Web Application Firewall

Last updated 11-06-23

The distributed Web Application Firewall (WAF) solution protects our public-facing web applications and application program interfaces (APIs) from cyber threats that can deface an organization's information, conduct bot-driven fraud attempts, or degrade communications or interfaces.

The WAF combines signature and behavior-based protection for web applications, acting as an intermediate proxy to inspect internet application connections. This service protects against multiple threats frequently targeting web application vulnerabilities, such as the Open Worldwide Application Security Project (OWASP) Top 10.

This service can be used to protect both cloud-hosted and on-premises public-facing applications.

The WAF service protects SecureAccess Washington (SAW)-integrated applications at no additional cost to agencies that leverage SAW integration.

Helpful information

Service category
Security

Service availability
24/7/365

Planned maintenance
Planned maintenance is performed after hours and coordinated with agency representatives.

Related services
Managed Firewall
Vulnerability Assessment

How to request service
Submit a request for service through our Customer Portal.

Service owner
Deputy CISO Security Operations

Intended Customers

The WAF service is available to large, medium, and small agencies, boards, commissions, and Tribal governments on the State Government Network (SGN) or Public Government Network (PGN).

The Web Application Firewall (WAF) protects web applications from common attacks such as SQL injection, cross-site scripting, and denial of service. The WAF filters, monitors, and blocks malicious traffic before it reaches the web server, preventing exploitation of vulnerabilities in the application code or logic.

Applications not protected by a WAF are exposed to a higher risk of being compromised, damaged, or stolen by cybercriminals. Without a WAF, attackers can more easily access sensitive data, manipulate functionality, disrupt availability, or even take over the entire application. This can result in financial losses, reputational damage, legal liabilities, and regulatory penalties for the application owners and users.

Service Features

- Load balancing and reverse proxy functionality.
- Bot protection using behavioral analytics.
- Layer 7 DDoS protection from botnet and automated attacks.
- Automated threat mitigation.

The features described above have already been implemented for approximately 40 agencies across 300 web applications that leverage SAW integration.

The WAF service currently blocks over two million malicious connection attempts per month across the following attack vectors:

- Geolocation violations (country blocks).
- SQL injection attempts.
- HTTP parser attacks.

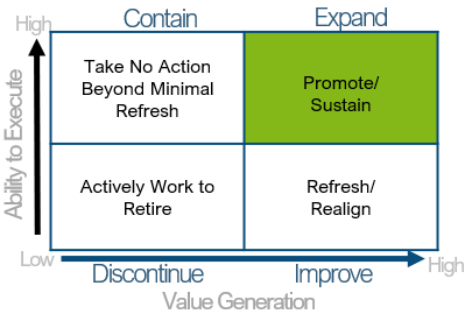
Customer Engagement

- Monthly Technology Management Council (TMC), Business Management Council (BMC), and Enterprise Security Governance (ESG) meetings for agency CIOs and IT and business leaders to inform and sponsor enterprise strategy, policy, and investments.
- Office of Cybersecurity (OCS) open office hours for hot-topic engagements.
- Regularly scheduled meetings between customers and business relationship managers (BRM) to connect, advise, address concerns and provide solutions.

- Weekly group calls for state CIOs and CISOs to provide updates on important and immediate issues and actions.
- Regular outreach to solicit feedback, provide updates and inform agencies on emerging projects, initiatives and services.
- Requests for new consultations and modifications to existing applications.

Action plan

Current activity



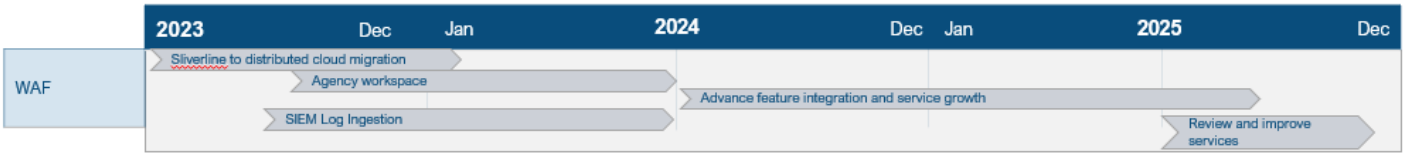
- Migrating WAF services from the F5 Silverline solution to the F5 Distributed Cloud (XC) WAF service, offering more flexibility to agencies and additional API protection.
- Building out agency WAF workspaces for those agencies that directly consume this service outside of the SAW deployment.
- Coordinating with customer agencies to conduct migration with expected completion by the end of 2023.
- Develop enterprise-wide WAF strategy to maximize protective postures across agency internet-facing applications, with road map strategy expected to be complete by end of FY24.
- Define and mature retention capabilities for logs.

One- to two-year goals

- Integrate WAF solution into the Enterprise SIEM for log visibility.
- Onboard additional agencies with the expectation to double the current coverage across the enterprise, growing from 18 to 30 agencies by the end of FY 25.
- Conduct risk assessments across the attack surface for high-value, high-risk application coverage, prioritizing web applications that store and manage constituent data, with a goal of 100% web applications that manage PII be protected by the end of FY25.
- Start enterprise needs assessment across the attack surface and build a metrics-driven decision package for the 25-26 biennium to support this as an enterprise-allocated service.

Three- to five-year goals

- Conduct ROI analysis and assess market offerings to mature the service.
- Expand service offering and ensure cloud app integration.
- Assess, select and modernize the service as future capabilities grow in this space.



Service review and fully loaded service budget projection

Revenue source

The Security Operations Center (SOC) is funded through the Office of Cybersecurity Central Service Model (CSM). Annually, the Office of Financial Management uses the financial model to allocate funding support from state agencies that use the service.

Expenditures

Expenses for the SOC consist primarily of salaries and benefits for 11 security analysts, cloud-based solutions for analyzing and managing threats, and WaTech services (i.e., virtual server hosting, intra-agency).