TRACEABLE

F5 + Traceable

360 degrees of Intelligent API security

- Installs in minutes
- Integrates with Big-IP routing infrastructure
- Provides API-specific protection
- Maintains data lake of requests for threat hunting
- Provides a unified view of hybrid environments

Traceable Value

Traceable delivers a comprehensive API Catalog, with each API endpoint assessed for security posture, API security testing, API runtime protection, API abuse and fraud protection, and threat analytics.

1. Discover
   - Visibility of all APIs and their specifications (known, shadow, orphaned, 3rd party)
   - Auto documentation of all APIs, including spec conformance analysis
   - Risk assessment, sensitive data visibility, drift management, and more

2. Protect
   - Detection and blocking of OWASP Top 10 and OWASP API Top 10
   - Detection and alerting of sophisticated and long-running attack sequences
   - Protect from API-specific attacks and API Abuse, including fraud
   - Testing of APIs for security vulnerabilities before they go into production

3. Analyze
   - Identification of threat actors based on repeated malicious behavior
   - Root cause analysis and threat hunting through explorable API transaction data lake

Deployment

Leveraging standard features of F5 Big-IP, Traceable monitors inbound and outbound network traffic and identifies suspicious API patterns that might indicate malicious behaviors. The BIG-IP system enables Traceable to inspect traffic with support for the Clone Pool and Interface Mirroring features.

F5 Clone Pools

The Clone Pool is F5's recommended method for copying production traffic from BIG-IPs to sniffer devices. The Clone Pool receives all of the same traffic from the BIG-IP as the load-balancing pool. As a clone pool member, Traceable will also receive this traffic. Clone Pool mirroring offers completely out-of-band detection and blocking.

F5 Interface Mirroring

Interface Mirroring is a simplified method of capturing a copy of traffic from any port, or set of ports, to a separate port where a VM with the Traceable agent is installed. Interface mirroring sends traffic at wire speed to dedicated devices for troubleshooting and analysis purposes (in this case, the Traceable agent).

Traceable platform relay

The Traceable platform relay is part of the deployment that is local to the customer environment and can be installed as a virtual machine, as a container, or as a Linux daemonset. If Big-IP is virtualized, several cloud-based deployment options are also available. The Traceable platform relay is responsible for initial analysis of the cloned traffic, such as redacting sensitive data, and also manages the connection to the Traceable platform where the bulk of the processing is conducted and the management console is hosted. In addition to SaaS, the Traceable platform can also be deployed on local compute resources or in the cloud.

Traceable and F5 Advanced WAF

AWAF is an optional module that can be added to F5 Big-IP. If it is already in place, it makes sense to configure AWAF to protect from DDoS and scanner attacks and forward the good traffic and the traffic that needs further analysis to Traceable.

Even with AWAF in place, Traceable provides many security benefits in addition to what's available in AWAF. These include:

- API Catalog and posture management
- API security testing
- Detection of API Specific attacks
- Detection of API Abuse
- User and Threat Analytics