

## What's Inside

- 2 Drive Efficiencies with a Comprehensive Web Application Firewall Service
- 2 Defend with Proven Security Effectiveness
- 3 Comprehensive Attack Protection
- 3 Built-in Compliance and Reporting Capabilities
- 3 Receive Expert Policy Building and Monitoring
- 4 Hybrid Policy Management and Deployment
- 4 Gain Attack Insights and Intelligence
- 4 The Silverline Web Application Firewall Architecture
- 5 The Silverline Cloud-Based Platform
- 5 Flexible Licensing
- 5 F5 Security Operations Center
- 5 More Information

## Get Expert Service to Protect Web Applications and Achieve Compliance

Organizations that move application workloads to the cloud face challenges protecting enterprise data. As security attacks across traditional and cloud environments become more sophisticated, in-house security teams often struggle to stay up to date on the latest attacks and protection measures, and deliver consistent policies and compliance across environments. A lack of consistency can result in security vulnerabilities, higher expenses, and a slower response to threats and compliance issues.

F5® Silverline™ Web Application Firewall is a cloud-based service built on BIG-IP® Application Security Manager™ (ASM)—with 24x7x365 support from highly specialized security experts to help organizations protect web applications and data, and enable compliance with industry security standards, such as PCI DSS.

### Key benefits

#### Ensure application security and compliance

Get comprehensive protection from advanced layer 7 attacks, OWASP Top Ten application security risks, and zero-day attacks—and enable compliance with key regulatory mandates.

#### Get 24x7x365 expert service

Receive 24x7x365 access to web application firewall (WAF) experts who build, proactively monitor, and fine-tune WAF policies against known and emerging threats.

#### Deploy flexibly across hybrid environments

Ensure consistent web application security, availability, and user experiences across traditional and cloud data centers.

#### Defend with proven security effectiveness

Leverage security efficacy with technology built on the NSS Labs–recommended BIG-IP ASM, based on tests that demonstrate 99.89 percent overall security effectiveness.

#### Drive operational and cost efficiencies

Remove the complexity of WAF management, increase the speed to deploy new policies, and decrease operational expenses.

#### Gain attack insights and intelligence

Access reports through the cloud-based customer portal and incorporate external intelligence for securing apps against identified threats.



## Drive Efficiencies with a Comprehensive Web Application Firewall Service

The growth of cloud-hosted web applications has been accompanied by increasingly sophisticated security attacks and risks that threaten enterprise data. As a result, administrators and security teams face challenges keeping up to date on the latest attacks and protection measures. At the same time, they must meet the stringent compliance requirements for online commerce and data sharing across traditional and cloud environments.

Organizations must choose between employing specialized IT security teams in-house—resulting in higher expenses and increased time to deploy policies—or offloading the complex WAF policy management and compliance to a service to drive efficiencies.

The Silverline Web Application Firewall service delivers comprehensive, efficient layer 7 protection and compliance for enterprise data and web applications across all environments. The service also includes expert support from highly specialized security experts who remove the complexity of WAF policy management, increase the speed to deploy new policies, and free up internal IT resources and budget for other projects.

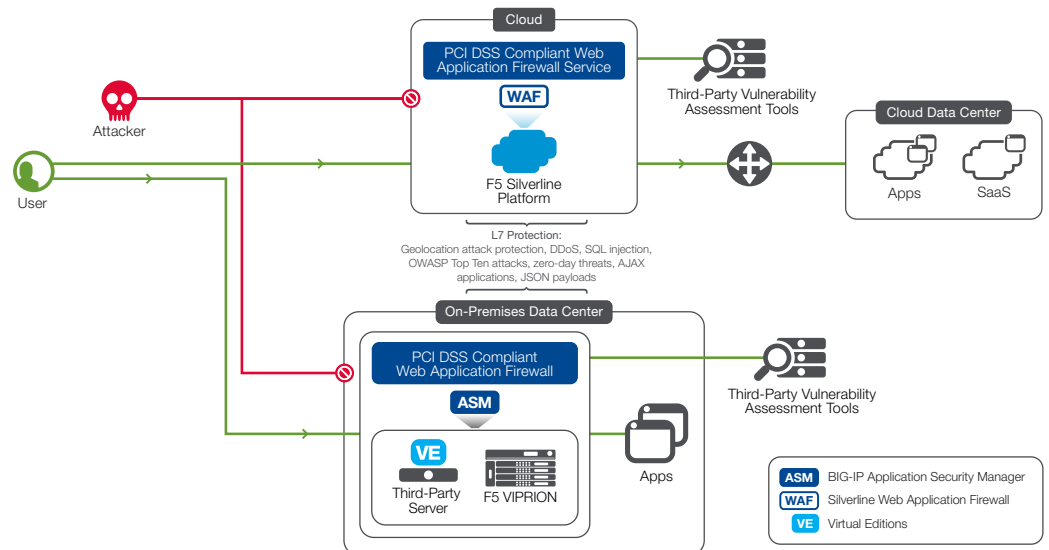


Figure 1: The Silverline Web Application Firewall service protects web applications no matter where the app is hosted—in the private cloud, the public cloud, or a physical data center.

## Defend with Proven Security Effectiveness

Silverline Web Application Firewall is built on BIG-IP ASM, which is recognized as the most scalable WAF on the market and is deployed in more data centers worldwide than any other WAF. NSS Labs recommends BIG-IP ASM based on tests that demonstrate 99.89 percent overall security effectiveness with minimal false positives (0.124 percent) as compared with competitors. [To learn more, read the product analysis report.](#)

## Comprehensive Attack Protection

Silverline Web Application Firewall provides comprehensive geolocation attack protection from layer 7 distributed denial-of-service (DDoS), SQL injection, OWASP Top Ten application security risks, cross-site scripting (XSS), and zero-day web application attacks. It prevents execution of fraudulent transactions, stops in-browser session hijacking, and secures AJAX applications and JSON payloads. The service also delivers proactive bot defense capabilities that provide always-on protection—preventing automated layer 7 DoS attacks, web scraping, and brute force attacks. Silverline Web Application Firewall provides live updates for attack signatures to ensure up-to-date protection, geolocation-based blocking, and an integrated XML firewall. For more details on these attack protections, please see the [BIG-IP ASM datasheet](#).

## Built-in Compliance and Reporting Capabilities

Advanced, built-in security protection and remote auditing help organizations comply with industry security standards, including the Payment Card Industry Data Security Standard (PCI DSS), HIPAA, Basel II, and SOX—cost effectively and without multiple appliances, application changes, or rewrites. Silverline Web Application Firewall reports previously unknown threats, such as layer 7 DoS and SQL injection attacks, and mitigates web application threats to shield the organization from data breaches.

## Receive Expert Policy Building and Monitoring

Websites are diverse, complex, and constantly changing—requiring policies with hundreds if not thousands of clear and precise rules. The Silverline Web Application Firewall service includes the highest level of service in the industry with F5 Security Operations Center (SOC) experts who manage policy changes while balancing the strictest security controls with legitimate user access.

Unlike other WAF service vendors that provide self-service capabilities and expect the customers to handle most of the configurations and policy management, the F5 SOC experts are available 24 hours a day, 7 days a week, 365 days a year. These experts build, monitor, and fine-tune policies to protect web applications and data from new and emerging threats.

### Expert policy creation

F5 SOC experts are available to work with customers to rapidly deploy policies and create more advanced policies based on heuristic learning and specific application-security needs. Policies can be created to work in conjunction with existing BIG-IP ASM configurations.

### Expert policy staging

F5 SOC experts work to reduce false positives by staging and testing policies in a live environment using attack signatures, file types, URLs, and other parameters. These tests determine if changes are needed before a policy is enforced, without reducing current protection levels. Policies are redesigned and retested until they are ready for live implementation.

## Hybrid Policy Management and Deployment

Silverline Web Application Firewall provides a simplified approach to deploying policies across traditional and cloud environments. With a centralized deployment of WAF policies from the Silverline cloud-based platform, organizations can reduce IT overhead, minimize configuration errors, and ensure the overall effectiveness of each policy to protect web applications no matter where they reside in the network.

## Gain Attack Insights and Intelligence

The Silverline Web Application Firewall service includes access to the Silverline customer web portal—enabling administrators to securely communicate with F5 SOC experts and view centralized threat-monitoring reports. The customer portal provides immediate attack details and enhanced visibility into the mitigation techniques used to detect and prevent the application attack. Details include source geo-IP mapping, blocked vs. alerted attacks, blocked traffic, blocked attack types, alerted attack types, threats, bandwidth used, hits/sec, and the type of traffic and visits (bots v. humans).

### Integration for agility and adaptability

The ability to respond to frequent changes in attack methods is a key component of web application security. By integrating with third-party products, Silverline Web Application Firewall provides a dynamic and adaptable security solution. Data can be uploaded from WhiteHat Sentinel, IBM Rational AppScan, HP WebInspect, Cenzic Hailstorm, and QualysGuard Web Application Scanning products. These products offer vulnerability assessment, auditing, and real-time database reporting to provide security breach reviews, attack prevention, and compliance.

## The Silverline Web Application Firewall Architecture

Silverline Web Application Firewall is a security service built on F5's unique BIG-IP ASM web application firewall to protect applications from OWASP Top 10 threats and other zero-day threats.

### Silverline Web Application Firewall protects against application attacks including:

- OWASP Top Ten attacks
- Layer 7 DoS and DDoS
- Brute force
- Parameter and HPP tampering
- Sensitive information leakage
- Buffer overflows
- Cookie manipulation
- Various encoding attacks
- Forceful browsing
- Hidden fields manipulation
- Request smuggling
- XML bombs/DoS
- Web scraping
- Reverse engineering
- Application tampering
- Zero-day web application attacks
- AJAX/JSON web threats

### Security Operations Center services include:

- Expert policy setup
- Policy fine-tuning
- Policy staging
- Proactive alert monitoring
- False positives tuning
- Detection tuning
- Whitelist/Blacklist configuration

### Additional security features:

- RFC compliance
- Bot protection
- VA Scan importation with third-party DAST Vendors
- PCI compliance reports
- Web scraping prevention
- Geolocation-based blocking

## The Silverline Cloud-Based Platform

Silverline is F5's cloud-based application services platform. Its services can be deployed on-demand to achieve seamless scalability, security, and performance for applications in traditional and cloud environments. By combining F5's on-premises application services with Silverline services, organizations can achieve faster response times, unparalleled visibility and reporting, and cost efficiencies.

## Flexible Licensing



### F5 Silverline Web Application Firewall Service

Available in 1-year and 3-year subscriptions based on the number of sites protected and monthly bandwidth required.

## F5 Security Operations Center

The F5 Security Operations Center offers world-class support and guidance to help you get the most from your F5 Silverline investment. Whether it's providing fast answers to questions, guidance on your security questions, or assisting with modifications to your implementation, the F5 SOC can help ensure your applications are always secure, fast, and reliable. For more information about the full line of F5 Global Services, visit [f5.com/services](https://f5.com/services).

## More Information

To learn more about Silverline Web Application Firewall, visit [f5.com](https://f5.com) to find these and other resources.

### Silverline Web Application Firewall

[Silverline platform](#)

### Related products

[BIG-IP Application Security Manager](#)

### Reports

[Gartner Web Application Firewall Magic Quadrant, 2014](#)

[NSS Web Application Firewall Product Analysis for BIG-IP ASM](#)

F5 Networks, Inc. 401 Elliott Avenue West, Seattle, WA 98119 888-882-4447 [f5.com](https://f5.com)

Americas  
[info@f5.com](mailto:info@f5.com)

Asia-Pacific  
[apacinfo@f5.com](mailto:apacinfo@f5.com)

Europe/Middle East/Africa  
[emeainfo@f5.com](mailto:emeainfo@f5.com)

Japan  
[f5j-info@f5.com](mailto:f5j-info@f5.com)

Solutions for  
an application world.

