Google Cloud

Solution Brief

Modernize Application Security

Digital transformation continues to accelerate around the world. Modernization of applications and architectures has become the driving force and enabler behind most business strategies, affecting everything from back-office functions all the way through to the customer experience. With this modernization and shift to cloud, organizations are experiencing new levels and variations of risk, made worse by complexity and still unfamiliar technology stacks. Security challenges for apps include:

41% of organizations juggle between 200 and 1,000 applications.

F5 2022 State of Application Strategy Report

- Complex hybrid cloud architectures
- Missing insights and visibility from end to end
- Slow shift in security focus to identity and zero trust
- Securing legacy alongside modern apps
- Threats that are maturing, automating, and ever-changing
- Balancing performance with security

An alarming 76% of organizations would turn off security measures to improve performance.

F5 2022 State of Application Strategy Report

It's a New Age for Apps and Attackers

AppDev and DevOps automate everything from code build to service deployment. Attackers also use automation to launch attacks. Security must adapt to attackers that retool to bypass countermeasures—without frustrating users. This ability to react as apps and attackers adapt can dramatically improve business outcomes by slashing fraud losses, providing better customer experiences, and maximizing operational efficiencies and business intelligence.

F5 and Google Cloud can help you:

Stay Ahead of Threats

The proliferation of architectures, cloud, and third-party integrations has dramatically increased the attack surface. Major application vulnerabilities are discovered daily, and attackers are quickly weaponizing them using automation frameworks to find and exploit them for monetary gain.

Integrate Security

Effective application security is automated and integrated. Automation improves effectiveness by launching and stabilizing security controls earlier in the development lifecycle. This leads to higher effectiveness with less manual effort. Integration also reduces strain on security resources.

Go to Market Faster

Organizations need consistent and automated security in order to effectively manage the growing complexity of securing applications across architectures, clouds, and developer frameworks—all at the speed of application development.

The Value of Adaptive Applications

Adaptive applications bring intelligence and real-time changes to the world of application deployments, which today are mostly static and manual. F5 and Google Cloud enable organizations to secure and deliver extraordinary digital experiences through **adaptive applications** that grow, shrink, defend, and gain insights to evolve more quickly to changing environments.

More rapidly detect and neutralize security threats

Improve performance and resilience

Speed deployment of new apps

Easily unify policy across environments

Cloud services provided by Google Cloud enable the foundation for a modernized application, allowing for multi-tier and distributed architectures over cloud- or container-native services. F5's portfolio of automation, security, performance, and insight capabilities empowers customers to create, secure, and operate adaptive applications that reduce costs, improve operations, and better protect users.

Together with Google Cloud, our goal is to deliver frictionless security that complements performance, automation, and insight to deliver and scale the application experience.

Google Cloud Secure Platform for Your Applications

Google Cloud is a more flexible, secure cloud provider that embraces open source, making it the best platform to migrate infrastructure and modernize applications. It's also the most multi-cloud "friendly" of the major cloud providers and provides pioneering capabilities around Kubernetes as well as big data and analytics. Google Cloud has always prioritized security; the platform's strong security and cutting-edge encryption allow companies to safely store and analyze sensitive personally identifiable information. Google Cloud can provide you:

- Google hardware built in-house, controlled, and hardened
- Data at rest and commutations over internet to Google Cloud automatically encrypted
- Around-the-clock ops team threat detection and incident response
- Custom data center design with multiple layers of physical and logical protection
- One of the largest private and highly secure backbones in the world

Important Aspects of Application Security

Mitigate Application Vulnerabilities

Shield your apps from devastating vulnerability exploits.

Protecting your apps against critical risks—such as the threats listed in the OWASP Top 10—requires comprehensive and adaptive security. F5 solutions provide a strategic stopgap against common vulnerabilities like injection and XSS and mitigate emerging exploits that target open source software and security misconfiguration across clouds.

Mitigate Bots and Abuse

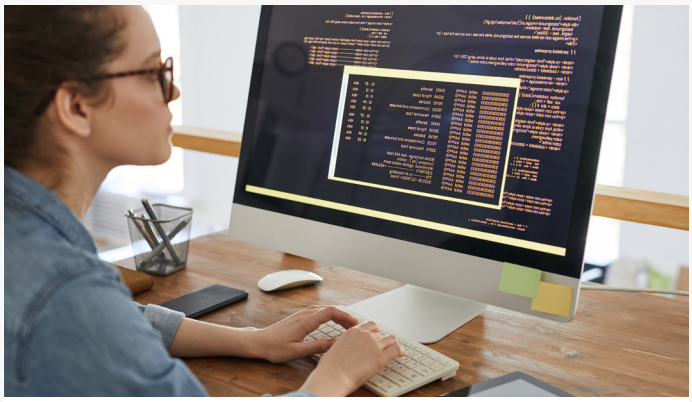
Deter attackers that use malicious automation to commit account takeover and fraud.

Just as enterprises adopt automation to gain process efficiencies, attackers have embraced bots and automation to scale their attacks, bypass security countermeasures, and compromise customer accounts. F5 solutions automatically adapt to changing attack tactics without inserting user friction–ensuring business success and customer satisfaction.

Secure APIs and Third-Party Integrations

Safely embrace the new digital economy.

APIs are the cornerstone of modern applications and allow organizations to quickly integrate new capabilities into their digital experiences. Attackers know it can be challenging to identify and protect these application interdependencies, given there are upwards of 200 million APIs in use. F5 solutions dynamically discover and automatically protect all digital touchpoints with robust and resilient API security.



Protect Against DDoS Attacks

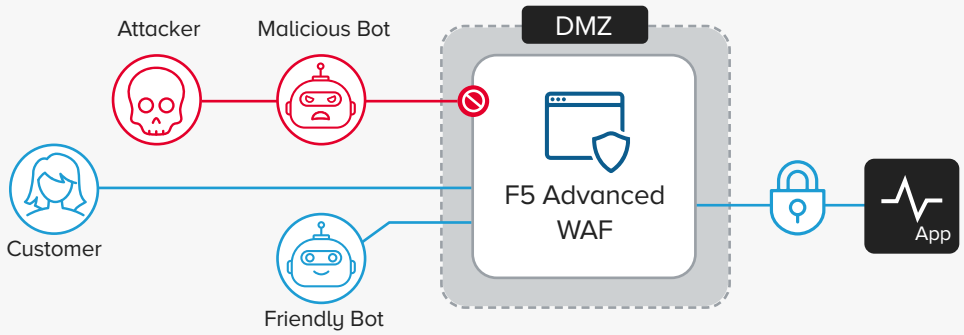
Keep your applications secure and available.

Businesses of all sizes run the risk of being hit with a DDoS attack. The common goal of these attacks is to make your application or network unavailable, but the attacks themselves can differ. F5 offers solutions to combat each type of attack in a deployment model that makes sense for your needs.

F5 Solutions for Application Security

Advanced WAF

The F5 Advanced WAF is a web application firewall with comprehensive protection for websites, mobile apps, and APIs. Leveraging behavioral analytics, automated learning capabilities, and risk-based policies, the F5 Advanced WAF secures applications against threats, including application-layer DDoS attacks, malicious bot traffic, all OWASP Top 10 threats, and API protocol vulnerabilities. Powerful reporting capabilities allow for easy, real-time analysis of attacks for fast, informed security decisions.

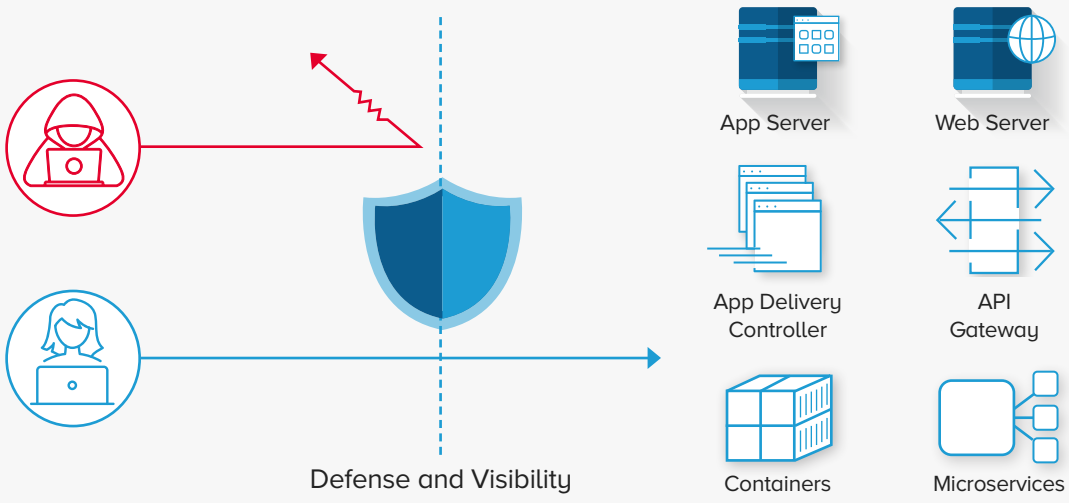


Advanced WAF detects bots without server agents or dedicated appliances.

NGINX App Protect

Want to use the same WAF across all your environments from on-premises to cloud to Kubernetes?

NGINX App Protect is a modern app security solution built on F5's market-leading security expertise that creates WAF consistency from on-premises to cloud to Kubernetes. The security-as-code design makes it easy to integrate security into Agile and DevOps workflows.



Discover F5 solutions in the Google Cloud Marketplace or visit f5.com to learn more.

F5 | Google Cloud