WHITE PAPER

Secure and Accelerate Multi-Cloud Success with F5, Intel, and Google Cloud

85% OF ORGANIZATIONS ARE MANAGING MULTIPLE APPLICATION ARCHITECTURES AND LOCATIONS[6]

The growth of public cloud creates new challenges in multi-cloud environments

As businesses across the globe continue their journey toward digital transformation, investments in the public cloud are projected to continue their surge, where worldwide spending is poised to grow by more than 20% in 2023, reaching a staggering $591.8 billion.[1] However, as organizations race towards harnessing the potential that the cloud has to offer, security and compliance risks have emerged as significant roadblocks to realizing the full benefits of cloud technology.[2]

Navigating the security landscape of multi-cloud environments presents several unique challenges. Organizations often wrestle with limited visibility and inconsistent policies across their environments. The expanded threat landscape and the growing use of cloud services have also compounded the difficulty of securing web applications.[3]

Amid these hurdles, there is a noticeable trend towards consolidation, with 75% of organizations set to streamline their security tools to cover both cloud and on-premises environments.[4] In line with this trend, F5's 2023 State of Application Strategy Report points out that a substantial 88% of businesses are adopting a platform approach to security, at least in certain areas.[5]

Meanwhile, on the application delivery front, organizations face their own set of challenges as the security of newer, containerized applications pose a unique set of problems. As such, striking the right balance between accelerated multi-cloud adoption and secure, effective application delivery that users will enjoy is more important than ever before.

PARTNERSHIP HIGHLIGHTS

- Long-standing F5 and Google Cloud partnership
- 15-year F5 and Intel partnership
- Wide range of customers across various industries globally
- 30 unique offerings from F5 on the Google Cloud Marketplace
- Intel QAT-enabled Google Cloud instances accelerate F5 solutions

Unlocking robust cloud security through strategic partnerships

Traversing the trail toward secure and accelerated multi-cloud success can be a formidable undertaking for many organizations. However, strategic partnerships can provide the necessary expertise and solutions to tackle these challenges effectively. One such alliance can be found between F5 and Google Cloud. Together, they are driven by a shared vision for adaptive applications that couple frictionless security with superior performance, intelligent automation, and sharp insight to enhance and scale application experiences for the most advanced cloud-enabled applications imaginable.

Evolving to be a part of the Accelerated by Intel® program, the F5 and Intel partnership is another example that stands as a testament to a shared commitment to long-standing innovation and unparalleled excellence in the global cloud computing ecosystem.

Central to the F5 and Intel collaboration is the integration of Intel® QuickAssist Technology (Intel® QAT), which accelerates F5 products, including F5® BIG-IP® Virtual Edition (VE). By offloading compute-intensive workloads to the Intel QAT hardware, significant gains can be found in CPU efficiency, data footprint reduction, power utilization, and application throughput. This is particularly useful for accelerating bulk cryptography, public key cryptography, and compression tasks. The integration of Intel QAT leads to enhanced performance on cloud instances supported by Intel QAT.

In a move that further widens the accessibility and utility of this technology, Google Cloud has also made available instances that are enabled by Intel QAT, thereby amplifying the benefits of the F5 and Intel partnership to an even broader customer base.

The three use cases that follow exemplify how these industry leaders have come together to solve complex customer challenges and deliver superior, secure hybrid cloud environments.

Use case: Modern security for your multi-cloud environment

As organizations venture further into multi-cloud environments, they confront a plethora of security challenges, such as constructing consistent security policies across diverse environments. Likewise, simplifying management and ensuring visibility across the multi-cloud landscape can be daunting tasks.

These challenges, however, can be effectively tackled with the integrated solutions provided by the strategic partnership between F5, Google Cloud, and Intel. The key features of these solutions include:

Centralized Management

Using F5® BIG-IQ® Centralized Management or the F5® Distributed Cloud Console, businesses can simplify management and increase visibility across diverse environments. These tools offer declarative interfaces, fostering ease in management and promoting automation and orchestration capabilities.

Vendor Alignment

The collaborations have resulted in a cohesive, integrative security platform that enables vendor consolidation, creating a streamlined, unified approach to security.

Advanced Threat Protection

F5® BIG-IP® SSL Orchestrator®, accelerated by Intel QAT, delivers faster protection against sophisticated threats such as ransomware and encrypted threats. BIG-IP Advanced WAF additionally helps protect against credential theft.

Unified, Secure Access

With F5® BIG-IP® Access Policy Manager® (APM), businesses can implement zero-trust access, single sign-on, and conditional access, creating a robust, unified access strategy.

Diverse Flexibility

These solutions offer flexibility to cater to diverse business needs, available as SaaS, on-premises, virtual, or cloud.

As a result, organizations can anticipate favorable outcomes, including:

- Remove barriers to cloud migration.
- Simplify management with end-to-end visibility.
- Achieve broad protection from L3 through L7.
- Enforce consistent security policies across multiple clouds or on-premises.
- Enjoy faster security processing, potentially leading to significant cost reductions.

Use Case: Extend Google Cloud security to mitigate fraud and automated attacks

Security threats are continually evolving, posing significant challenges to organizations. Modern attacks predominantly target the application layer, leading to potential slowdowns and service outages. The nature of automated attacks is especially concerning, as they adapt swiftly to evade detection measures. Moreover, application programming interfaces (APIs) require L7 security and must be optimized across multiple networking layers to ward off threats of compromise and downtime. A troubling statistic presented by the Google Cybersecurity Action Team shows that nearly 20% of security incidents among Google Cloud customers were due to API compromise.[7]

Mitigating fraud and automated attacks in a digital landscape presents its own set of unique challenges. The strategic partnerships between F5, Google Cloud, and Intel address these issues, offering comprehensive solutions with key features such as:

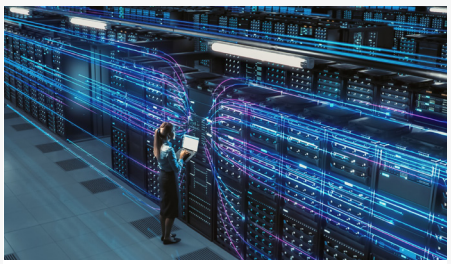
Real-time Bot Control: The solution can halt bots that can cause issues like DDoS attacks, credential stuffing, and fake account creation in real-time.

Adaptive Attack Prevention: By integrating Google Cloud reCAPTCHA with F5® Distributed Cloud Bot Defense, the solution can detect and prevent highly adaptive attacks, offering protection against evolving threats.

Fraud Protection: The use of AI and ML helps in detecting and combatting rapid retooling, a common characteristic of modern fraud attempts.

API Security: Secure APIs and third-party integrations reduce the risk of security breaches and the compromise of critical information.

Upon implementing these solutions, businesses can expect several significant outcomes:



Robust defense against threats across the entire network stack, including modern threats that continually adapt and evolve.

Reduced risk of service slowdowns or outages due to automated attacks on applications and APIs.

Frictionless security that offers comprehensive protection without inconveniencing users.

Use Case: Modernize and secure applications no matter where they run

The process of modernizing and securing applications, regardless of where they operate, presents several hurdles for organizations. A 2023 study found that 40% of app deployments use modern architectures, a notable rise from 33% the previous year.[8] As these modernization efforts progress, they invariably create new scenarios that need robust protection, regardless of the focus: virtualized, Kubernetes, or serverless apps. Kubernetes security concerns caused significant impact, causing 67% of organizations to delay or slow application deployment.[9]

Modernizing and securing applications across various platforms can be challenging. The collaborative solutions provided by F5, Google Cloud, and Intel address these challenges with several unique features:

Automated Security Rules: By connecting Google Kubernetes Engine to F5 BIG-IP, applications can automatically inherit security rules.

Advanced Protection: F5® BIG-IP® Advanced WAF® secures applications and APIs from layer 7 attacks, bots, and threats listed in the OWASP Top 10.

Security Integration: These solutions can be integrated directly into the Continuous Integration/Continuous Delivery (CI/CD) pipeline, providing security from the start of the application lifecycle.

Enhanced Performance: F5® BIG-IP® Virtual Edition (VE) performance is significantly boosted by Intel-powered acceleration, ensuring fast and efficient operations.

Implementing these solutions can result in several significant outcomes:

Applications are secure from inception to production, providing a safer environment for faster deployment and easier use.

Enhanced visibility into clusters and applications is achieved across multiple platforms, enabling more effective monitoring and management.

Kubernetes applications are safeguarded against threats, reducing the risk of breaches and potential operational disruptions.

Enhance Google Cloud security with Intel-powered F5 solutions

By leveraging the power of Intel QAT acceleration in F5 solutions, businesses can considerably enhance their Google Cloud security with high performance at the core through symmetric and asymmetric encryption, as well as lossless compression in hardware, effectively offloading compute-intensive operations to the Intel QAT accelerator. This results in significant performance gains for F5 solutions.

This unique blend of technologies paves the way for secure, scalable, and fast applications delivered with a consistent end-user experience, a vital asset for multi-cloud success. Moreover, comprehensive security coverage aids in thwarting sophisticated or large-scale attacks more effectively and efficiently.

Streamlining deployment and management processes significantly reduces complexity, thus allowing organizations to focus more on strategic tasks and advanced threats as well as reduce the total cost of ownership.

With multiple F5 solutions readily available via the Google Cloud Marketplace, purchasing and deployment of these solutions becomes an effortless task. The unification of F5, Google Cloud, and Intel thus form a powerful partnership committed to driving security, efficiency, and multi-cloud success for modern businesses around the world.

Modernize your business and applications with confidence

Embrace the future confidently by modernizing your business and applications. Start your transformative journey today by harnessing the power of synergistic partnerships.

Learn more

Sources:

1. Gartner, Gartner Forecasts Worldwide Public Cloud End-User Spending to Reach Nearly $600 Billion in 2023
2. Accenture, The race to cloud: Reaching the inflection point to long sought value, January 2023
3. ESG Research, Trends in Modern Application Protection, May 2022
4. Gartner, Gartner Survey Shows 75% of Organizations Are Pursuing Security Vendor Consolidation in 2022
5. F5, 2023 State of Application Strategy Report
6. Ibid.
7. Google Cybersecurity Action Team, Threat Horizons April 2023
8. F5, 2023 State of Application Strategy Report
9. Red Hat, 2023 State of Kubernetes Security Report