APPLICATION PROTECTION SOLUTIONS GUIDE

APP-CENTRIC SECURITY IN TODAY'S MULTI-CLOUD WORLD

Securing your apps and your business in the digital economy

Digital transformation is completely reshaping the way organizations do business, and apps are firmly at the core—they *are* the business. Together with cloud-based services, these apps create a platform for new business models, innovative service offerings, and enhanced customer experiences that drive new business revenue. It's now commonplace to have apps deployed in a multitude of ways—from private and public clouds to co-location facilities and container environments. Today, 9 out of 10 organizations use multiple cloud platforms.[1]

Apps are the business

There are

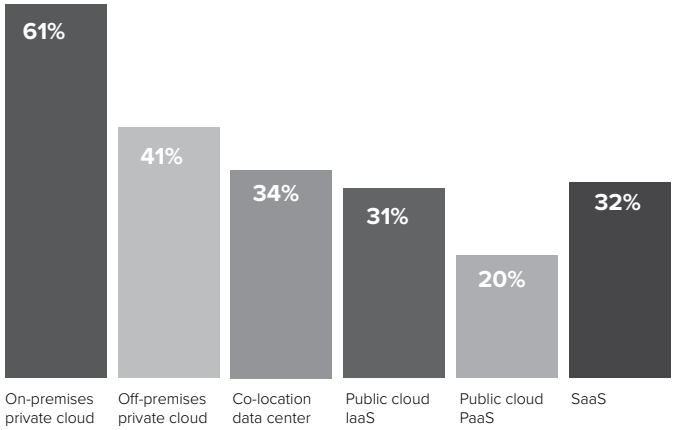
765

applications in a typical organization

34%

of these apps are considered mission-critical[2]

It's a multi-cloud world



59%

use between two to six cloud platforms[1]

However, there's a flip side to digital transformation and the advantages it brings: while our app-centric, multi-cloud world fuels new opportunities for businesses, it also creates new opportunities for attackers.

[1] 2018 State of Application Delivery Report, F5
[2] 2018 Application Protection Report, F5 Labs

With apps everywhere and accessible anywhere, there is increased risk

As apps become the doorways to your data and cloud platforms—some operated by third-party providers—the number of threats to apps rises exponentially.

Today, cybercrime tools have become commoditized and more easily available, resulting in a corresponding rise in the number and types of attacks. At the same time, targeted attacks, such as those from organized crime and nation states, are becoming more sophisticated and can cause business impacts including application downtime, compromised sensitive data, and fraudulent transactions.

Multi-cloud means multi-risks

86%

of data breaches now occur at the app level[3]

38%

of organizations have "no confidence" of knowing where their applications reside[3]

$8 million

is the self-reported cost of an average app attack[4]

For the connected enterprise, the scale of the challenge can seem overwhelming, and it can make staying on top of security feel like a losing battle.

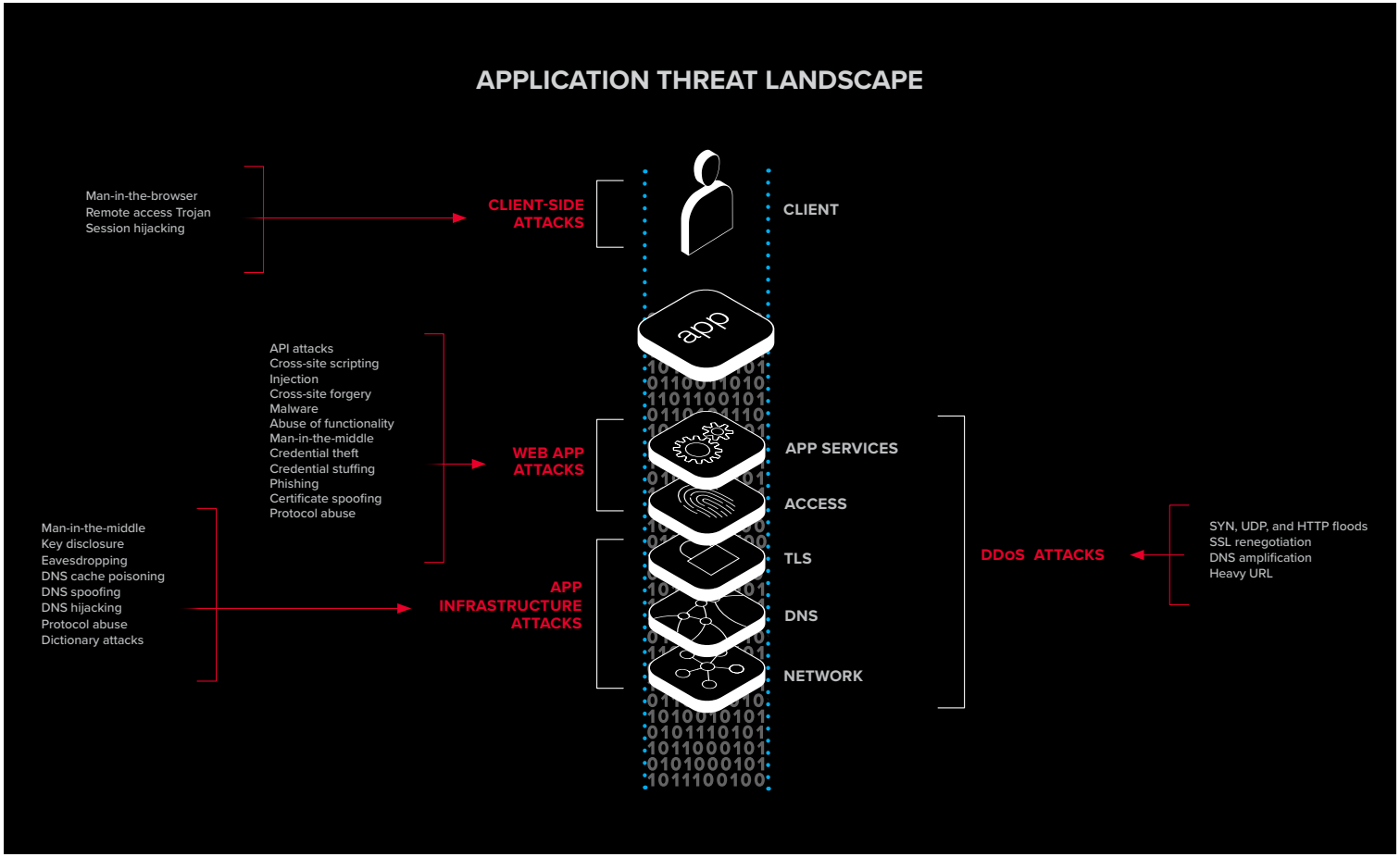
But it doesn't have to be.

[3] F5 Labs Report: Lessons Learned from a Decade of Data Breaches
[4] 2018 Application Protection Report, F5 Labs

Take an app-centric approach to security

An app-centric approach to security—focusing on securing the apps themselves and access to them—can minimize your risk in today's app-first, multi-cloud world.

To prioritize your efforts effectively, you first must understand the app itself—its key components and its areas of vulnerability. Consider the cloud platforms the app resides on; the data that travels from the user to the app; the DNS that resolves the IP address to access the app; the web and application servers; and the associated APIs that are leveraged by other applications and systems.



Application Threats at Each Tier

The client tier consists of application clients that access a Java EE server and that are usually located on a different machine from the server. The clients make requests to the server.

Client

- Cross-site request forgery
- Cross-site scripting
- Man-in-the-browser
- Session hijacking
- Malware
- Unauthorized/fraudulent transactions
- Malicious scripts
- Certificate forging
- Mobile app tampering

Web servers, content delivery networks, and app or database servers are the base for web application services. Also part of this tier are frameworks, libraries, and plugins, and internal code that provides an app's core functionality. Attackers frequently scan for unpatched components within this tier, making it the focus of common attacks, such as injection or business logic flaws.

App Services

- API attacks
- Injection
- Malware
- DoS and DDoS
- Cross-site scripting
- Cross-site request forgery
- Man-in-the-middle
- Abuse of functionality
- Botnet attacks

Access is the gateway to the data that an app processes or stores. This tier provides web, mobile, and API clients the ability to authenticate and get authorization to access an application, so it needs to be secure and efficient. An analysis of breach records shows that 33 percent of web app breaches are access related, with phishing, brute force, and credential stuffing attacks leading the way.[5]

Access Control

- Credential theft
- Credential stuffing
- Session hijacking
- Brute force
- Phishing

[5] F5 Labs Report: Lessons Learned from a Decade of Data Breaches.

Application Threats at Each Tier

The transport layer security tier includes HTTPS, TLS, and even the outdated SSL protocol. It provides confidentiality for clients and apps communicating over untrusted networks, ensuring attackers can't tamper with data in transit. Flawed libraries or implementations can lead to vulnerabilities like Heartbleed or denial-of-service attacks. TLS is also used to hide payloads that target other tiers of the app.

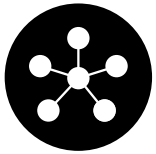
Transport Layer Security

- DDoS
- Key disclosure
- Protocol abuse
- Session hijacking
- Certified Spoofing

The "address book" of the Internet, DNS translates domain names into IP addresses so browsers can load Internet resources. This tier includes all DNS servers needed by the client and the app, as well as the relevant registrars of those apps' domains. App availability can be disrupted if its DNS suffers a DDoS attack. Alternatively, DNS can be targeted in a hijacking attempt that can compromise an app's confidentiality or integrity.

Domain Name System

- Man-in-the-middle
- DNS cache poisoning
- DNS spoofing
- DNS hijacking
- Dictionary attacks
- DDoS



Clients and apps need a network to connect. Many applications exist on or communicate over the biggest network—the Internet. An app also typically resides on an internal network, allowing app admins to connect and make changes. The network tier is a target of multiple types of DDoS attacks. Compromised internal networks can lead to unauthorized disclosure, alteration, or destruction of data.

Network

- DDoS
- Eavesdropping
- Protocol abuse
- Man-in-the-middle

By understanding the components of an app and taking an app-centric approach, you can choose the right solutions to protect against risks. As threats evolve, you can also stay ahead of new vulnerabilities by leveraging actionable threat intelligence.

Solutions for a multi-cloud, app-driven enterprise

If you want to protect the capabilities that drive your business, it means protecting the apps that make them happen.

F5 uniquely enhances your organization's security strategy with the broadest portfolio of app-centric security solutions and services on the market. With F5, you can extend robust and customizable security policies and controls across multiple clouds, on-premises environments, and deployment models like containers and co-location services. Monitor and manage everything from a single point of control to simplify management, optimize performance and more efficiently address constantly changing risk factors.

DDoS Protection	App Infrastructure Protection: TLS/SSL visibility and orchestration	App Infrastructure Protection: Intelligent DNS	Web App and API Protection	Access Management
Ensure your apps are always up and running, protected against multi-vector DDoS attacks	Go beyond visibility with orchestration of TLS/SSL encrypted traffic	Secure your DNS infrastructure to ensure your customers—and your employees—can access your critical web and application services	Protect against application exploits and web fraud, deter unwanted bots and other automated threats, and ensure appropriate authentication and authorization for APIs	Enable secure anytime, anywhere access to apps wherever they reside

DDoS Protection: Ensure your apps are always up and running, protected against multi-vector DDoS attacks

Business challenges

Whether they are designed as targeted acts of mischief, retaliation, protest, or extortion, all DDoS attacks have one objective: to disrupt the availability of your apps and stop you from doing business with customers. It's become more challenging to protect applications from such attacks because:

- Apps are spread across different data centers and cloud platforms, increasing complexity, risk and cost
- On-premises DDoS solutions are less effective for public cloud apps
- Organizations lack in-house resources to regularly detect, analyze and mitigate increasingly complex DoS attacks
- Traditional threshold-based detection methods are ineffective against advanced DDoS, and may even contribute to network slow-down

F5 DDoS Protection Solution

F5 DDoS Protection provides seamless, flexible, and easy-to-deploy solutions that enable a rapid response, no matter what type of attack you're combating.

USE CASES

Protect your app infrastructure

DDoS attacks against DNS, network and TLS tiers can render your networks, applications or other supporting infrastructure inaccessible. Mitigate attacks targeted at both the network and app services layers; detect targeted L7 requests and then rate limit the connection in hardware at L4.

F5 DDoS Protection:

- Mitigates lower-level attacks with purpose-built hardware for improved scalability
- Allows you to choose between a hybrid solution with on-demand or always-on cloud scrubbing or outsource your protection entirely with fully managed DDoS protection services
- Provides a high capacity and scalable platform that will protect your network against high volume DNS volume attacks when firewalls fail
- Improves network optimization via efficient network traffic routing to the most optimal DNS/app service in the network
- Blocks access to malicious IP domains with a domain reputation service such as SURBL or Spamhaus

Protect your web apps

Layer 7 attacks are more common in today's threat landscape. Attackers use low-and-slow attacks that avoid network level detection to degrade app performance or bring down the app altogether.

F5 DDoS Protection:

- Automatically detects and mitigates DoS attacks with a continuous feedback loop that monitors resource stress
- Provides bot detection, behavioral analysis, deep attack inspection, and on-demand cloud scrubbing activation
- Enables faster detection by shunning traffic that matches discovered signatures/bad actors and utilizing real-time decryption capabilities
- Protects against targeted, multi-layered, blended attacks and reduces overall time-to- response with almost infinite scale

F5 DDoS Protection Products

F5 DDoS Hybrid Defender – Comprehensive DDoS threat coverage in a simple, dedicated appliance with native, cloud-based scrubbing services | *Learn more*

F5 Silverline DDoS Protection – Fully managed, cloud-delivered protection service that detects and mitigates large-scale, TLS/SSL, or application-targeted attacks in real time—defending your business from even those attacks that exceed hundreds of gigabits per second | *Learn more*

Management models

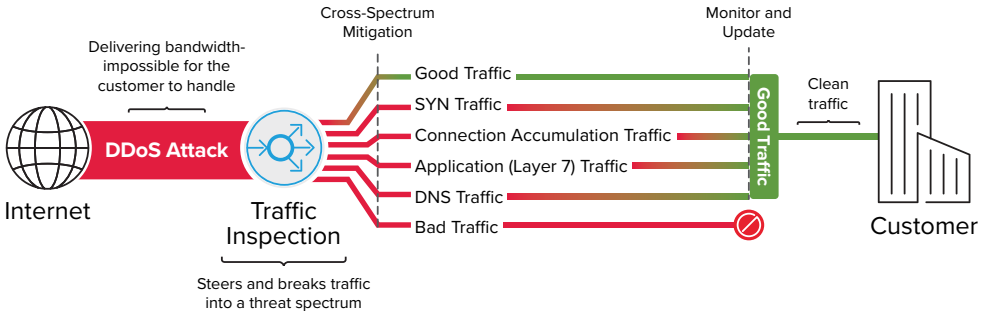
- Self-managed
- Fully managed by F5

Licensing options

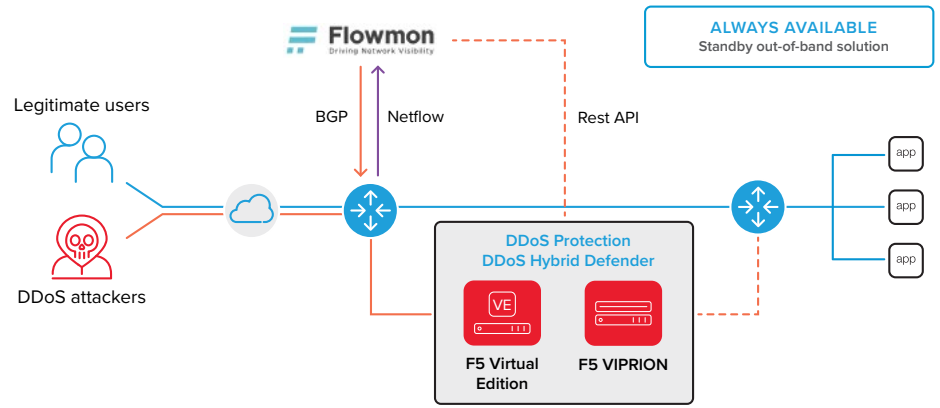
- Hardware + Software Perpetual
- High Performance Virtual Edition
- Managed (Subscription)

Deployment models

INLINE

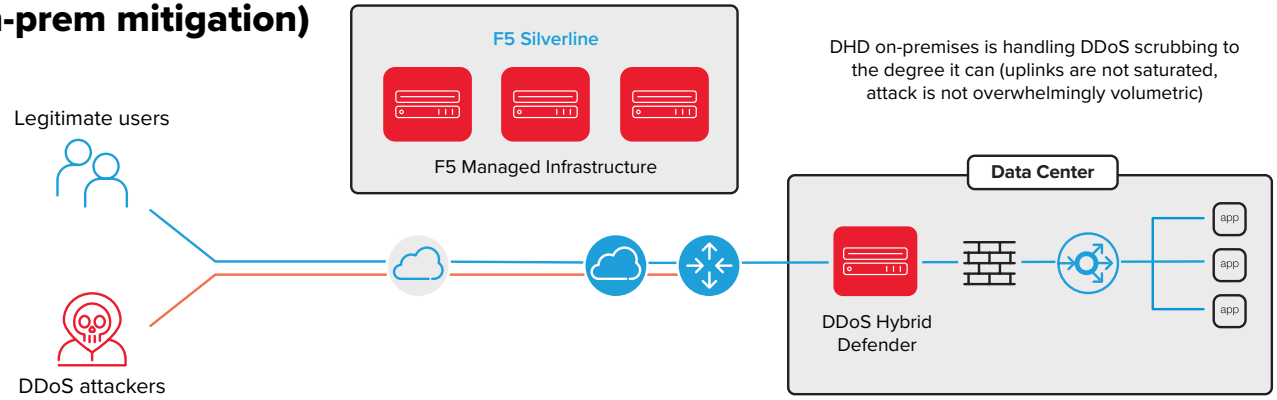


OUT-OF-PATH

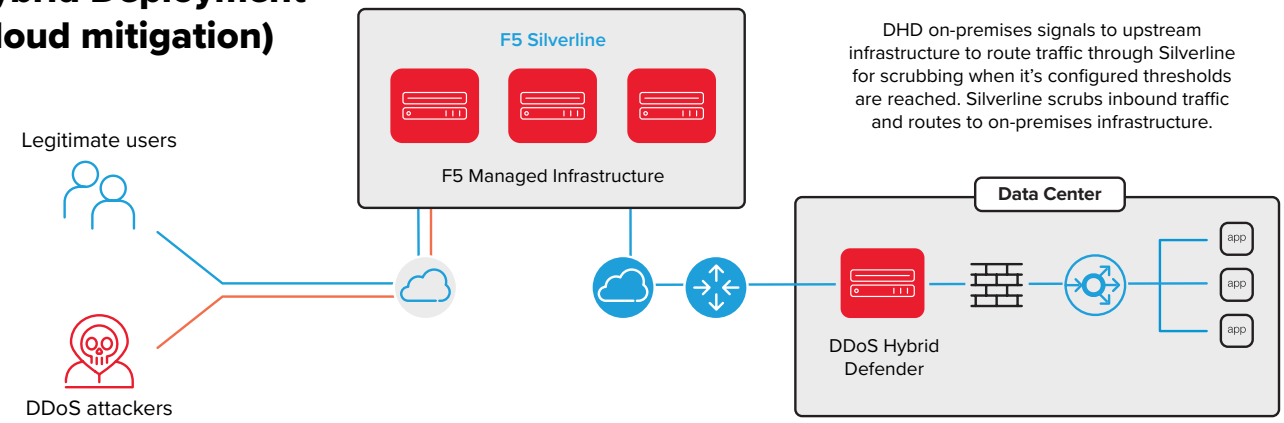


HYBRID (a combination of cloud and on-premises)

Hybrid Deployment (on-prem mitigation)



Hybrid Deployment (cloud mitigation)



Learn more

- eBook: A guide to DDoS protection: choosing the right model
- Customer story: Heritage Bank improves DDoS protection

App Infrastructure Protection: Go beyond visibility with orchestration of TLS/SSL encrypted traffic

Business challenges

Cryptographic protocols—like Secure Sockets Layer (SSL) and its successor Transport Layer Security (TLS)—exist to prevent adversaries from eavesdropping and tampering with data. However, encryption is a double-edged sword as attackers can use TLS as a tunnel for hiding attacks and malware from security devices. Organizations struggle to address this challenge given:

- IT is burdened with inefficiencies such as daisy-chaining multiple security inspection devices and tedious manual configuration of different traffic scenarios
- Inspection devices like a next-gen firewall, an IDS/IPS, or a malware sandbox don't see into encrypted TLS/SSL traffic or suffer degraded performance when decrypting
- Many new security products cannot decrypt TLS/SSL traffic without slowing down network performance
- SSL 3.0, despite being deprecated by the IETF in 2015, continues to be used for 11% of all traffic on the Internet. What's more, many new vulnerabilities have been discovered for SSL 3.0[6]

[6] Report: The 2017 TLS Telemetry Report

F5 App Infrastructure Protection

With F5 TLS/SSL solutions, you can move beyond visibility with orchestration of your encrypted traffic. Gain not only the ability to see inside the packets coming into your applications or going out from your network, but orchestrate capabilities as well—a full proxy for both TLS/SSL and HTTP that provides policy-based traffic steering to a service chain based on risk and dynamic network conditions.

USE CASES

Enable end-to-end encryption

Managing TLS/SSL connections between users and apps can be tedious and expose your business to security risks.

F5 helps to:

- Centralize and simplify the management of keys, certificates and ciphers used in end-to-end encryption
- Cost-effectively protect data-in-transit by encrypting everything from the client to the server
- Maximize existing security investments and minimize risk with a dynamic, policy-based approach to TLS/SSL inspection

Inspect encrypted traffic

TLS/SSL can function as a tunnel that attackers use to hide attacks and malware from security devices that can't see into encrypted TLS/SSL traffic.

F5 enables TLS/SSL visibility by offering:

- Support of multiple deployment modes, easily integrating into complex architectures to centralize decryption functions for both inbound and outbound traffic
- Policy-based traffic steering for intelligent routing of traffic based on classification criteria, flow information, or custom criteria

Protect TLS/SSL protocol

Attackers and security researchers are constantly trying to find new ways to break today's popular methods of encrypting data-in-transit. Often, a flaw in the protocol design, a cipher, or an underlying library is the culprit.

F5 solutions enable:

- Centralized management of your TLS/SSL configuration which enables better app performance
- Seamless flexibility in updating your TLS/SSL configurations as needed

F5 App Infrastructure Protection Products

BIG-IP Local Traffic Manager – Gain full awareness and control over all traffic—encrypted or otherwise—entering and exiting your network, from basic load balancing to complex traffic management | *Learn more*

F5 SSL Orchestrator – Enjoy high-performance decryption of inbound and outbound SSL/TLS traffic, enabling security inspection to expose threats and stop attacks | *Learn more*

BIG-IP Advanced Firewall Manager – Guard your network against incoming threats that enter the network on the most widely deployed protocols | *Learn more*

F5 Advanced Web Application Firewall – Protect apps and data from known and unknown threats, defend against bots that bypass standard protections, and virtually patch app vulnerabilities | *Learn more*

Management models

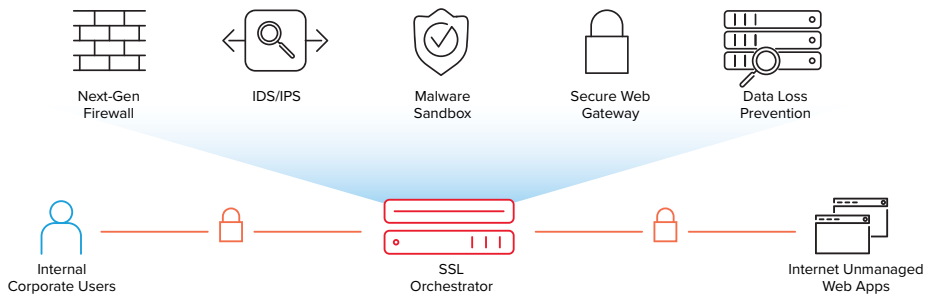
- Self-managed

Licensing options

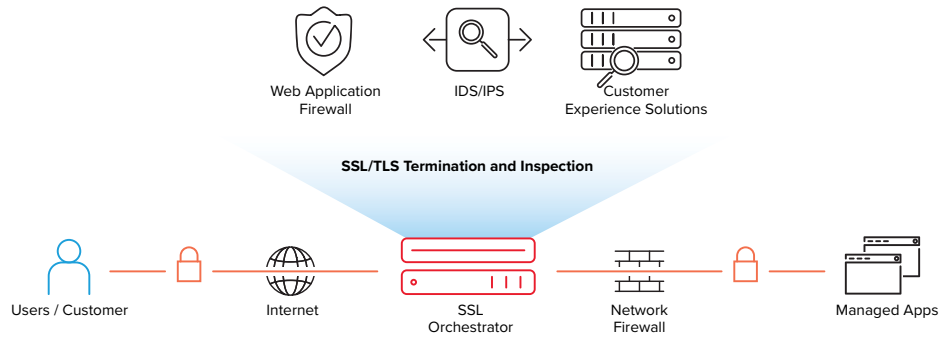
- Software Subscription/ELA
- Hardware + Software Perpetual
- Virtual Edition + Software Perpetual

Deployment models

OUTBOUND



INBOUND



Learn more

- Report: The 2017 TLS Telemetry Report
- Customer story: MDV detects, blocks threats embedded in SSL without sacrificing performance

App Infrastructure Protection: Secure your DNS infrastructure against attacks cloaked in encrypted traffic

Business challenges

Securing DNS infrastructures from complex DDoS attacks and protecting DNS query responses from fake redirects are essential given the advanced state of security threats today. However, organizations can find it challenging to protect the DNS architecture because:

- Many products are unable to monitor DNS infrastructure and app health at scale and on demand
- DDoS attacks, cloaked in regular traffic, can overload DNS servers with requests and prevent other users from connecting to the requested site
- Customers can be unknowingly hijacked and diverted to a fake site where credentials can be stolen through methods like DNS hijacking and DNS cache poisoning
- Apps are spread across different data centers and cloud platforms, increasing complexity, risk and cost

F5 Intelligent DNS Solution

F5 Intelligent DNS solutions gives you full visibility, control and automation over your encrypted traffic. Prevent attacks on SSL/TLS, DNS and the network, and keep your apps secure and available at all times.

USE CASES

Prevent DNS hijacking

DNS hijacks redirect traffic to a website designated by the attacker—such as a fake banking website that looks like the actual one—to steal credentials.

With F5, you can:

- Ensure secure communications without requiring computationally costly cryptographic operations
- Enable validation for any combination of resolving, caching, and DNS response functionality
- Easily integrate with existing DNS infrastructure, increase DNS performance at the network edge, and mask the DNS back-end infrastructure resulting in higher productivity, server consolidation, faster responses, and protected DNS management

Stop DNS DDoS attacks

A DNS DDoS attack can degrade or disable a web app's ability to respond to legitimate traffic and is difficult to distinguish from normal heavy traffic.

With F5 you can:

- Hyperscaling to process more requests per second when required, leading to greater productivity and less downtime
- Mitigating DNS threats by blocking access to malicious IP domains, thus protecting your users and your reputation
- Automatically directing users to the site with the best performance based on app, location, business and network conditions
- Scale up to 200x a traditional DNS Server (up to 40 M RPS) by configuring DNS Express mode
- Gain high-speed response and DDoS protection with in-memory DNS

USE CASES

Detect DNS tunneling

Many firewalls and IPS solutions do not address the more modern threats to DNS infrastructure, like DNS tunneling. Managing DNS attack vectors requires inspection of the entire DNS query for deeper markers of either good or bad behavior without disrupting service performance.

F5 Intelligent DNS provides:

- DNS Protocol Validation that scrubs the incoming DNS queries to only answer valid clients and requests
- Query type filtering and rate limiting features that can further protect DNS resources
- Intelligent per-Client IP rate limiting for inhibiting malicious activity without adversely affecting performance
- Detailed stats with high-speed DNS logging, reporting, and advanced analytics for security troubleshooting

Response policy zones

Malicious domains are a basic tool for cybercriminals. With a domain name service (DNS) response policy zone (RPZ) as a firewall mechanism, you can block known malicious Internet domains and sub domains automatically.

F5 Intelligent DNS enables:

- Centralized location in your infrastructure to stop clients from trying to resolve blacklisted domains
- Response Policy Zones (RPZ) which filters out and provides NXDOMAIN / Redirect for known bad domains
- URL Filtering for granular policy controls using categories
- IP Intelligence which blocks access based on the resolved IP

F5 App Infrastructure Protection Products

BIG-IP DNS – Secure your infrastructure at hyperscale during high query volumes and DDoS attacks, and ensure apps are highly available—even between multiple instances and across hybrid environments | *Learn more*

Management models

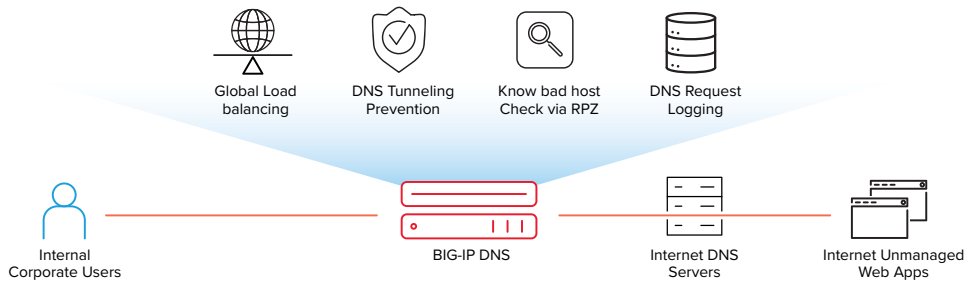
- Self-managed

Licensing options

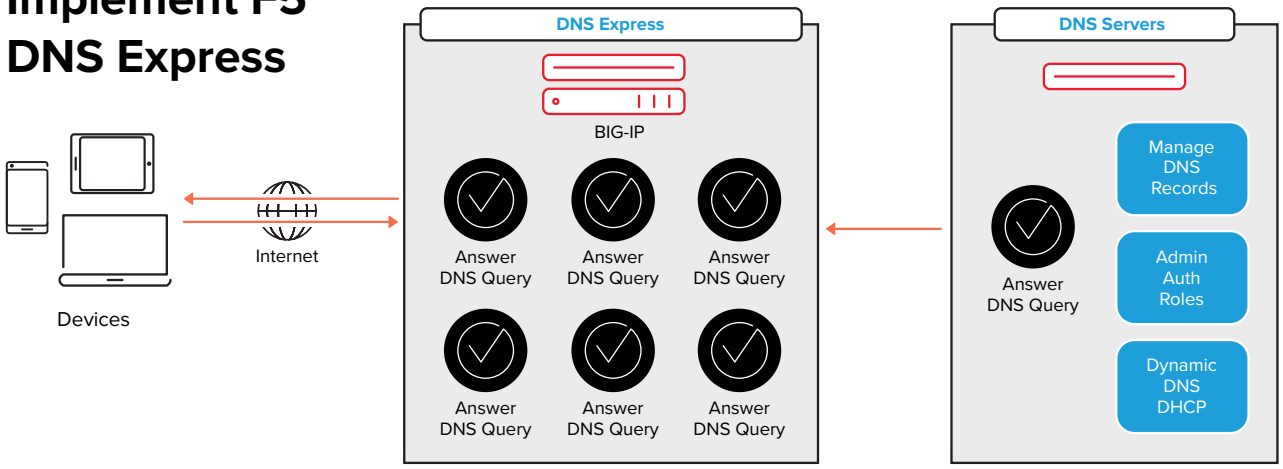
- Hardware + Software Perpetual
- Virtual Edition + Software Perpetual

Deployment models

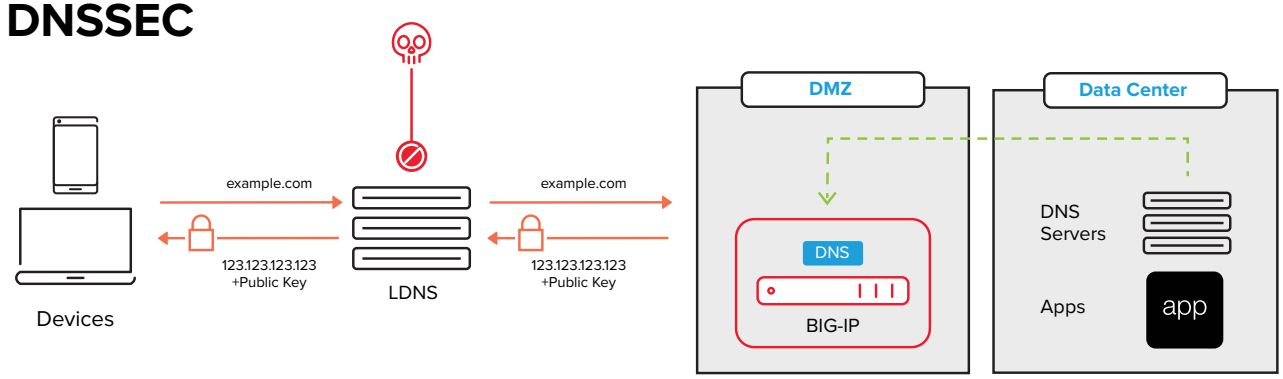
INTELLIGENT DNS OUTBOUND



Implement F5 DNS Express



DNSSEC



Learn more

- Video: An introduction to BIG-IP DNS load balancing
- Customer story: Heritage Bank improves DDoS Protection

Web App and API Protection: Protect against application exploits, deter unwanted bots and other automated threats, reduce costs in the cloud

Business challenges

Today, web attacks are the leading cause of data breaches[7] with half of all apps vulnerable to attacks[8]. For most organizations, this problem is a complex one. While there's pressure to release new apps to market quickly, there are many factors that make securing apps problematic:

- Attacks, like DoS, are moving beyond the network to target the app layer
- The proliferation of APIs creates additional threat vectors
- Organizations lack onsite resources to identify, monitor and mitigate threats as they emerge
- Vulnerabilities need to be fixed as quickly as they are identified
- Patching and upgrading apps in live environments is complex, cumbersome and may lead to unscheduled downtime
- The growing prevalence of automated and bot-based attacks not only target web apps but also mobile apps which traditional WAFs leave unprotected

[7] F5 Labs Report: Lessons Learned from a Decade of Data Breaches.
[8] WhiteHat data

F5 Web App and API Protection

F5's Web App and API Protection helps you defend against new and emerging threats with advanced countermeasures and app layer visibility that helps ensure that your defenses remain effective over time. F5 solutions can protect against application exploits, deter unwanted bots and other automation for *all* your apps—web-based or mobile, deployed on-premises or in the cloud.

USE CASES

Prevent web fraud

Fraudsters can be extremely sophisticated and there is no single solution or technology that can be fully relied upon to thwart them. However, implementing defenses that make your applications a more challenging target will greatly increase the probability that criminals will focus their attention and efforts elsewhere.

F5 helps you:

- Mitigate sophisticated threats, including web injection, credential grabbing, and man-in-the-browser (MiTB)
- Identify phishing attacks before they are launched—at the point where attackers are creating and testing spoofed domains
- Inspect all users, whether they are browsing from a desktop, mobile device, set-top box, or even a game console

Mitigate bot attacks

Some bots are benign or can even be helpful, as is the case with digital assistants. But like any tool, bots can be co-opted by attackers.

F5 provides:

- Proactive, automatic detection of bad bots to prevent them from accessing your web application(s)
- A combination of challenge-based and behavior-based techniques that identify and filter out bad bot traffic
- Traffic management tools that employ machine learning to quickly build and implement mitigations for addressing new threats

USE CASES

Secure your APIs

As businesses build and release more apps, the number of APIs—which enable apps to communicate automatically with one another—has risen exponentially. Unfortunately, this also increases the threat surface for each app.

F5 enables:

- Secure authorization between apps based on standard and open methods across web, mobile and desktop
- DevOps teams to rapidly create and manage application services without worrying about cross-app vulnerabilities

Protect user credentials

Many web apps exposed on the Internet are protected by nothing more than user names and static passwords. While many organizations encrypt data in transit, malware and client-side attacks can steal credentials directly from the web browser, before data can undergo encryption.

F5 offers:

- App-level field encryption that protects data and credentials as they pass between the user and server
- Real-time encryption that mitigates the risk of compromised data
- Simple deployments with no need for coding, end-user clients, or agents on the web server

Defend against OWASP top 10 risks

Understanding and defending against web application vulnerabilities typically requires focused security expertise, a task that few developers can realistically undertake while getting actual development done at the same time. Fortunately, having the right tools in place can mitigate risk and speed development of your apps.

With F5, you can:

- Protect your apps against existing and emerging attacks without having to update the apps themselves
- Combine machine learning, threat intelligence, and deep application expertise to stop even the most advanced threats in their tracks
- Comprehensive protection that easily fits into your environment—whether it's on-premises or in the cloud

Prevent unauthorized app access

More than half of data breaches involve weak, default or stolen passwords—mostly due to password fatigue. The best practice of using a unique and complex password for every service is impractical given the growing number of apps accessed by users.

F5 provides:

- Secure anytime, anywhere access through integrated, standards-based identity federation, single sign-on (SSO), and adaptive multi-factor authentication (MFA)
- Dynamically adaptive authentication and authorization based on user context, device, and application attributes
- Easier integration with existing or new MFA methods including one-time password (OTP) via email and certificate checks

Of reported breaches, web attacks are most prevalent followed by phishing and then credential hacks.

F5 Labs 2018 Application Protection Report

F5 Web App and API Protection Products

F5 Advanced Web App Firewall – Identify and block attacks that other WAF solutions can't. F5 Advanced WAF offers unique features that include app-layer encryption, credential and data theft prevention and L7 DoS detection based on machine learning and behavioral analytics | *Learn more*

Rules for AWS WAF – Protect against automated attacks on AWS-hosted apps. F5 Rules for AWS WAF makes it easy to deploy without changes to your infrastructure and stops a broad range of vulnerability scanners, web scrapers, DoS tools, and forum spam tools | *Learn more*

F5 Advanced WAF and BIG-IP Cloud Edition (Azure and AWS) – Virtual edition offering the full suite of advanced WAF capabilities in the public cloud | *Learn more*

F5 Silverline WAF – A cloud-based managed service or express self-service that protects web apps and data from ever-evolving threats, wherever they may reside | *Learn more*

BIG-IP Access Policy Manager (APM) – Gain secure anytime, anywhere access to applications, wherever they reside, through context-based access control. Access Policy Manager also enables API authentication and authorization, and provides API request rate limiting and quota enforcement | *Learn more*

Websafe and Mobilesafe – Reduce the risk of fraud when delivering web and mobile-based app services; built on a platform that analyzes several points of data so you can identify odd behaviors and score users accessing your applications | *Learn more*

Management models

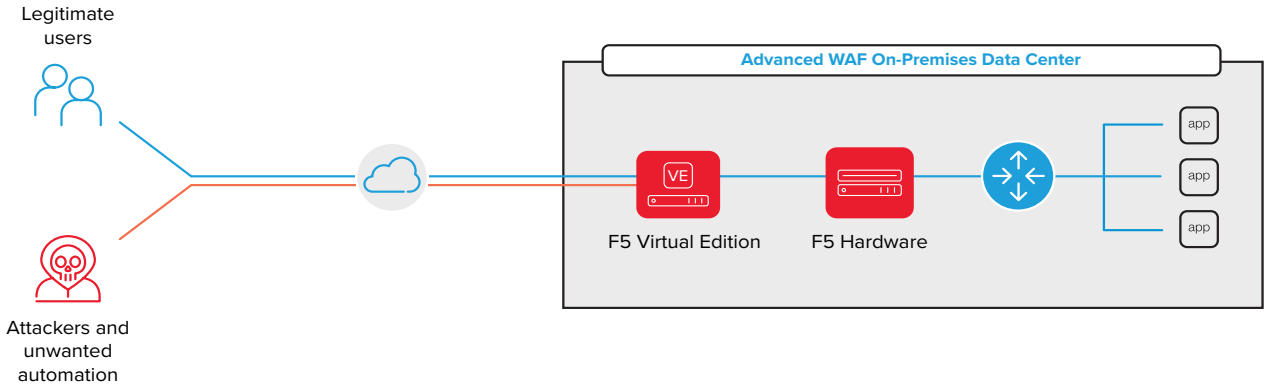
- Self-managed
- Fully managed by F5
- Express Self-service

Licensing options

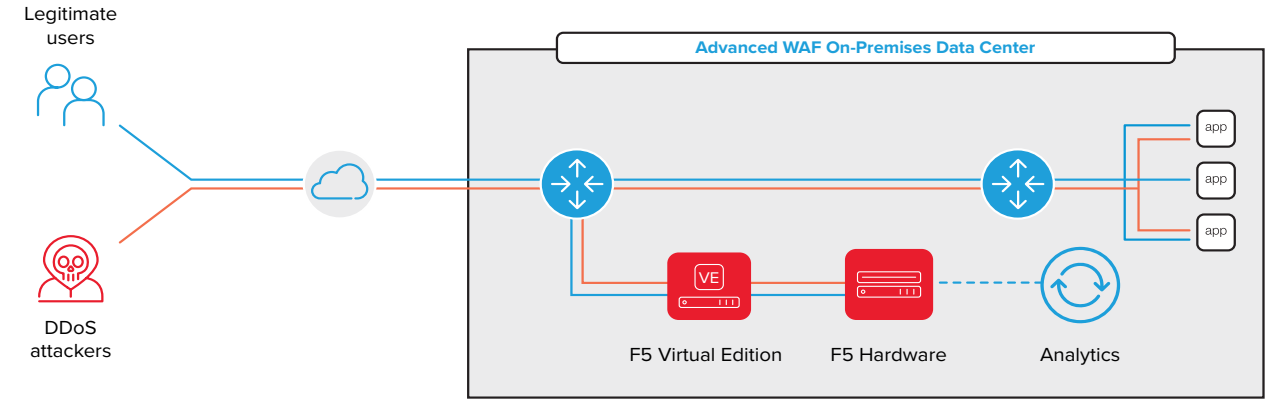
- Software Utility (Marketplace)
- Software Subscription/ELA
- Hardware + Software Perpetual
- Virtual Edition + Software Perpetual
- Per-App Virtual Editions
- Subscription (full)
- Subscription (self-service)

Deployment models

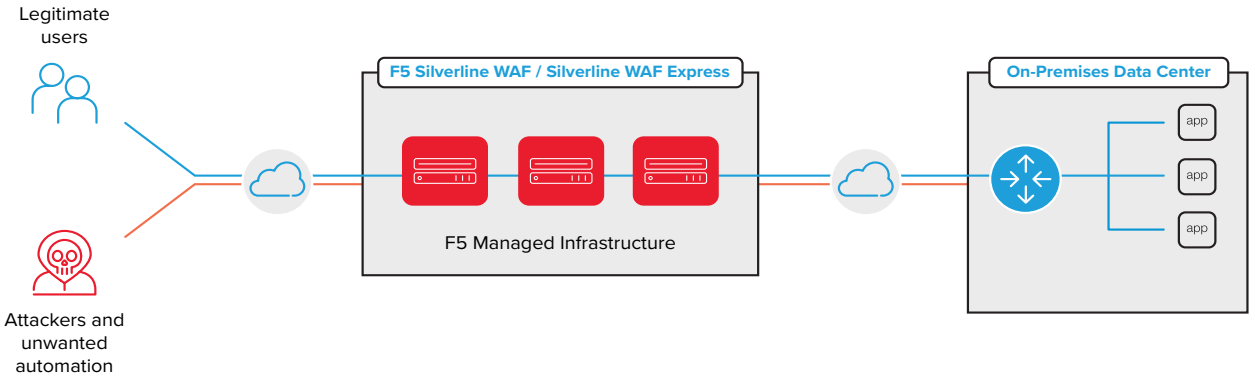
ON-PREMISES – INLINE BLOCKING



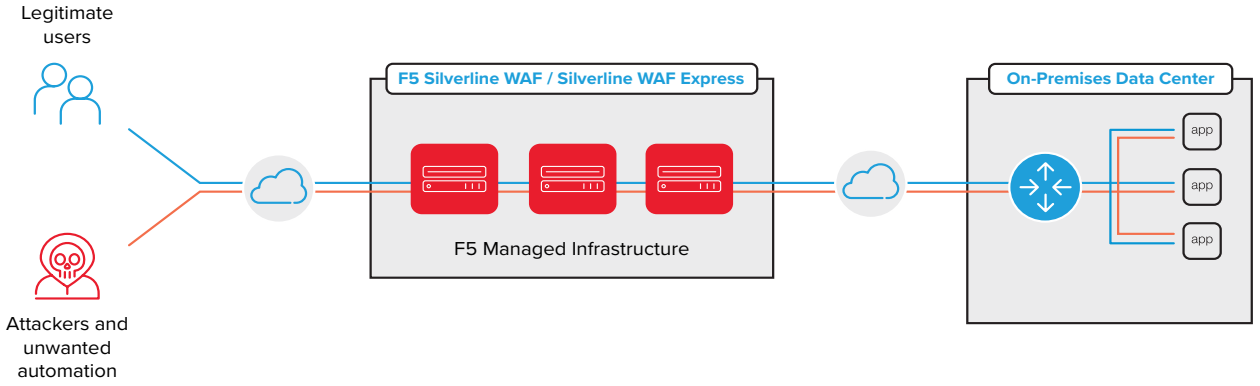
ON-PREMISES – OUT-OF-PATH MONITORING



CLOUD-DELIVERED – INLINE BLOCKING



CLOUD-DELIVERED – INLINE MONITORING



Learn more

- Report: F5 positioned as a Leader in The Forrester Wave for Web Application Firewalls, Q2 2018
- What Makes a WAF Advanced?
- eBook: The hidden ROI of cloud-friendly security
- Whitepaper: Advanced app threats require an advanced WAF
- Customer story: Premier management company secures healthcare data with F5 cloud-based WAF

Access Management: Enable secure anytime, anywhere access to apps wherever they reside

Business challenges

Whether they are customers, partners or employees, your users expect to easily connect to apps from anywhere and on any device. Yet, as the volume of apps, users, devices and access points grow, organizations struggle to manage and enable secure access that doesn't disrupt the user experience and slow productivity. Often, the challenges are:

- User access needs are constantly changing, and manual methods of creating and enforcing access policies cannot keep up
- Confidential corporate data may be downloaded and stored on unauthorized or personal devices
- Fragmented identities and decentralized apps introduce significant risk because of the challenges of enforcing security policies across different apps, cloud platforms and on-premises environments

F5 Access Management

F5 Access Management places identity at the front line of your defense.

USE CASES

Ensure secure access to web apps

As users become more mobile and apps are hosted in numerous data centers and clouds, the traditional network perimeter loses its meaning, and access management becomes exponentially tougher.

F5 access management provides:

- Access security by streamlining and protecting authentication and managing access to apps
- A centralized access proxy that moves the security perimeter to apps, users, and devices
- Enhanced authentication capabilities, integrating with multi-factor authentication (MFA)

Secure and scale your VDI environment

Virtual desktop infrastructure (VDI), while beneficial to the business, can lead to rising security, performance and management issues as more users are added.

F5 solutions:

- Reduce the complexity of your VDI and network design via infrastructure consolidation
- Scale up easily as your business grows
- Enable a centralized gateway for authentication and access, making your VDI more secure and easing the management burden with granular access policies

USE CASES

Secure access to Office 365

Office 365 has become a staple of business productivity. However, this means the federation of user identity and access management becomes increasingly complex for users who need remote access.

F5 allows you to:

- Integrate, simplify, and enhance security of your Microsoft Active Directory Federation Services (ADFS) infrastructure
- Prevent unauthorized access with single sign-on (SSO) and several native and integrated options of multi-factor authentication (MFA)

Secure your APIs

As businesses build and release more apps, the number of APIs—which enable apps to communicate automatically with one another—have risen exponentially. Unfortunately, this also increases the threat surface for each app.

F5 access management:

- Ensures API authorization controls and consistent access policies across all apps, providing a vital first line of defense
- Works across clouds and is deployed the same regardless of app language and frameworks

F5 Access Management Product

Access Policy Manager – Secure, simplify, and protect user access to apps and data while protecting credentials and enabling API security with the most scalable access gateway on the market | *Learn more*

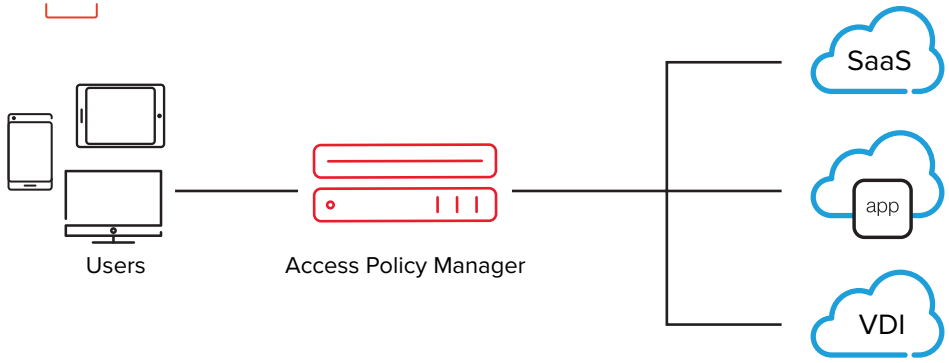
Management models

- Self-managed

Licensing options

- ELA
- Virtual Edition (Software Perpetual)
- Bring Your Own License (BYOL)

Centralized Point of Access Control



Learn more

- Report: The perimeter – an identity crisis
- Customer story: Dizzion secures virtual desktops for global customers with F5 and VMware

Businesses that depend on apps, depend on F5—solutions backed by industry-leading expertise

The world's largest enterprises, service providers, financial and educational institutions, government entities, and consumer brands rely on F5 to stay ahead of security, cloud, and mobility trends.

Our unmatched knowledge of apps is backed by our teams of experts—from F5 Labs to our Security Incident Response Team—that provide the intelligence, insights and initiative to help you stay informed, stay safe, and stay responsive even in the face of attacks.

F5 Labs: delivering actionable threat intelligence

The security researchers at F5 Labs process global application threat data from F5 and our partners into actionable intelligence. We monitor the dark net for the latest malware variants and threat actor behavior, collect global attack data, and create threat monitoring tools. F5 Labs publishes the team's findings to help the business and security community stay informed on the latest threats.

Security Incident Response Team (SIRT): keep your business running despite attacks

No matter how well you protect against security breaches, you also need a plan in place to respond, mitigate and recover quickly in the event attacks do occur. Our rapid response team at F5 SIRT will help you manage the receipt, investigation, and public reporting of security vulnerability information related to F5 products, platforms, and partners.

Security Operations Center (SOC): 24x7 real-time threat monitoring

F5 SOC protects customers from malware, phishing, and web fraud with proactive, 24x7 real-time global threat monitoring. Our SOC specialists have an unrivalled breadth and depth of industry experience, and leverage industry-leading F5 products combined with state-of-the-art security tools to ensure the best protection possible for your applications.

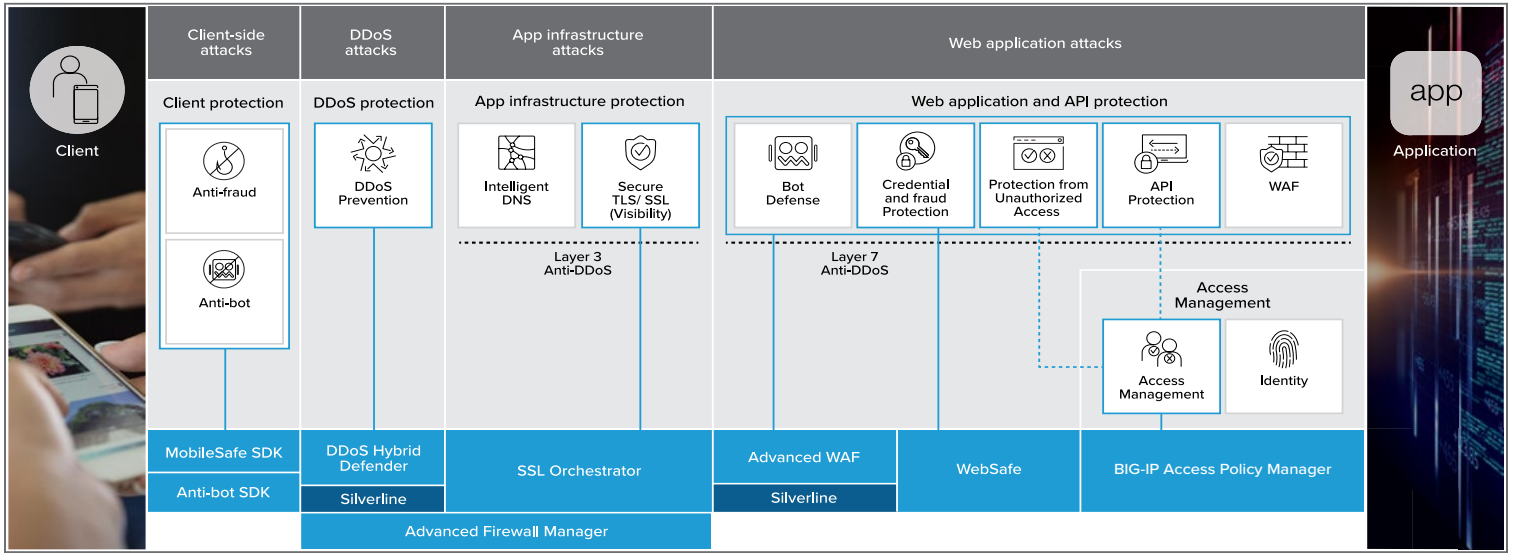
Professional Services: maximize your investment in F5 solutions

F5 Professional Services provides a full range of consulting services to support you throughout the entire lifecycle of your F5 solution deployment. Our consultants can help you speed up deployment of F5 solutions and make them work better for your business.

Ready to think app-security first?

When the app is your business, F5 makes sure your app remains available, is accessible by the right people with access to the right information, and ultimately ensures the integrity of your data and brand. It's our long history of understanding all aspects of the app—how its constructed, how it operates, and its supporting infrastructure—that enables us to deliver solutions, services, and products that protect against the primary risks associated to your apps—no matter where they reside. And, with the latest threat intelligence and access to security experts, you gain the support and confidence needed to navigate today's ever-changing threat landscape.

F5 Application protection across the App Stack



Ready to think app-security first?
Visit https://www.f5.com/company/contact