OMDIA

ON THE RADAR

Publication date
16 Dec 2020

Author
Rik Turner
Principal Analyst

F5 integrates and automates app security

Shifting security left in the development process

OMDIA

Brought to you by Informa Tech

Summary

Catalyst

Organizations are increasingly moving processes and services online and into the cloud, making use of the skills, software and services of others, in order to improve flexibility and access. Capabilities and needs vary considerably, but all seek more protection for their online applications and services. F5 offers next-generation application security (NGAS) products and services, encompassing web application firewall (WAF), bot and DDoS protection, with a broad range of deployment options on-premises, in the cloud and as-a-service.

Omdia View

As organizations transform access to their assets and processes, digitally connecting customers and their supply chains, with new applications and services to meet changing demands, they increase the risk that something will go wrong, or that they will be targeted by those with malicious intent. The data used by these applications often represents the organization's most valued assets, and, along with the applications and services consuming it, it needs protection.

That protection has to incorporate multiple elements working in concert. Problems can be caused by the injection of fake content, rogue scripts or malware, or simply by something overloading or overwhelming resources so they are no longer available to legitimate users. Such problems may come from the deliberate actions and attacks of individuals and groups, from automated bots co-opted into probing defenses, or from unidentified vulnerabilities in software, services and APIs.

With the pressures on the pace of application development and an 'always-on, always connected' ethos in business, coupled with greater use of open source and third-party services to cope with demands, the risks are only rising. F5 provides application security products and services to mitigate software and application vulnerabilities, protect against abuse at the business logic level by bots, and secure APIs.

Why put F5 on your radar?

With varied forms of attack and software vulnerabilities, organizations need to be able to protect all types of applications, from traditional and legacy ones that still have a useful purpose despite many changes, to new ones taking advantage of modern development techniques and resources delivered as a service. F5 offers a range of next-generation application security capabilities, integrated into multiple different insertion points, depending on the particular types of app deployments and level of customer management.

Market Context

The software development environment has changed. Development cycles have shortened, partly due to pressure for business evolution, and partly to user expectations raised by the way web and mobile applications have rapidly emerged, updated and evolved. Attitudes, processes and tooling within software development itself have also changed. Cumbersome, linear development processes have been replaced by Agile and DevOps, where multi-disciplinary teams collaborate and use continuous cyclical processes to refine and improve (a.k.a. continuous integration and continuous delivery, or CI/CD). Functionality has become fine-grained with microservices and containers, and is aggregated from a variety of sources, internal and third party.

Universal connectivity and the use of resources drawn from open-source software, services in the cloud and multiple third-party APIs has massively opened the attack surface and expanded the risk. There is a need for much closer attention to security and reliability, not just in the development pipeline, but also at runtime, as applications and services are deployed and used.

Individual legacy approaches to testing and validation cannot cope with the pace, diversity or scarcity of resources. This increases the need for automation and integration of multiple types of checking, testing and protection, all through the development, deployment and production lifecycle.

Security thinking and teams are already merging into DevOps, as DevSecOps starts to become a reality, but increasingly security protection and testing for software quality and reliability are merging, both in the development pipeline and at runtime. This can be seen as vendors from both spheres are developing or acquiring new functionality and services to provide a more comprehensive offering, to deliver next-generation application security (NGAS).

More integration, both technically in products and platforms, and also commercially through acquisitions and partnerships, is inevitable, but the pipeline and runtime elements are likely to progress at different paces. For some it will be sufficient to automate and merge static, dynamic, and interactive code analysis tools and test procedures, as well as software composition analysis (SCA), during the development process; others will keep their focus to runtime and the behaviors and responses of applications and APIs to network activities, automated threats and runtime errors. In each element, however, there is already significant M&A, development and integration activity, and this will continue, causing a re-alignment of the application security market.

Product/Service Overview

F5 identifies security control points within network infrastructure, access to an application, as well within the application layer itself. Its deployment options range through self-managed, fully managed, and as-a-service, and its WAF engine is integrated in multiple insertion points:

- **F5 Advanced WAF** is designed to deploy into DevOps environments, integrating directly into the development automation pipeline using its capability to declare the configuration as code. This means security can become part of DevOps CI/CD automation and tested like any other part of an application's functional specification. Security policy and configuration are created and maintained by SecOps and consumed as code, pulled from a source code repository. It provides malicious bot protection, application-layer content encryption, API inspection, and behavioral analytics to help defend applications and APIs against attacks. The bot defenses use a combination of signatures, challenge- and behavior-based techniques to identify and filter unwanted automation traffic from attempting reconnaissance, vulnerability exploitation, and opportunistic hacking. It includes F5 DataSafe to encrypt browser input data (e.g. login credentials) at the application layer as it passes from the browser through to the WAF, to protect against malware and man-in-the-browser (MITB) threats without needing to update the web application itself.

  Protection against DoS attacks comes from analyzing traffic behavior using machine learning and data analysis. The WAF learns the application behavior, then combines the behavioral heuristics of traffic with the level of stress identified on servers to determine DoS conditions. Anomalies such as performance dips or traffic spikes can be detected and mitigated as required by continuously monitoring the protected server health and using machine learning heuristics to apply dynamic signatures specific to the attack. This provides accurate detection without false positives. The signatures, created on the fly, are deployed as required for real-time protection. This provides accurate L7 DoS detection without blocking legitimate traffic.

- **NGINX App Protect** is also designed to deploy into DevOps environments, like the Advanced WAF, and shares a common JSON-based policy format.. App Protect runs natively on the F5 NGINX Plus platform and is deployed as a lightweight software package that is agnostic to the underlying infrastructure. Deployment modes for NGINX Plus include a per-pod proxy for microservices, an ingress controller for Kubernetes pods, an API gateway, and in a load balancer. App Protect's security controls are ported directly from F5's advanced WAF technology, providing a comprehensive set of WAF attack signatures that F5 claims has been extensively field-tested to generate virtually no false positives, allowing them to be deployed in "blocking mode" in production environments. App Protect covers the OWASP

Top 10 web application security risks, enforces protocol compliance, defends against common evasion techniques, provides denylisting, checks cookies and protects APIs. F5's DataGuard technology is also integrated to prevent sensitive data leakage. App Protect's security controls are ported directly from F5's advanced WAF technology, providing a comprehensive set of WAF attack signatures that F5 claims has been extensively field-tested to generate virtually no false positives NGINX App Protect also consumes cyber threat intelligence (CTI) directly from F5. This CTI feed (F5 Threat Campaigns) provides intelligence on active attack campaigns in the wild and often utilize a combination of attack methods that may not trigger an existing security policy.

- **Essential App Protect** offers cloud-delivered app security in a checkbox-driven WAF service with a SaaS delivery model, offered in the AWS Marketplace or F5 Cloud Services portal. Essential App Protect utilizes the same WAF engine as Advanced WAF and NGINX App Protect. It applies the F5 WAF controls and signatures, protects against malicious IP addresses, includes the F5 Threat Campaigns intelligence feed, and protects sensitive data with F5 DataGuard. It is designed with DevOps environments in mind and supports hybrid and multi-cloud applications across multiple platforms with configurations that are consistent, using a graphical dashboard, APIs, or Ansible playbooks.
- **F5 Silverline** managed service offering comprises Silverline WAF, Silverline DDoS protection Silverline Shape Defense (bot protection), and Silverline Threat Intelligence. The WAF has managed provisioning and enabling of services, comes with pre-built policies and rules created by F5, and offers a guided transition from learning mode to protected mode. DDoS protection is fully provisioned and configured to monitor and prevent multi-layered network and application attacks, L3-L7. There are deployment options are to either run continuously to monitor all traffic and stop attacks from reaching the network, or to be initiated on demand, when a site is under attack. Shape Defense mitigates fraudulent and unwanted traffic, blocking the full range of OWASP automated threats to web applications using F5's patented telemetry and signature collection, plus its machine learning capabilities, which is in the process of being incorporated into most F5 services. Threat Intelligence has flexible deployment options to identify probes, scans and brute force attacks, and to restrict network and infrastructure access for known bad actors or rogue IP addresses, such as those hosting phishing sites or other fraudulent activities.

Company Information

Background

F5, originally named F5 Labs and formerly branded F5 Networks, was founded in February 1996 by Jeff Hussey, who led it to IPO on Nasdaq in June 1999. The company has had a number of changes of leadership since IPO, and is currently headed up by CEO François Locoh-Donou, who joined in 2017 having previously held roles at Ciena and Photonetics.

There was one funding round before IPO in 1998, and a post-IPO equity round by Elliott Management Corp and Ridge Ventures in November 2020. F5 has made 10 acquisitions since IPO, the most recent ones being open-source web server provider NGINX, in March 2019, and web and mobile application security provider, Shape Security, announced in December 2019.

Current Position

There are several options available for how to deploy F5 Advanced WAF – software, as-a-service, in the public cloud, and on-premises hardware. The software option can be deployed on a hypervisor in the customer's data center or private cloud. Public cloud service provider marketplace deployment is available in AWS, Microsoft Azure and Google Cloud Platform. The Silverline WAF is cloud-based, either self-managed or by the F5 Security Operations Center (SOC). F5's hardware option is to use a platform from its BIG-IP iSeries range.

F5 Advanced WAF is available in several purchasing options:

- subscriptions based on number of instances and 1-, 2-, or 3-year terms, including maintenance and support for version updates;
- perpetual licensing, also based on number of instances, and
- enterprise licensing agreements over 3-year terms and including product maintenance and support.

Future Plans

F5's vision for application security is to have a complete stack of security services with

- app and API protection and management,
- anti-bot and anti-fraud protection, plus additional services including
- DNS,
- DDoS,
- content delivery and caching, and
- access management.

The idea is to provide all these as self-serve, SaaS, and fully managed services, with centralized management, analytics and automated risk mitigation, offered with consistent licensing and pricing across the range of services. This 'one-stop shop' approach is around three quarters of the way to completion, and F5 is adding more in the early part of 2021 with advanced app protection and anti-bot protection. Increasingly, the AI platform from the acquisition of Shape Security is being integrated into products and services.

Key facts

Table 1: Data sheet: F5

Product/Service name	F5 Advanced WAF, Silverline managed services, WAF, DDoS Protection and Shape Defense	**Product classification**	Application security
Version number	F5 Advanced WAF, 16.0	**Release date**	F5 Advanced WAF, April 2018
Industries covered	All	**Geographies covered**	All
Relevant company sizes	Enterprise	**Licensing options**	Appliances Physical appliance (perpetual), virtual appliance (perpetual and subscription), Enterprise License Agreements (ELA), managed services
URL	https://www.f5.com/products/security/advanced-waf https://www.f5.com/products/security/silverline	**Routes to market**	2 tier distribution (partners/channel), direct, public cloud marketplace
Company headquarters	Seattle, US	**Number of employees**	~5,300

Source: Omdia

Appendix

On the Radar

On the Radar is a series of research notes about vendors bringing innovative ideas, products, or business models to their markets. On the Radar vendors bear watching for their potential impact on markets as their approach, recent developments or strategy could prove disruptive and of interest to tech buyers and users.

Author

Rik Turner, Principal Analyst, Cybersecurity

Rom Bamforth, Associate Analyst

Citation Policy

Request external citation and usage of Omdia research and data via citations@omdia.com.

Copyright notice and disclaimer

The Omdia research, data and information referenced herein (the “Omdia Materials”) are the copyrighted property of Informa Tech and its subsidiaries or affiliates (together “Informa Tech”) and represent data, research, opinions or viewpoints published by Informa Tech, and are not representations of fact.

The Omdia Materials reflect information and opinions from the original publication date and not from the date of this document. The information and opinions expressed in the Omdia Materials are subject to change without notice and Informa Tech does not have any duty or responsibility to update the Omdia Materials or this publication as a result.

Omdia Materials are delivered on an “as-is” and “as-available” basis. No representation or warranty, express or implied, is made as to the fairness, accuracy, completeness or correctness of the information, opinions and conclusions contained in Omdia Materials.

To the maximum extent permitted by law, Informa Tech and its affiliates, officers, directors, employees and agents, disclaim any liability (including, without limitation, any liability arising from fault or negligence) as to the accuracy or completeness or use of the Omdia Materials. Informa Tech will not, under any circumstance whatsoever, be liable for any trading, investment, commercial or other decisions based on or made in reliance of the Omdia Materials.

Contact Us

omdia.com

askananalyst@omdia.com