SOLUTION OVERVIEW

5G Security

Enabling strategic defenses in a multi-cloud, distributed network.

5G SECURITY BENEFITS

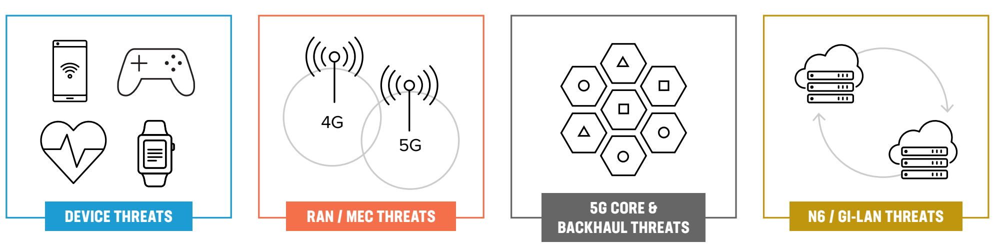
- Increased traffic visibility
- Increased network control
- Real-time anomaly detection
- Increased revenue

The introduction of 5G has helped bring to life innovations that were unimaginable just five years ago. We are now living in an era where mobile technology is no longer a luxury, but a necessity, as service providers undertake a digital transformation to stay relevant. 5G brings about increased network complexity driven by an explosion of access points and wireless devices. This also increases the threat landscape that will be exposed to sophisticated and malicious attacks. As the attack surface increases, it will become harder to assess risks and intercept cybersecurity threats. Maintaining trust, safeguarding personal information, and providing a reliable network are the cornerstones needed to establish a security framework.

Service providers have the daunting task of building a network that lives up to the expectations that 5G offers. The network should mitigate increased complexities by automating as much as possible, using intelligence for real-time anomaly detection and healing, and, above all, ensuring unparalleled customer Quality of Experience (QoE). As networks evolve, so does the threat landscape. Establishing a strong security posture in the face of evolving threats depends on two key components: understanding the threat landscape and treating security as a prerequisite when designing your networks.

Understanding the 5G Threat Landscape

Service providers are evolving their business models as they drive toward a global 5G network rollout. New business models enable service providers to expand into industry verticals like healthcare, manufacturing, and financial services, for example. This in turn contributes to the exponential increase in the number of connected IoT devices, making 5G networks an even more appealing target for cybercriminals who can take advantage of the larger threat landscape. The diagram below depicts common security vulnerabilities within a 5G network.

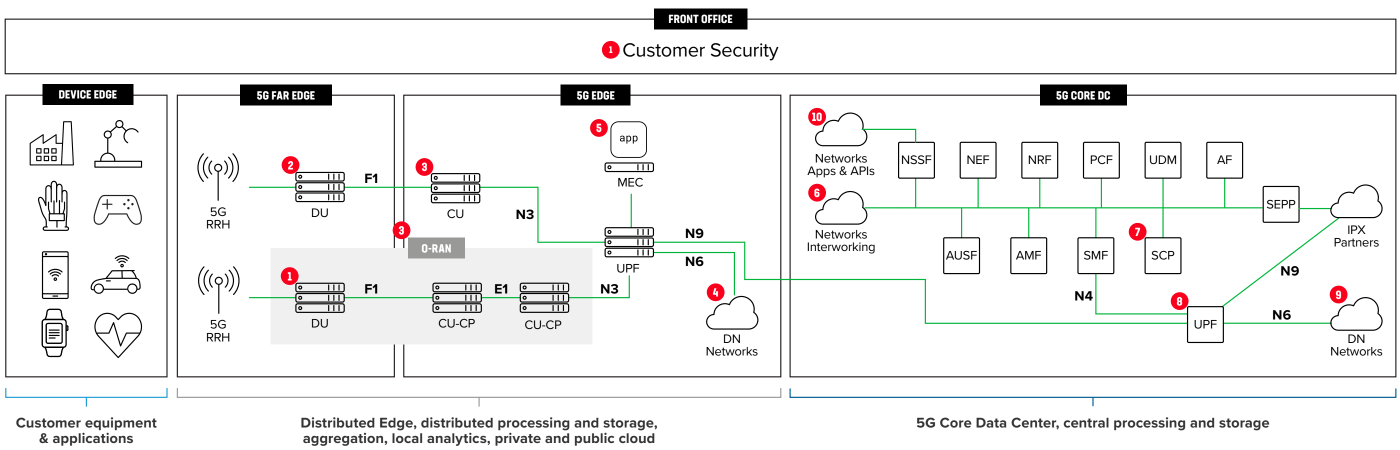


DEVICE THREATS	RAN / MEC THREATS	5G CORE & BACKHAUL THREATS	N6 / GI-LAN THREATS
Malware Botnets DDoS Attacks Unauthorized Access Device Compromise Physical Access	Compromised Mobility Nodes/ Rogue Nodes Signaling Storm MEC Vulnerabilities MEC APP Sniffing	API Abuse IoT Segmentation Attacks from Roaming Partners DDoS Attacks Weak Network Security Controls Packet Snooping	DDoS Attacks Improper Access IPv4 Address/Port Exhaustion IPv6 Threats IoT Core Integration API Vulnerabilities

Figure 1: Security challenges 5G mobile network operators face

F5 Security Solutions for 5G

F5 has an extensive security solution family capable of tackling cybersecurity attacks, mitigating network vulnerabilities, and protecting service providers' front office operations. F5 provides network security controls that are built into the industry's leading programmability and application delivery services, so they enable scalable and efficient security throughout your entire infrastructure. The figure below is a snapshot of some of F5's security offerings.



Device Edge

1. F5 Anti-Fraud and Bot Protection

5G Far Edge: vRAN DU

2. vRAN-DU 5G Cloud-Native Infrastructure
   - BIG-IP Service Proxy for Kubernetes
   - Carrier-Grade Aspen Mesh
   - Security: DDoS Mitigation with SmartNIC integration support

5G Edge: vRAN CU and MEC

3. vRAN-CU 5G Cloud-Native Infrastructure
   - BIG-IP Service Proxy for Kubernetes
   - Carrier-Grade Aspen Mesh
   - Security: AWAF, DDoS Mitigation with SmartNIC integration support
4. N6 LAN
   - Consolidated N6 LAN: CGNAT, DDoS, Firewall, TCP Optimization, Video Optimization, DPI, LDNS, Subscriber Security Services
5. MEC
   - NGINX Ingress Controller and Service Mesh, App Protect, API Gateway, WAF
   - Security: IoT Security, AWAF, DDoS Mitigation with SmartNIC integration support

5G Core DC

6. 5G Infrastructure
   - BIG-IP Service Proxy for Kubernetes
   - Carrier-Grade Aspen Mesh
7. Network Signaling – SCP
8. N6 LAN
   - Consolidated N6 LAN: CGNAT, DDoS, Firewall, TCP Optimization, Video Optimization, DPI, LDNS, Subscriber Security Services
9. Web and App Protection
   - F5 Anti-Fraud and Bot Protection
   - NGINX – Ingress Controller, App Protect, API Gateway, App/Web Server
10. API Gateway – NGINX+ Controller

● F5 Services

Figure 2: F5 security solutions for service providers

F5 has long developed and delivered security for service provider networks and continues to do so even as the pace of technology evolution has quickened. The breadth of available security solutions span the entire 5G network and extend into the front office. We'll examine the common 5G security issues and take a deeper dive into F5's solutions.

F5 SECURITY SOLUTIONS FOR 5G

- API protection
- Cloud-native infrastructure solution
- Signaling and roaming security
- Securing and consolidating N6 LAN
- Front office customer security

API PROTECTION: A MUST-HAVE IN 5G API-DRIVEN ECOSYSTEMS

The ability to expose the 5G core to third parties using APIs makes 5G a technological disruptor. This enables applications to be programmed for use through mobile connectivity and edge computing. What we mean by programmability in 5G is the ability to abstract, encapsulate, and expose internal capabilities and enable instructions via APIs. In a 5G network, programmability is made possible by implementing a service-based architecture (SBA) on a cloud-native infrastructure.

Within the 5G core there is the Network Exposure Function (NEF). The NEF invokes microservices requiring data to be exposed via its southbound APIs. Network exposure is needed for developers to test and develop innovative technology in conjunction with 5G by giving developers access to exposed network services. 5G enables service providers and the enterprise industry to easily activate new capabilities and expose them through APIs—and this can be done at the edge of your network or via your 5G core. APIs must be analyzed, authenticated, and secured before they're allowed on the network, and they must be managed throughout their life cycles to ensure their safety.

APIS MUST BE ANALYZED, AUTHENTICATED, AND SECURED BEFORE THEY'RE ALLOWED ON THE NETWORK, AND THEY MUST BE MANAGED THROUGHOUT THEIR LIFE CYCLES TO ENSURE THEIR SAFETY.

API Gateways Guard Your 5G NEF and Edge

Innovation is a key cornerstone of 5G and is not possible without the extensive use of APIs. As 5G standalone (SA) core networks are rolled out and the edge moves beyond a commodity to enable pervasive connectivity for enterprise industry verticals, academia, and small and medium enterprises (SME), we'll see the growing need to protect the 5G network from an increased threat landscape. The API gateway, available as part of NGINX Plus, is a cloud-native solution that simplifies security for microservices architectures. It meets the recommended requirements for integrated authentication and authorization and is ideally suited for use in 5G environments.

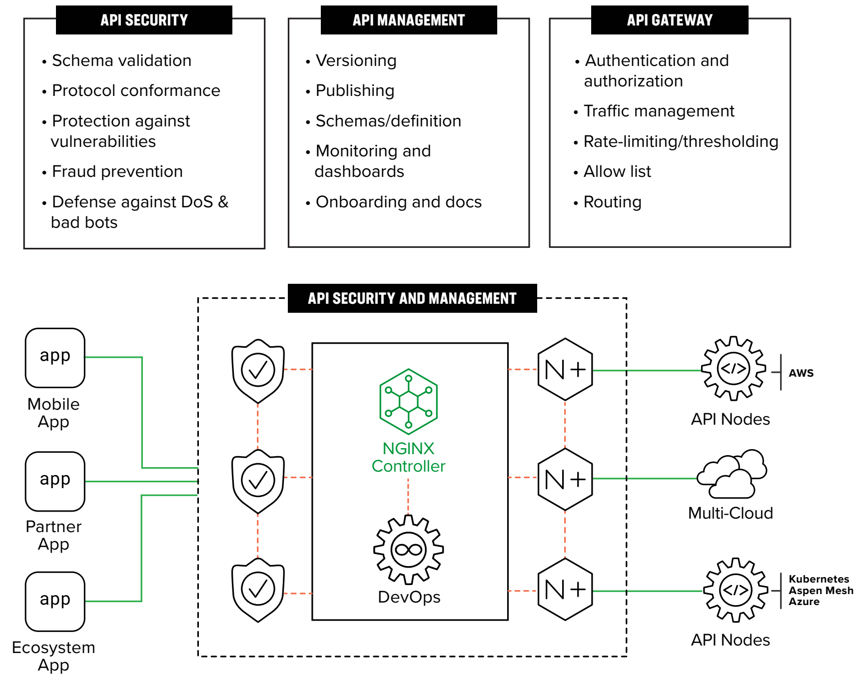


Figure 3: F5 is the only vendor that can deliver API management, high-performance API gateways, and advanced security controls all in one solution.

Learn more about F5's API solution.

CLOUD NATIVE INFRASTRUCTURE SECURITY

AS SERVICE PROVIDERS BEGIN MIGRATING TO CLOUD-NATIVE INFRASTRUCTURE, SECURITY MUST BE CONSIDERED UPFRONT TO ENSURE DATA IS PROTECTED.

Service providers implementing a cloud-native infrastructure are pioneers in their digital transformation journey. The one-size-fits-all approach no longer applies to 5G networks, where multiple cloud deployments are merely a starting point. 5G infrastructure is built on a cloud- native, containerized architecture, where container workloads are managed using Kubernetes. As service providers begin migrating to cloud-native infrastructure, security must be considered upfront to ensure data is protected. In a cloud-native infrastructure architecture, security controls need to be applied at multiple points in the network and across multiple layers. Implementing security at container ingress can ensure malicious traffic stays out of a service provider's network. Kubernetes traffic between multi-vendor and multi-site network functions can be encrypted and authenticated built on mutual Transport Layer Security (mTLS). The diagram below depicts F5's cloud-native infrastructure solution with F5® BIG-IP® Service Proxy for Kubernetes (BIG-IP SPK) and Carrier-Grade Aspen Mesh.

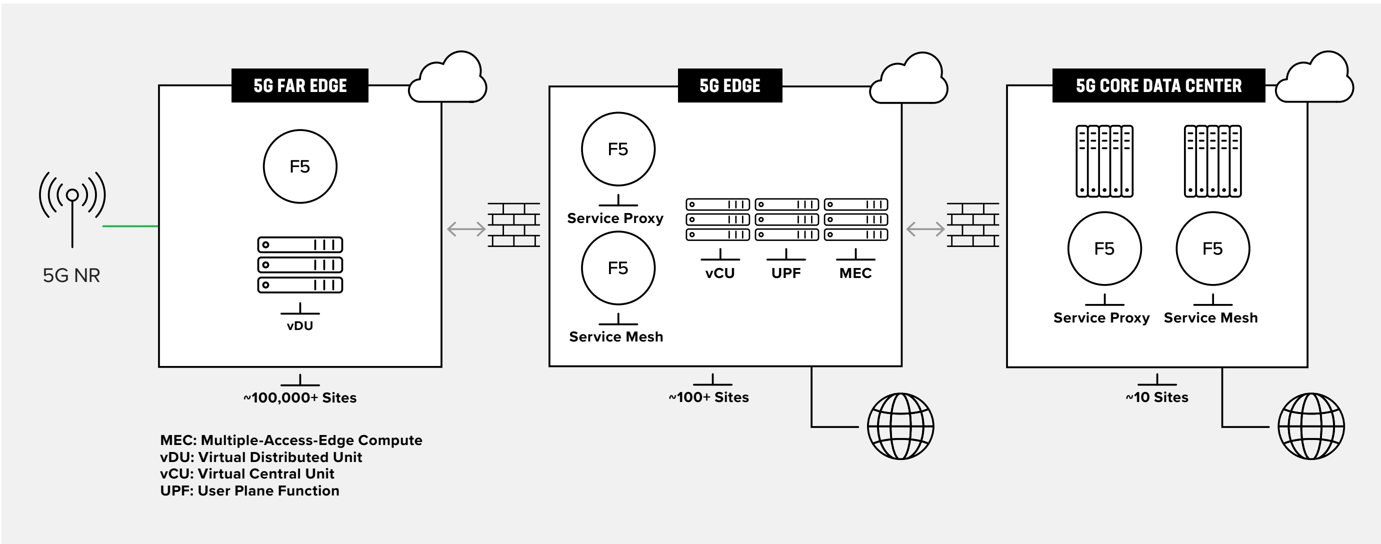


Figure 4: F5's cloud-native infrastructure solution

How F5 Secures Your Cloud-Native Infrastructure

F5 provides security solutions for service providers implementing a cloud-native infrastructure for both BIG-IP SPK and Carrier-Grade Aspen Mesh.

Security services such as distributed denial-of-service (DDoS) protection, firewall, and web application firewall (WAF) can be applied at container ingress to prevent malicious traffic from entering the cluster and impacting 5G core network functions and customer applications. Carrier-Grade Aspen Mesh provides a service mesh that builds on open source Istio and is implemented by providing a proxy instance, called a sidecar, for each service instance. Sidecars handle interservice communications, monitoring, and security-related concerns—offering an abstraction layer for individual services (applications). By providing a sidecar data plane at every app (CNF container), Carrier-Grade Aspen Mesh can intercept all ingress and egress container traffic. This capability enables CNF sidecar traffic capture, including intra-node CNF traffic and pre-encryption tapping, and also reduces SSL load for brokers. The service proxy easily integrates with existing infrastructure, provides full packet visibility, is scalable and extensible, and uses existing packet broker APIs. The service proxy also provides encryption through mutual transport layer security (mTLS) to secure service-to-service communication.

BY PROVIDING A SIDECAR DATA PLANE AT EVERY APP (CNF CONTAINER), CARRIER-GRADE ASPEN MESH CAN INTERCEPT ALL INGRESS AND EGRESS CONTAINER TRAFFIC.

Learn more about F5's cloud-native infrastructure solution.

SIGNALING AND ROAMING SECURITY

Signaling is the nerve center for mobile networks, which makes it an ideal target for attacks. Attackers have successfully exploited vulnerabilities in signaling protocols SS7, Diameter, and SIP used in 2G, 3G, and 4G, causing denial-of-service and even allowing attackers to carry out fraud. Attacks against signaling protocols can be devastating for a mobile provider's reputation and erode customer trust. Enhancements have been made to protect these important signaling protocols, such as introducing signaling firewalls.

The roaming interface is another favorite point of attack for cybercriminals, exploiting vulnerabilities in the General Packet Radio Service (GPRS) Tunneling Protocol. The GPRS Tunneling Protocol (GTP) is used between roaming partners and is a target for attackers. 5G's security-first approach introduced the Security Edge Protection Proxy (SEPP) specifically for protecting the roaming interface. The introduction of the SEPP, and greater focus from standards bodies like the GSMA to better define security requirements for GTP, are making the roaming interface more secure in 5G.

How F5 Secures Your Signaling and Roaming Interface

F5 has extensive experience in providing signaling and roaming security solutions that can address security concerns for mobile providers transitioning from their existing 4G networks to 5G.

F5 provides Diameter and GTP firewall security solutions for mobile providers who are still looking to address security gaps on their existing 4G network. F5's solutions provide mobile operators the scalability, flexibility, performance, and control needed to mitigate the most aggressive, volumetric DDoS attacks.

BIG-IP SPK'S SIGNALING FIREWALL WILL SUPPORT DIAMETER, SIP, GTP, AND SCTP ALONG WITH HTTP/2 TO SMOOTH THE TRANSITION FROM 4G TO 5G.

For those mobile providers who are aggressively deploying cloud-native infrastructure for their 5G SA core, F5 provides signaling firewall functionality as part of BIG-IP SPK to protect the Kubernetes cluster. Security at ingress to the cluster is an ideal position, as it prevents malicious traffic from ever entering the cluster, and allows for focusing hardware optimizations (e.g., SmartNIC) in a single place. In addition, BIG-IP SPK's signaling firewall will support Diameter, SIP, GTP, and SCTP along with HTTP/2 to smooth the transition from 4G to 5G.

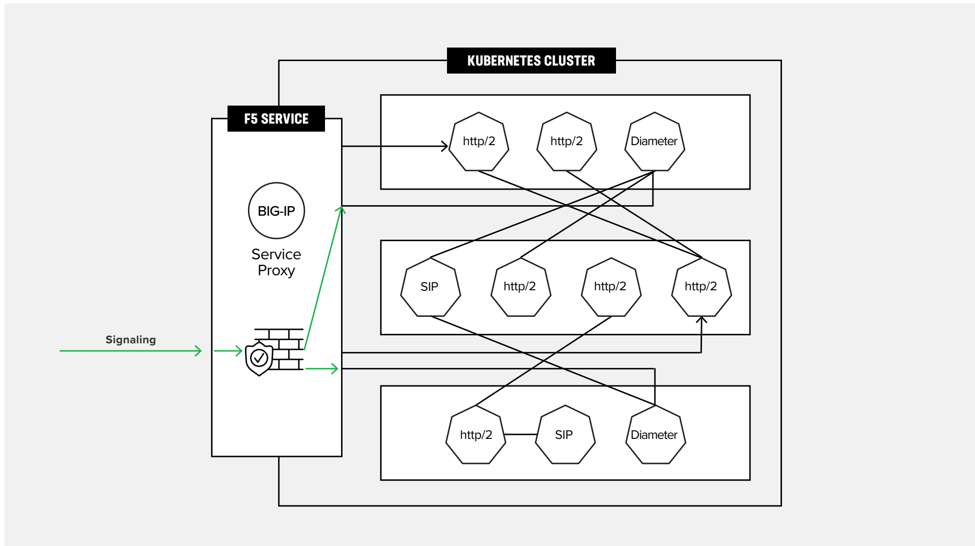


Figure 5: BIG-IP Service Proxy for Kubernetes (BIG-IP SPK) signaling security

Learn more about F5 Signaling and Roaming solutions.

SECURING AND CONSOLIDATING N6 LAN

The N6 LAN (previously known as S/Gi-LAN) is the interface that lies between the User Plane Function (UPF) and the internet. The N6 LAN functions are often consolidated to optimize network performance and reduce costs. This interface is the gateway to the internet and must be properly secured. Security features that are normally located here include:

- Carrier-Grade Network Address Translation (CGNAT)
- N6 (Gi) Firewall
- IoT Firewall
- DDoS
- Subscriber Security Services
- Secure DNS Cache

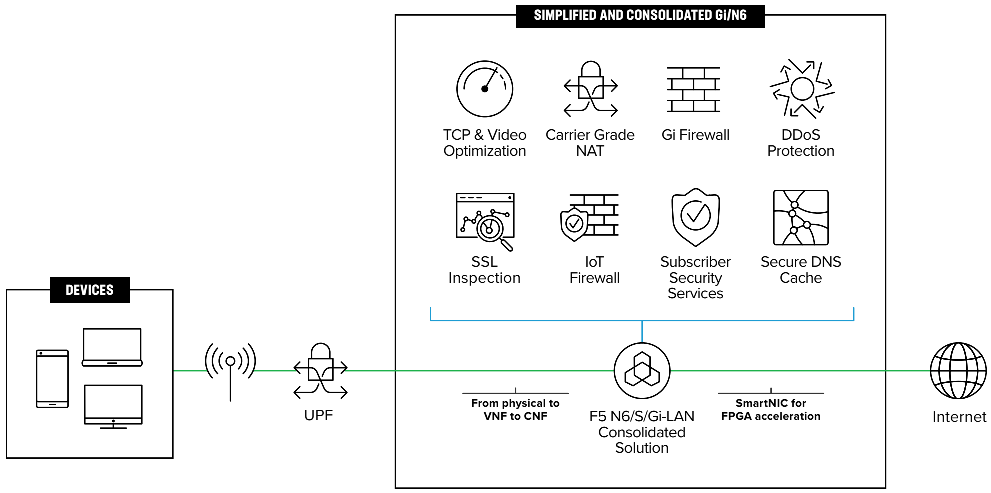


Figure 6: F5's N6/S/Gi-LAN consolidated solution lowers CPU needs and simplifies automation, reducing CapEx and OpEx.

A containerized and consolidated N6 LAN solution from F5 helps you build a cost-effective model, improving time to market for new services and decreasing network complexity. F5's cloud-native network functions (CNFs) are a core component within an efficient, virtual N6 LAN, providing solutions such as virtual policy enforcement, virtual firewall, virtual Application Delivery Controller (ADC) services, and many more, offering the widest range of services on the N6 LAN to date.

A service provider might begin the consolidation with CGNAT functionality combined with Gi Firewall and DDoS protection as the primary requirement. DNS is also key and can be added—with a focus on DNS caching and DNS security. Layered on top of that might be TCP and/or video optimization techniques. Additional, subscriber-aware subscriber security can also be added, including IoT firewall or parental controls.

How F5 Secures Your N6/Gi-LAN

By using F5's unified platform to deliver network services, service providers can:

- Significantly reduce cost structures by lowering capital and operating costs.
- Dramatically simplify service delivery architecture, boosting service velocity with a unified platform.
- Gain key NFV and containerized capabilities to virtualize and dynamically scale services.
- Monetize the network via content-aware and subscriber-aware services.
- Optimize the network with sophisticated reporting and analytics.
- Provide unparalleled security, ensuring customer trust.

Learn more about F5 N6 LAN solutions.

FRONT OFFICE CONSUMER SECURITY

Telecommunications companies are among the world's most targeted organizations, attracting highly sophisticated and well-resourced attackers. This is especially true as the industry increasingly moves into the role of mass media conglomerate. One misstep by a skilled and otherwise perfect security team could result in millions of dollars in losses, embarrassing headlines, costly fines, and brand damage that lasts for decades. It's not enough for security teams to patch vulnerabilities like those described in the OWASP Top Ten. It's not enough to have red teams and blue teams. It's not enough to have a robust bug bounty program. These are all steps in the right direction, but even if perfectly executed, they still fall short of providing lasting protection for your organization.

F5 protects its telecommunications customers from online fraud and abuse. A byproduct of this protection is visibility—billions of transactions from web and mobile applications pass through the F5 network every day. This visibility gives F5 unparalleled insight into the types of attacks that target inherent vulnerabilities across the entire telecommunications industry. Security teams must understand these attacks, why they happen, how to protect against them, and why traditional countermeasures alone don't work.

How F5 Mitigates Bots and Abuse

Service providers strive to make their technology available to anyone, everywhere. The race for the killer app continues at full speed, and 5G innovation creates new opportunities for cyberattacks. F5 will stop cyberattacks in their tracks so you can continue to offer unfaltering QoE.

F5 SOLUTIONS ADAPT AND MAINTAIN FULL EFFECTIVENESS EVEN AS ATTACKERS RETOOL AND EVOLVE TO OVERCOME COUNTERMEASURES. F5 SOLUTIONS ALSO REDUCE OR REMOVE HIGH-FRICTION MECHANISMS, INCLUDING CAPTCHA AND MFA, THEREBY IMPROVING THE OVERALL USER EXPERIENCE.

Security must adapt to attackers who retool to bypass countermeasures—regardless of the attackers' tools, techniques, or intent—without frustrating users with login prompts, CAPTCHA, and multi-factor authentication (MFA). This includes omnichannel protection for web applications, mobile applications, and API interfaces; protection against scans that attempt to exploit application vulnerabilities; and client-side defenses that prevent sensitive data theft through browser or third-party exploits. Threat intelligence across similar attack profiles and risk surfaces provides unparalleled accuracy. This allows mitigations to maintain full efficacy as attackers retool and adapt to countermeasures—stopping even the most advanced cybercriminals and state actors. The ability to react as applications and attackers adapt dramatically improves business outcomes, including:

- Reduced losses due to fraud and abuse.
- Better application performance and uptime.
- Measurable cost savings for hosting and bandwidth.

F5 solutions adapt and maintain full effectiveness even as attackers retool and evolve to overcome countermeasures. F5 solutions also reduce or remove high-friction mechanisms, including CAPTCHA and MFA, thereby improving the overall user experience.

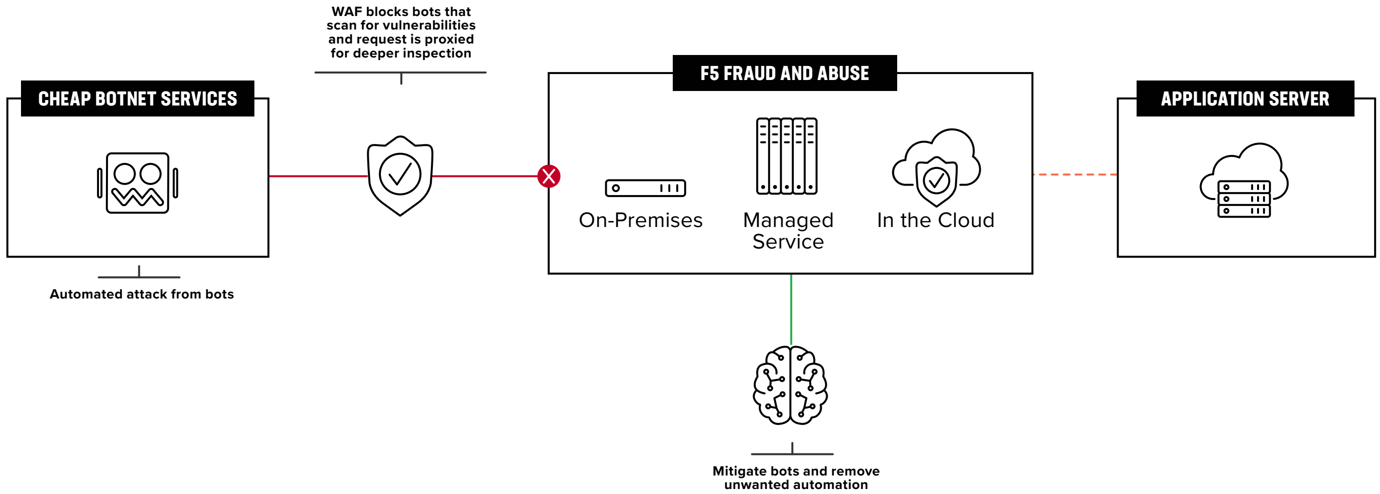


Figure 7: Neutralize fraud and abuse that jeopardize strategic business outcomes.

Learn more about mitigating bots and abuse.

How F5 Helps Protect Against Human-Driven Fraud

Fraud is a human problem more than a technical one. Therefore, the best approach to online fraud protection is to react as attackers adapt and evaluate truth and intent without frustrating users and compromising the user experience. Technology enables the business to address these issues at scale by stopping attacks that can otherwise lead to fraud while maximizing customer engagement across web and mobile applications.

In addition to maintaining efficacy and resilience as attackers retool and adapt to countermeasures, online fraud protection must provide insights to fraud-management ecosystems. This will enable organizations to identify fraudulent transactions in real time across the entire user journey and share actionable intelligence with business leaders to optimize real customer interactions.

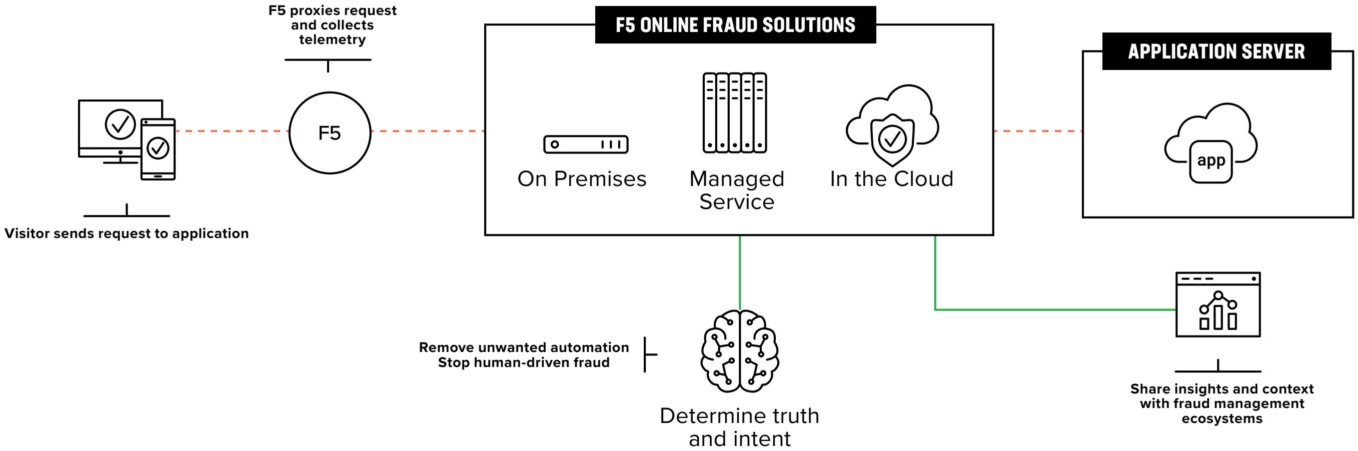


Figure 8: Organizations can stop human-driven fraud by reacting quickly as attackers adapt

Learn more about F5's security solutions.

Conclusion

Security underscores the entire 5G network. It's critical to architect networks with security in mind and not after your network is attacked. F5 provides a rich set of security solutions for your 5G networks that fulfill every aspect of the threat landscape—from front office devices all the way to the 5G core threats. F5 provides subscriber-aware solutions that scale with your network, enabling you to automate and innovate while maintaining customer trust.

To learn more, contact your F5 representative, or visit F5.com.