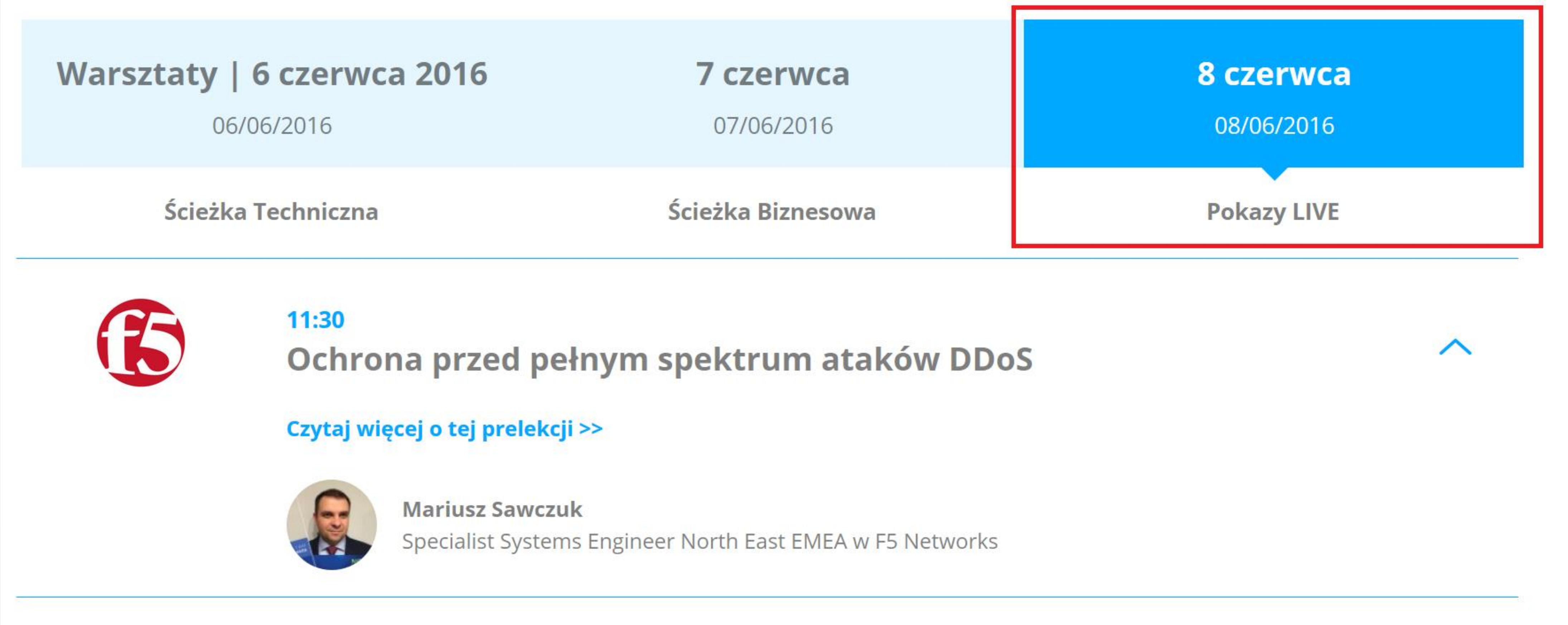
Zarządzanie zasadami dostępu do aplikacji czyli F5 Access Policy Manager

Maciej Iwanicki, Systems Engineer

Zapraszamy również jutro!



Warsztaty | 6 czerwca 2016
06/06/2016
Ścieżka Techniczna

7 czerwca
07/06/2016
Ścieżka Biznesowa

8 czerwca
08/06/2016
Pokazy LIVE

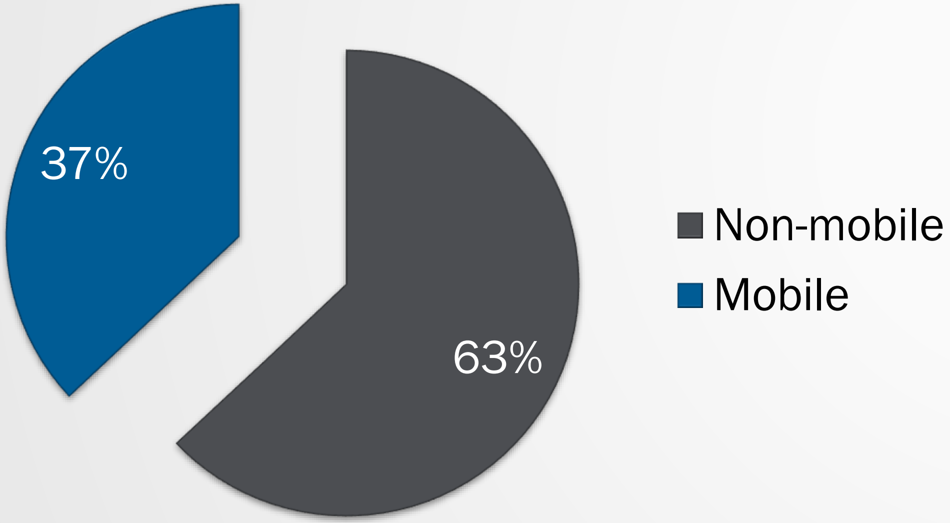
11:30
Ochrona przed pełnym spektrum ataków DDoS

Czytaj więcej o tej prelekcji >>

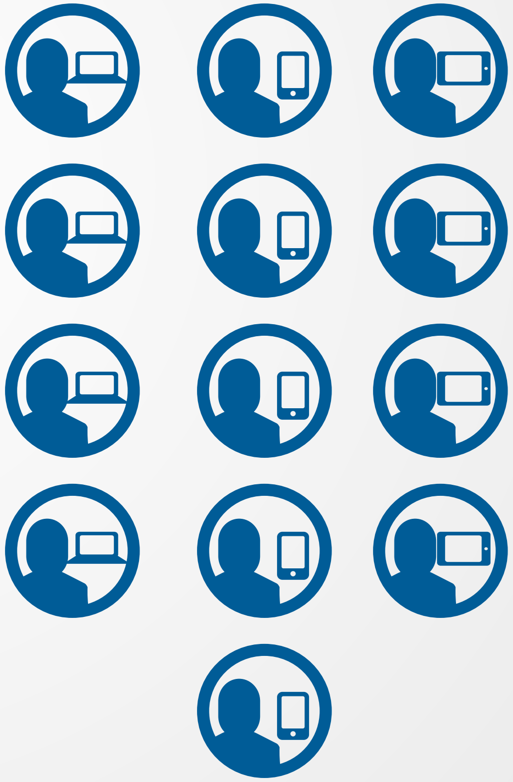
Mariusz Sawczuk
Specialist Systems Engineer North East EMEA w F5 Networks

The “new norm” is a worldwide mobile workforce

Workforce by end of 2015



~1.3 Billion mobile workers by end of 2015



Source: Worldwide Mobile Worker Population 2011–2015 Forecast, IDC, December 2011

Controlling and managing access more difficult than ever

Employees

Partner

Customer

Administrator

Manage access based on identity

IT challenged to:

- Control access based on granular attributes, such as user-type and role
- Unify access to all applications (mobile, VDI, web, client-server, SaaS)
- Provide fast authentication and SSO
- Audit and report access and application metrics

Authentication, authorization, and SSO to all apps with F5 Application Policy Manager (APM)

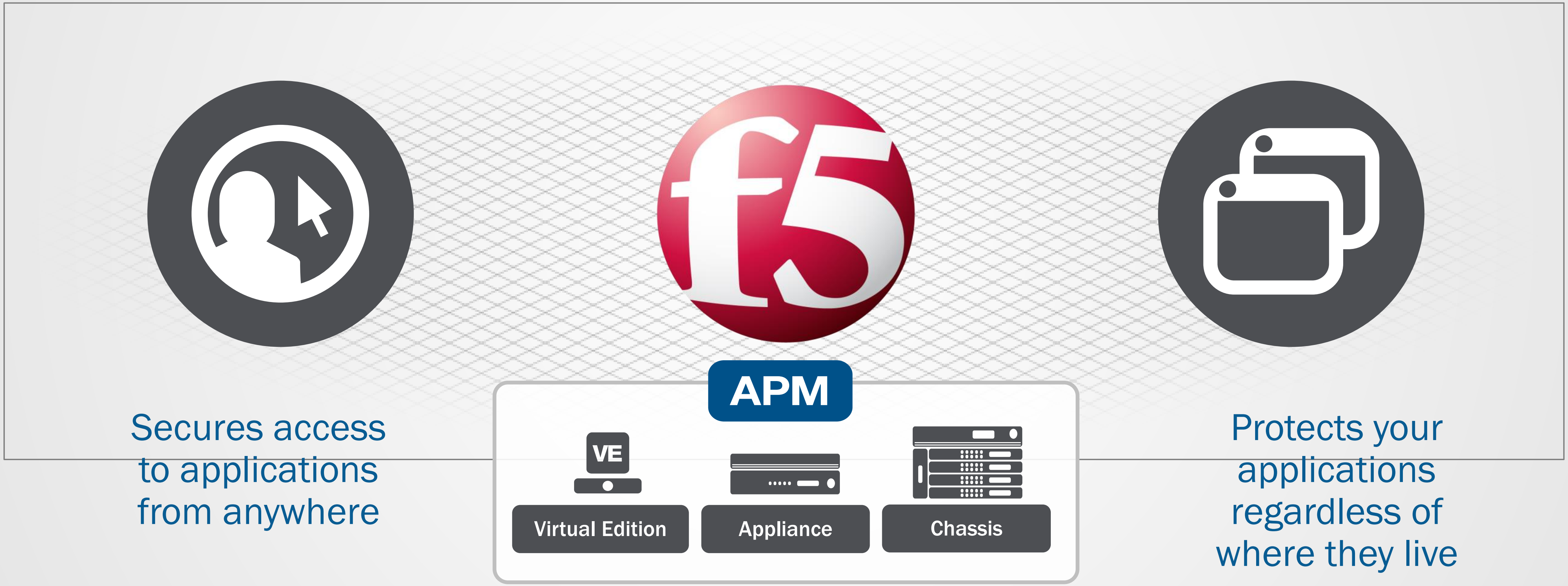
Context-aware policy enforcement

Scalability and performance

Access control over third-party SaaS

Simplified policy management

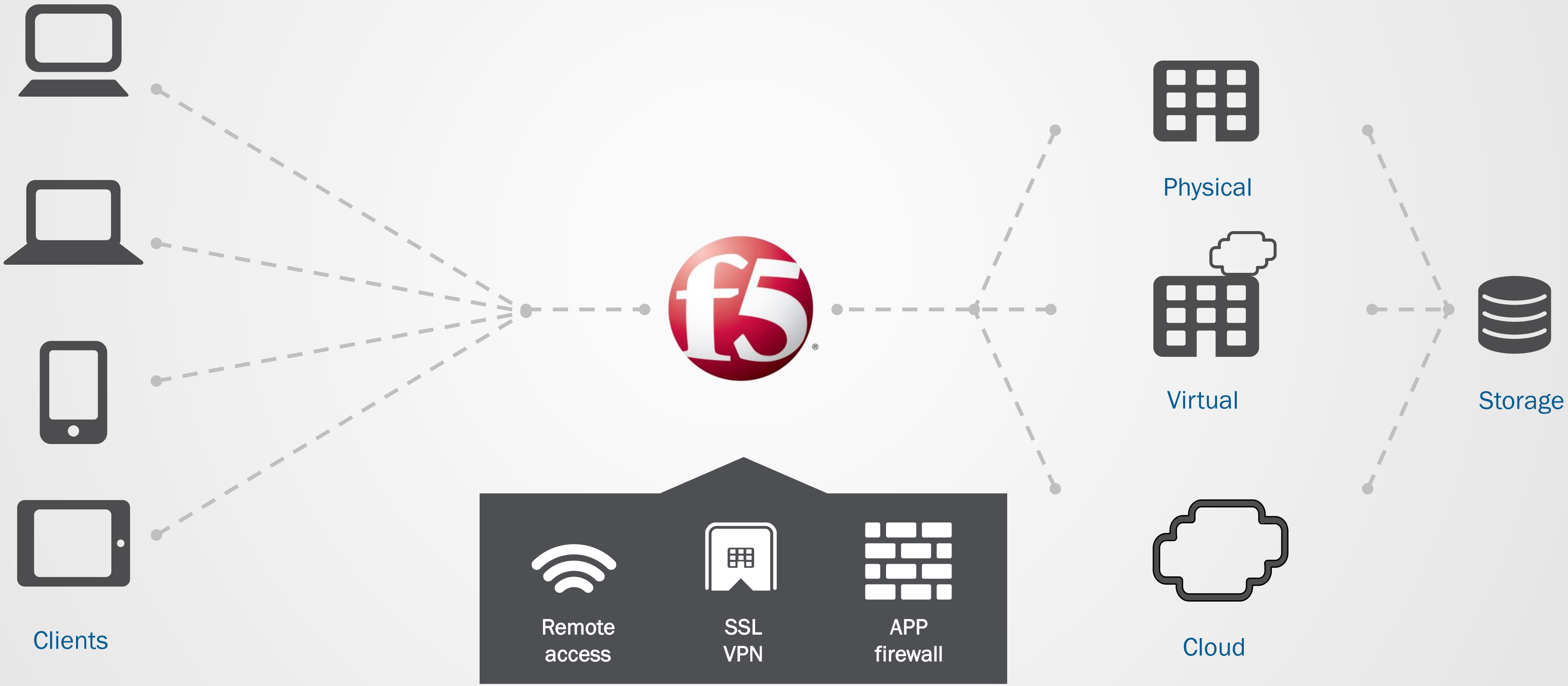
Maintain complete visibility and control across applications and users



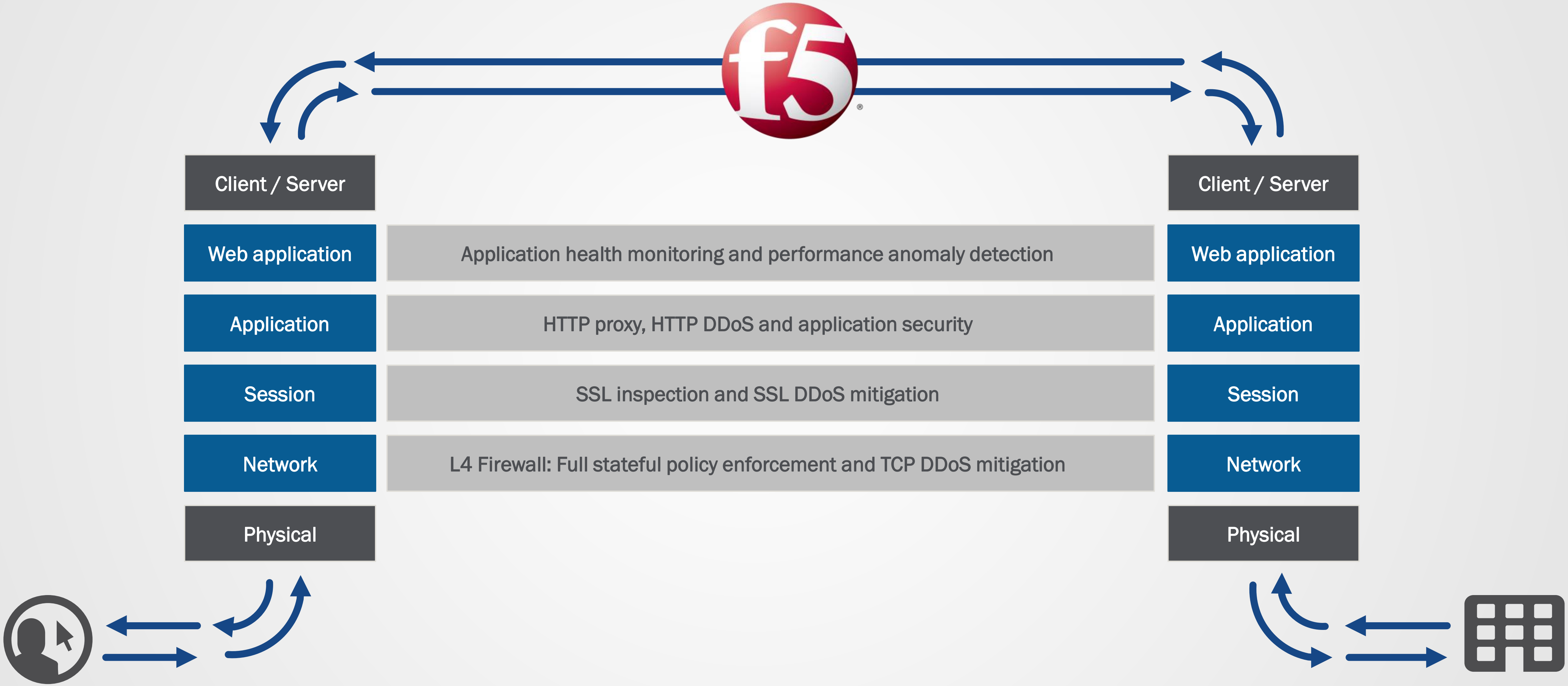
Secures access to applications from anywhere

Protects your applications regardless of where they live

Security at the critical point in the network

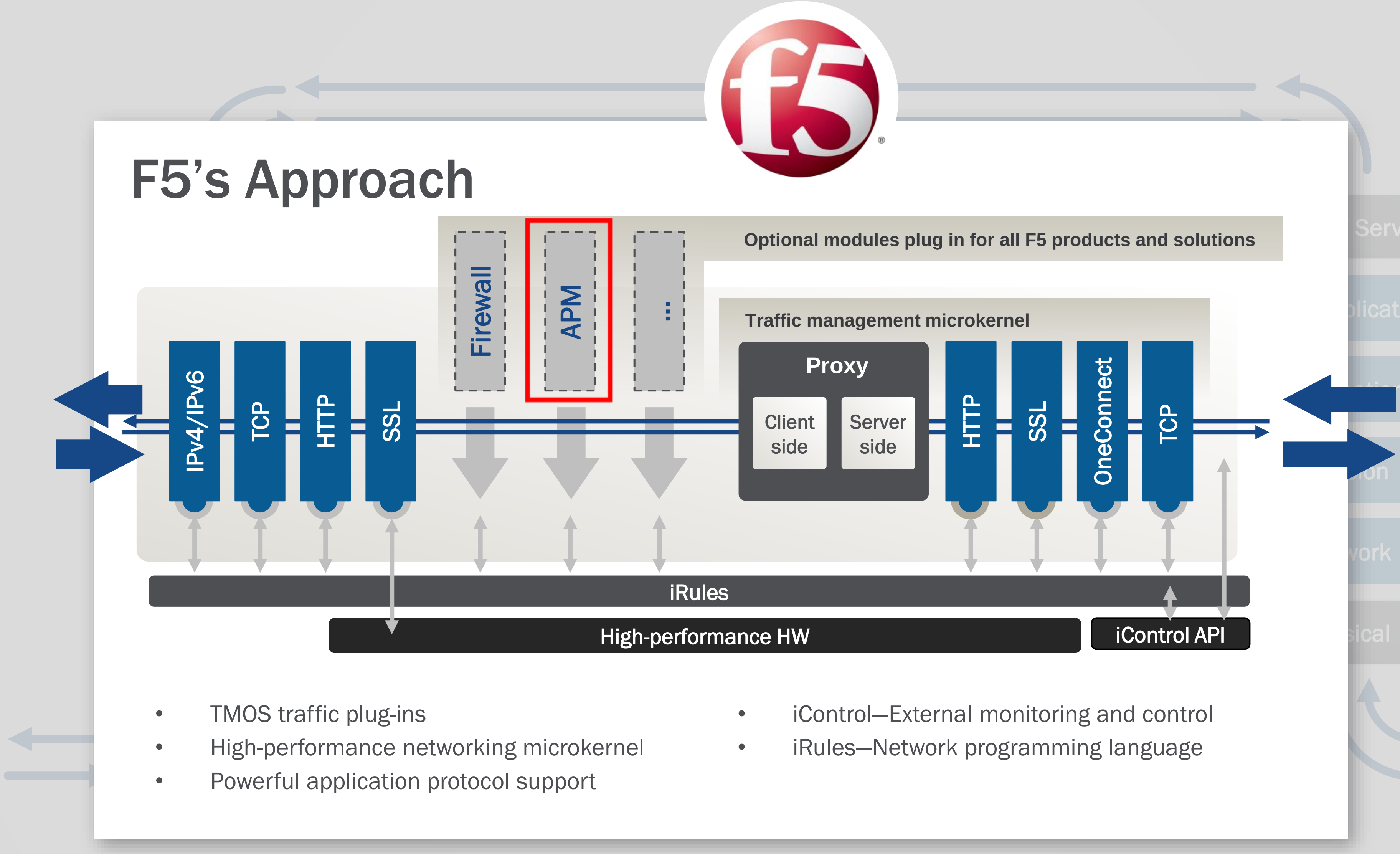


Full proxy security



Client / Server		Client / Server
Web application	Application health monitoring and performance anomaly detection	Web application
Application	HTTP proxy, HTTP DDoS and application security	Application
Session	SSL inspection and SSL DDoS mitigation	Session
Network	L4 Firewall: Full stateful policy enforcement and TCP DDoS mitigation	Network
Physical		Physical

Full proxy security

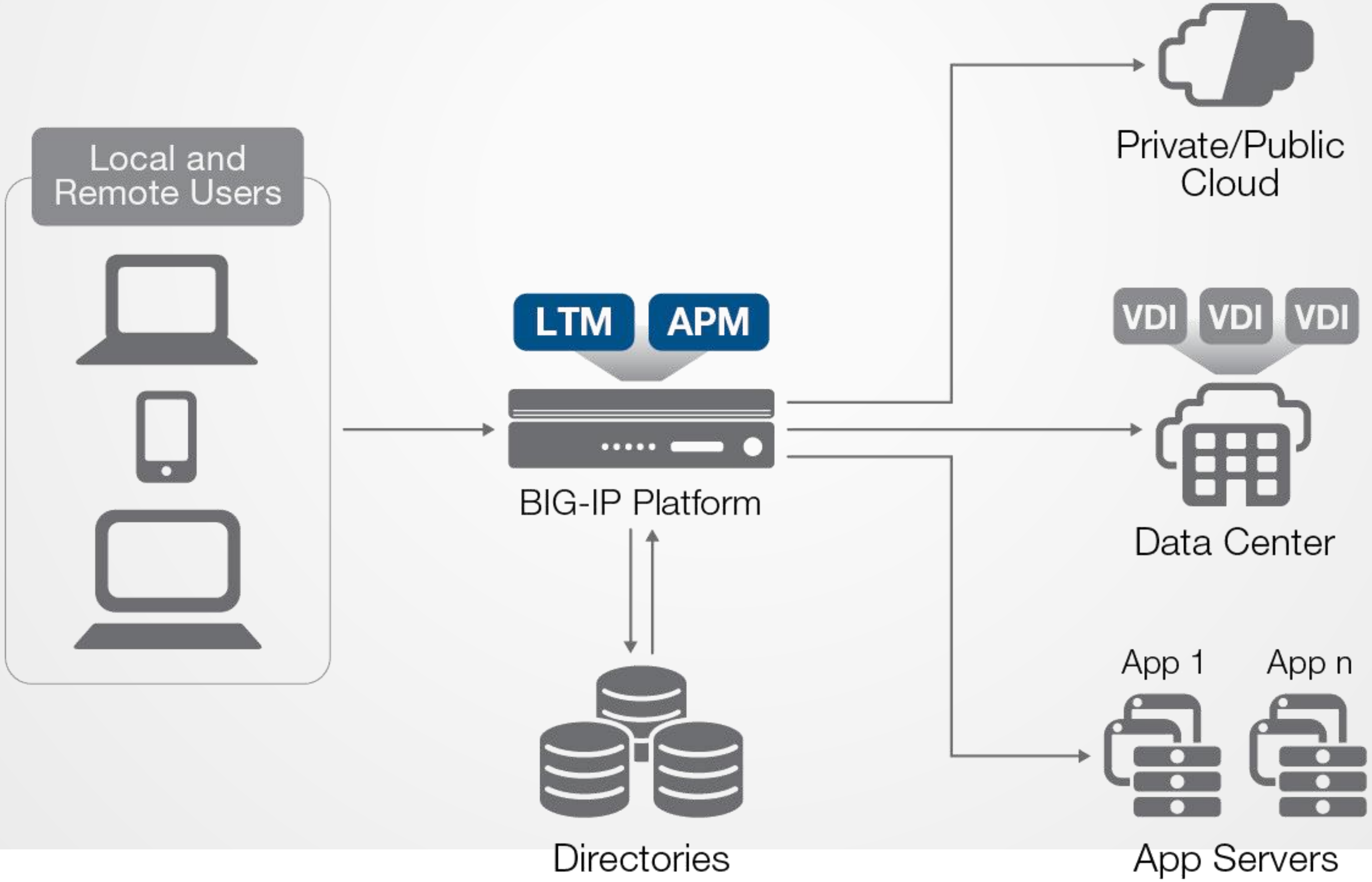


F5's Approach

- TMOS traffic plug-ins
- High-performance networking microkernel
- Powerful application protocol support
- iControl—External monitoring and control
- iRules—Network programming language

BIG-IP Access Policy Manager (APM)

- Industry's most scalable access gateway
- Consolidates remote access, Web access management, enterprise mobility management, identity federation and secure web gateway in a single platform
- Protects against data loss, virus infection, and rogue device access
- Replaces web access proxy tiers for common applications reducing infrastructure and management costs

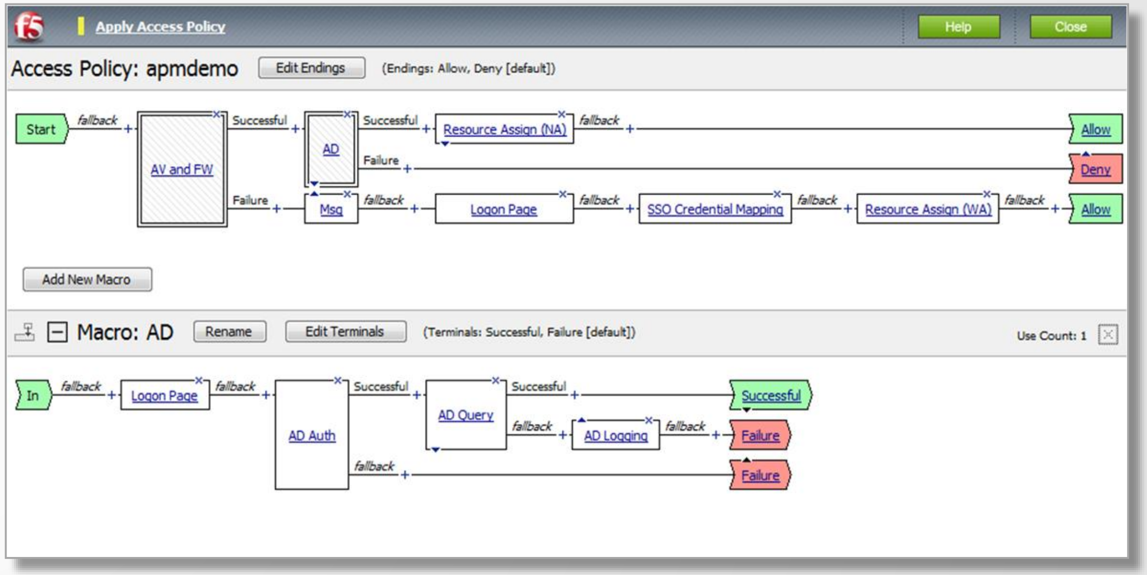


BIG-IP APM

Unified access and control for BIG-IP

Features

- Scales up to 2M users on a single device
- Centralizes single sign-on (SSO) and access control services
- Full proxy L4-L7 access control at BIG-IP speeds
- Adds endpoint inspection to the access policy
- Visual Policy Editor (VPE) provides policy-based access control
- VPE Rules – programmatic interface for custom access policies
- Supports IPv6

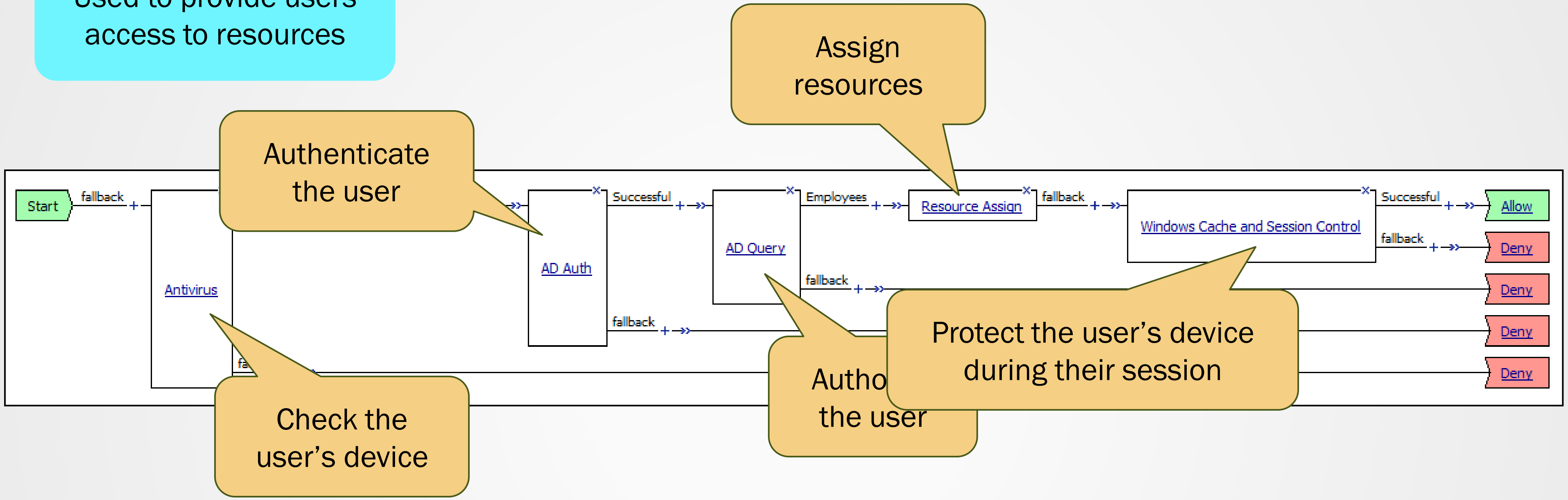


Benefits

- Consolidates authentication infrastructure
- Simplifies remote, web, and application access control

Access Policies

Used to provide users access to resources



Assign resources

Authenticate the user

Check the user's device

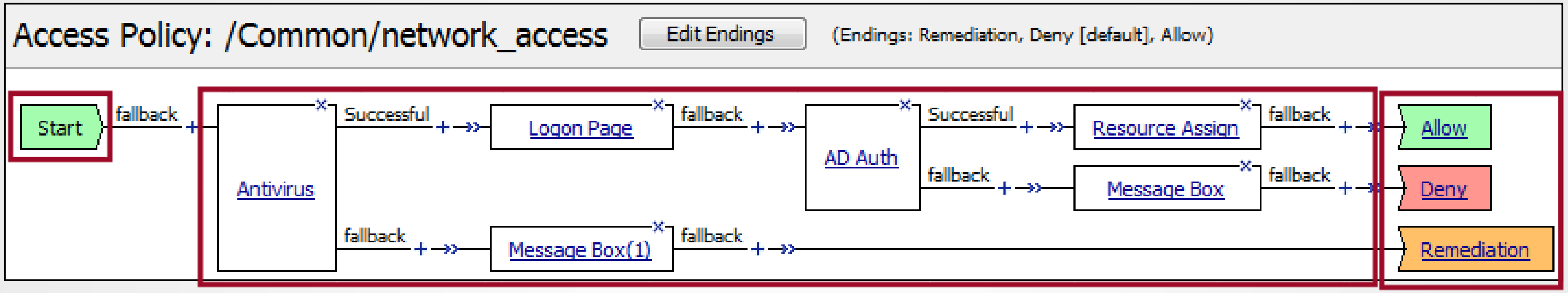
Autho the user

Protect the user's device during their session

Access Policy Components

Each access policy has one starting point

An access policy can have multiple ending points



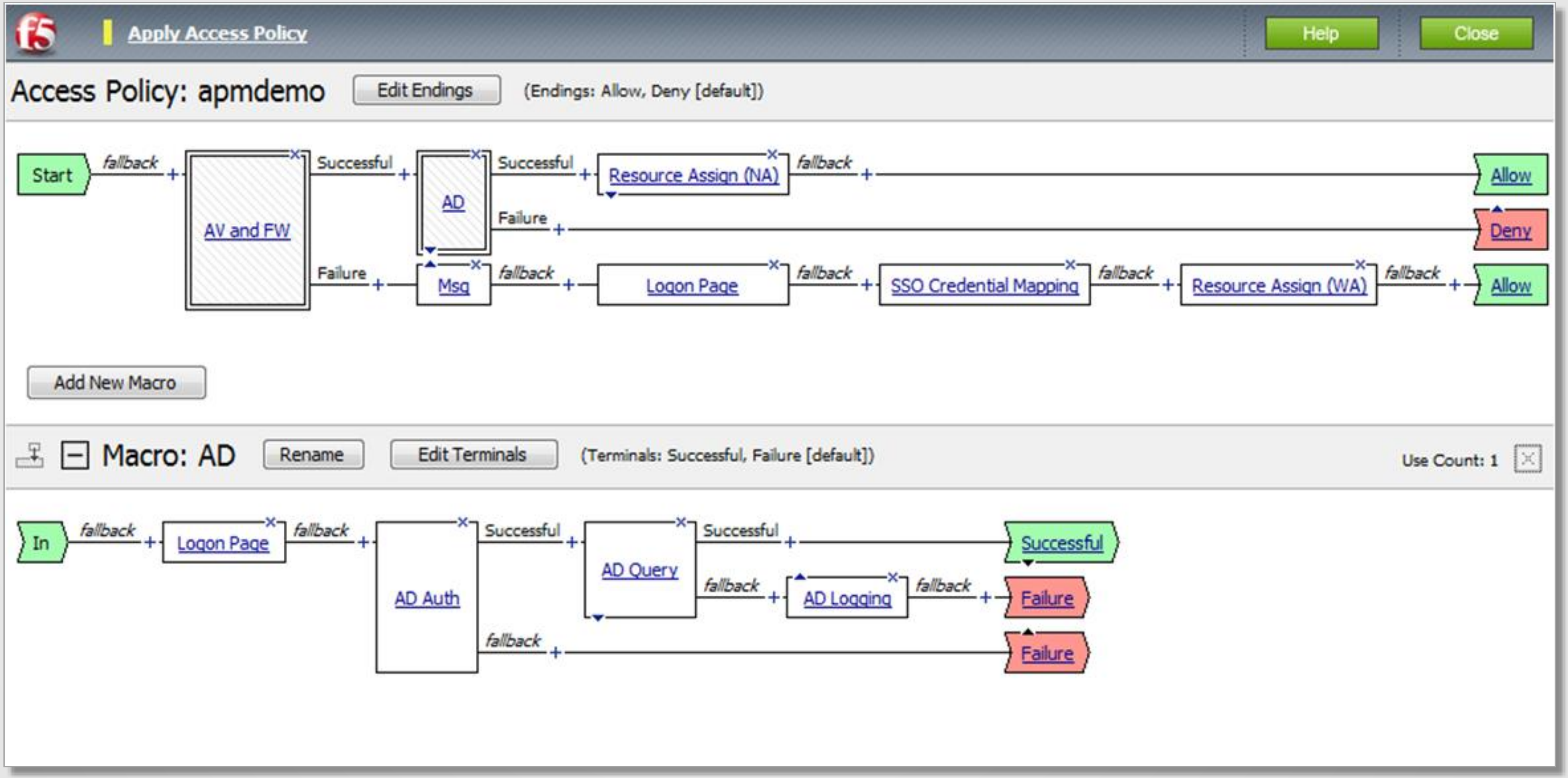
Access Policy: /Common/network_access

Edit Endings

(Endings: Remediation, Deny [default], Allow)

An access policy contains items and branches

Visual Policy Editor (VPE)



Apply Access Policy

Help Close

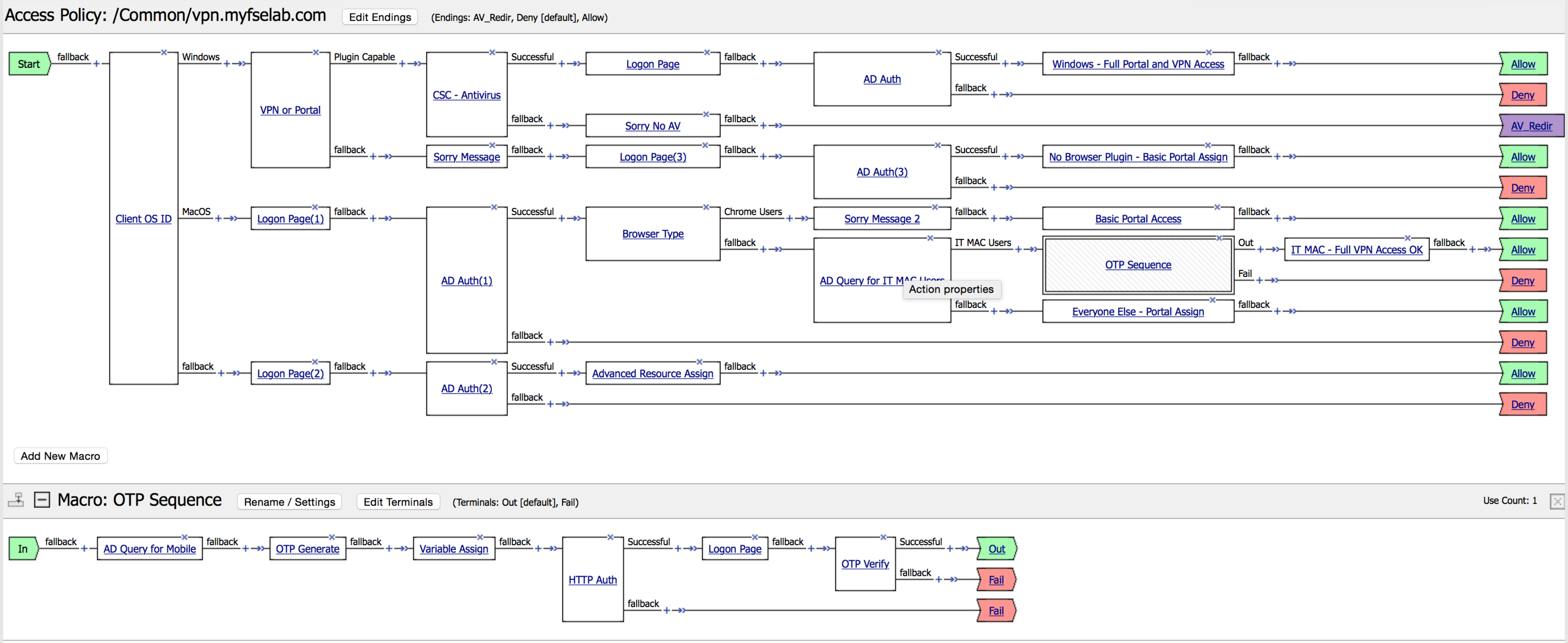
Access Policy: apmdemo Edit Endings (Endings: Allow, Deny [default])

Add New Macro

Macro: AD Rename Edit Terminals (Terminals: Successful, Failure [default])

Use Count: 1

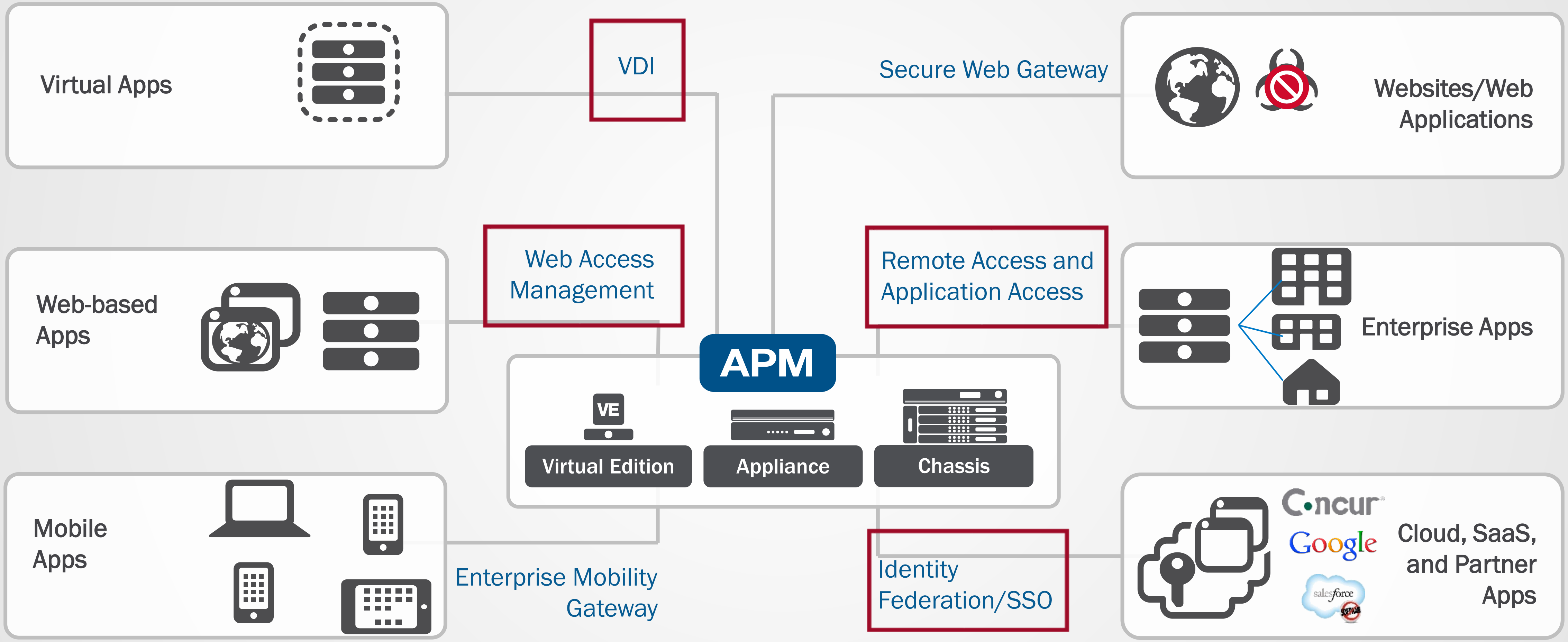
Building Access Policies with VPE



Access Policy: /Common/vpn.myfselab.com   Edit Endings   (Endings: AV_Redir, Deny [default], Allow)

Macro: OTP Sequence   Rename / Settings   Edit Terminals   (Terminals: Out [default], Fail)   Use Count: 1

F5 BIG-IP Access Policy Manager Drives Identity Federation, Single Sign On, and Adaptive Authentication



Virtual Apps

VDI

Secure Web Gateway

Websites/Web Applications

Web-based Apps

Web Access Management

Remote Access and Application Access

Enterprise Apps

APM

Virtual Edition

Appliance

Chassis

Mobile Apps

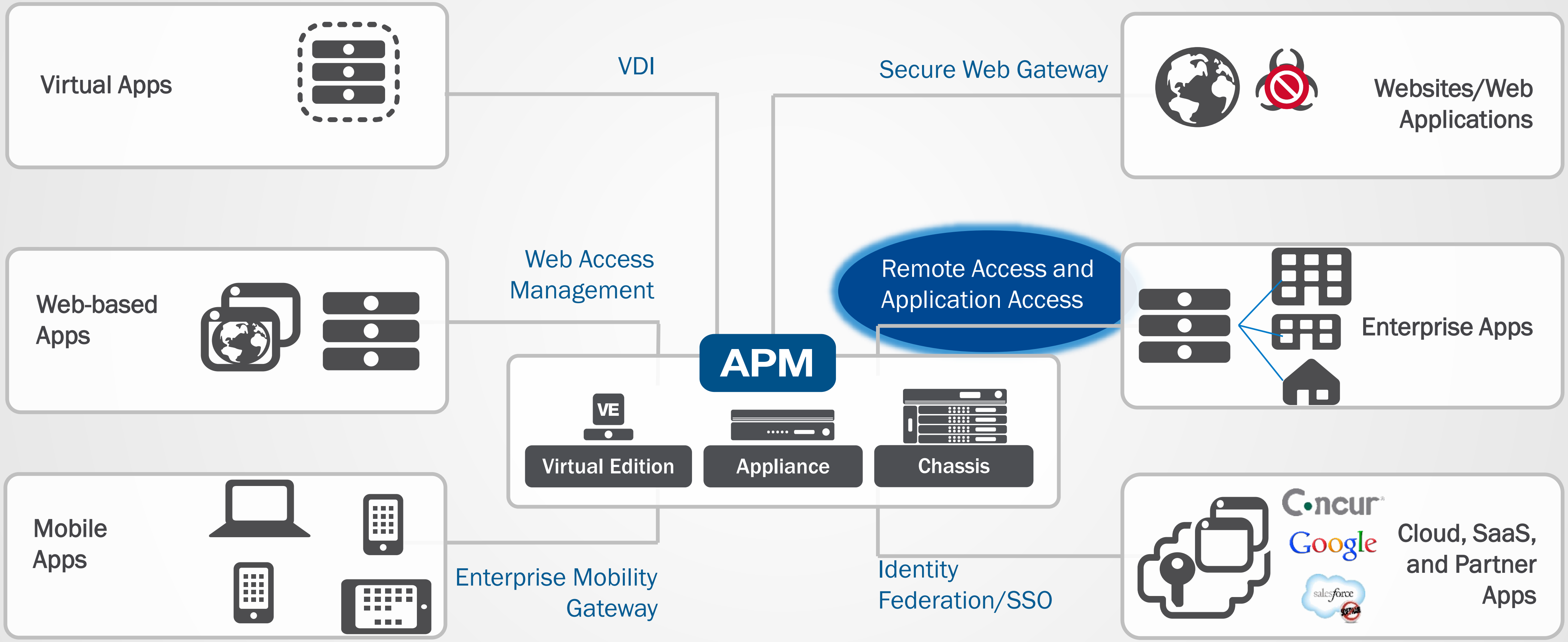
Enterprise Mobility Gateway

Identity Federation/SSO

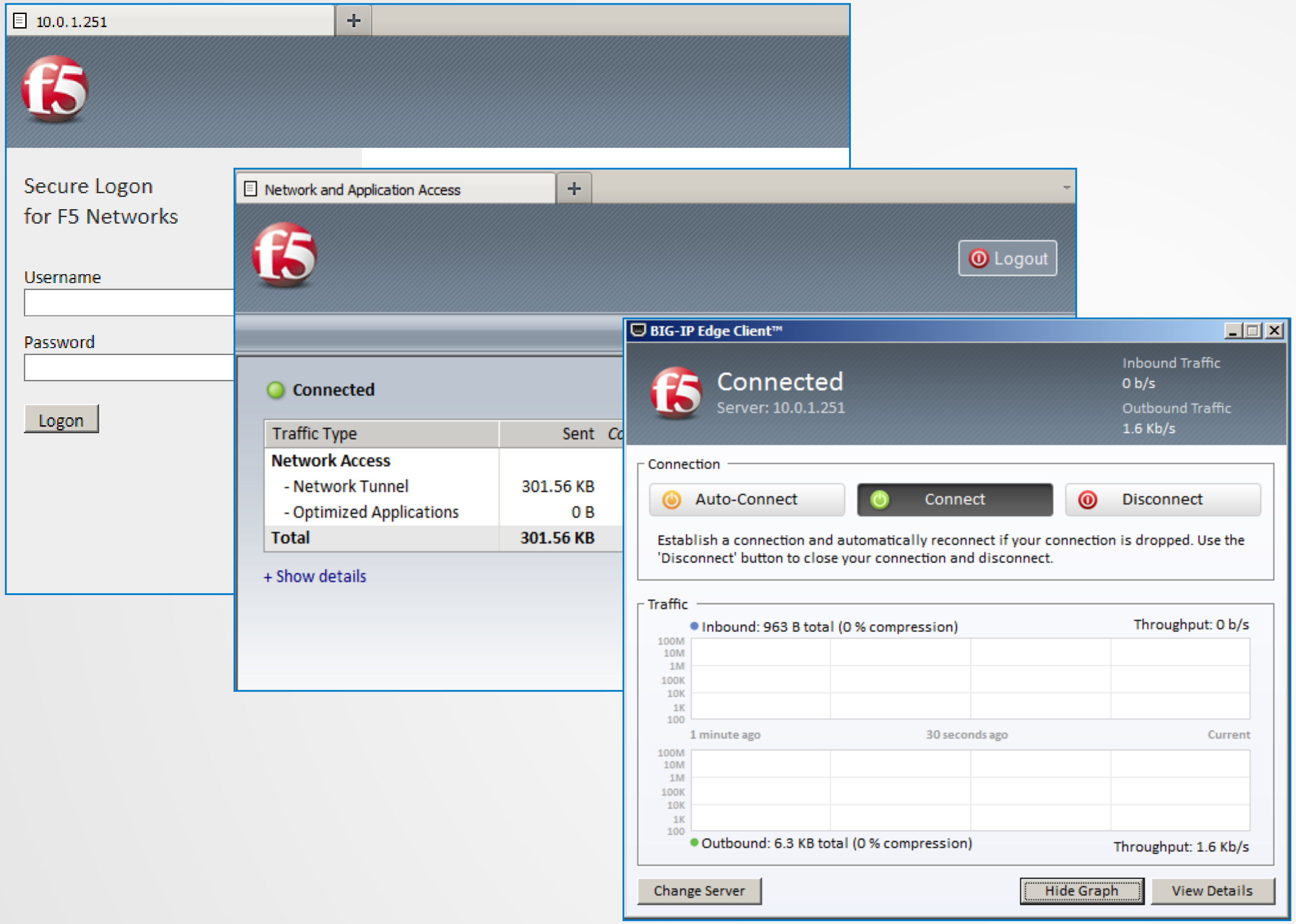
Cloud, SaaS, and Partner Apps

Remote Access and Application Access

F5 BIG-IP Access Policy Manager Drives Identity Federation, Single Sign On, and Adaptive Authentication



APM SSL VPN



10.0.1.251

Secure Logon
for F5 Networks

Username

Password

Logon

Network and Application Access

Logout

Connected

Traffic Type	Sent
Network Access	
- Network Tunnel	301.56 KB
- Optimized Applications	0 B
Total	**301.56 KB**

+ Show details

BIG-IP Edge Client™

Connected
Server: 10.0.1.251

Inbound Traffic
0 b/s
Outbound Traffic
1.6 Kb/s

Connection

Auto-Connect | Connect | Disconnect

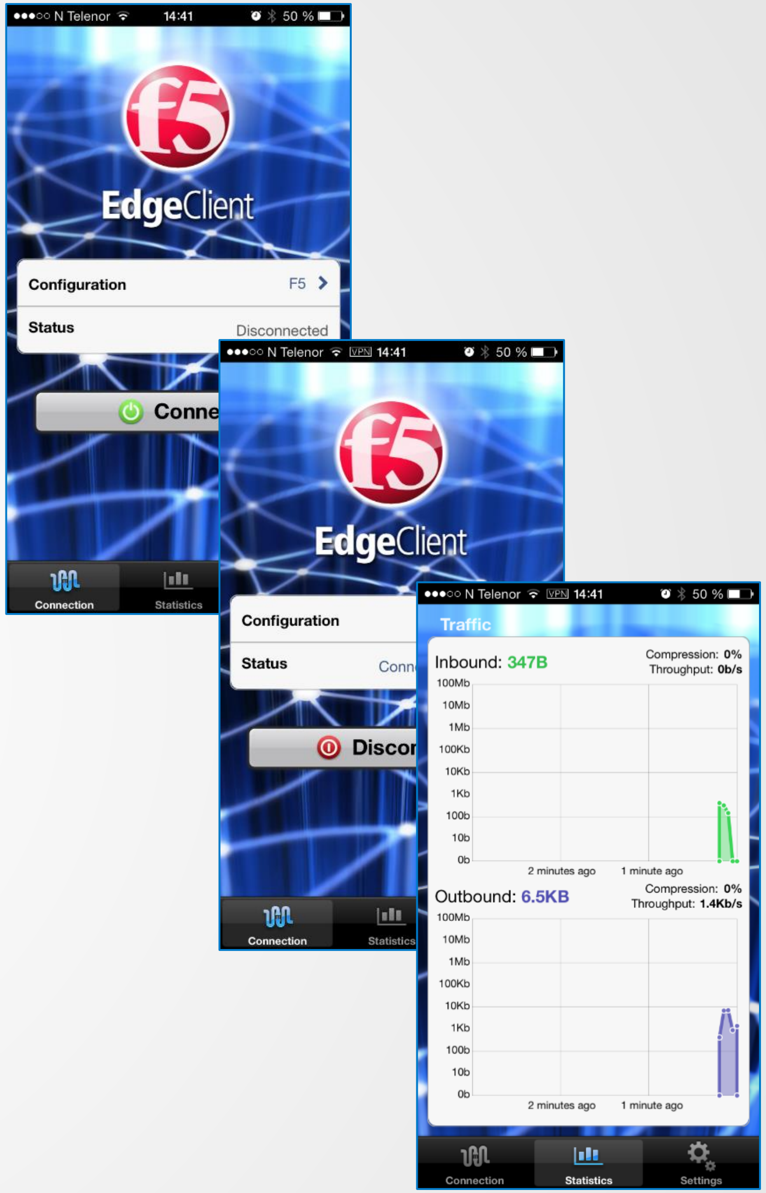
Establish a connection and automatically reconnect if your connection is dropped. Use the 'Disconnect' button to close your connection and disconnect.

Traffic

Inbound: 963 B total (0 % compression) Throughput: 0 b/s

Outbound: 6.3 KB total (0 % compression) Throughput: 1.6 Kb/s

Change Server | Hide Graph | View Details



●●●○○ N Telenor 14:41 50 %

EdgeClient

Configuration F5

Status Disconnected

Connect

Configuration

Status Connected

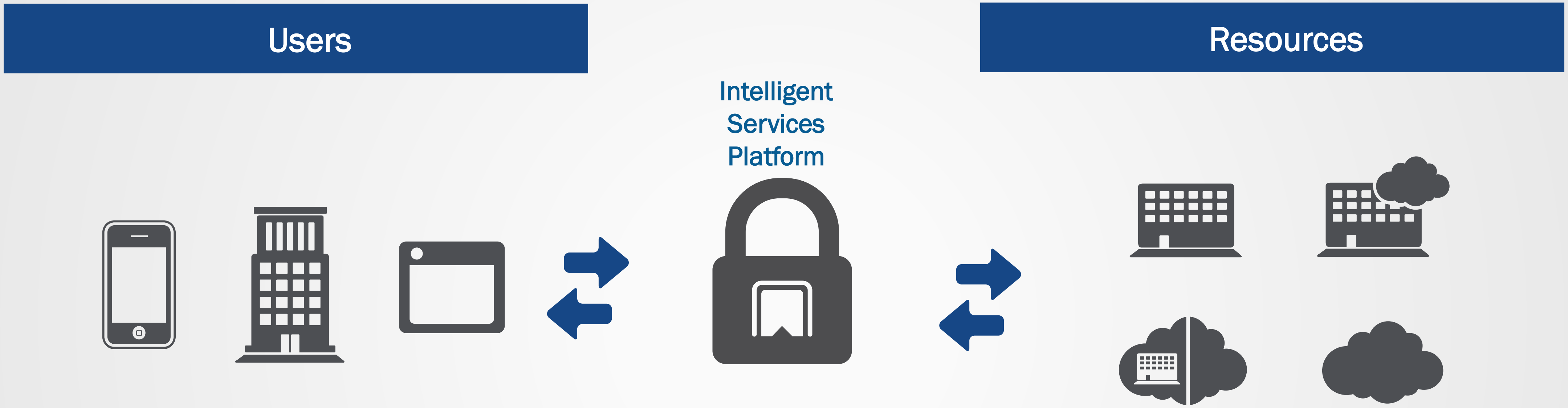
Disconnect

Traffic

Inbound: 347B Compression: 0% Throughput: 0b/s

Outbound: 6.5KB Compression: 0% Throughput: 1.4Kb/s

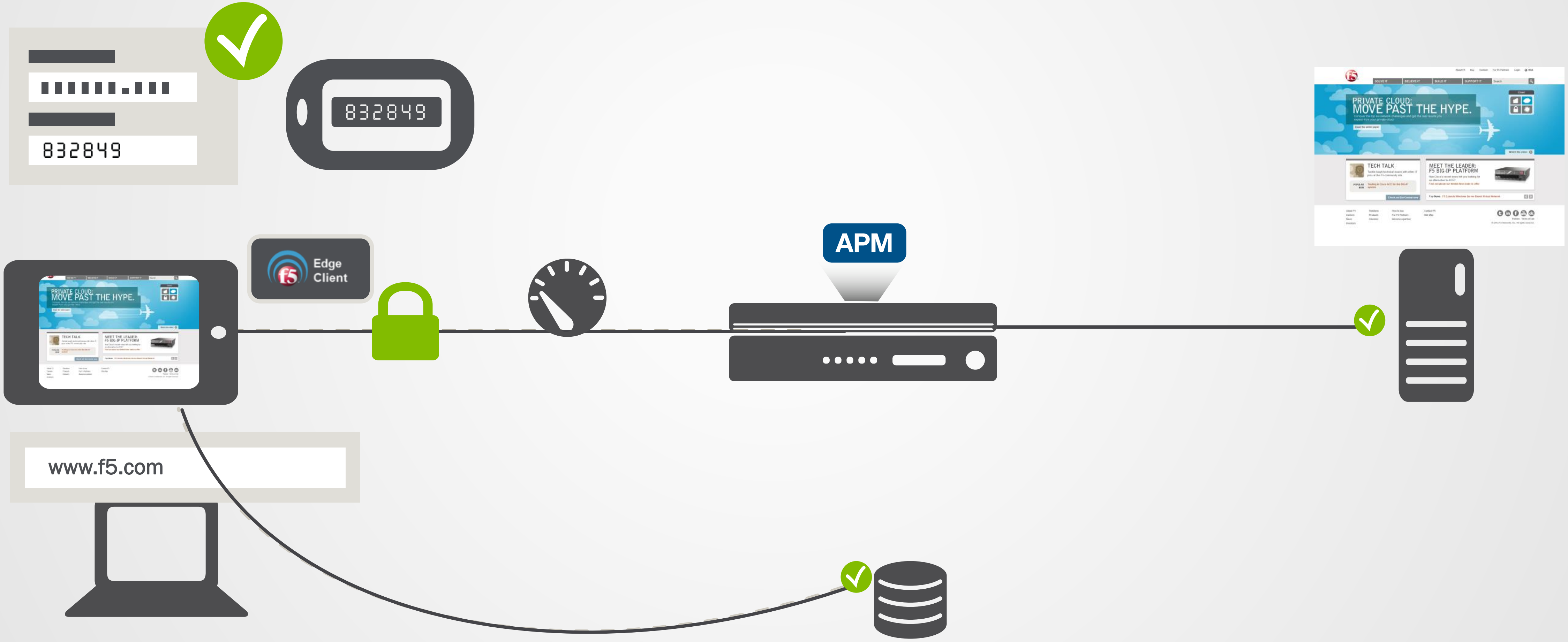
Remote access and application access challenges



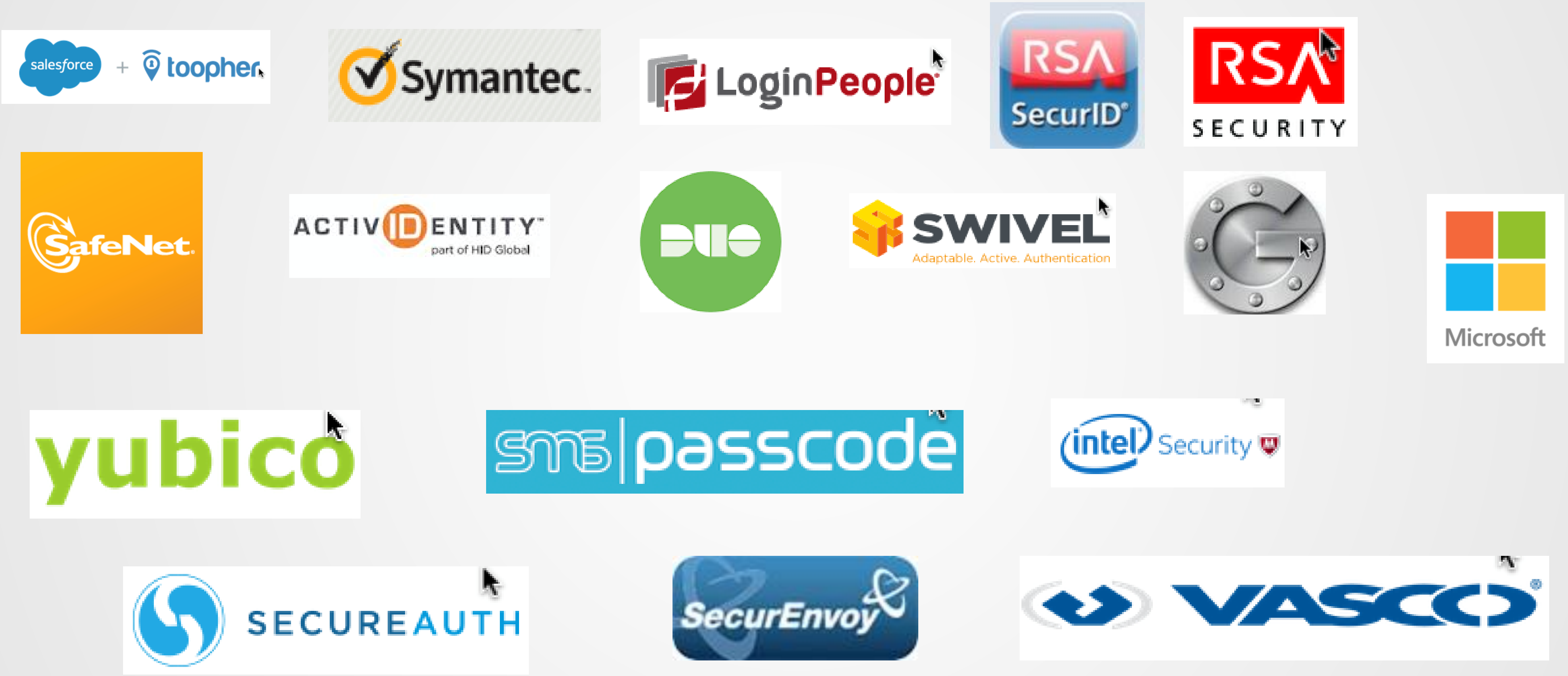
- Enabling secure remote access to corporate resources from any network, from any device
- Ensuring secure and fast application performance for remote users
- Protecting network resources, applications and data from malware, theft or hack, and/or rogue and unauthorized access

Fast, secure remote access

- Fast and secure connections maximize productivity for global users
- Seamless integration minimizes cost and simplifies end user experience

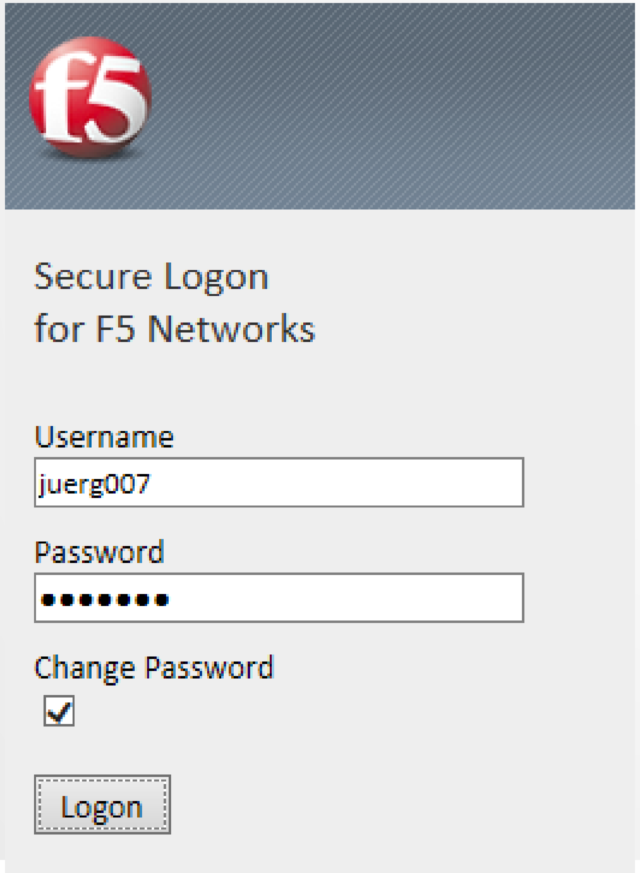


A Rich, Powerful Ecosystem of MFA Partners



Logon Page

- Customizable

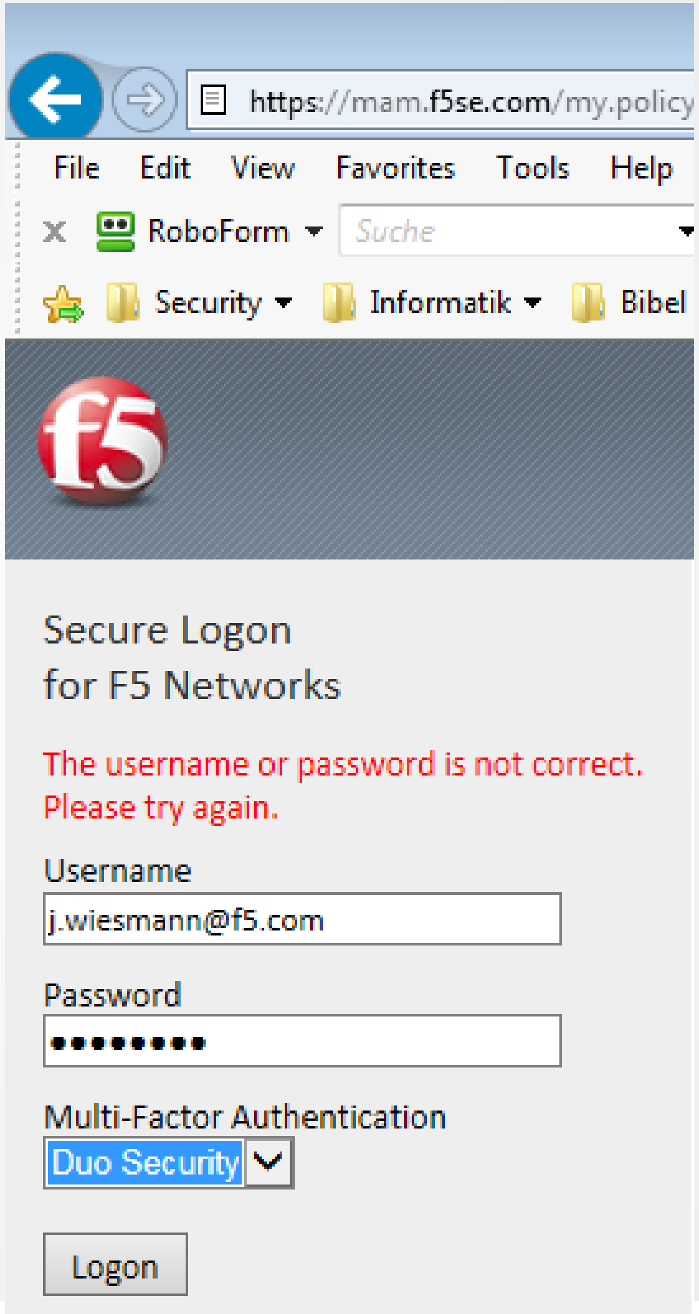


Secure Logon
for F5 Networks

Username: juerg007

Password: •••••••

Change Password: ☑



https://mam.f5se.com/my.policy

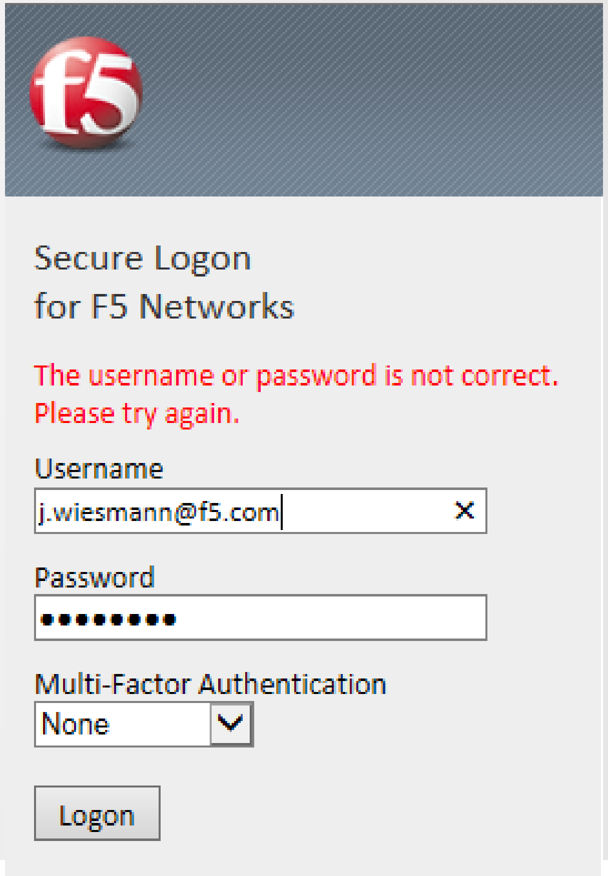
Secure Logon
for F5 Networks

The username or password is not correct.
Please try again.

Username: j.wiesmann@f5.com

Password: ••••••••

Multi-Factor Authentication: Duo Security



Secure Logon
for F5 Networks

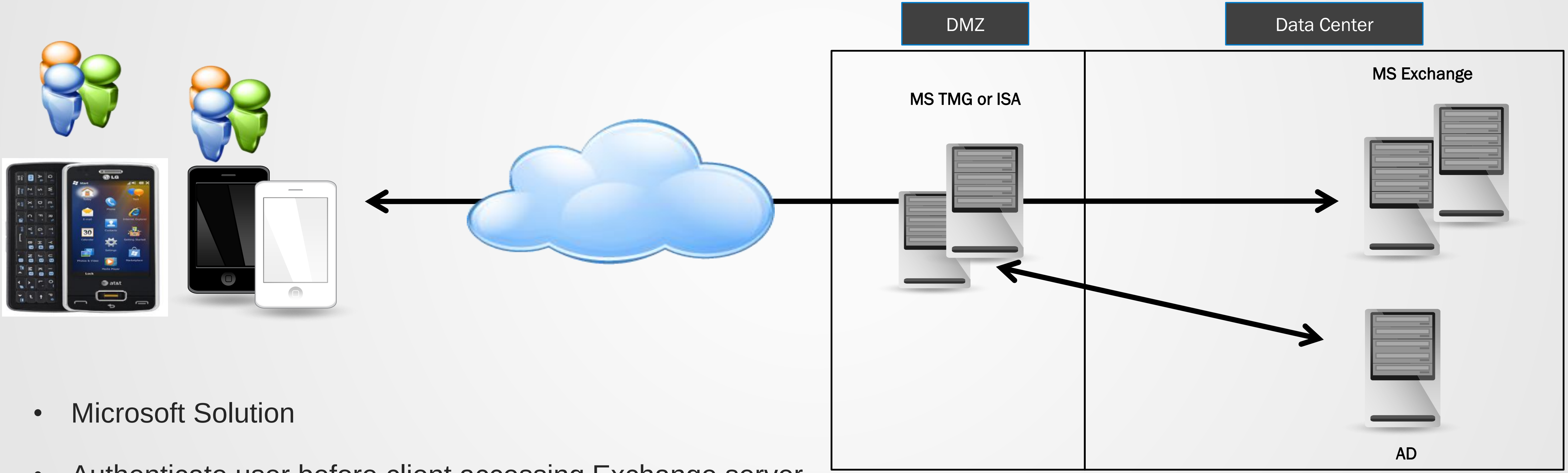
The username or password is not correct.
Please try again.

Username: j.wiesmann@f5.com

Password: ••••••••

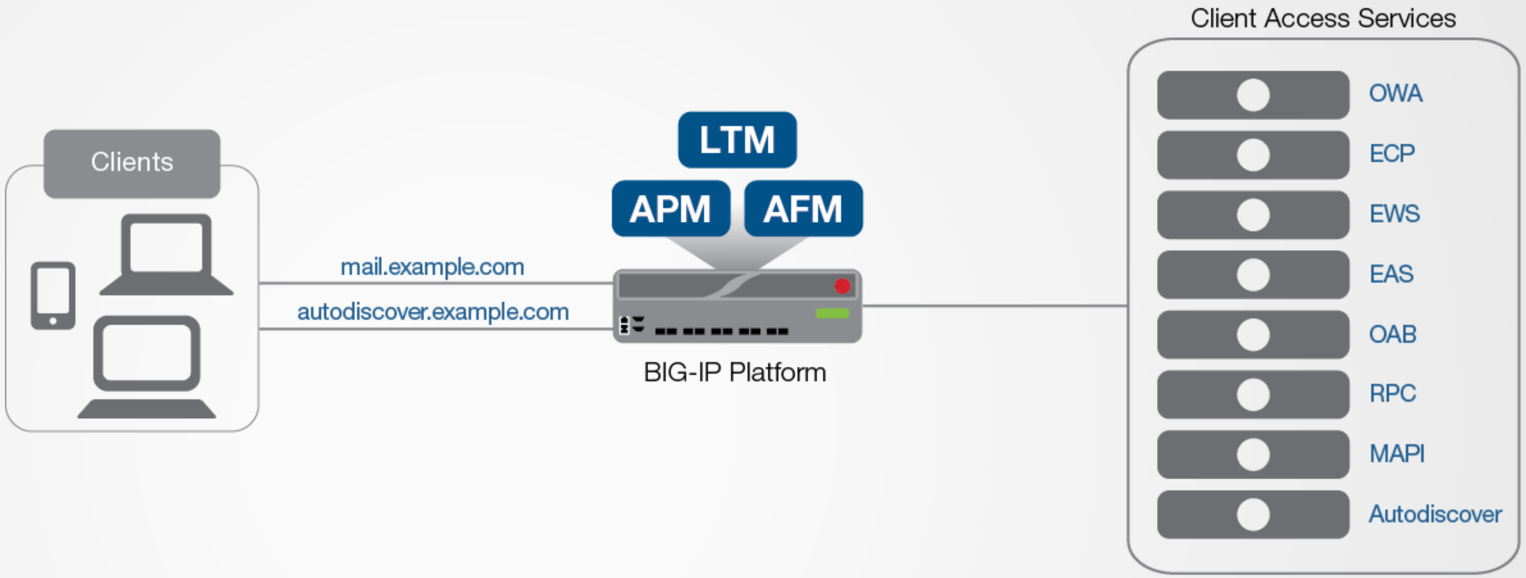
Multi-Factor Authentication: None

ActiveSync, Microsoft Solution



- Microsoft Solution
- Authenticate user before client accessing Exchange server
- Exchange can verify deviceid
- AD group check and basic url filter can be implemented on TMG

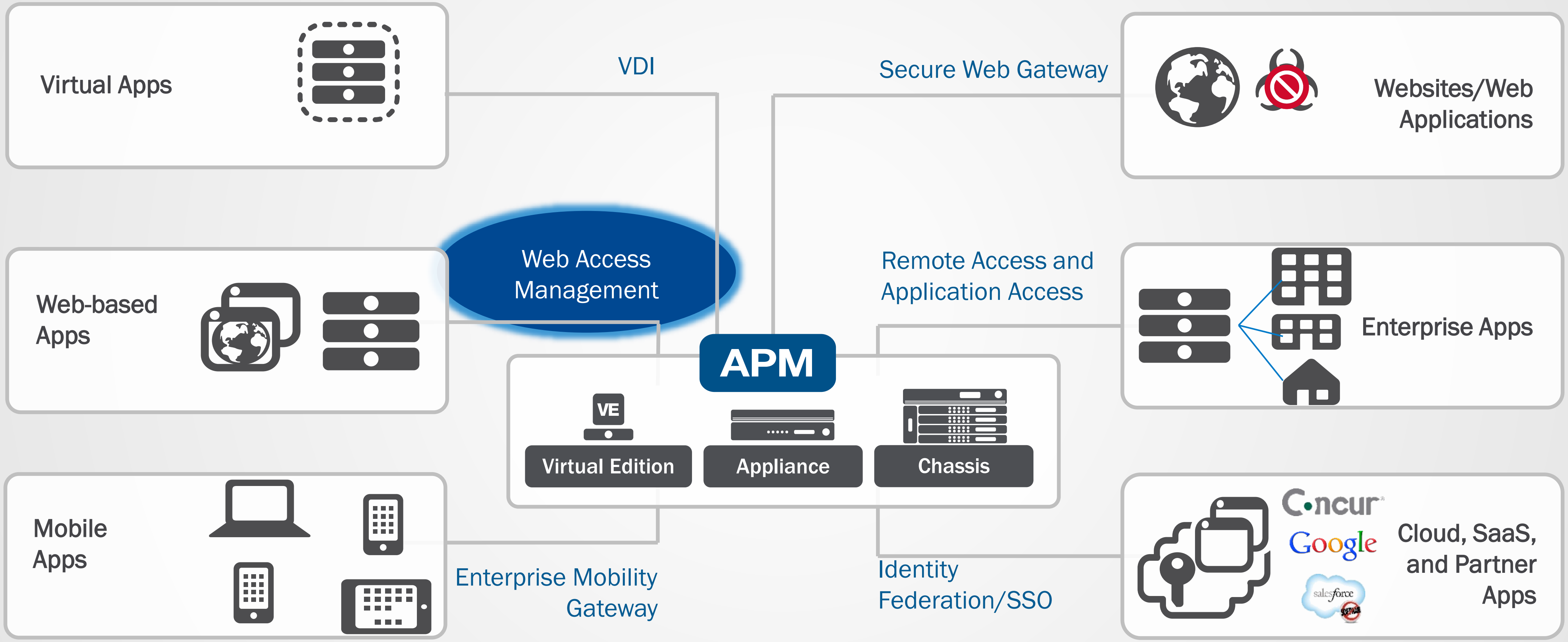
ActiveSync, F5 BIG-IP APM Solution



- SSL Offload
- Verify and enable access based on
  - User /password, AD group membership
  - IP location, Deviceid , Devicestype , Useragent
  - Brute force detection
  - ActiveSync commands used
  - URI (allow acces request to /Microsoft-Server-Activesync)

Web Access Management

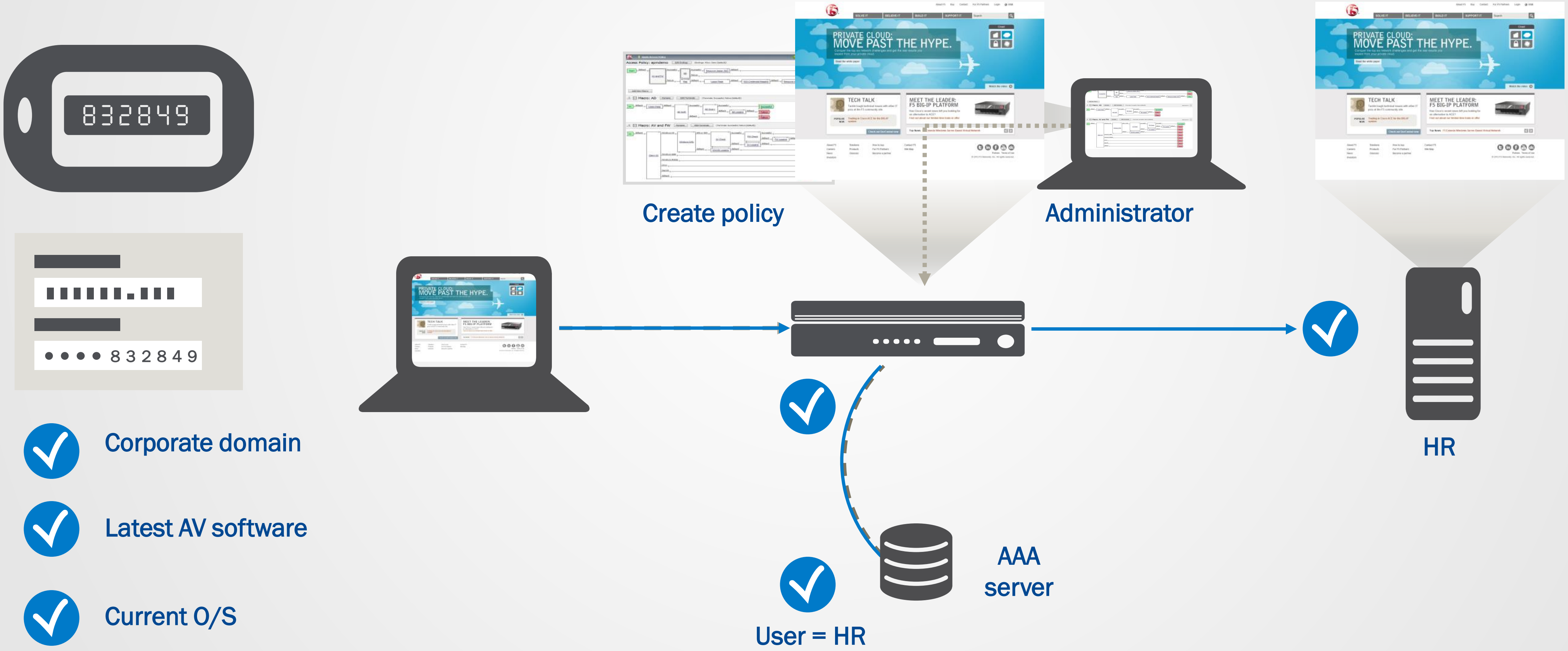
F5 BIG-IP Access Policy Manager Drives Identity Federation, Single Sign On, and Adaptive Authentication



© F5 Networks, Inc

Enhanced Web Access Management

- Proxy web applications to provide authentication, authorization, endpoint inspection, and more
- All Layer 4-7 ACLS through F5's Visual Policy Editor



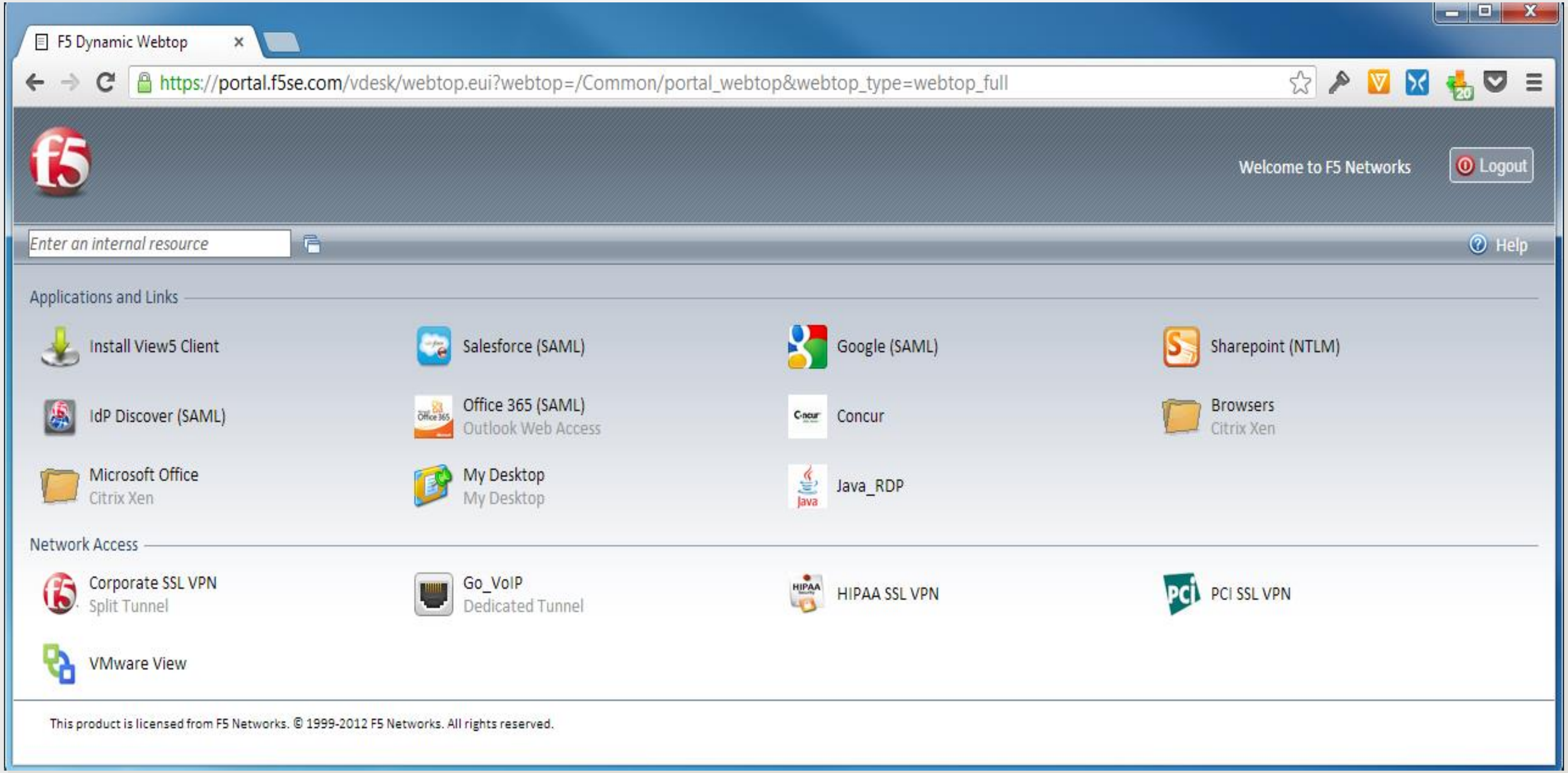
Application Authentication

- Control /Authenticate a User on APM before he reaches Application
- Building Security Zones using Authentication

- Adding Authentication / one or two Factor when required
- https://www.f5.com → No authentication
- https://www.f5.com/intranet/ → One Factor Authentication
- https://www.f5.com/intranet/HR/ → Two Factor Authentication

- Prerelease - Step-up Authentication… (12.1)

Web portal



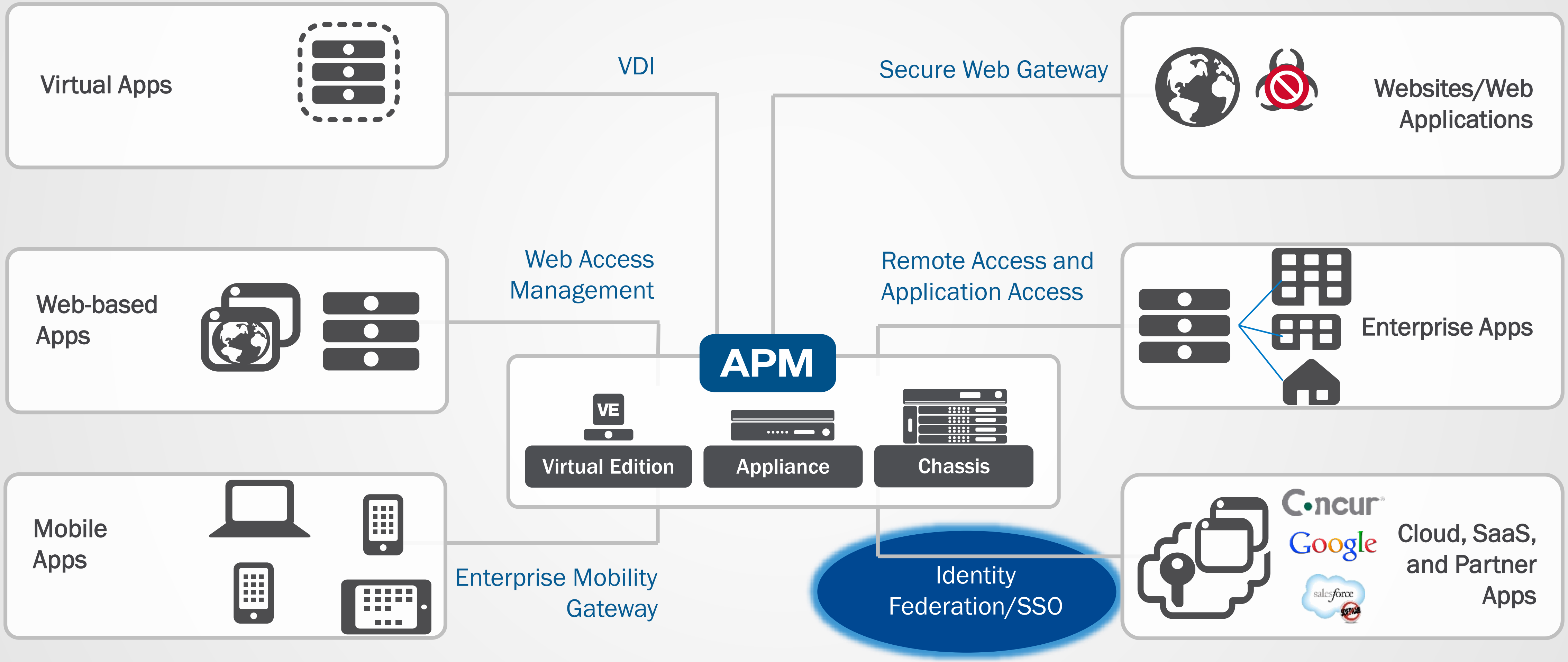
https://portal.f5se.com/vdesk/webtop.eui?webtop=/Common/portal_webtop&webtop_type=webtop_full

This product is licensed from F5 Networks. © 1999-2012 F5 Networks. All rights reserved.

Web portal with access to only user authorized apps

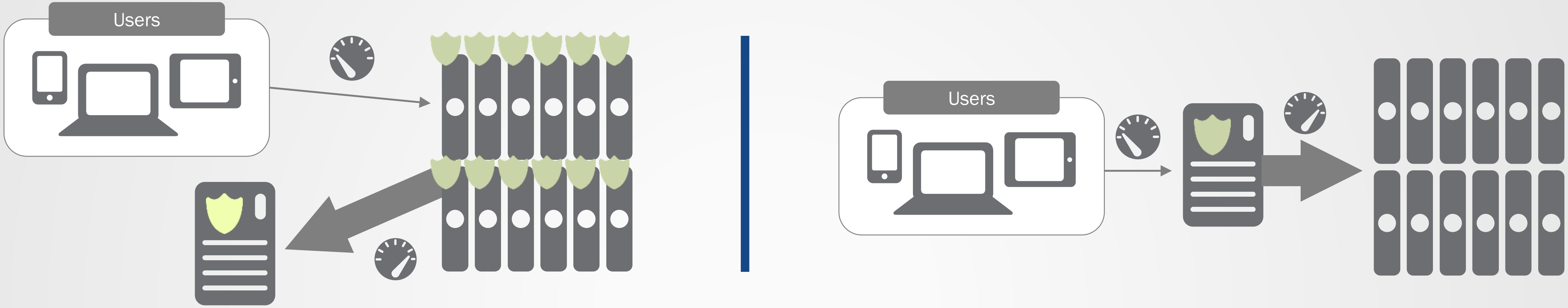
Identity Federation and Single Sign-on

F5 BIG-IP Access Policy Manager Drives Identity Federation, Single Sign On, and Adaptive Authentication

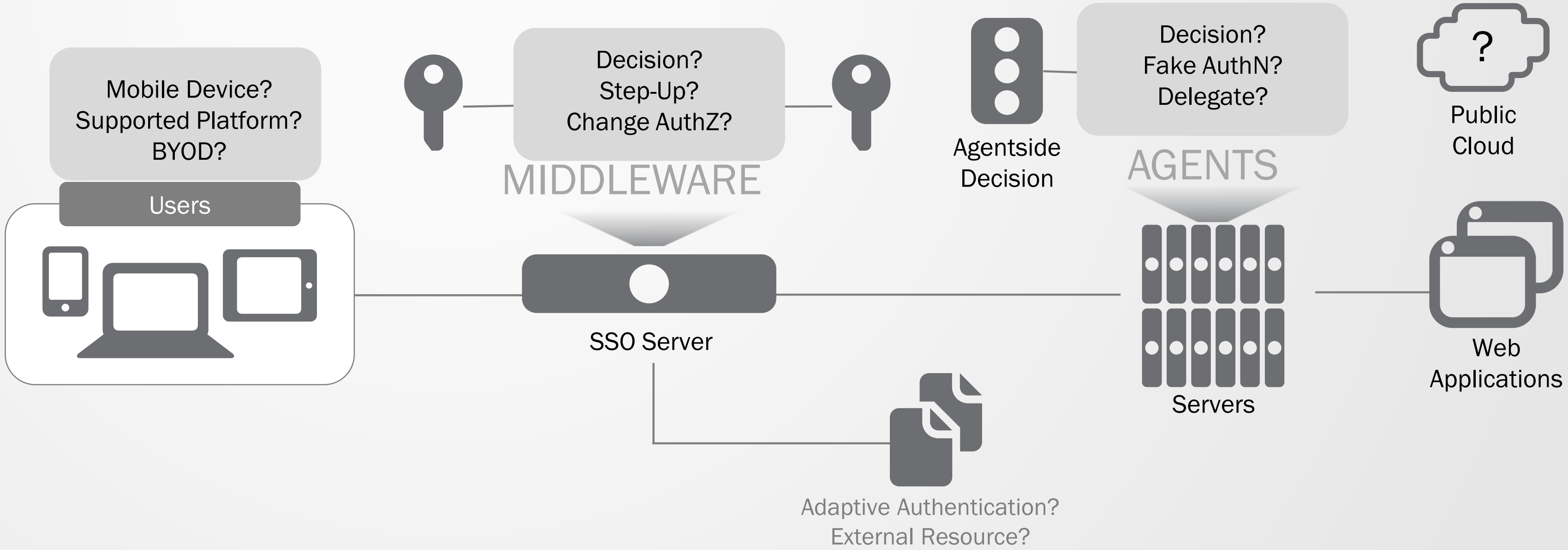


Single Sign-On (SSO) challenges

- Too many agents or proxies

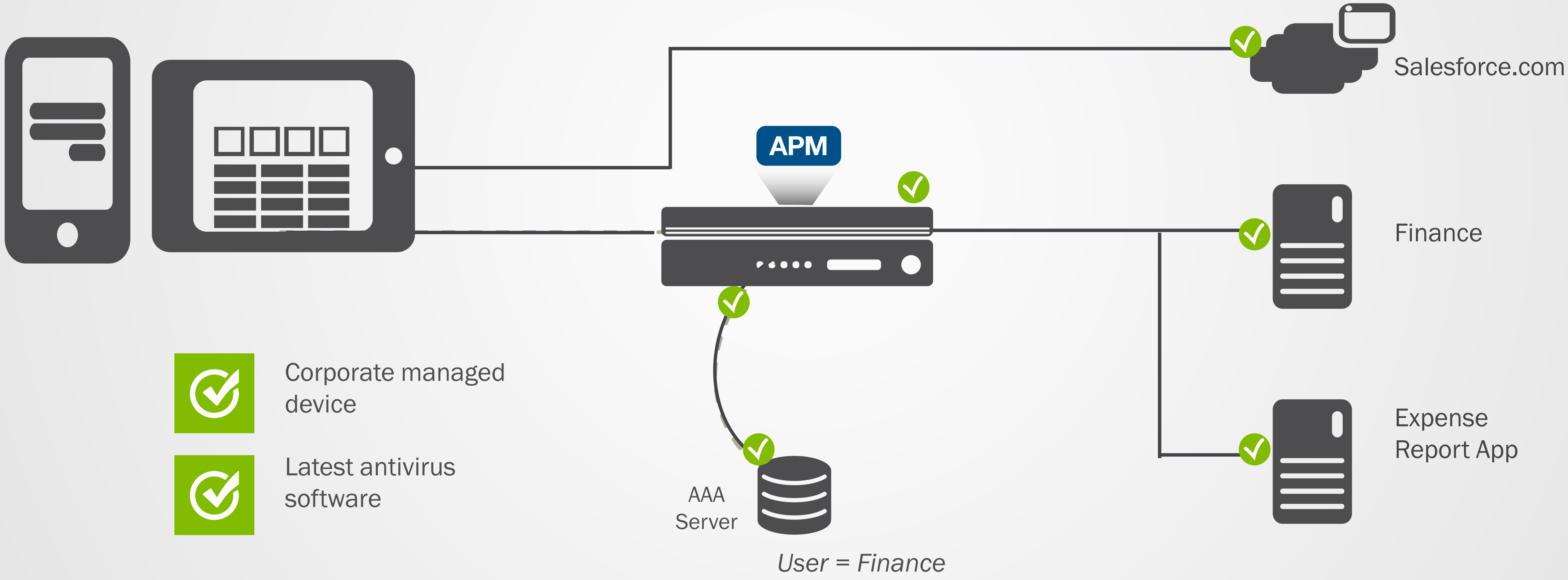


- Difficult to visualize single sign-on topology and deployment
- Single sign-on require flexibility

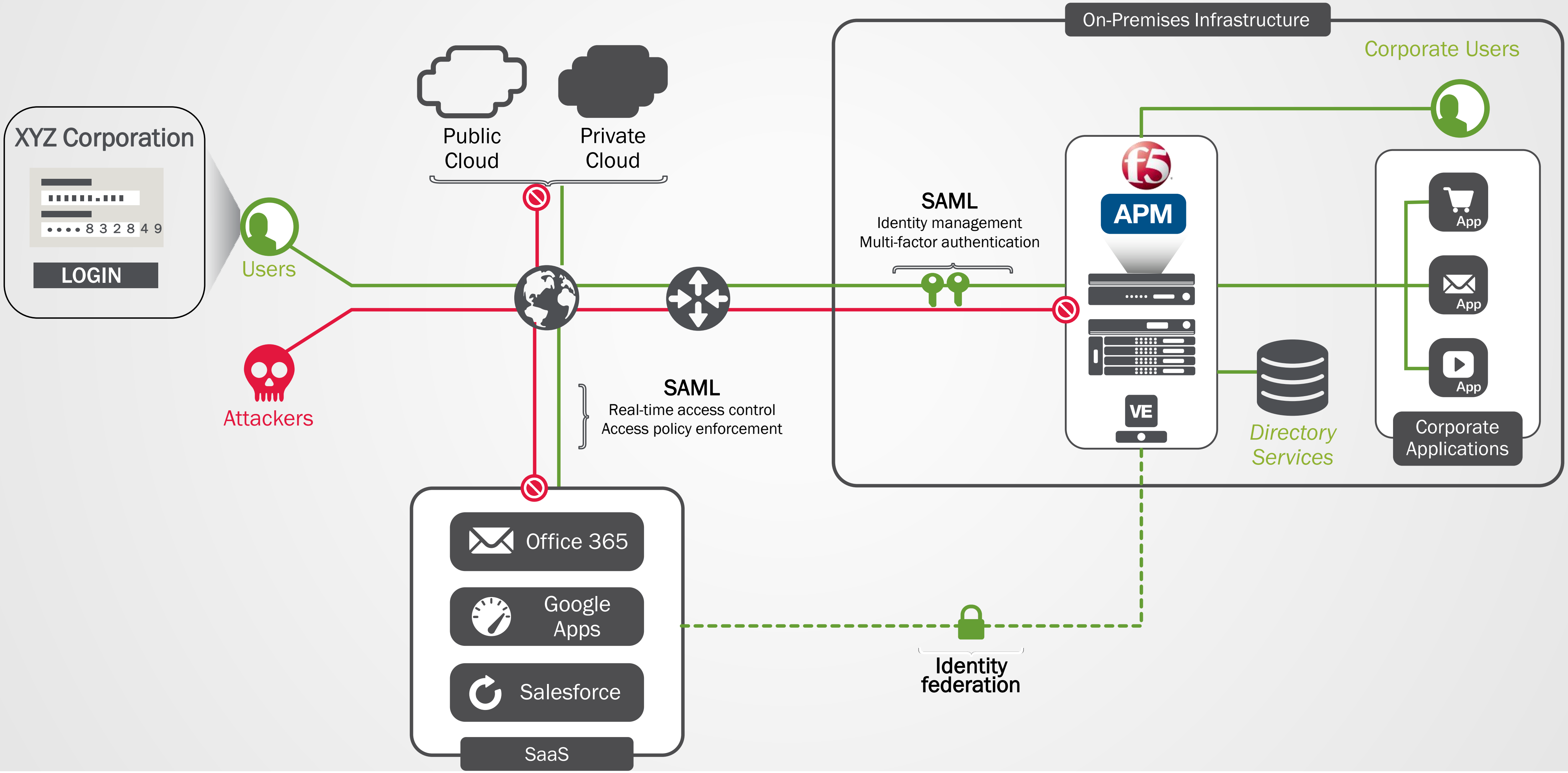


Identity Federation (SSO) benefits

- Dramatically reduces infrastructure costs while increasing user productivity
- Provides seamless access to all web resources
- Enhances user experience
- Instantly provisions and de-provisions access to cloud apps

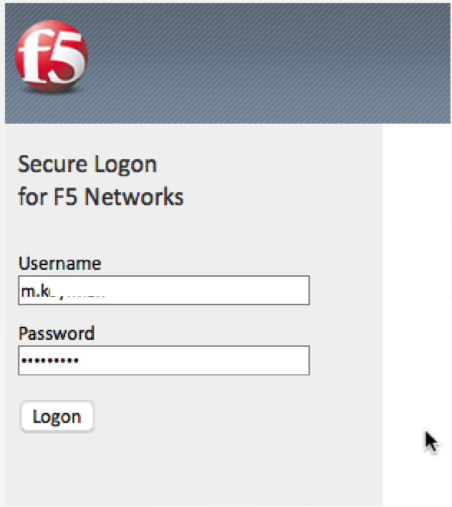


BIG-IP APM
Identity Federation/SSO with Adaptive Authentication



APM’s Webtop Unifies Access to All Apps, Including Those Using Identity Federation/SSO

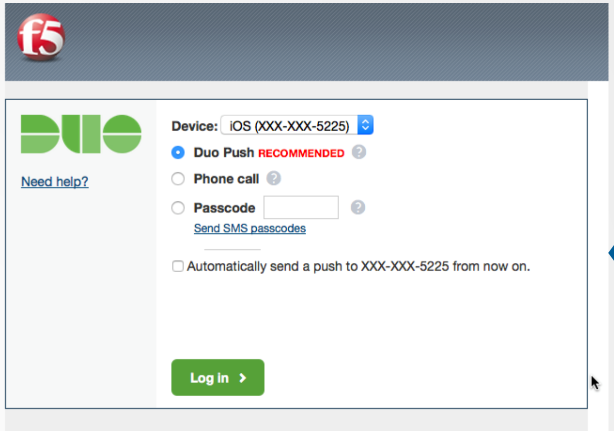
APM’s webtop including app access via identity federation, SSO, and adaptive authentication



Secure Logon
for F5 Networks

Username: m.k[redacted]

Password: •••••••••



Device: iOS (XXX-XXX-5225)

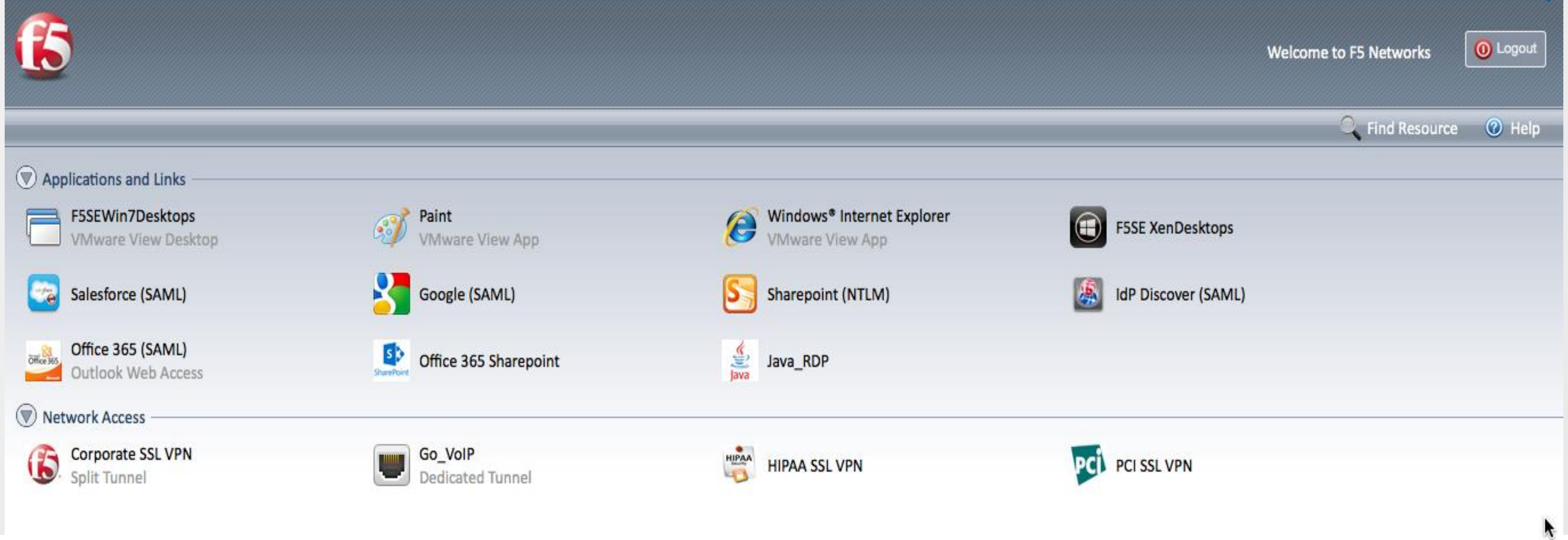
● Duo Push RECOMMENDED

○ Phone call

○ Passcode

Send SMS passcodes

□ Automatically send a push to XXX-XXX-5225 from now on.



Applications and Links

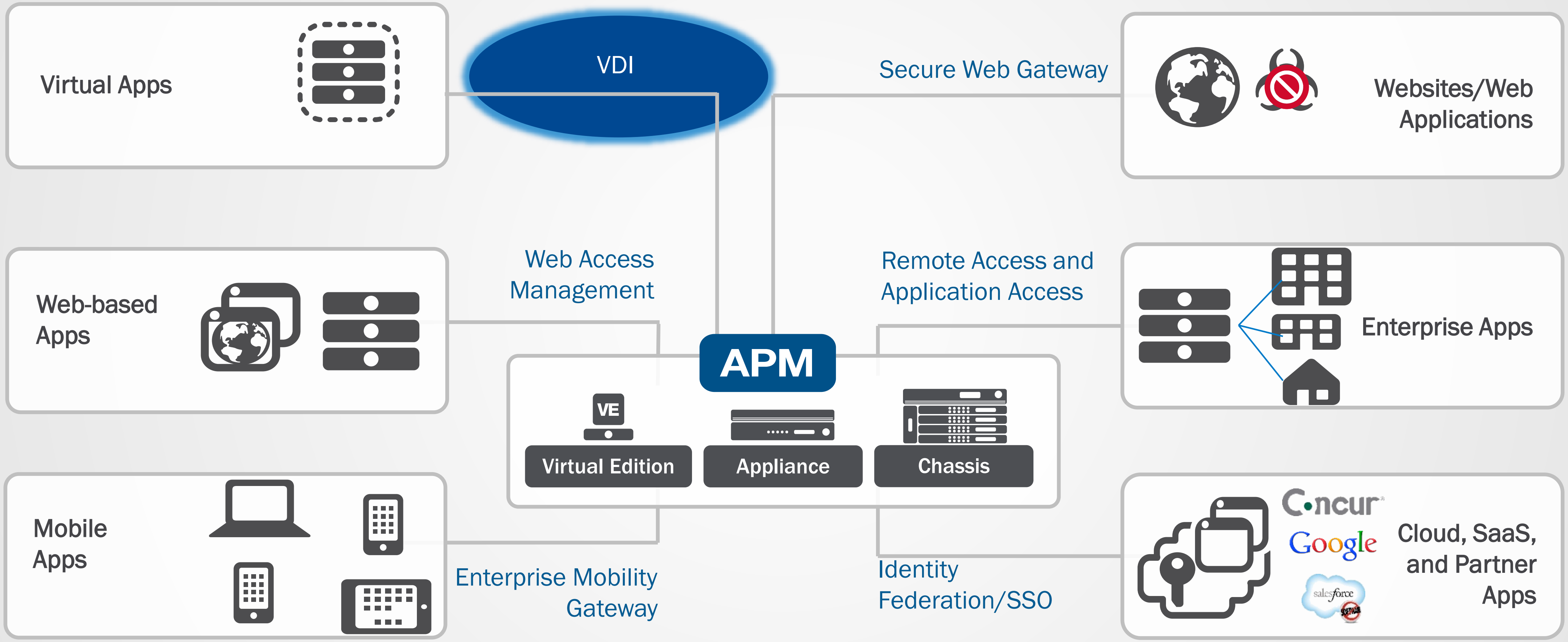
F5SEWin7Desktops VMware View Desktop	Paint VMware View App	Windows® Internet Explorer VMware View App	F5SE XenDesktops
Salesforce (SAML)	Google (SAML)	Sharepoint (NTLM)	IdP Discover (SAML)
Office 365 (SAML) Outlook Web Access	Office 365 Sharepoint	Java_RDP	

Network Access

Corporate SSL VPN Split Tunnel	Go_VoIP Dedicated Tunnel	HIPAA SSL VPN	PCI SSL VPN

Simplify VDI

F5 BIG-IP Access Policy Manager Drives Identity Federation, Single Sign On, and Adaptive Authentication



Virtual Apps

VDI

Secure Web Gateway

Websites/Web Applications

Web-based Apps

Web Access Management

Remote Access and Application Access

Enterprise Apps

APM

Virtual Edition

Appliance

Chassis

Mobile Apps

Enterprise Mobility Gateway

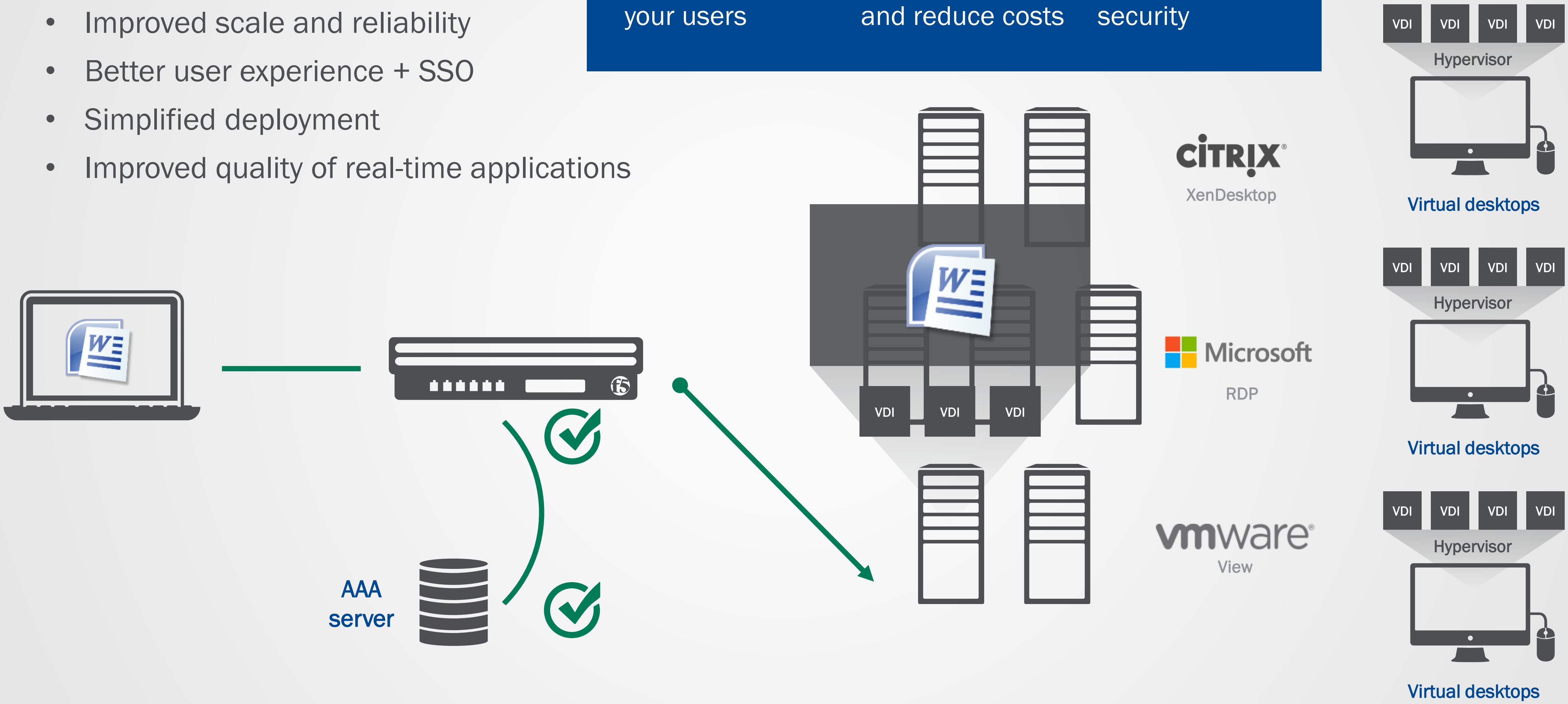
Identity Federation/SSO

Cloud, SaaS, and Partner Apps

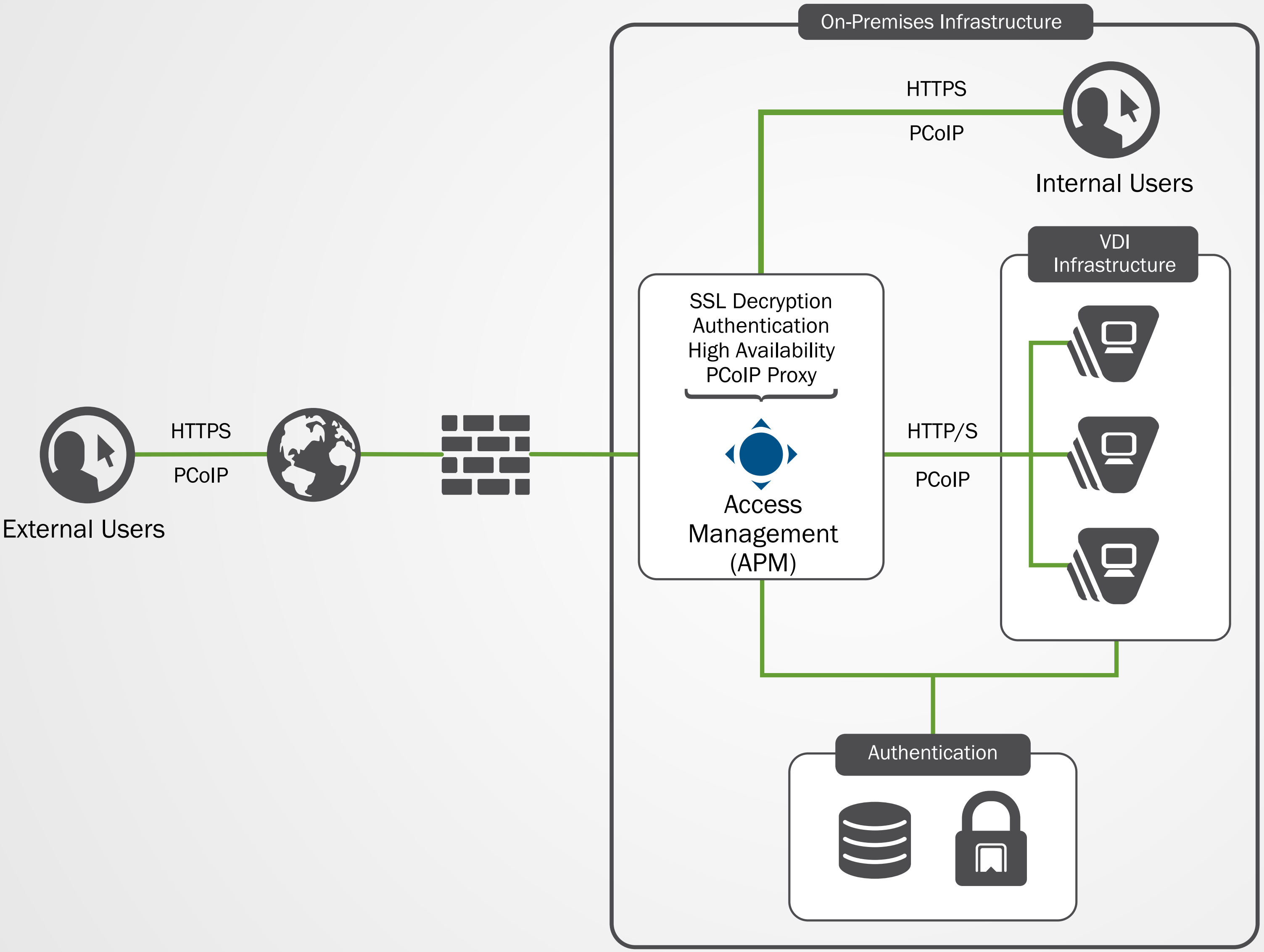
Simplified VDI

- Improved scale and reliability
- Better user experience + SSO
- Simplified deployment
- Improved quality of real-time applications

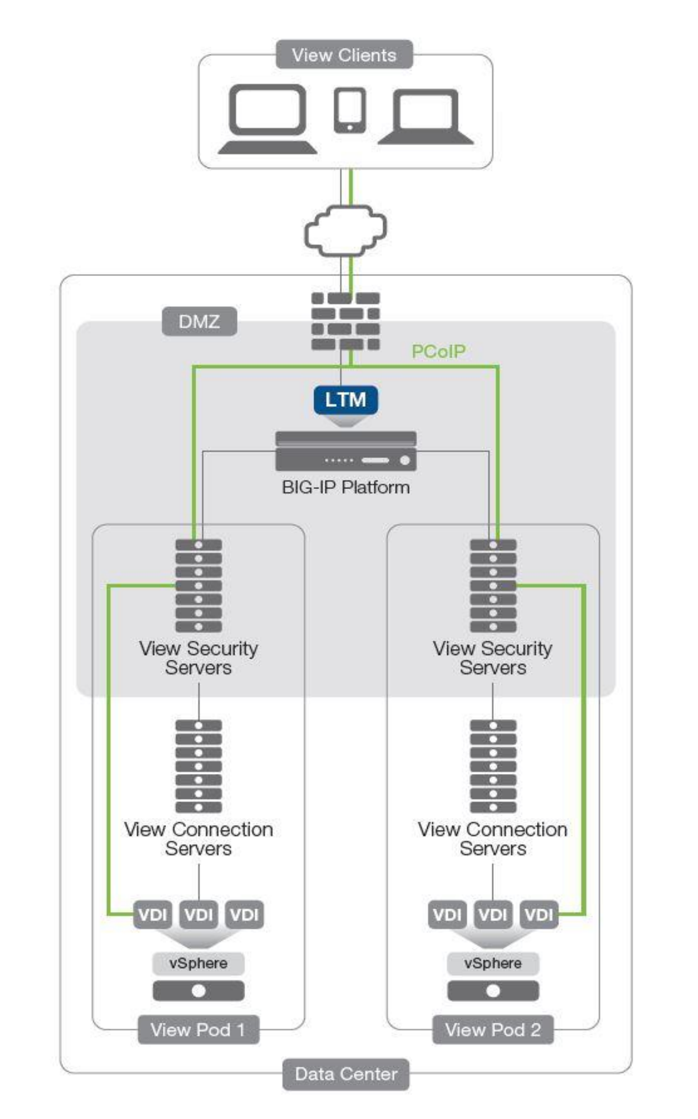
- Optimize the experience for your users
- Simplify infrastructure and reduce costs
- Unify access control and security

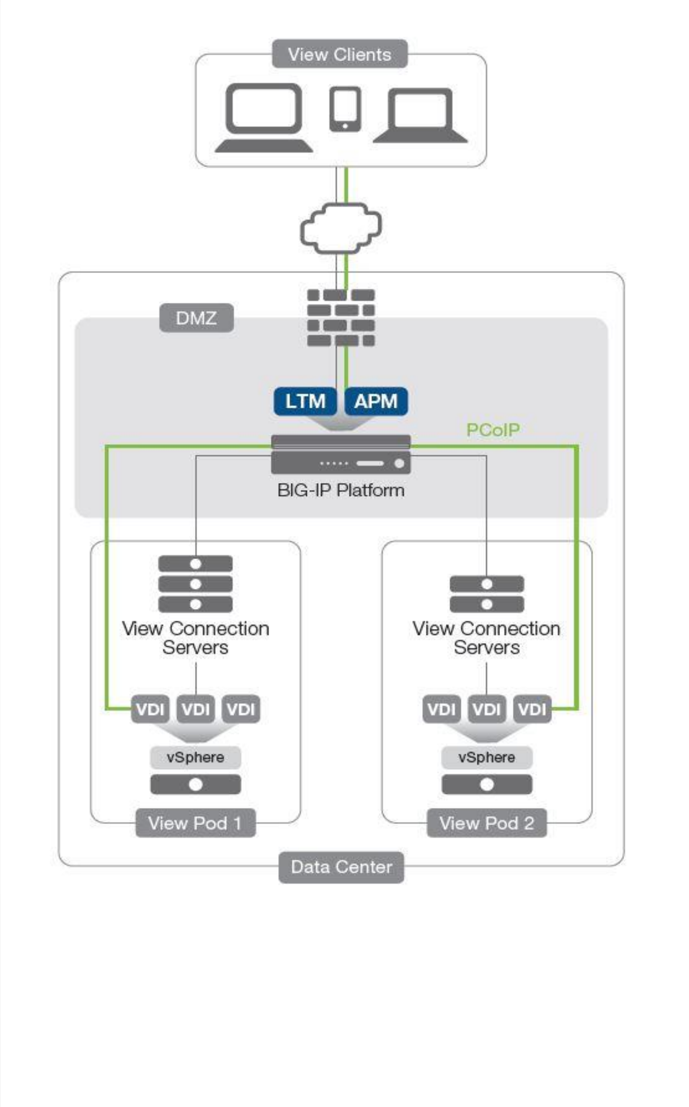


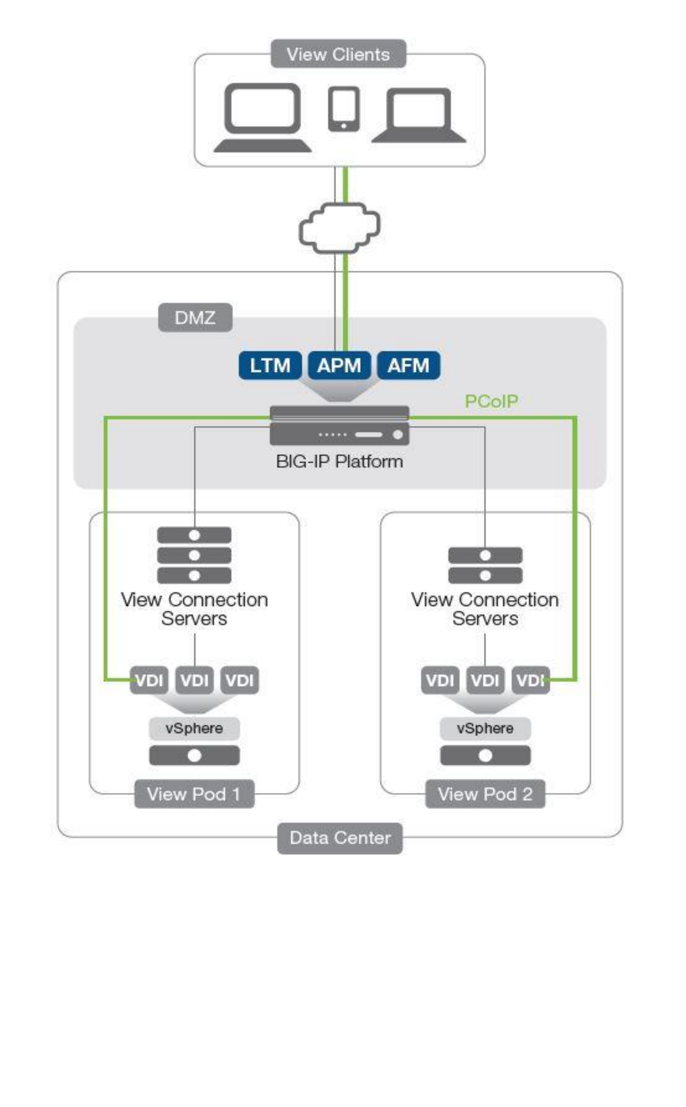
VMware Horizon View architecture



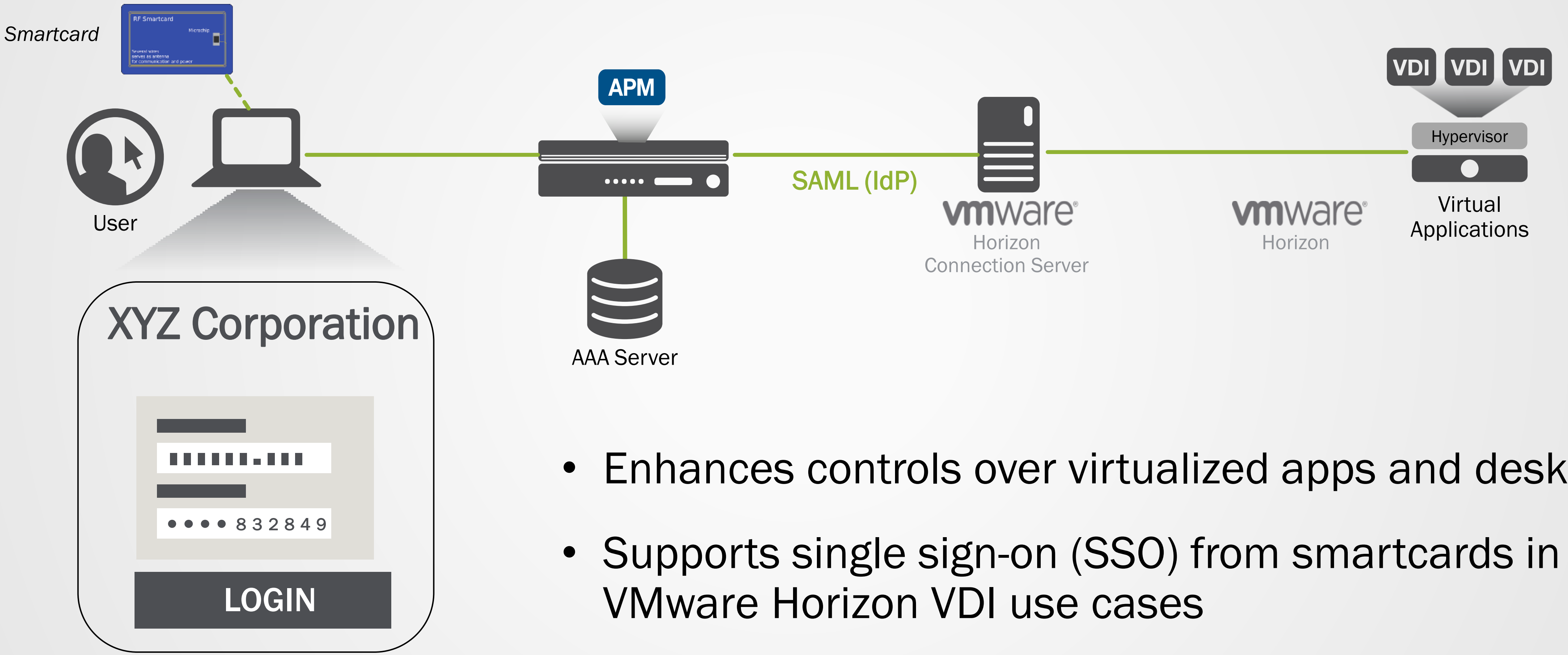
PCoIP Proxy – Simplify your architecture







Smartcard Single Sign-On (SSO) Support for VMware Horizon PCoIP Proxy

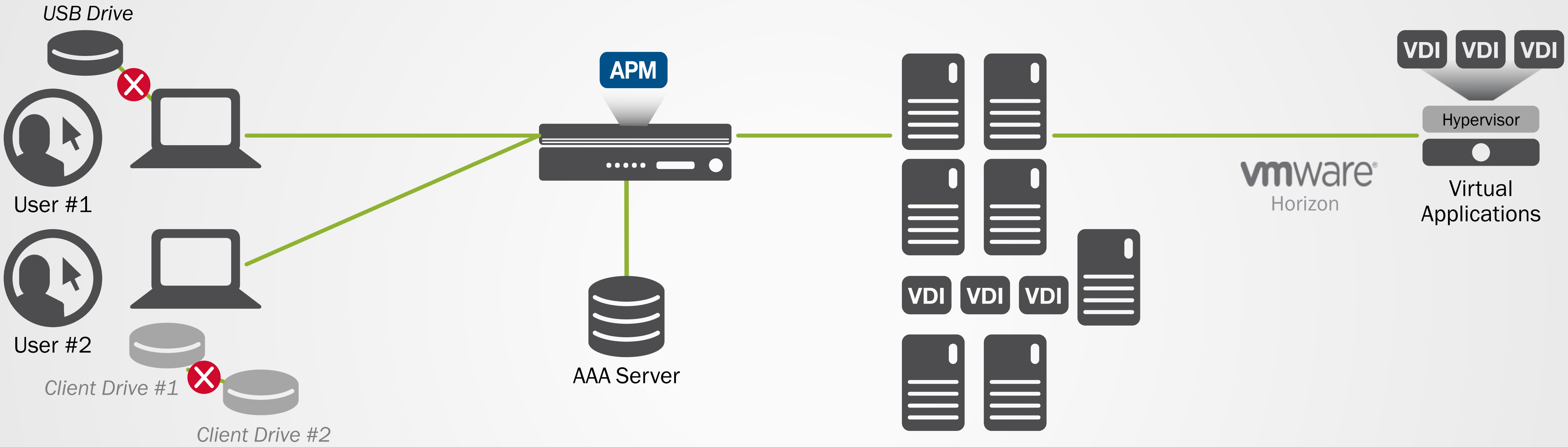


Two-factor authentication

- RSA SecurID
- RADIUS

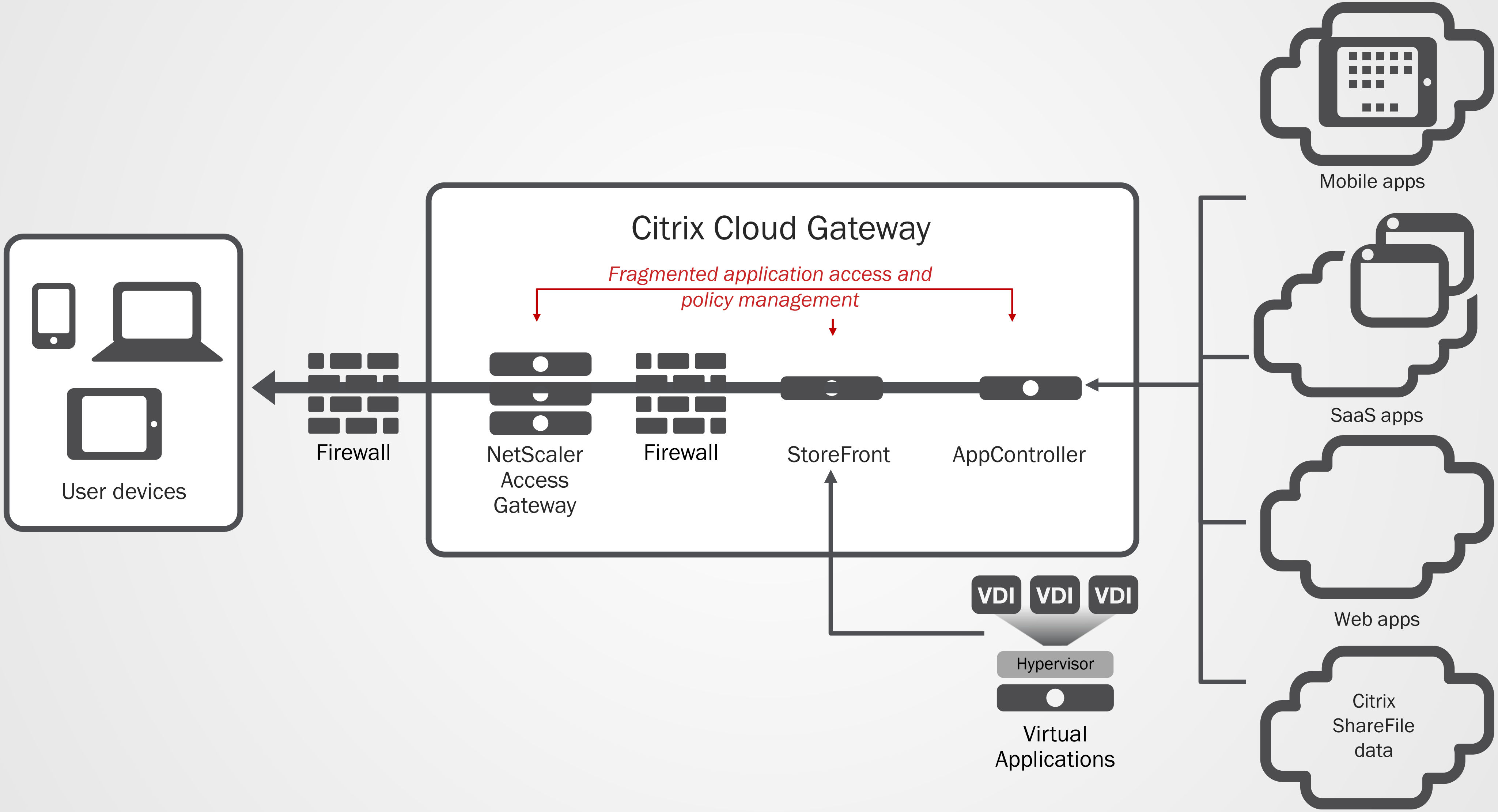
- Enhances controls over virtualized apps and desktops
- Supports single sign-on (SSO) from smartcards in VMware Horizon VDI use cases
- Enables two-factor authentication with RSA SecurID and RADIUS

Support and Control USB Redirection and Client Drive Mapping for VMware Horizon



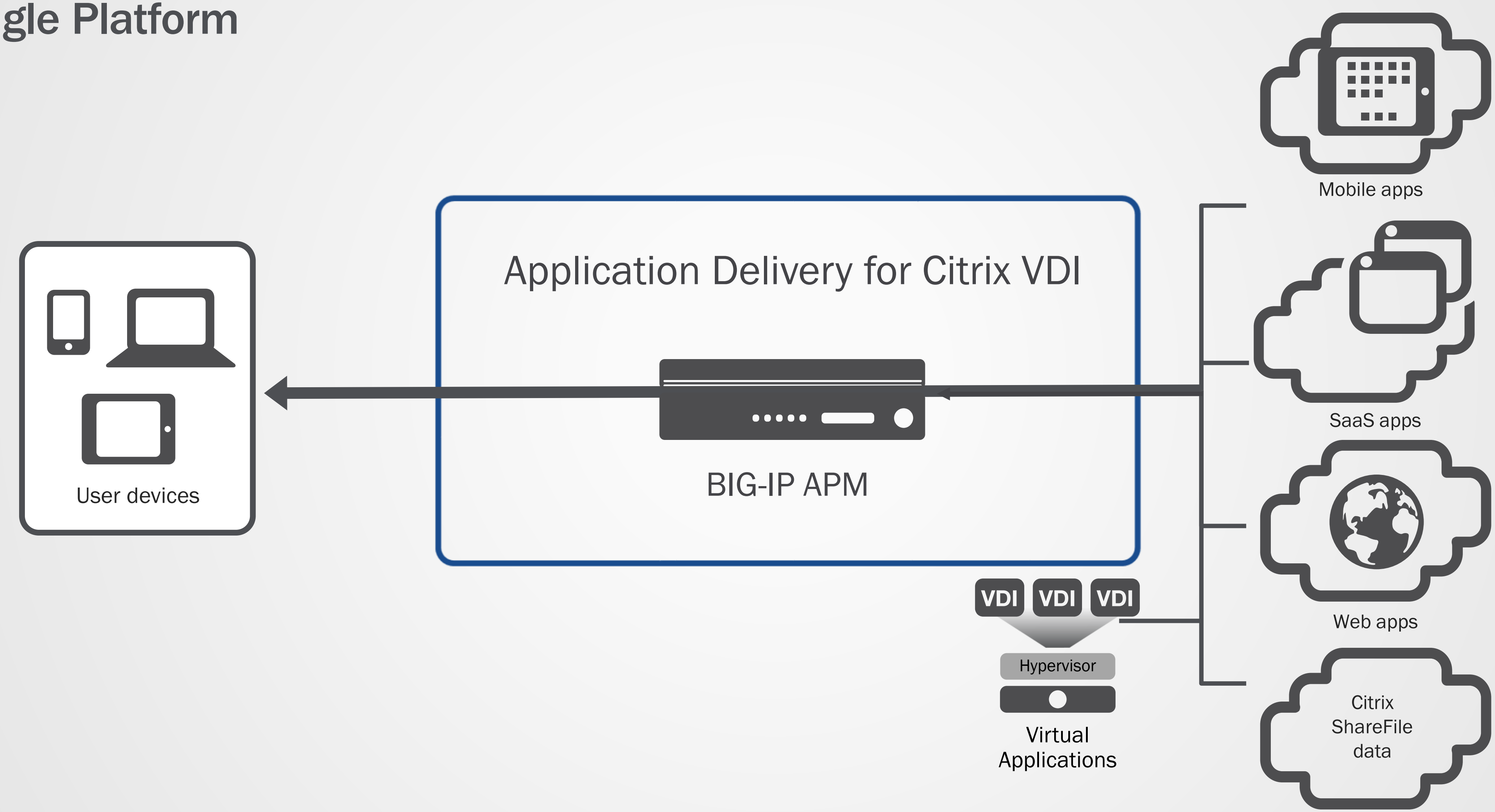
- Mitigates and protects against data loss for managed accounts and devices
- Empowers control – via identity-aware, context-based policies – over the use of USB devices by VMware Horizon users and their devices
- Also enables identity-aware, context-based control over client drive redirection for VMware Horizon users

Operational complexities of Citrix Cloud Gateway



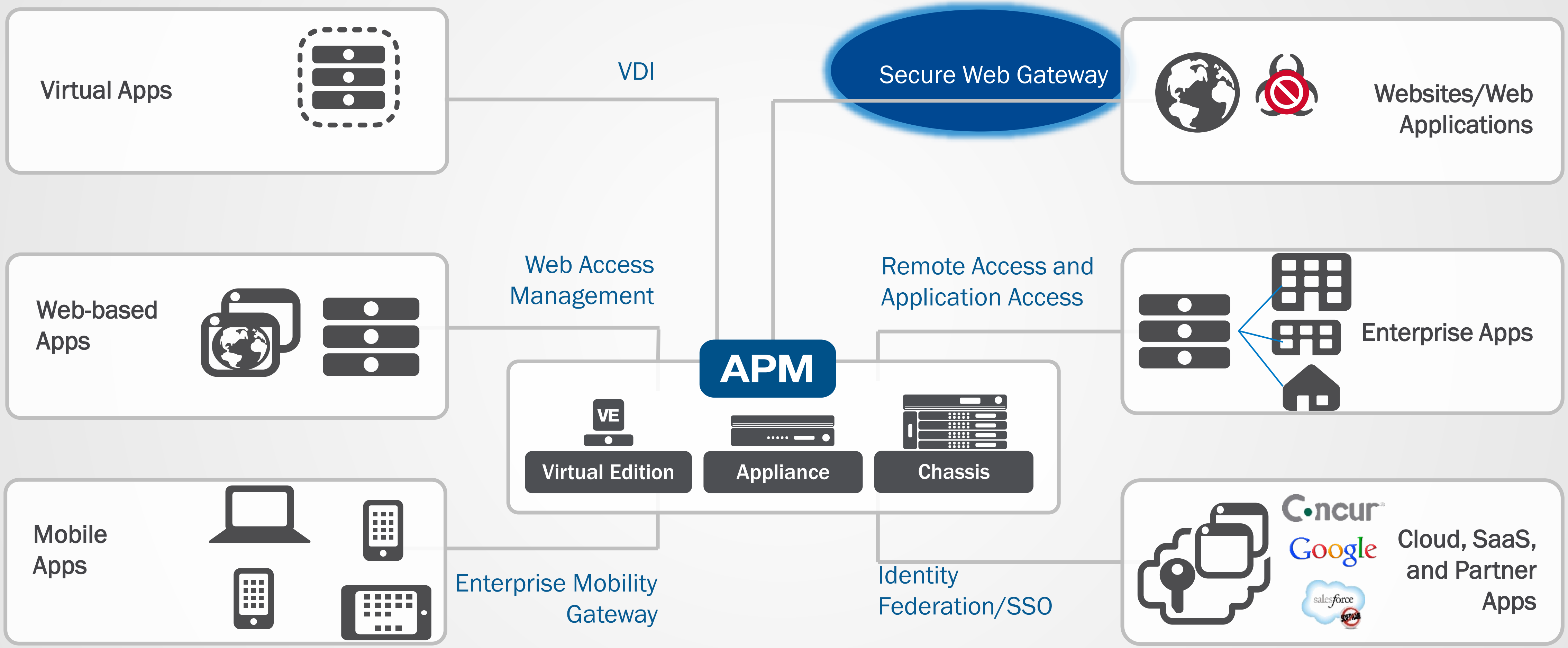
Application delivery for Citrix VDI

Single Platform



Secure Web Gateway

F5 BIG-IP Access Policy Manager Drives Identity Federation, Single Sign On, and Adaptive Authentication



Web access is a necessary part of an employee’s day

Washington, DC To New York, NY   Feb 7 - Feb 10

Print / E-mail

Click on a column, row, or cell in the grid below to filter your results.

Hide matrix

All 100 results	Delta	United	Continental	Multiple Carriers	US Airways	American	Frontier	Midwest Airline
Nonstop 64 results	268.37 20 results	273.40 20 results	--	--	273.40 24 results	--	--	--
1 stop 36 results	--	--	150.80 1 results	212.10 13 results	--	402.80 20 results	417.80 1 results	417.8 1 resul

Displaying: 100 out of 100 results. The least cost item is: 150.80 Baggage Fee Policies

<<Previous | Page: 1 of 10 | Next>> | Al

Sort: ● Policy ○ Price ○ Carrier ○ Depart ○ Duration ○ Emissions

Carrier	Depart	Arrive	Duration	Emissions	Class
Delta 5904	Feb 7 7:30am Washington, DC (DCA)	Feb 7 8:33am New York, NY (LGA)	Stops: 0 1h 3m	135.2 lbs CO2	Embraer E-175 Economy: T

So, web defense is a necessity today

Security
Against web-based threats and malware

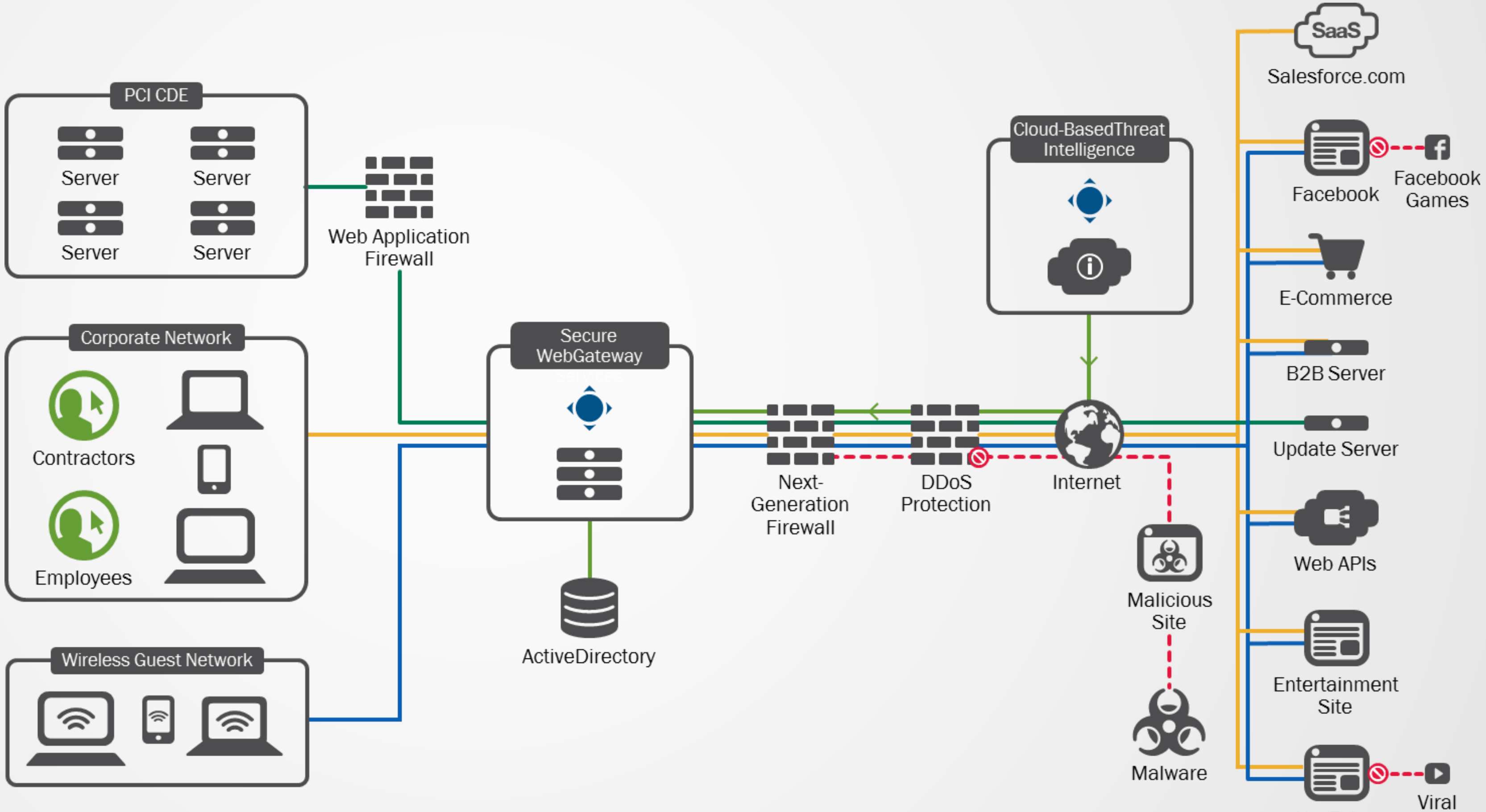
Productivity
Controlling access to time-wasting web sites

Accessibility
Managing web access and bandwidth allocation

Compliance
With corporate acceptable use policies (AUP) and regulatory policies

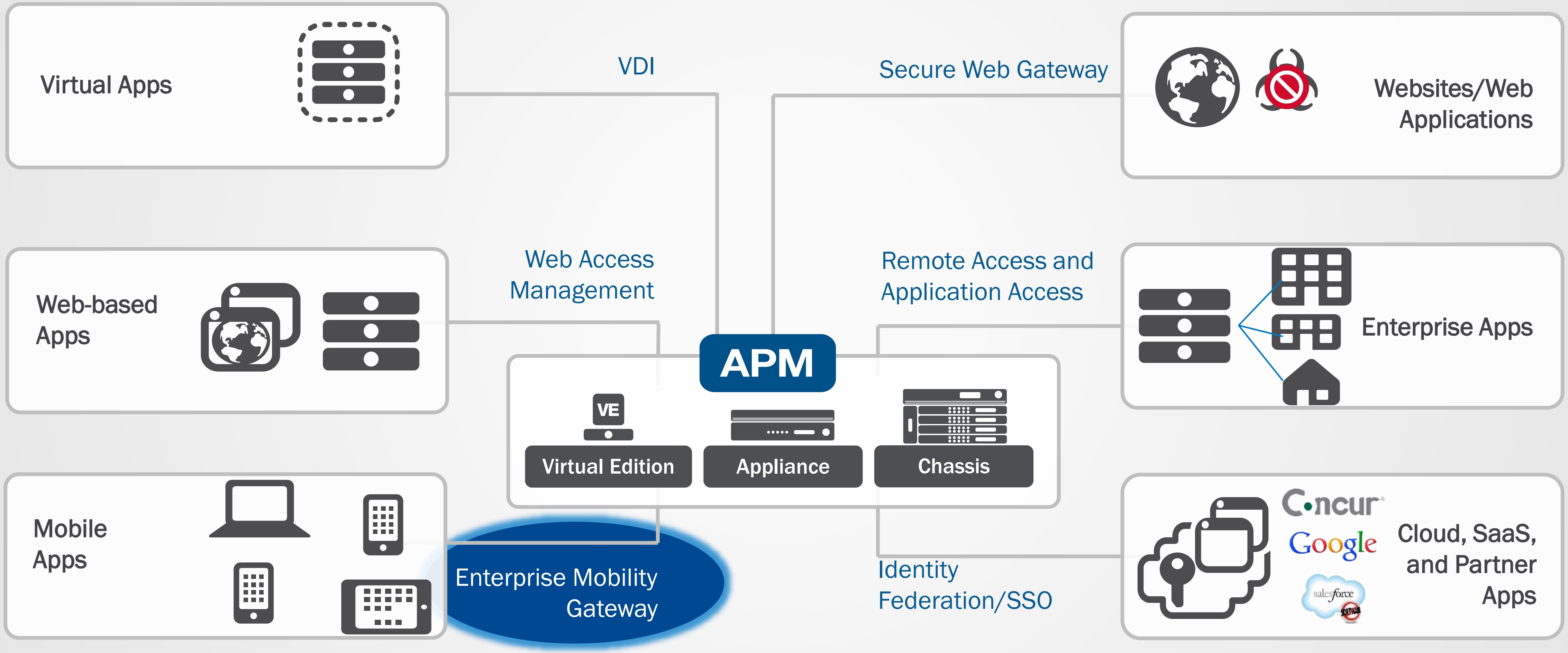
F5’s high-performance, on-premises secure web gateway

- URL categorization and filtering
- Web application controls
- Advanced web-based and embedded malware protection
- Fast SSL inspections and bypass
- Fast and effective threat detection *(based on Websense ThreatSeeker)*
- Detailed reporting and logging



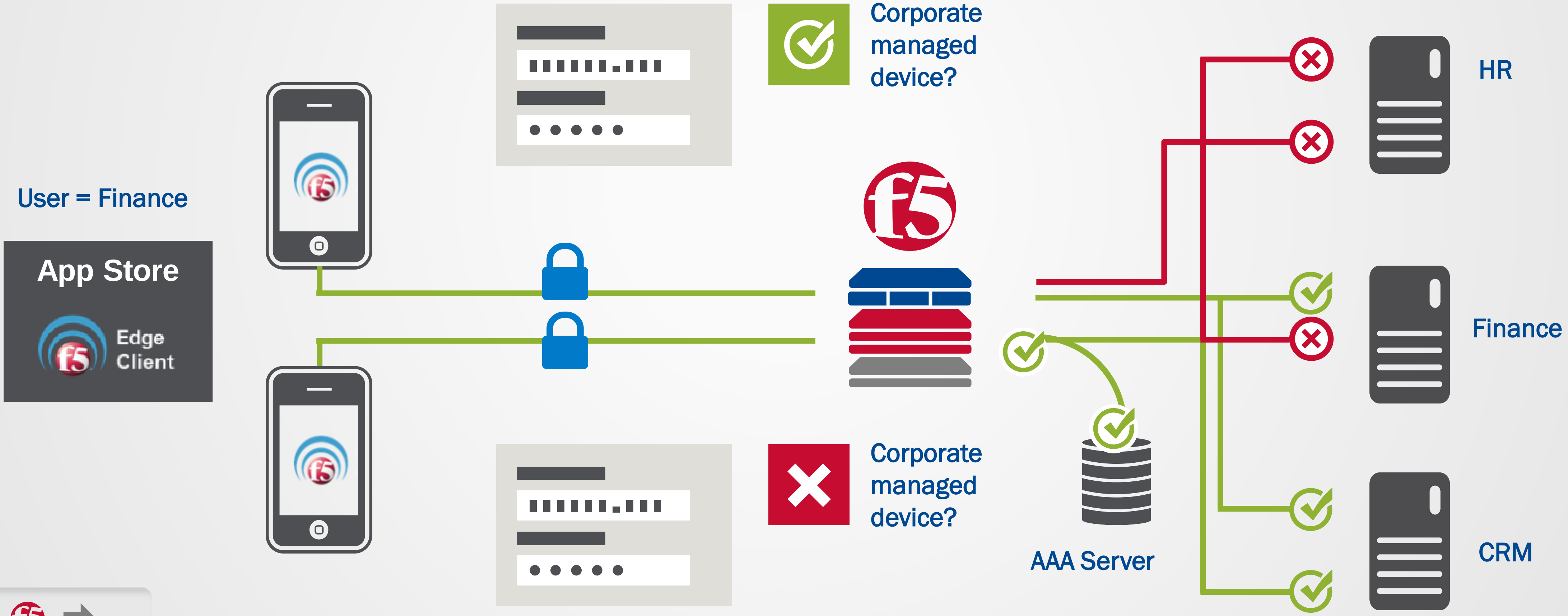
Enterprise Mobility Management (EMM)

F5 BIG-IP Access Policy Manager Drives Identity Federation, Single Sign On, and Adaptive Authentication

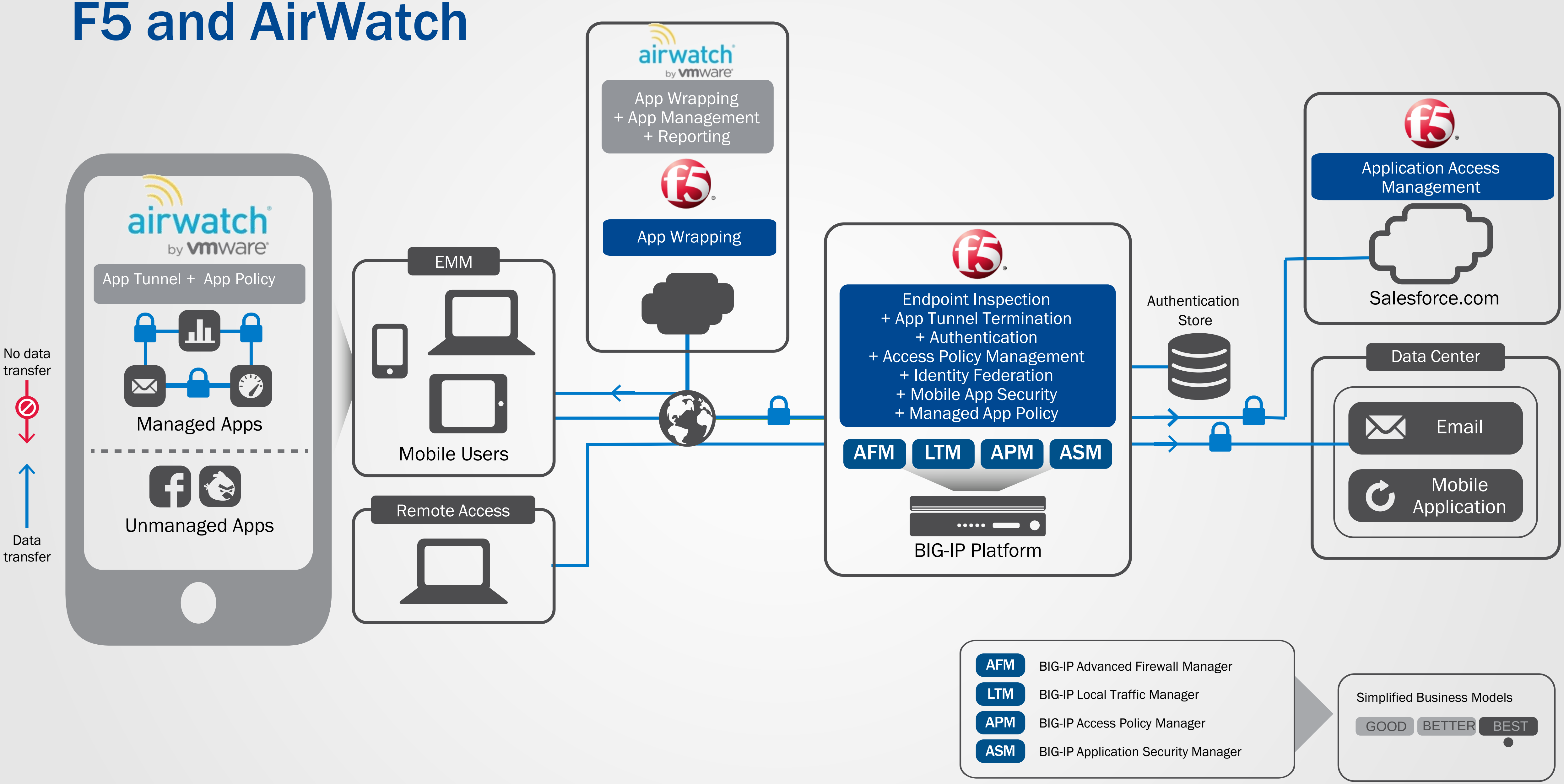


Enterprise Mobility Management (EMM)

- Ensure devices connect securely and adhere to a security posture baseline, regardless of ownership
- Reduce the risk of malware infecting the corporate network from corporate or personal mobile device



F5 and AirWatch



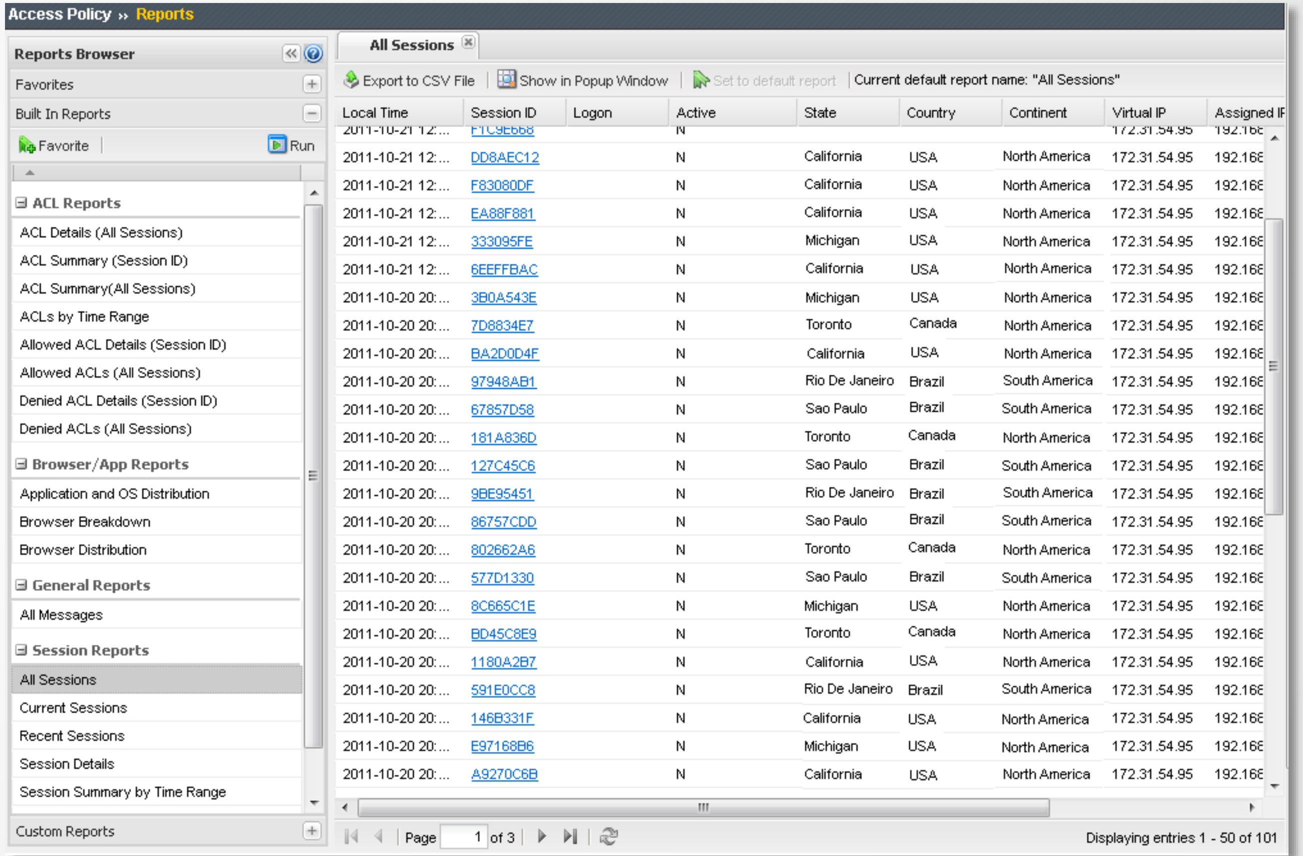
AFM	BIG-IP Advanced Firewall Manager
LTM	BIG-IP Local Traffic Manager
APM	BIG-IP Access Policy Manager
ASM	BIG-IP Application Security Manager

Reporting

Sample detailed report

Gain a deeper understanding of:

- All sessions with geo-location
- Local time
- Virtual IP
- Assigned IP
- ACLs
- Applications and OSs
- Browsers
- All sessions
- Customize reports
- Export for distribution



Current default report name: "All Sessions"

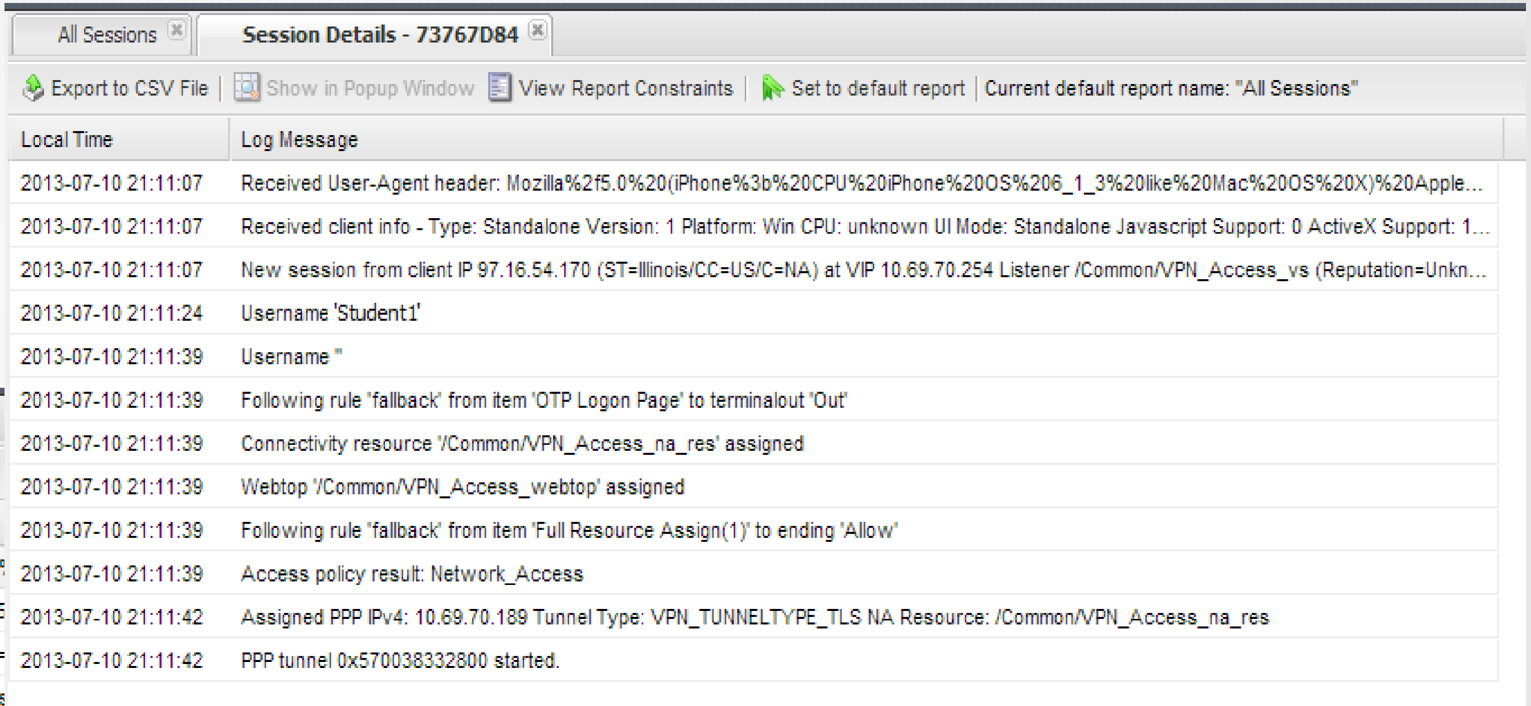
Local Time	Session ID	Logon	Active	State	Country	Continent	Virtual IP	Assigned IP
2011-10-21 12:...	F1C9E668		N				172.31.54.95	192.168
2011-10-21 12:...	DD8AEC12		N	California	USA	North America	172.31.54.95	192.168
2011-10-21 12:...	F83080DF		N	California	USA	North America	172.31.54.95	192.168
2011-10-21 12:...	EA88F881		N	California	USA	North America	172.31.54.95	192.168
2011-10-21 12:...	333095FE		N	Michigan	USA	North America	172.31.54.95	192.168
2011-10-21 12:...	6EEFFBAC		N	California	USA	North America	172.31.54.95	192.168
2011-10-20 20:...	3B0A543E		N	Michigan	USA	North America	172.31.54.95	192.168
2011-10-20 20:...	7D8834E7		N	Toronto	Canada	North America	172.31.54.95	192.168
2011-10-20 20:...	BA2D0D4F		N	California	USA	North America	172.31.54.95	192.168
2011-10-20 20:...	97948AB1		N	Rio De Janeiro	Brazil	South America	172.31.54.95	192.168
2011-10-20 20:...	67857D58		N	Sao Paulo	Brazil	South America	172.31.54.95	192.168
2011-10-20 20:...	181A836D		N	Toronto	Canada	North America	172.31.54.95	192.168
2011-10-20 20:...	127C45C6		N	Sao Paulo	Brazil	South America	172.31.54.95	192.168
2011-10-20 20:...	9BE95451		N	Rio De Janeiro	Brazil	South America	172.31.54.95	192.168
2011-10-20 20:...	86757CDD		N	Sao Paulo	Brazil	South America	172.31.54.95	192.168
2011-10-20 20:...	802662A6		N	Toronto	Canada	North America	172.31.54.95	192.168
2011-10-20 20:...	577D1330		N	Sao Paulo	Brazil	South America	172.31.54.95	192.168
2011-10-20 20:...	8C665C1E		N	Michigan	USA	North America	172.31.54.95	192.168
2011-10-20 20:...	BD45C8E9		N	Toronto	Canada	North America	172.31.54.95	192.168
2011-10-20 20:...	1180A2B7		N	California	USA	North America	172.31.54.95	192.168
2011-10-20 20:...	591E0CC8		N	Rio De Janeiro	Brazil	South America	172.31.54.95	192.168
2011-10-20 20:...	146B331F		N	California	USA	North America	172.31.54.95	192.168
2011-10-20 20:...	E97168B6		N	Michigan	USA	North America	172.31.54.95	192.168
2011-10-20 20:...	A9270C6B		N	California	USA	North America	172.31.54.95	192.168

Page 1 of 3

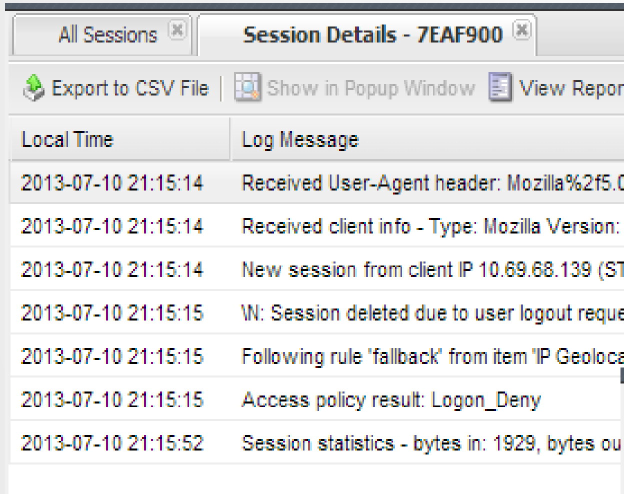
Displaying entries 1 - 50 of 101

Reporting in APM

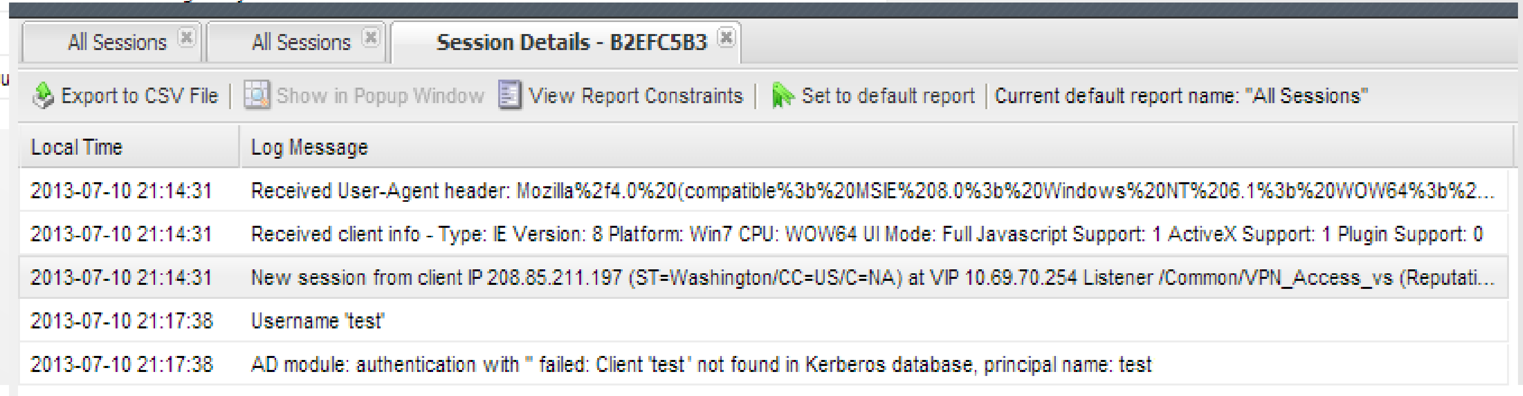
Clicking on individual Session IDs shows the flow of VPE actions



Local Time	Log Message
2013-07-10 21:11:07	Received User-Agent header: Mozilla%2f5.0%20(iPhone%3b%20CPU%20iPhone%20OS%206_1_3%20like%20Mac%20OS%20X)%20Apple...
2013-07-10 21:11:07	Received client info - Type: Standalone Version: 1 Platform: Win CPU: unknown UI Mode: Standalone Javascript Support: 0 ActiveX Support: 1...
2013-07-10 21:11:07	New session from client IP 97.16.54.170 (ST=Illinois/CC=US/C=NA) at VIP 10.69.70.254 Listener /Common/VPN_Access_vs (Reputation=Unkn...
2013-07-10 21:11:24	Username 'Student1'
2013-07-10 21:11:39	Username ''
2013-07-10 21:11:39	Following rule 'fallback' from item 'OTP Logon Page' to terminalout 'Out'
2013-07-10 21:11:39	Connectivity resource '/Common/VPN_Access_na_res' assigned
2013-07-10 21:11:39	Webtop '/Common/VPN_Access_webtop' assigned
2013-07-10 21:11:39	Following rule 'fallback' from item 'Full Resource Assign(1)' to ending 'Allow'
2013-07-10 21:11:39	Access policy result: Network_Access
2013-07-10 21:11:42	Assigned PPP IPv4: 10.69.70.189 Tunnel Type: VPN_TUNNELTYPE_TLS NA Resource: /Common/VPN_Access_na_res
2013-07-10 21:11:42	PPP tunnel 0x570038332800 started.



Local Time	Log Message
2013-07-10 21:15:14	Received User-Agent header: Mozilla%2f5.0%
2013-07-10 21:15:14	Received client info - Type: Mozilla Version: 5
2013-07-10 21:15:14	New session from client IP 10.69.68.139 (ST=
2013-07-10 21:15:15	\N: Session deleted due to user logout reques
2013-07-10 21:15:15	Following rule 'fallback' from item 'IP Geolocation Match' to ending 'Deny'
2013-07-10 21:15:15	Access policy result: Logon_Deny
2013-07-10 21:15:52	Session statistics - bytes in: 1929, bytes ou

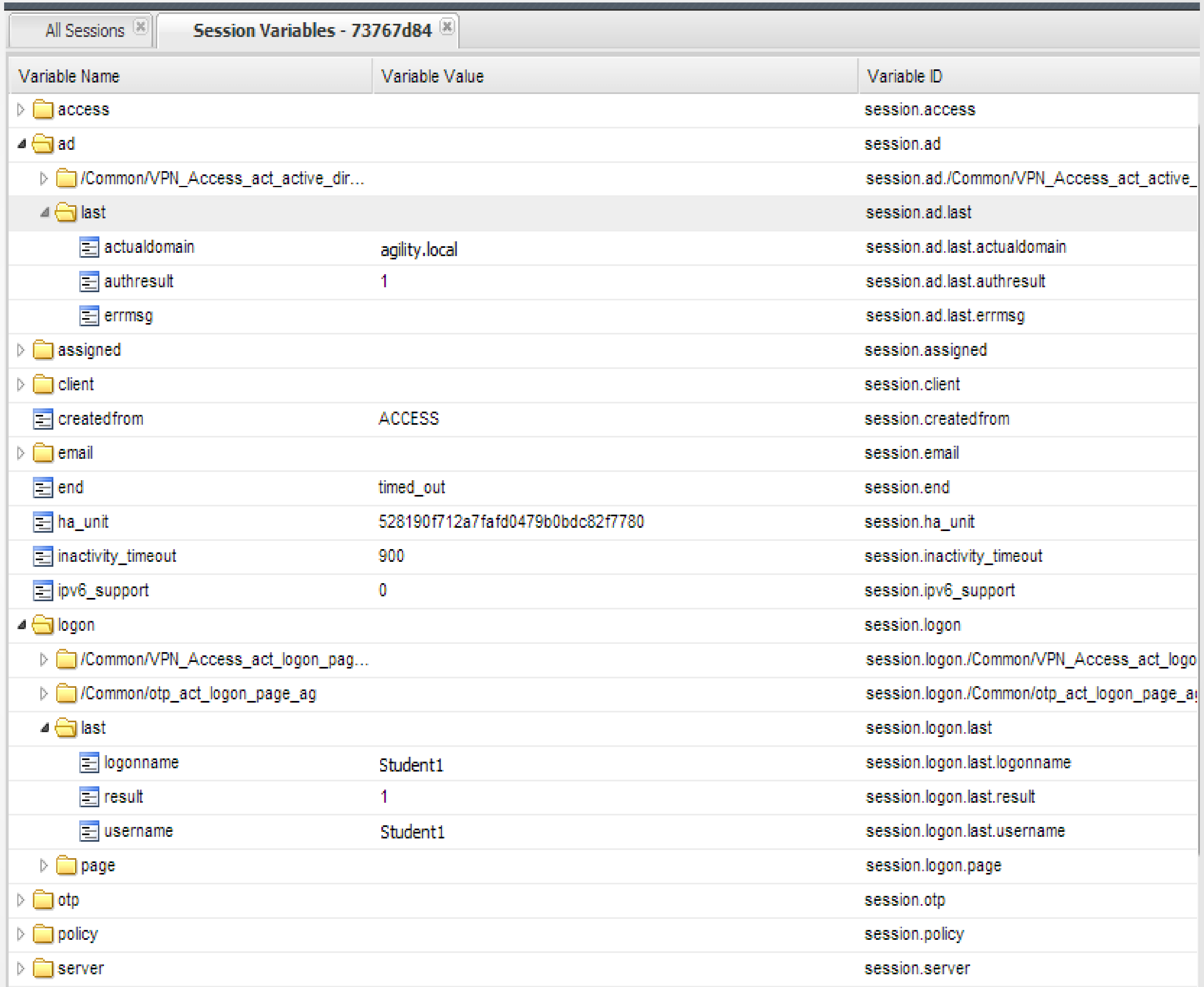


Local Time	Log Message
2013-07-10 21:14:31	Received User-Agent header: Mozilla%2f4.0%20(compatible%3b%20MSIE%208.0%3b%20Windows%20NT%206.1%3b%20WOW64%3b%2...
2013-07-10 21:14:31	Received client info - Type: IE Version: 8 Platform: Win7 CPU: WOW64 UI Mode: Full Javascript Support: 1 ActiveX Support: 1 Plugin Support: 0
2013-07-10 21:14:31	New session from client IP 208.85.211.197 (ST=Washington/CC=US/C=NA) at VIP 10.69.70.254 Listener /Common/VPN_Access_vs (Reputati...
2013-07-10 21:17:38	Username 'test'
2013-07-10 21:17:38	AD module: authentication with '' failed: Client 'test' not found in Kerberos database, principal name: test

Reporting in APM

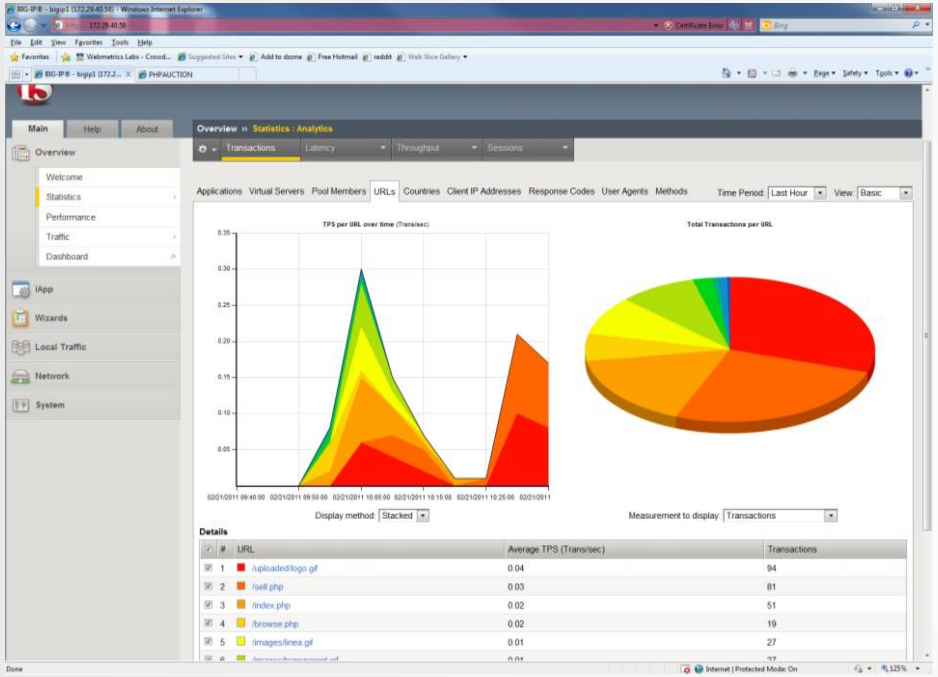
Clicking on “View Session Variables” shows per-session
variables populated during the user’s logon attempt

- AD results
- Antivirus info
- Browser info
- Resources assigned
- Mobile info
- Cert info
- Etc Etc Etc



Variable Name	Variable Value	Variable ID
access		session.access
ad		session.ad
/Common/VPN_Access_act_active_dir...		session.ad./Common/VPN_Access_act_active_
last		session.ad.last
actualdomain	agility.local	session.ad.last.actualdomain
authresult	1	session.ad.last.authresult
errmsg		session.ad.last.errmsg
assigned		session.assigned
client		session.client
createdfrom	ACCESS	session.createdfrom
email		session.email
end	timed_out	session.end
ha_unit	528190f712a7fafd0479b0bdc82f7780	session.ha_unit
inactivity_timeout	900	session.inactivity_timeout
ipv6_support	0	session.ipv6_support
logon		session.logon
/Common/VPN_Access_act_logon_pag...		session.logon./Common/VPN_Access_act_logo
/Common/otp_act_logon_page_ag		session.logon./Common/otp_act_logon_page_a
last		session.logon.last
logonname	Student1	session.logon.last.logonname
result	1	session.logon.last.result
username	Student1	session.logon.last.username
page		session.logon.page
otp		session.otp
policy		session.policy
server		session.server

Access and application analytics



Time Period: Last Hour

View: Basic

Display method: Stacked

Measurement to display: Transactions

Details

☑	#	URL	Average TPS (Trans/sec)	Transactions
☑	1	🟥 /uploaded/logo.gif	0.04	94
☑	2	🟧 /sell.php	0.03	81
☑	3	🟧 /index.php	0.02	51
☑	4	🟨 /browse.php	0.02	19
☑	5	🟨 /images/linea.gif	0.01	27
☑	6	🟩 [illegible]	0.01	27

Stats grouped by application and user

Provides:

- Business intelligence
- ROI reporting
- Capacity planning
- Troubleshooting
- Performance

Stats collected

- Client IPs
- Client geographic
- User agent
- User sessions
- Client-side latency
- Server latency
- Throughput
- Response codes
- Methods
- URLs

Views

- Virtual server
- Pool member
- Response codes
- URL
- HTTP methods

Summary

Solution Summary

Unified Access solution

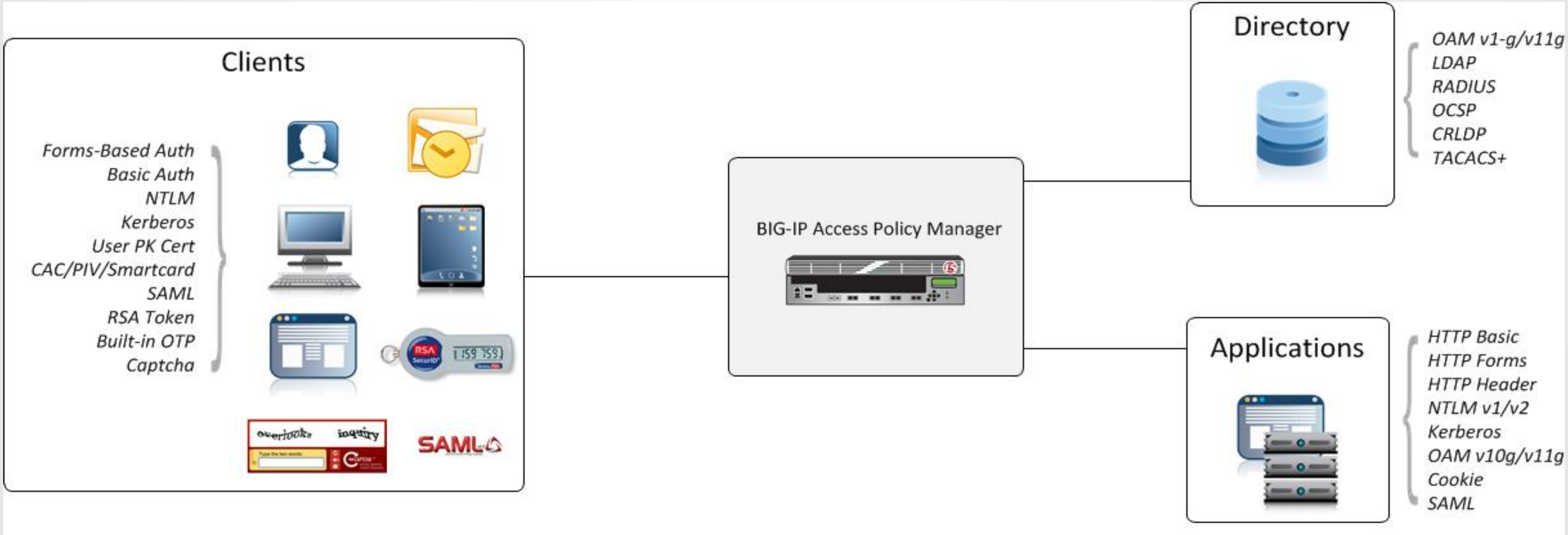
- ✓ Managing mobile applications & devices
  - Support BYOD initiatives
- ✓ Securing Web usage
  - Reduces malware risks
- ✓ Federating identity
  - Instantly provisions/deprovisions access to SaaS apps
- ✓ Secure accelerated remote access
  - Fast and safe remote connections

Authentication All in One and Fast SSO

F5 BIG-IP Access Policy Manager

- APM is more than a remote access product
- APM benefits any application with a web front-end requiring authentication

- Many customers have a remote access product
- But few have good flexible web authentication



What makes F5 IAM different

Integrated acceleration

Superior scalability

Native one-time password support

Integrates captured data into enforceable access and security policies

1 Stop

One-stop for all access policy

Solutions for an application world.

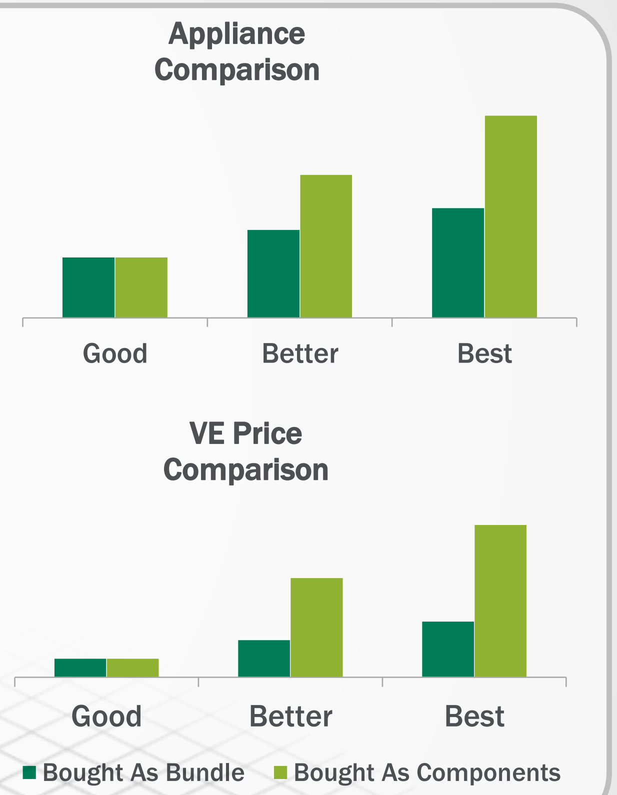
Simplified business models and licensing

New Good, Better, Best (GBB) Bundle Offerings: Delivers greater value and future proofs your datacenter

Benefits

- Make it easier to adopt advanced F5 functionality
- Consolidate into fewer common configurations
- Save when purchasing bundles

GBB Capabilities			
Modules/Services	**Good**	**Better**	**Best**
BIG-IP Local Traffic Manager	✓	✓	✓
BIG-IP Global Traffic Manager		✓	✓
Application Acceleration Manager		✓	✓
BIG-IP Advanced Firewall Manager		✓	✓
SDN Service		✓	✓
Advanced Routing		✓	✓
BIG-IP Access Policy Manager			✓
BIG-IP Application Security Manager			✓



Virtual Edition | Appliance | Chassis

Network [Physical • Overlay • SDN]