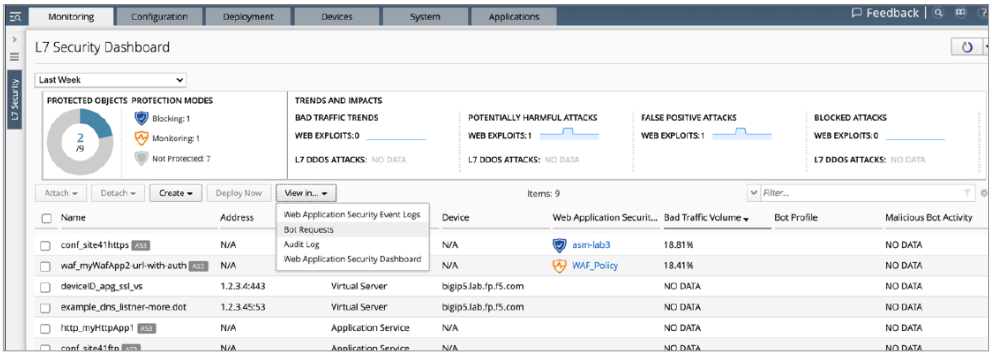


Figure 2: Ensure application security performance from the BIG-IQ L7 Security Dashboard, which enables users to drill into important security events and metrics such as WAF status, malicious traffic volume, web exploits, DDoS attacks, bot traffic, and more.

BIG-IQ can inject automation into BIG-IP Advanced WAF creation, provisioning, and ongoing management workflows with Application Services 3 (AS3) Extension templates. BIG-IQ and AS3—part of the F5® BIG-IP® 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 Threat Campaigns, or manage security holistically using BIG-IP Advanced WAF features like detection and denial-of-service (DoS) protection 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.

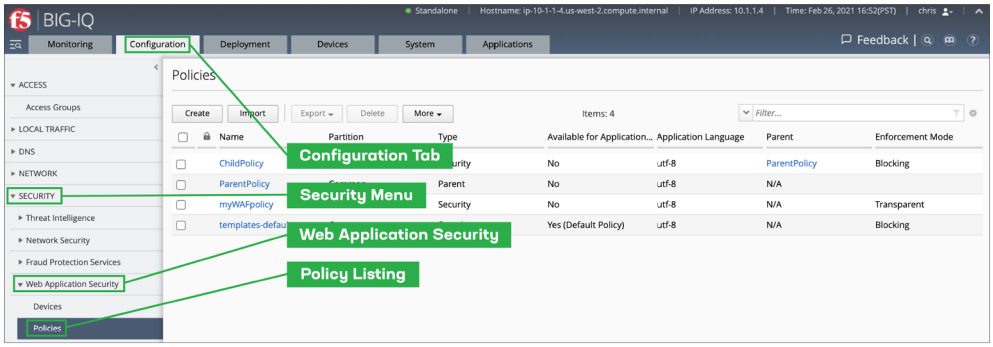


Figure 3: View BIG-IP Advanced WAF policies across deployments for immediate visibility and insight—and share in audits to simplify compliance.

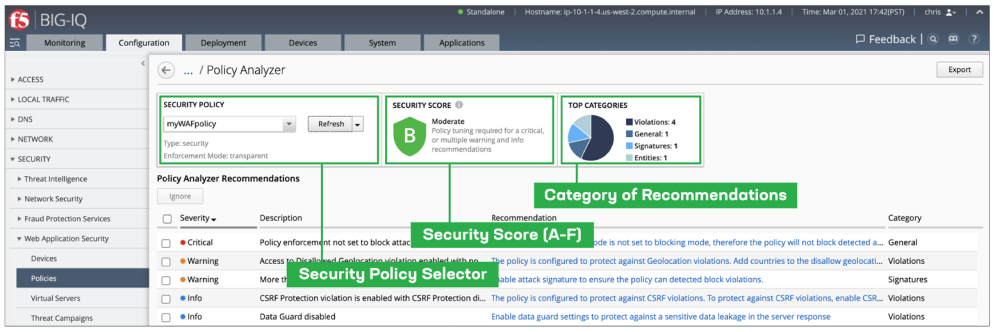


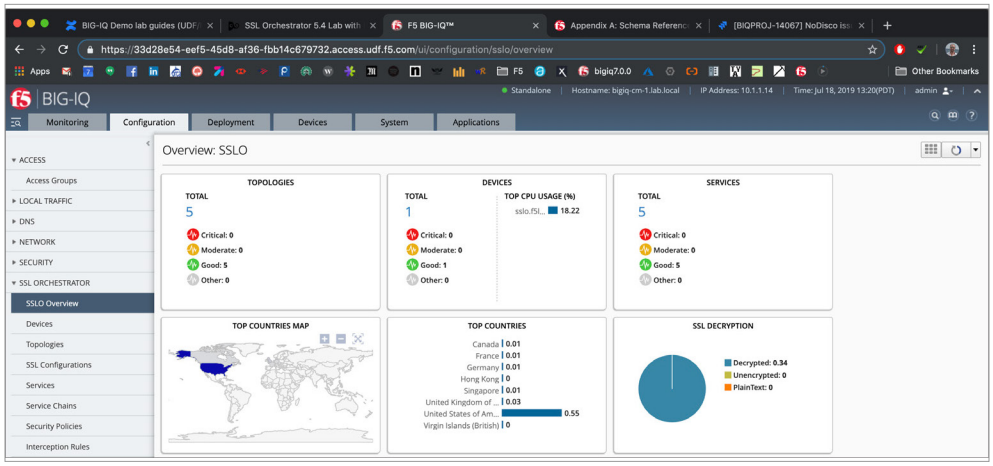
Figure 4: Use the BIG-IQ Configuration Analyzer to easily audit security policies, detect violations and anomalies, and enable strong application protection.

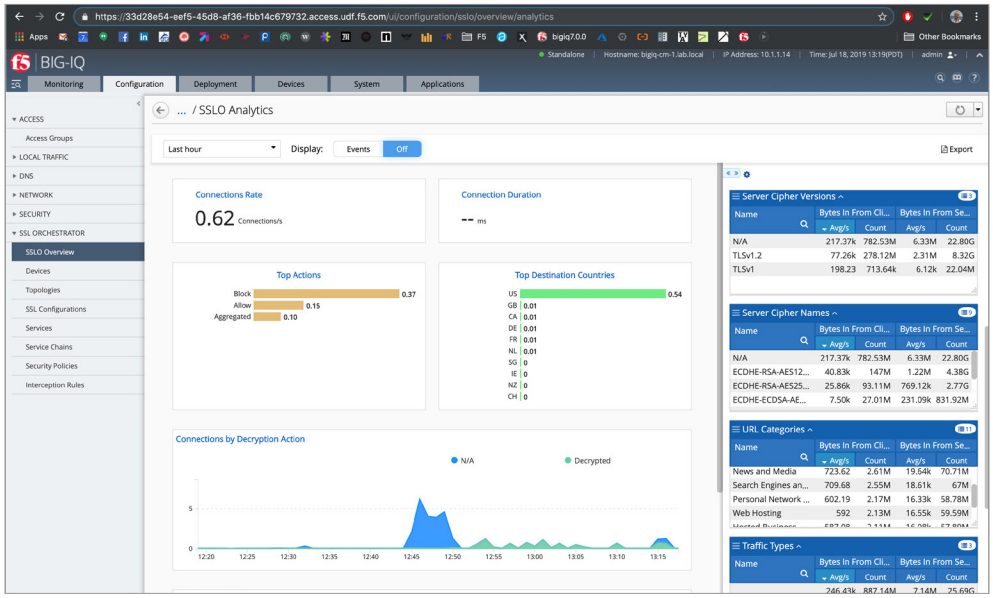
Security teams can ensure consistency and compliance across F5 security and application delivery solutions by easily comparing WAF policies side-by-side in a table format. Policy comparison views enable SecOps teams to identify inefficiencies, redundancies, and weaknesses in different policies for quicker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

BIG-IP 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 offers a dedicated dashboard to simplify and enhance management of the numerous topologies supported by BIG-IP SSL Orchestrator for multi-site deployments. Administrators can easily configure and manage SSL Orchestrator to decrypt and re-encrypt traffic for multiple devices via API. Additionally, the BIG-IP SSL Orchestrator dashboard provides unified visibility and traffic control, monitoring the health of security products and services in their security stack across topologies.

Figure 5 and 6: BIG-IQ provides both an at-a-glance and a comprehensive view of SSL traffic, topologies, devices, services, and key metrics with analytics.





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.

BIG-IP AFM

Managing each BIG-IP device, service, and/or security policy manually is time-consuming, increases the likelihood of human error, and leads to policy inconsistency. BIG-IQ enhances the manageability of BIG-IP AFM with troubleshooting, the ability to push updated configurations efficiently, and easy methods for maintenance and upgrades.

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 1500 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. BIG-IQ 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 BIG-IQ webpage and F5 Application Security webpage.