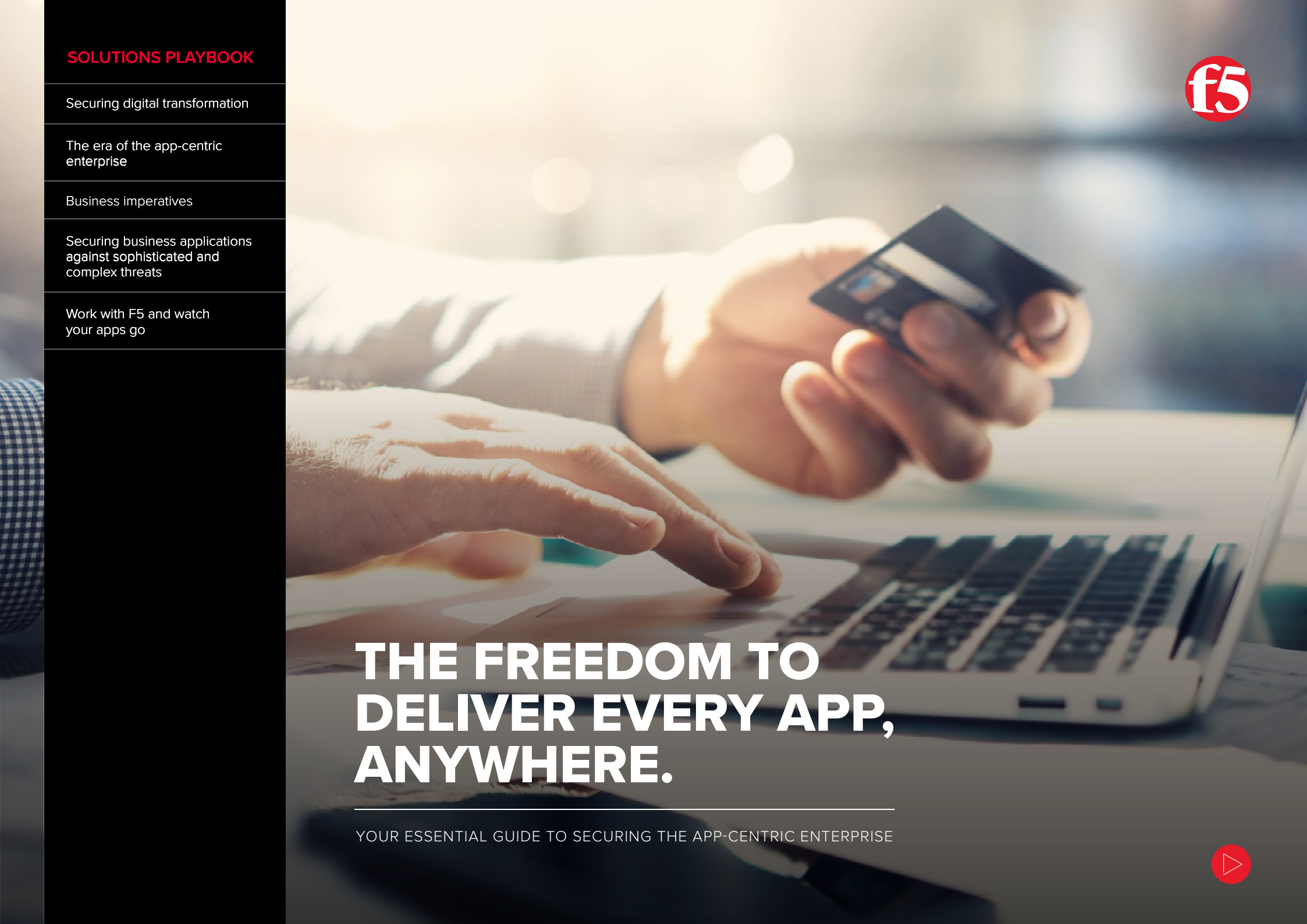
SOLUTIONS PLAYBOOK



THE FREEDOM TO DELIVER EVERY APP, ANYWHERE.

YOUR ESSENTIAL GUIDE TO SECURING THE APP-CENTRIC ENTERPRISE

Digital transformation is reshaping the modern enterprise, with applications representing a new class of assets and an important source of competitive differentiation. The digital economy requires these applications to be delivered with unprecedented speed, scale, and agility; without exposing the organization to business, security and regulatory risks.

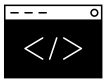
To help you navigate the varied and complex requirements needed to protect your business, we've created this easy-to-use playbook to provide relevant knowledge, solutions and resources that can help you create a safer, more secure digital transformation journey for your organization.

We hope you find it useful. If you have any questions or would like to know how F5 can help, please email

apacinfo@f5.com

The era of the app-centric enterprise

In F5's 2018 Report titled "The State of Application Delivery", more than 3,400 business and technology leaders and practitioners have revealed **five key trends** arising from the digital transformation wave sweeping across the Asia and the world:



Digital transformation built on IT optimization

Optimizing IT infrastructure is the primary driver for digital transformation projects, and is seen as the foundation for cloud adoption and automation necessary for app deployments.

72%
of enterprises see IT optimization as the primary benefit from digital transformation

Multi-cloud enables the "best cloud for the app" strategy

Today, enterprises select the cloud platform best suited to each app, leading to multi-cloud architectures. But no matter where each app resides, organizations will need to keep them running seamlessly and securely.

87%
of businesses leverage multi-cloud architectures

Application services are "must-haves"

An app-centric business leads to a rise in the use of application services, with security as the predominant service category. These include web application firewalls, network firewalls, SSL VPNs and anti-virus.

16
different applications services are deployed by organizations on average to keep their apps fast, safe, and available.

Security confidence falls as multi-cloud rises

Even as more apps are delivered from the cloud, lack of experience and skills in securing applications deployed in both public and private clouds (or a mix of both) are raising security and regulatory risks for organizations.

2/3
of organizations are not confident of their ability to defend against application-layer attacks in the cloud

Automation and standardization on the rise

To keep IT lean, reduce OpEx, and speed up time-to-market for app development, enterprises are embracing automation and standardization on platforms like VMware or OpenStack.

50%
of respondents have settled on a single network automation toolset

Business imperatives

With digital transformation firmly on the agenda, organizations are now grappling with several business challenges that arise out of a fast-evolving, application-centric and multi-cloud world. These include:

Increasing revenue dependence on applications

If a business-critical application in the cloud slows (or goes) down, vital processes from supply chain to marketing and sales could be affected.

Delivering consistently strong customer experiences

Customers have become accustomed to seamless experiences offered in well-known applications; whether these applications reside on-premise, in public or private clouds (or both).

Going to market at greater speed and efficiency

Businesses are under pressure to roll out new applications and services to customers quickly, yet without sacrificing quality or incurring higher costs.

Maintaining a strong security posture amidst greater complexity

As applications and platforms multiply, organizations need to stay on top of potential gaps and threats even as their infrastructure becomes more interconnected.

Meeting more and tougher regulatory requirements

Applications and data are not constrained by geographical boundaries. Enterprises will have to ensure that data sovereignty, privacy and handling requirements are met as it transverses the Internet into different jurisdictions.

Achieving the right balance between risk mitigation and cost

It's rarely economically feasible to mitigate all (or most) risk. Organizations will need to understand and prioritize their risk mitigation objectives, and to work with solution providers that can provide the appropriate level of protection at acceptable costs.

Securing business applications against sophisticated and complex threats

An app-centric environment introduces new risks: according to a recent study, 86 percent[1] of data breaches now occur at the app level. By fortifying security strategies with solutions and services focused specifically on the application, you can better secure access to applications and protect the ones that expose sensitive data, no matter where they live.

F5 offers solutions that cover the following requirements:

Need #1

Keep apps up and running - even when they are under attack (DDoS Protection)

Need #2

Secure apps rapidly - wherever they reside (WAF)

Need #3

Stop data leakage and serve legitimate customers (BOT Protection)

Need #4

See what's hidden in encrypted traffic (SSL Visibility)

Need #5

Secure access to apps on public cloud and SaaS platforms (Cloud Federation)

Need #6

Protect apps on public clouds (Public Cloud App Protection)

Need #7

Proactively detect and reduce web fraud (Fraud Protection)

Need #8

Identify and control access from any user and device (Access Management)

Need #9

Allow API access to apps without risk (API Protection)

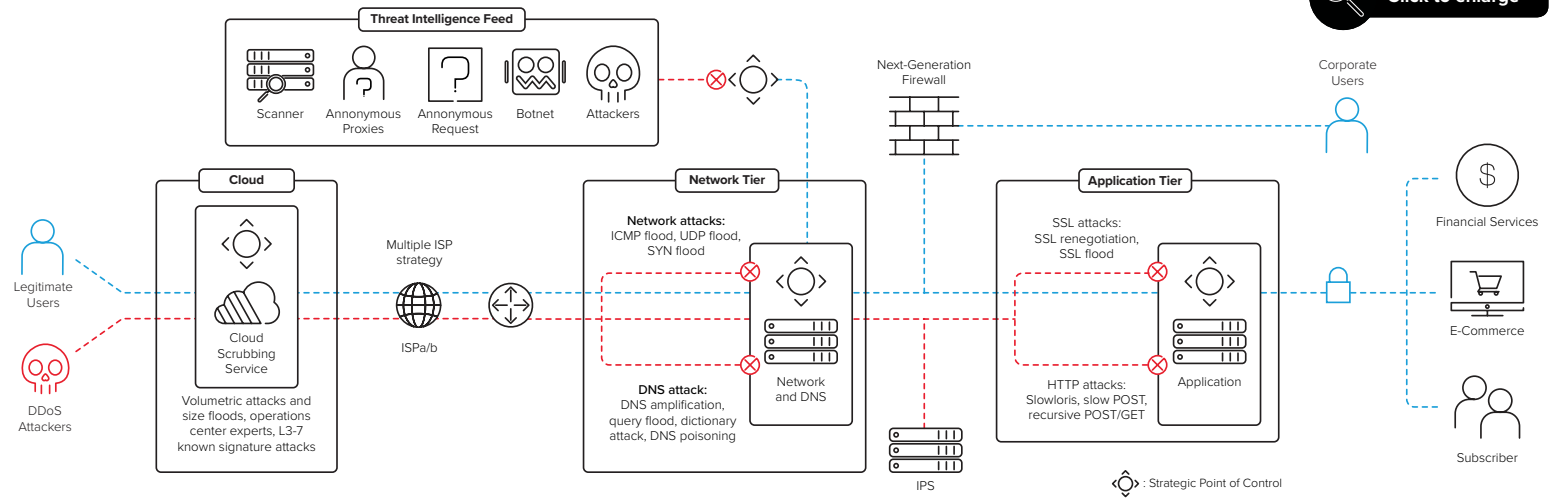
[1] Report: "Lessons learnt from a decade of data breaches", F5 Labs, November 2017

NEED #1

Keep apps up and running - even when they are under attack (DDoS Protection)

F5 DDoS Protection proactively identifies and mitigates a wide range of DDoS attacks

Click to enlarge



The challenge:

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

The solution:

F5 DDoS Protection

- Offers protection against full spectrum of DDoS attacks with multi-layered defense that combines cloud scrubbing and an on-premises appliance
- Supports flexible deployment options with inline and out-of-band mode to ensure apps remain available
- Detects and mitigates targeted multi-vector DDoS with sub-second attack detection and instant mitigation in inline mode
- Unique stress-based behavioral DDoS detection for Network and Application DDoS
- Seamlessly integrates on-premises and native cloud-based attacks

The benefits:

- Rapid identification and mitigation of a wide range of DDoS attacks
- Highly customizable through programmability features that protect against complex and unknown DDoS attacks
- Cost efficient and comprehensive DDoS protection from a single stack in a small footprint

Customer references:

- Government Service Insurance System, The Philippines
- Hansung University, Korea
- The University of Southern Queensland, Australia

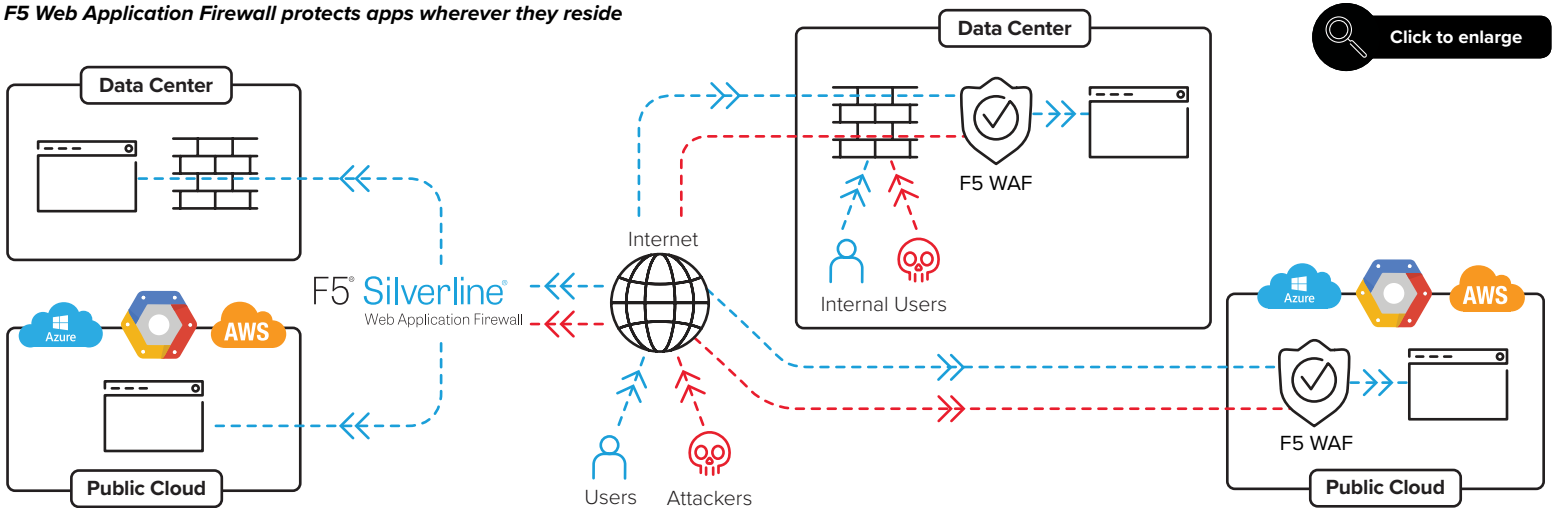
Learn more:

- eBook: "A guide to DDoS protection: Choosing the right model"

NEED #2

Secure apps rapidly - wherever they reside (WAF)

F5 Web Application Firewall protects apps wherever they reside



The challenge:

- Apps rushed to market without adequate testing may contain vulnerabilities
- Apps in live environment have inadequate maintenance window for patching and upgrades
- Risk of exposure to unknown, emerging threats or 'zero day' vulnerabilities
- Lack of web apps security skillset within organization
- Traditional web application security products require constant configuration changes and fine tuning

The solution:

F5 Web Application Firewall

- Comprehensive application protection including proactive bot defense, identity management, real-time threat protection, Layer 7 DDoS protection, and compliance enforcement
- Available as appliance, software or managed service; can be integrated with leading DAST solutions
- Full application visibility for both threat management and business intelligence
- Allows WAF deployment with pre-built security policies
- Machine learning allows WAF to learn and protect application with minimal manual intervention

The benefits:

- Comprehensive protection for your apps wherever they reside: on premise, or in private or public clouds
- Rapid deployment of security policies
- Low management costs and minimal intervention required
- Apps can be patched rapidly and achieve faster go-to-market timelines

Customer References:

- Infosys, India
- Alfacart, Indonesia
- Heritage Bank, Australia

Learn more:

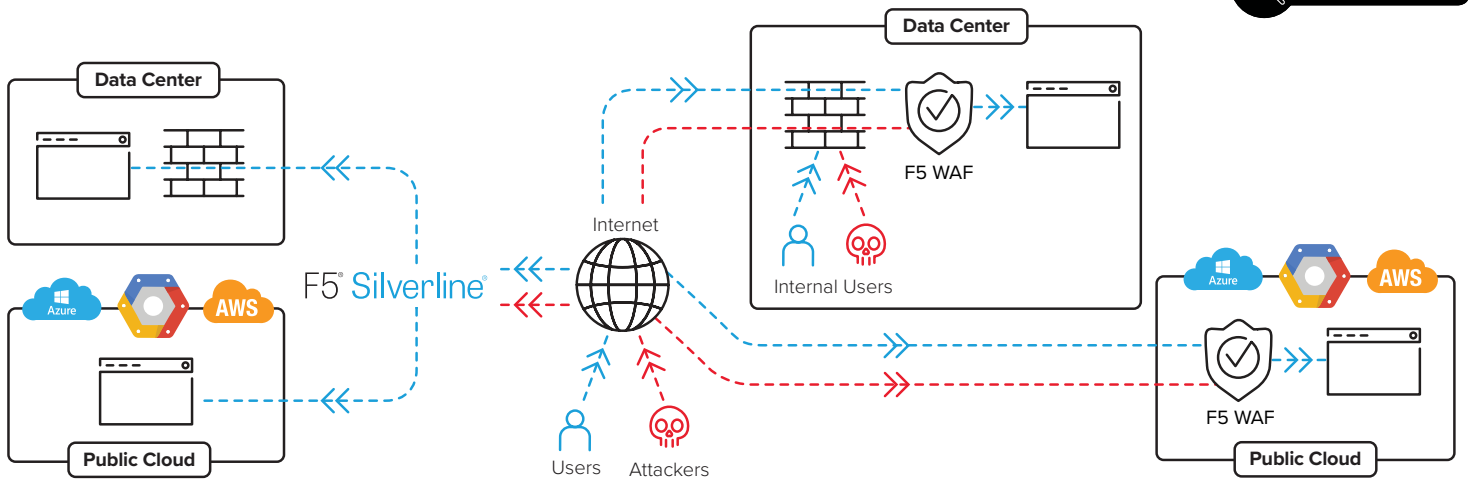
- Report: "F5 positioned as leader in 2017 Gartner Magic Quadrant for Web Application Firewall"
- Whitepaper: "How to choose the right WAF"

NEED #3

Stop data leakage and serve legitimate customers (Bot Protection)

F5 Proactive Bot Defense lets legitimate traffic in, keeps bad traffic out

Click to enlarge



The challenge:

- Businesses required to balance between need to expose data to customers and partners via apps and websites, yet prevent data leakage via malicious bots
- More than 50% of web traffic is bot traffic; difficult to tell good bots (e.g. trusted partner APIs and search engine crawlers) versus bad bots (e.g. scraper bots, scam bots)
- Malicious bots consume network resources, slows down legitimate user experience, and can be used to launch automated attacks against existing gaps
- As IoT trend grows, more mobile bots will be introduced that cannot respond to traditional challenge methods

The solution:

F5 Proactive Bot Defense

- Offers comprehensive bot detection and defense, including 900+ bot signatures right out of the box, for web and mobile apps
- Classify bots by signature or behavior before request hits apps
- Challenge suspicious or unknown web clients before request is accepted
- Provides anti-bot SDK for mobile apps
- Set limits on the rate of communication between bots and apps
- Can be customized to recognize and fingerprint specific bot patterns

The benefits:

- Proactively identifies web and mobile bots before requests hit apps
- Protects both web and mobile-based apps
- Ensures legitimate requests are served without any impact or slowdown to user experience

Customer References:

- ET NET

Learn more:

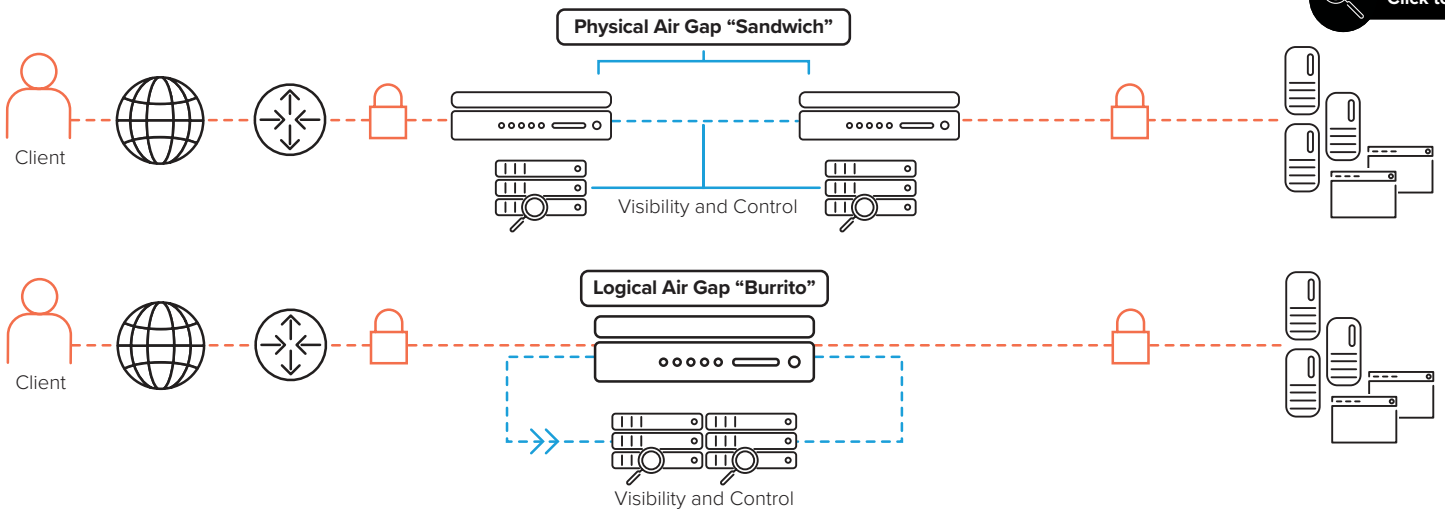
- eBook: "From DDoS to digital point of sale: bots mean business"

NEED #4

See what's hidden in encrypted traffic (SSL Visibility)

F5 SSL Visibility Solution eliminates SSL blind spots

Click to enlarge



The challenge:

- Widespread adoption of SSL: more than 75% of traffic will be SSL-encrypted by 2019
- However, SSL encryption is two-edged: traditional security products are blind to encrypted traffic
- Valuable data may leak out - or malware slipped in - over encrypted channels
- Many security products cannot decrypt SSL traffic without slowing down network

The solution:

F5 SSL Visibility Solution

- An integrated SSL solution which decrypts and re-encrypts inbound and outbound traffic
- Sends decrypted traffic to security products for inspection and mitigation
- Able to monitor and load balance SSL and non-SSL traffic to security products
- Easily integrated with 3rd party security solutions from FireEye, RSA and Symantec
- Superior SSL performance which scales well for high availability deployments

The benefits:

- Future-proofs existing security investments, and allows easy introduction of new security services
- Provides visibility for security services to deliver service without creating performance bottlenecks
- Simplifies network architecture via a single solution for both inbound and outbound traffic

Customer References:

- Directorate General of Taxes of Indonesia

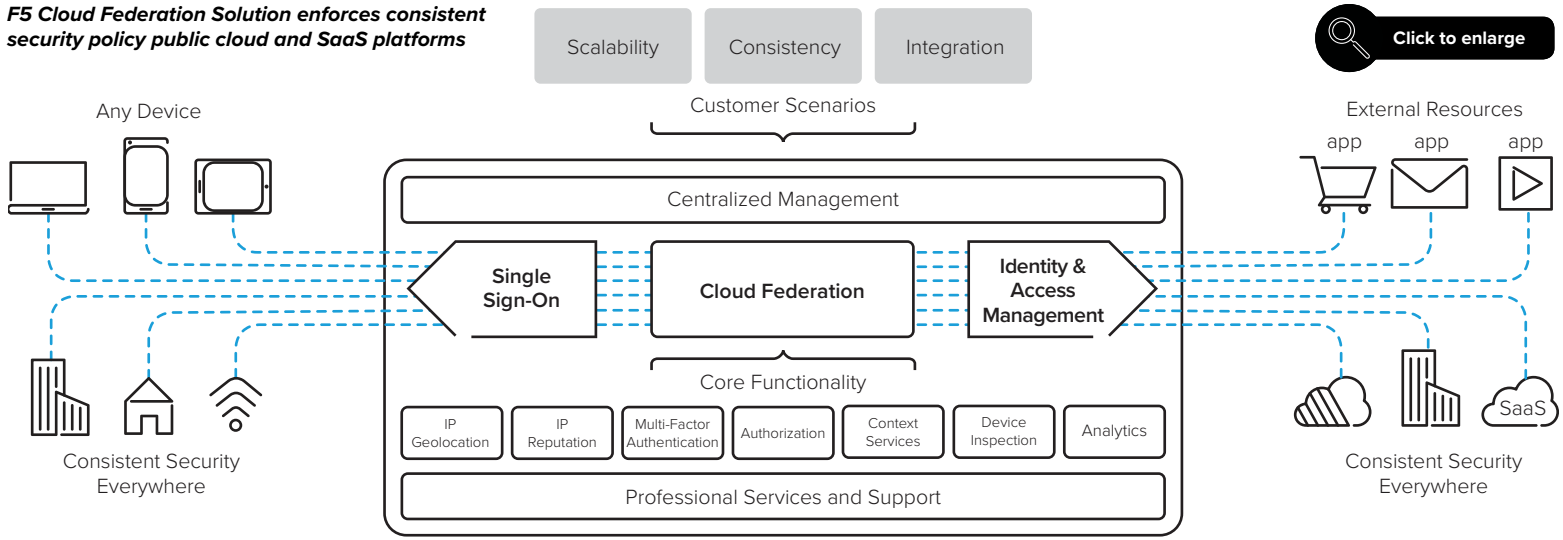
Learn more:

- IDC Report: "The blind state of rising SSL/TLS traffic: are your cyberthreats visible?"

NEED #5

Secure access to apps on public cloud and SaaS platforms (Cloud Federation)

F5 Cloud Federation Solution enforces consistent security policy public cloud and SaaS platforms



The challenge:

- As SaaS and public cloud adoption grows, business apps and data are accessible via simple login credentials from any device
- Confidential data can be downloaded/stored on unauthorized or personal devices
- Customer or employee login credentials vulnerable to theft
- Identify and access management complexity increases as more external SaaS platforms used

The solution:

F5 Cloud Federation Solution

- Leverages an organization's single sign-on (SSO) system to access multiple external SaaS providers
- Provides federation to SaaS and cloud platforms without exposing organization's underlying ADFS infrastructure
- Provides consistent, multi-factor authentication for all users across all SaaS systems accessed
- Utilizes open standards such as SAML and OAuth for exchanging authentication and authorization data between parties without needing to store identities outside of the organization
- Checks endpoint checks to identify type and security posture of device and enforces appropriate policies

The benefits:

- Enforces a consistent access policy across all SaaS and cloud-based platforms
- Reduces management costs for access account commissioning and decommissioning
- Eliminates password fatigue by implementing SSO across multiple SaaS platforms
- Reduces security complexity and improves user productivity
- Allows businesses to leverage benefits of SaaS without increasing security risks

Customer References:

- University of Southern Queensland

Learn more:

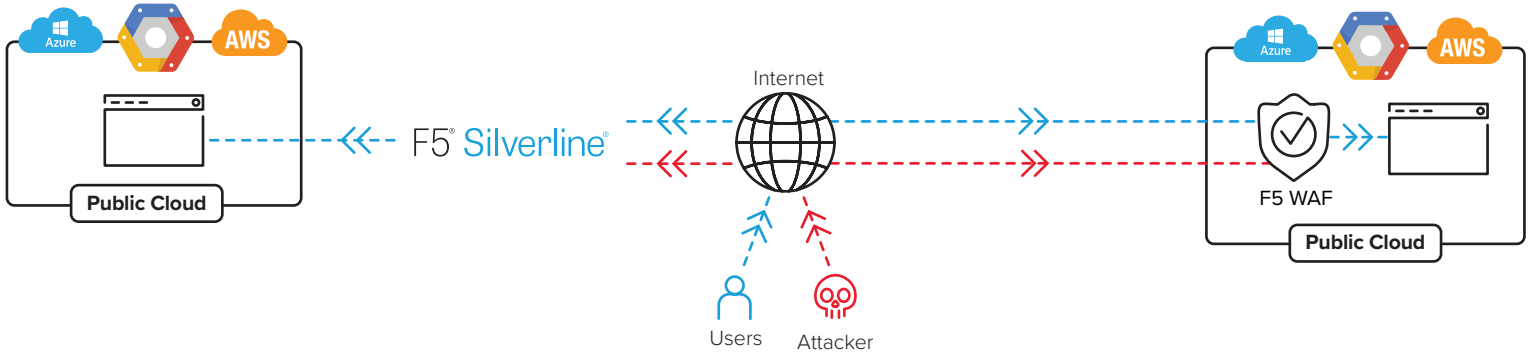
- Whitepaper: "Navigating a multi-cloud world with F5"

NEED #6

Protect apps on public clouds (Public Cloud App Protection)

F5 Public Cloud App Protection secures apps no matter they are deployed
– in the data center or in the public cloud

Click to enlarge



The challenge:

- Businesses leverage public cloud platforms for better agility and lower costs, but expose themselves to higher security risks
- Multi-cloud strategies increase security and management complexity as apps and data are moved onto disparate external platforms which aren't within organization's control
- Regulatory and compliance needs grow as data crosses geographical boundaries

The solution:

F5 Public Cloud App Protection

- Delivers intelligent, comprehensive L3–7 security services to protect cloud apps without sacrificing control, flexibility, and visibility
- Available on a 'pay-as-you-use' model for leading public clouds such as Amazon Web Services and Microsoft Azure or as a flexible WAF-as-a-Service model
- Offers a federated IAM and SSO system for application access from data center and into public cloud platforms
- Protects against web-based malware and persistent threats, and comprehensive endpoint device inspections

The benefits:

- Accelerates the move to public cloud, while minimizing risk and business impact
- Quickly and consistently deploy, configure and enforce security services across multiple public cloud environments
- Reduces the need to configure security services across different cloud platforms
- Flexibility from choice of deployments – either on 'pay-as-you-use' or 'WAF-as-a-Service'

Customer references:
- Alfacart, Indonesia

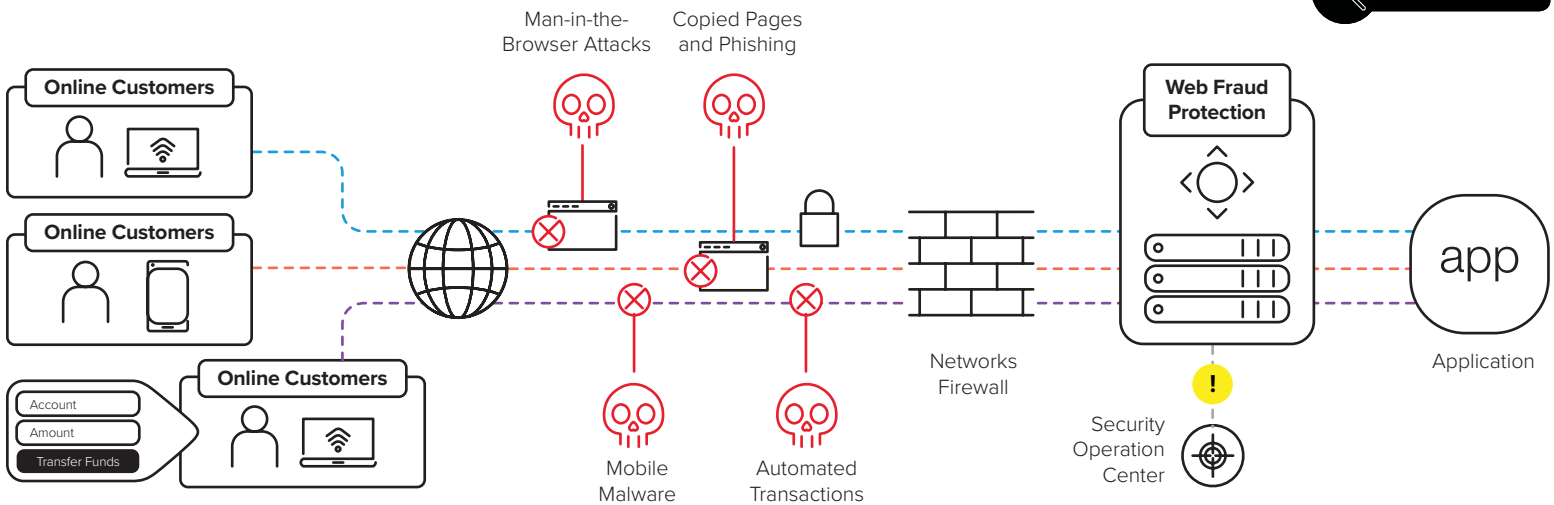
Learn more:
- Self-assessment: "Where are you in your public cloud journey?"
- Article: "Securing your cloud: What you really need to know"
- Whitepaper: "F5 Web Application Firewall for Azure Security Center"

NEED #7

Proactively detect and reduce web fraud (Fraud Protection)

F5 Web Fraud Protection Services mitigates risk from online payments fraud

Click to enlarge



The challenge:

- Rapid adoption of online financial transactions via web and mobile exposes businesses and customers to fraud
- Online threats, malware and social engineering techniques increasingly sophisticated: attackers finding newer means to compromise endpoints
- Organizations lack inhouse capabilities to manage app security or identify emerging online threats
- Need to meet payments, banking and transactions regulations across different jurisdictions

The solution:

F5 Fraud Protection Solution

- Designed specifically to meet challenges facing online businesses and defends against a full range of online threats – including malware targeted at financial apps, credential theft, use of compromised devices and transaction fraud
- Analyzes end-user behavior and device security posture without affecting customers' online experience
- Includes ongoing F5 Security Operations Center support to augment organization's existing security team and to ensure real-time response to emerging threats
- Integrates with businesses' existing SIEM and risk management systems

The benefits:

- Proactively detects and mitigates online fraud to protect banks and online businesses against financial and reputational loss
- Augments organizations' ability to stay on top of latest threats without increasing headcount or management costs
- Maintains a seamless user experience through a clientless security model which requires no behavioral change from user

Customer References:

- Bank Leumi

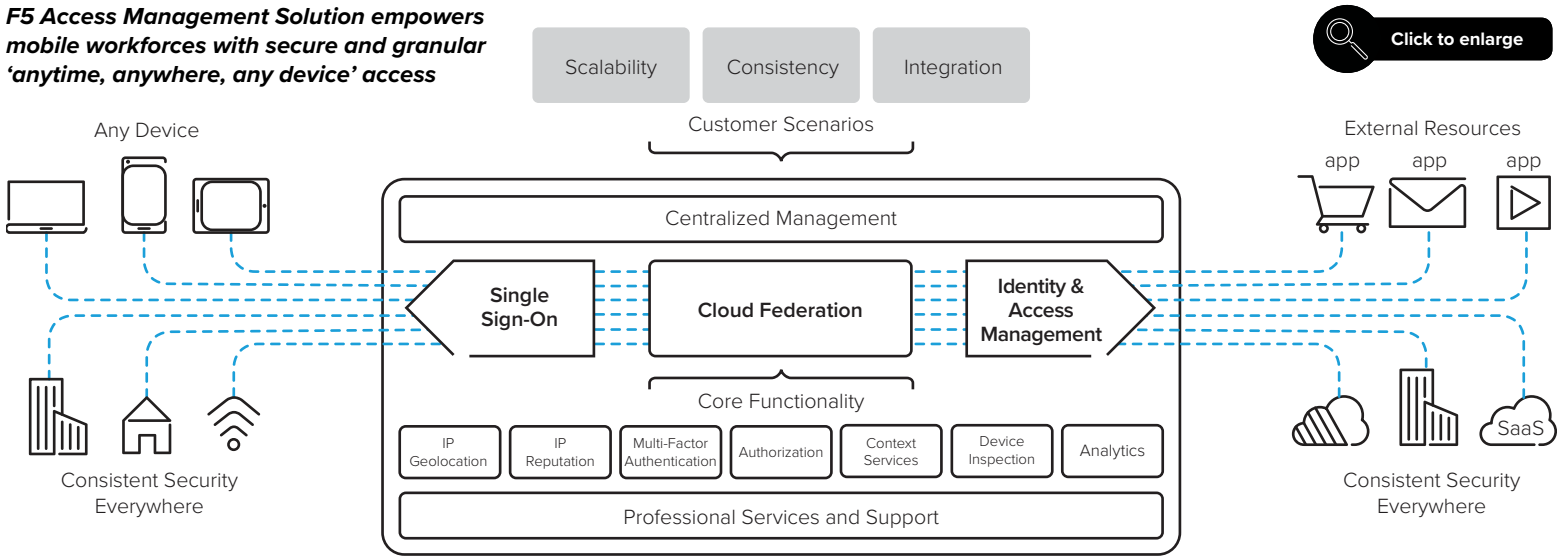
Learn more:

- eBook – "Fraud: It's not just for banks anymore"

NEED #8

Identify and control access from any user and device (Access Management)

F5 Access Management Solution empowers mobile workforces with secure and granular 'anytime, anywhere, any device' access



The challenge:

- Mobile workforces require access to corporate apps from any device, at any time and from any location for higher productivity, but increases risk of data loss and identity theft
- Confidential corporate data may be downloaded/ stored on unauthorized or personal devices
- Need to enforce a consistent level of security whether its internal or external access
- As number of users, devices and locations grow, organizations can quickly lose visibility

The solution:

F5 Access Management Solution

- Offers a comprehensive solution that covers remote access, web access and cloud federation
- Allows customization of security policies that provide centralized and granular authentication and access control for different categories of users
- Leverages SSO with built-in two-factor authentication for mobile apps
- Supports wide range of authentication standards such as SAML, OAuth, LDAP and Radius
- Highly programmable and customizable

The benefits:

- Provides full visibility of user and remote access behavior, with automatic enforcement of access policies at an individual user level
- Keeps identity and access under the control of the organization with ability to immediately authenticate or terminate user access, whether it's via web, mobile or desktop
- Reduces identify and access management complexity whilst improving user productivity

Customer references:

- Catholic Education South Australia, Australia
- Sheffield Hallam University, UK
- Kettering Health Network, US

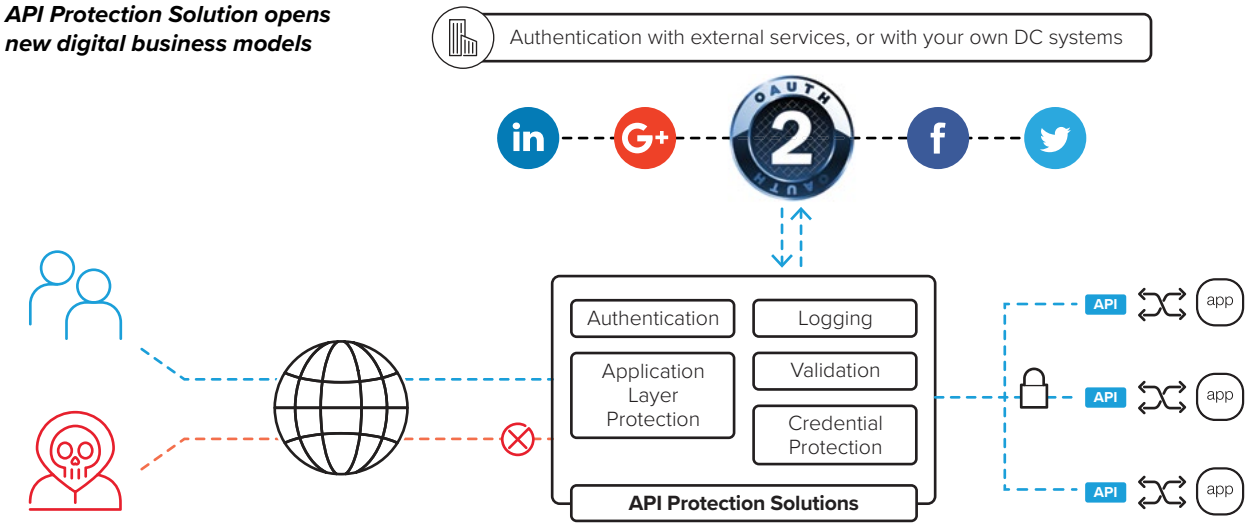
Learn more:

- Report – "The perimeter: an identity crisis"
- eBook – "Credential stuffing: A security epidemic"

NEED #9

Allow apps to talk to one another without risk (API Protection)

F5 API Protection Solution opens up new digital business models



The challenge:

- Apps are now commonplace: APAC organizations operate an average of 150 apps each, deployed in the data center and across multiple cloud platforms
- As businesses try to deliver new apps as quickly as possible, DevOp teams may sacrifice security and customer experience for speed-to-market
- Growing app footprints have resulted in the explosion of APIs which enable apps to communicate with one another, but which also increases the threat surface for each app
- Compliance requirements in strictly regulated industries may also slow down app development

The solution:

F5 API Protection Solution

- Offers comprehensive 'defense-in-depth' protection across the stack, covering application, access and network levels
- Allows DevOps to rapidly create and manage application services with iRules, iControl and iApps as well integration with automation and management tools
- Secures authorization between apps based on standard and open methods across web, mobile and desktop

The benefits:

- Opens up organization's digital footprint and app connectivity to a larger ecosystem without increasing risk
- Speeds up time-to-market and compliance through ease of programmability
- Protects against online threats, malware and data loss without sacrificing user experience

Learn more:

- Qualica

Work with F5 and watch your apps go

F5 secures applications and the data behind them—because that's where today's attacks happen.

With decades devoted to connecting users and applications, our solutions provide unparalleled visibility into hidden threats and offer the controls needed to manage access and reduce the risks of app attacks. Plus, our solutions support security for any infrastructure, from traditional data centers to cloud environments. This means users can securely access data on any device, in any environment, at any time.

THE F5 ADVANTAGE

- Comprehensive security solutions for today's app-centric business
- Rated a leader in web application security by Gartner
- Superior performance, highly scalable solutions for the most demanding requirements
- Compete app protection across all environments, delivered via flexible models
- Easy-to-manage solutions with full visibility, control and automation
- 49 out of Fortune 50 companies use F5

To learn how F5 can help you make your apps go,

apacinfo@f5.com

Regional offices:

Asia

Oceania

Regional Offices
ASIA

CHINA
Beijing Office

Unit 07-09, 17th Floor
Building Tower 1, China Central Place
No.79, Jianguo Road
Chaoyang District,
Beijing, PRC, 100025

市场销售热线: 400 991 8366
Phone: (+86) 10-56438000
Fax: (+86) 10-56438100

CHINA
Shanghai Office

Units 1119-20, 11th Floor
Building 1st., Corporate Avenue
No.222 Hubin Road
Luwan District,
Shanghai, PRC, 200021

市场销售热线: 400 991 8366
Phone: (+86) 21-61132588
Fax: (+86) 21-61132599

INDIA
Mumbai Office

Office No. 104 & 105
Sr.No.4 & CTS No.8
Village Parigkhari,
Balarama Building C-3
Bandra Kurla Commercial Complex
Bandra (East), Mumbai-400051
India

Phone: (+86) 10-56438000

CHINA
Chengdu Office

Room 1717, Level 17, Raffles City Tower 2,
No. 3 Section 4, South Renmin Road,
Wuhou District,
Chengdu, China, 610041

市场销售热线: 400 991 8366
Phone: (+86) 28-65118185/ 8192/ 8195

HONGKONG

Rooms 905-06, 9/F
Harbour Centre
25 Harbour Road
Wanchai
Hong Kong

Phone: (+852) 2827 1818
Fax: (+852) 2827 4000

INDIA
New Delhi Office

Suite 414, 4th Floor
Paharpur Business Centre
21, Nehru Place
New Delhi 110019

Phone: (+91) 011-41207477
Alt Phone: 011-26207477

CHINA
Guangzhou Office

Unit 1108, 11th Floor, R/F Center
No#10 Huaxia Road,
Zhujiang Xin Cheng Tianhe District
Guangzhou, PRC, 510623

市场销售热线: 400 991 8366
Phone: (+86) 20-38927557
Fax: (+86) 20-38927547

INDIA
Bangalore Office

Regus CBD Office No. 923 & 928
Level 9, East Wing,
Raheja Towers No 26-27 MG. Road,
Bangalore - 560 001
India

Phone: 080-67920946

INDONESIA

F5 Networks Singapore Pte Ltd
Indonesia Representative Office
45/F Menara BCA Grand Indonesia,
Jl. M.H. Thamrin No. 1,
Jakarta 10310, Indonesia

Phone: (+62) 21-2358 4665
Fax: (+62) 21-2358 4666

Regional Offices
ASIA

JAPAN

Akasaka Garden City 19F
4-15-1 Akasaka,
Minato-ku
Tokyo 107-0052
Japan

Phone: (+81) 3 5114 3200
Fax: (+81) 3 5114 3201

KOREA

Trade Tower 38th Floor, Room 3801,
511 Yeongdong-daero, Gangnam-gu,
Seoul, Korea 06164

Phone: (+822) 6000-6770
Fax: (+822) 6000-6780

MALAYSIA

Level 30
The Gardens North Tower
Mid Valley City
Lingkaran Syed Putra
59200 Kuala Lumpur

Phone: +60 03-2035 9702
Fax: (+603) 2035 9772

PHILIPPINES

Manila Philamlife Tower
18/F Philamlife Tower
8767 Paseo De Roxas
Makati City Metro,
Manila PI 1226

Phone: +63 (2) 830 8469/70/71

SINGAPORE

5 Temasek Boulevard
#08-01/02
Suntec Tower Five
Singapore 038985

Phone: (+65) 6533 6103
Fax: (+65) 6533 6106

TAIWAN

4F Suite 406, No. 129, Sec. 3
Min Sheng E. Rd.
Taipei 10596
Taiwan

Phone: (+886) 2 8712 6828
Fax: (+886) 2 8712 6960

THAILAND

Suite#44 , 1 QHouse Lumpini,
Level 27th floor
South Sathorn Road., Tungmahamek
Sathorn, Bangkok 10120
Thailand

Phone: (+66) 2610 3634, (+66) 2610 3766
Fax: (+66) 2610 3601

VIETNAM

10th Floor, Pacific Pl.Blvd.
Suite 1019
83 B LY Thuong Kiet Street
Hanoi, Vietnam

Phone: (+84 4) 3946 1006
Fax: (84) 4 3946 1025

Regional Offices
OCEANIA

AUSTRALIA
Brisbane Office

Level 19, Waterfront Place
1 Eagle St
Brisbane, QLD 4000
Australia

Phone: (+61) 7 3360 023

AUSTRALIA
Melbourne Office

Level 6, 575 Bourke Street
Melbourne,
VIC 3000
Australia

Phone: (+61) 3 9614 6014

AUSTRALIA
Sydney Office

Level 6, 140 Arthur Street
North Sydney,
NSW 2060
Australia

Phone: (+61) 2 9978 1555

AUSTRALIA
Canberra Office

Level 9, 2 Phillip Law Street
New Acton
Canberra, ACT 2601
Australia

Phone: (+61) 2 9978 1555

AUSTRALIA
Perth Office

Level 24 & 25 Allendale Square
77 St. Georges Terrace
Perth, WA 6000
Australia

Phone: (+61) 4 3961 4296

NEW ZEALAND

F5 Networks New Zealand
Level 4
22 Fanshawe street
Auckland 1010
New Zealand

Phone: (+64) 9 950 5305