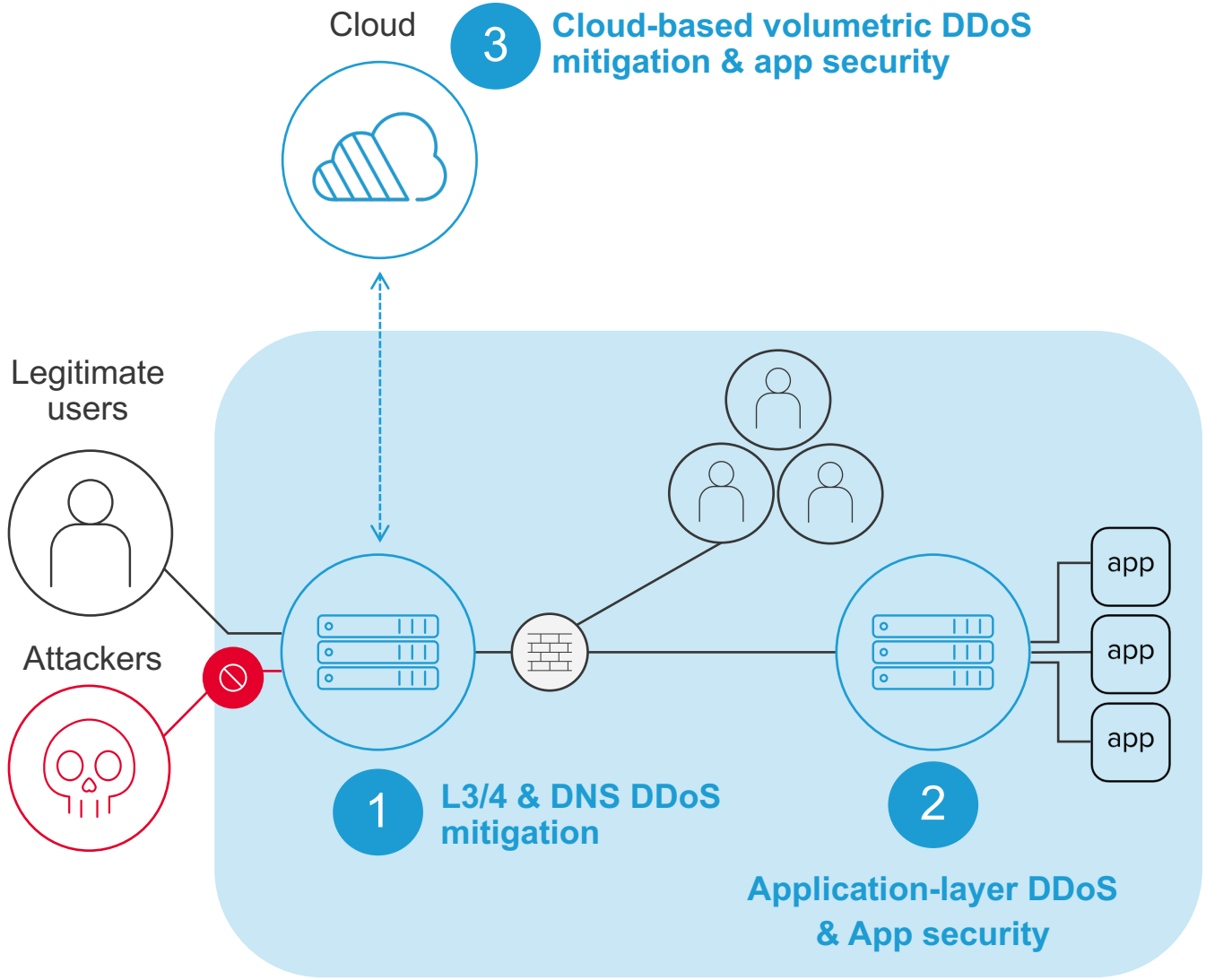
Comprehensive DDoS Protection with F5 Silverline

Managed Service Solution

Martin Oravec
Solutions Engineer, F5

DDoS Mitigation – a Multi-Layered Architecture



1 – Protect the Perimeter

- L3/4 floods and scans
- DNS targeted attacks

2 – Protect the Applications

- Low and Slow attacks
- SSL targeted attacks
- Bot detection techniques

3 – Cloud Scrubbing

- Prevent ”Full Pipe” problem
- L3-7 managed DDoS protection

The Evolution of F5 Silverline

CLOUD-BASED MANAGED SECURITY-AS-A-SERVICE

LAUNCH

2012 – 2014

Defense.net founded as DDoS Protection Service

Acquired by F5

F5 Silverline launched and fully operated by DDoS Security Experts

ENHANCE

2014 – 2018

F5 Technologies integrated into Platform

Improvements to Scale, Performance and Security Services

F5 Silverline Web Application Firewall Service Launched

EVOLVE

2018 – 2020

Cloud-Agile Regional Points of Presence introduced for capacity and global reach

F5 Silverline Shape Defense bot-mitigation service introduced after the acquisition of Shape Security

ADAPT

2021 and beyond

Alignment with F5 Adaptive Apps

Strategic development of SaaS and PaaS service

Silverline &
F5 Distributed Cloud

F5 BIG-IP | **F5 Distributed Cloud Services** | **F5 NGINX**

https://www.f5.com/company/news/press-releases/f5-protection-digital-world-f5-distributed-cloud-services

F5 Silverline Managed Services

Global SOC 24x7x365

Continuous Monitoring and Incident Response

- Seattle, WA, United States
- Warsaw, Poland
- Guadalajara, Mexico

Global Deployment Model

Fully Redundant and Globally Distributed Data Centers

- San Jose, CA, US
- Ashburn, VA, US
- Columbus, OH, US
- Frankfurt, Germany
- London, UK
- Singapore, SG
- Sydney, AU
- Hong Kong, HK
- Mumbai, IN
- Montreal, CA
- São Paulo, BR
- Manama, BH
- Tokyo, JP

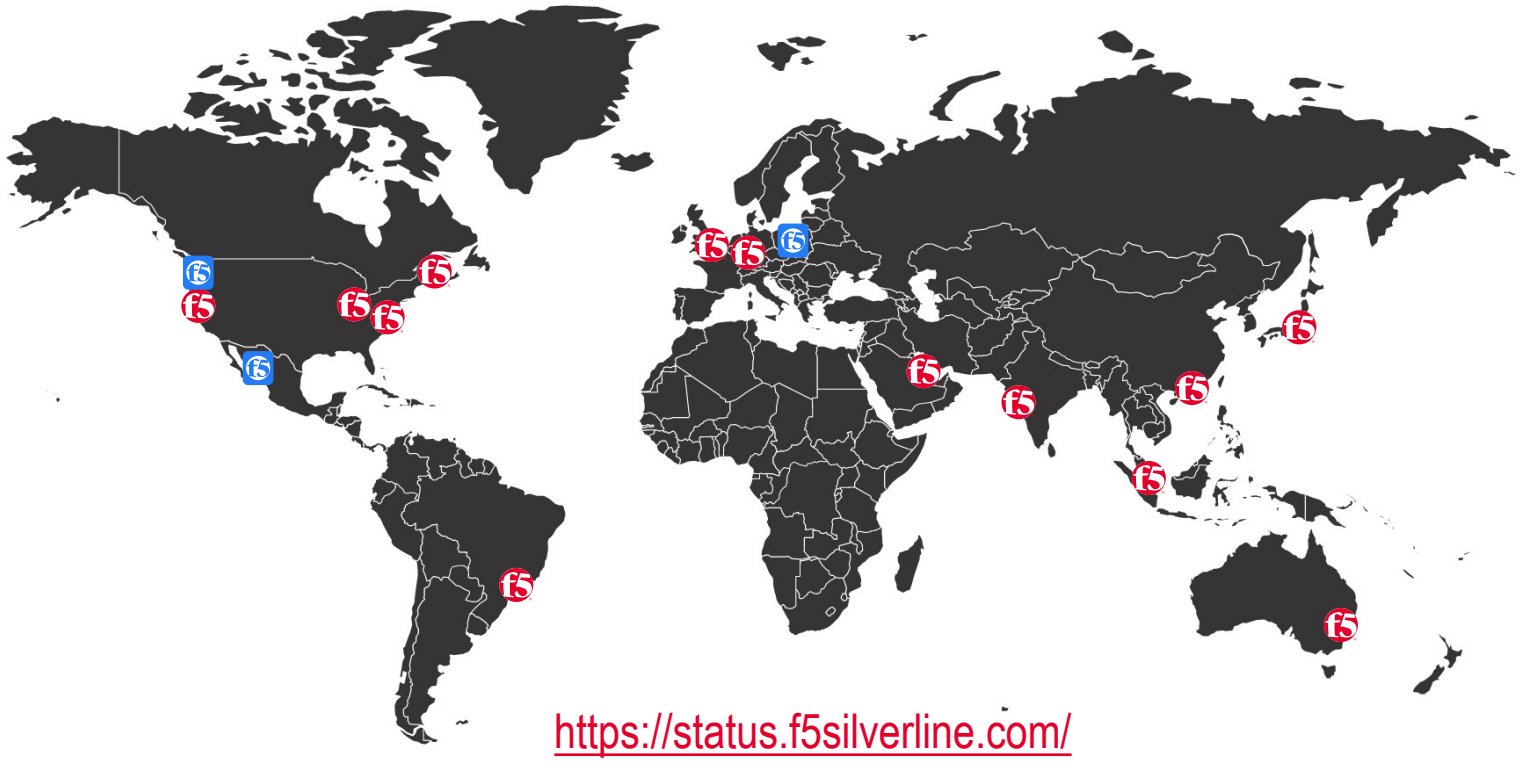
Bandwidth & Capacity

- Attack mitigation capacity over 4.0 Tbps
- Dedicated L3/L4 and L7 scrubbing infrastructures
- Guaranteed bandwidth with Tier 1 carriers and direct public clouds peering (Azure, AWS, GCP)

HIPAA Compliant

PCI DSS COMPLIANT

EQUINIX



https://status.f5silverline.com/

SOC Locations

Active PoP's

F5 Silverline Managed Security Services

DRIVE GREATER EFFICACY OF THREAT MITIGATION

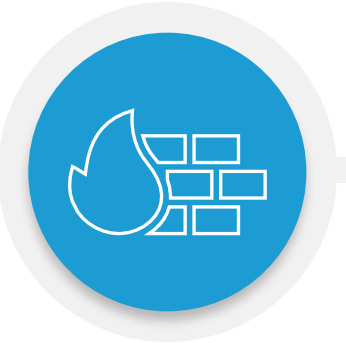
F5 Silverline Security Operations Centers

Silverline DDoS Protection

Defend against Denial of Service attacks

Silverline Shape Defense

Mitigate against Bots and automated attacks

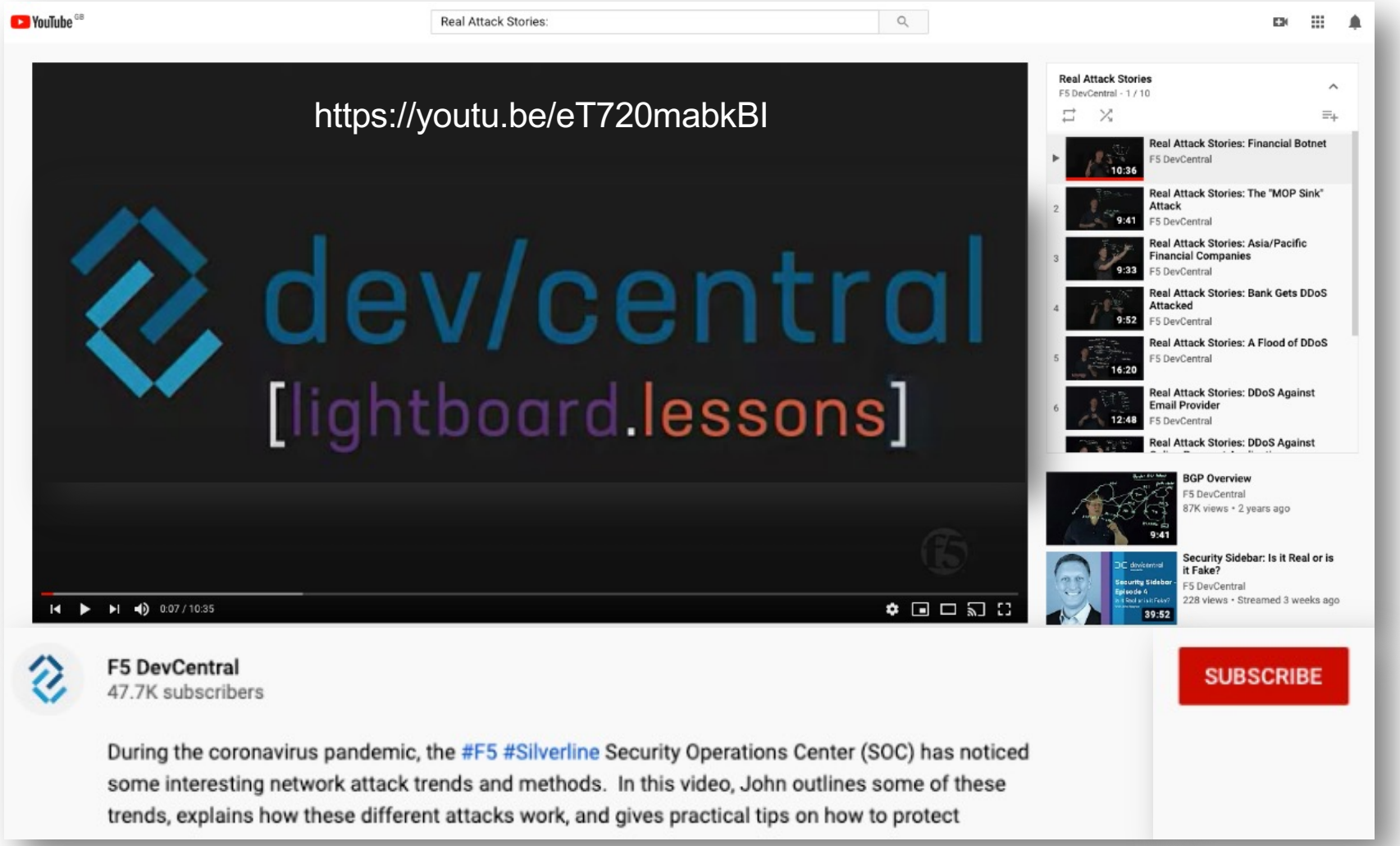


Silverline Web Application Firewall

Eliminate application level attacks

Silverline Threat Intelligence

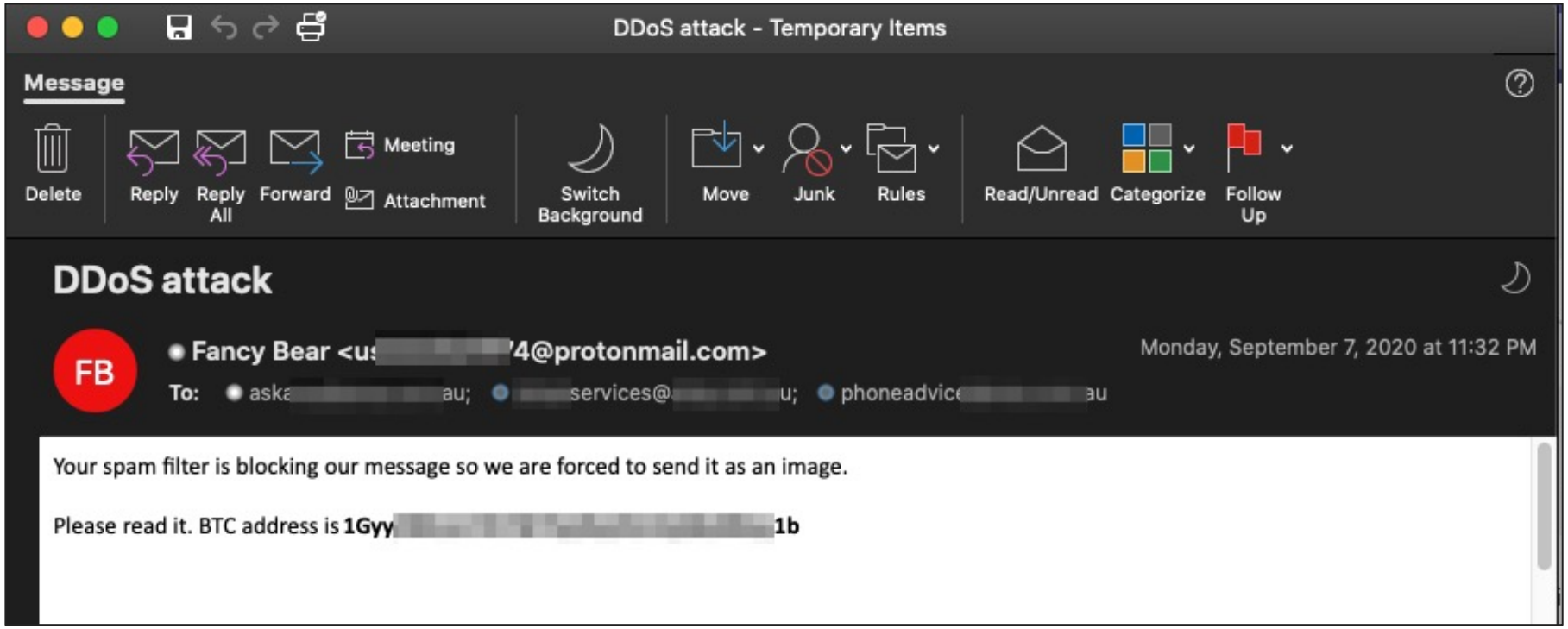
Real Attack Stories – DDoS Attack Trends During Coronavirus



What Are DDoS Ransom Notes?

ATTACKERS PIVOTED TOWARDS CRYPTO RANSOMWARE WITH WANNACRY AND ETERNALBLUE

You typically receive a nice and polite email telling you that you have been selected as the next DDoS target:



Protecting against DDoS is challenging:

Good vs. Bad Traffic

All traffic/connections look the same – hard to distinguish the good from the bad

Multiple Vulnerable Points

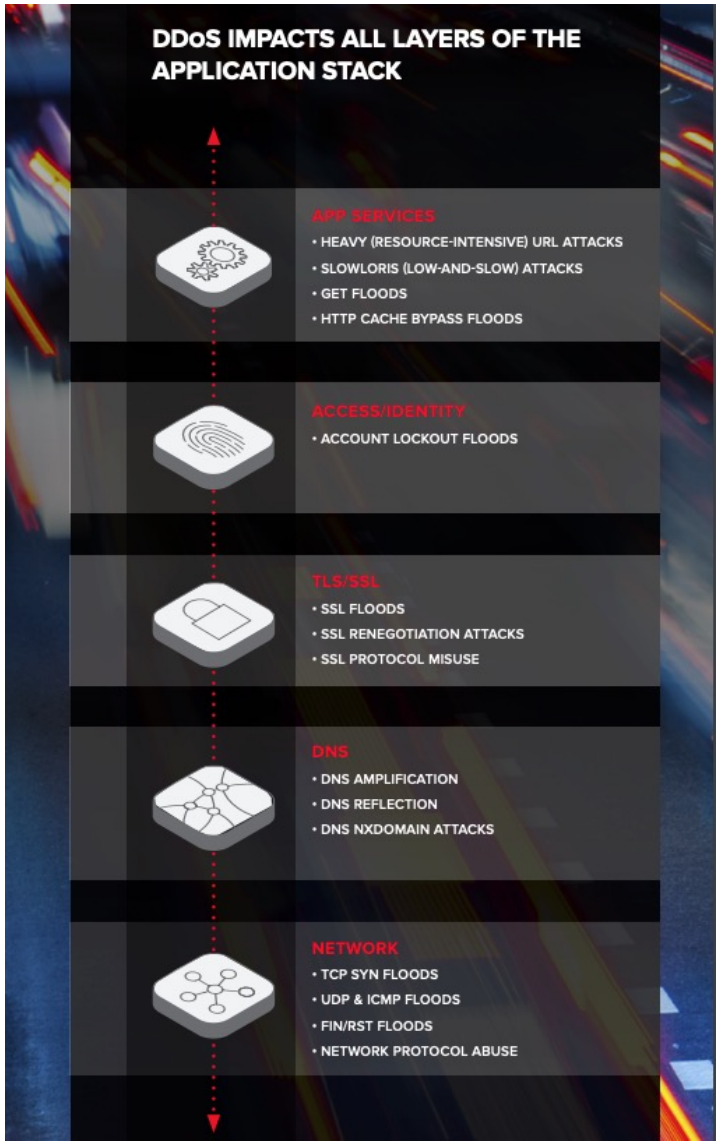
Attacks target weakest link network, WAN bandwidth, authentication, and applications

Sophisticated and Targeted

Multi vector attacks leveraging TLS connections, with malware planted on botnets

DDoS Attacks are Easy to Launch

Attacks can be crowd-sourced and monetized, launched by simple apps

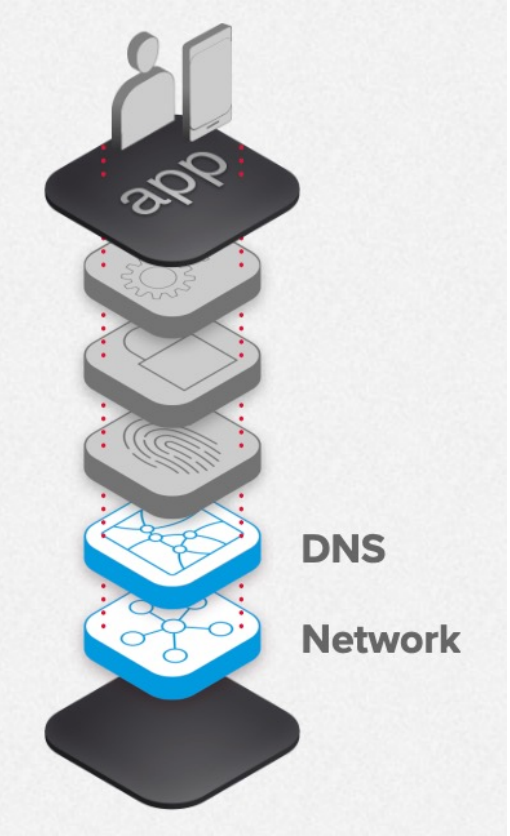


Silverline Customer Attack Mitigation Example

Standard Attacks, but Lot of Them

- 840Gbps / 25Mbps legitimate traffic
- Botnet of variety of clients – Windows, Linux, MikroTik, …

https://www.f5.com/labs/articles/threat-intelligence/ddos-against-a-financial-service-analysis-of-a-massive-attack

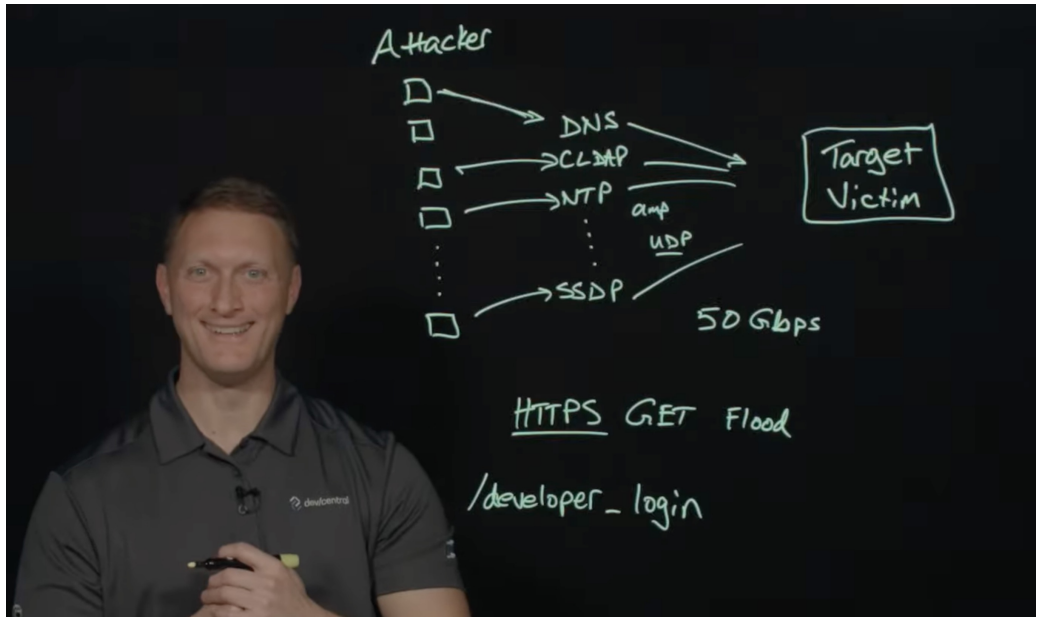


DNS amplification, DNS flood, DNS reflection
SYN flood, UDP flood

Silverline Customer Attack Mitigation Example

Financial / High-Tech DDoS Attacks

- Ransom attack example including “demo attack”
- Multi-vector amplification attack by a large botnet
- Amplification DNS, NTP, SSDP
- Attack that peaked at 50 Gbps
- Application attacked HTTPs

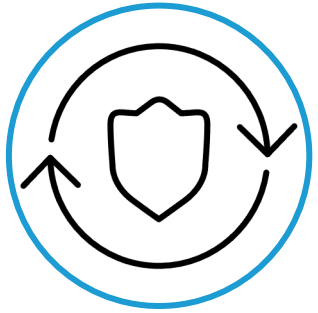


https://devcentral.f5.com/s/articles/Real-Attack-Stories-Asia-Pacific-Financial-DDoS

F5 Silverline

Silverline DDoS Protection

Effective Mitigation with Silverline DDoS Protection



SOC OPERATED DEFENSES

Multi-layered traffic inspection and mitigation techniques driven by Silverline SOC experts

ZERO-DAY PROTECTION

Customers benefit from collective defense intelligence and SOC awareness to minimize risk of zero-day DDoS

APPLICATION DDOS PROTECTION

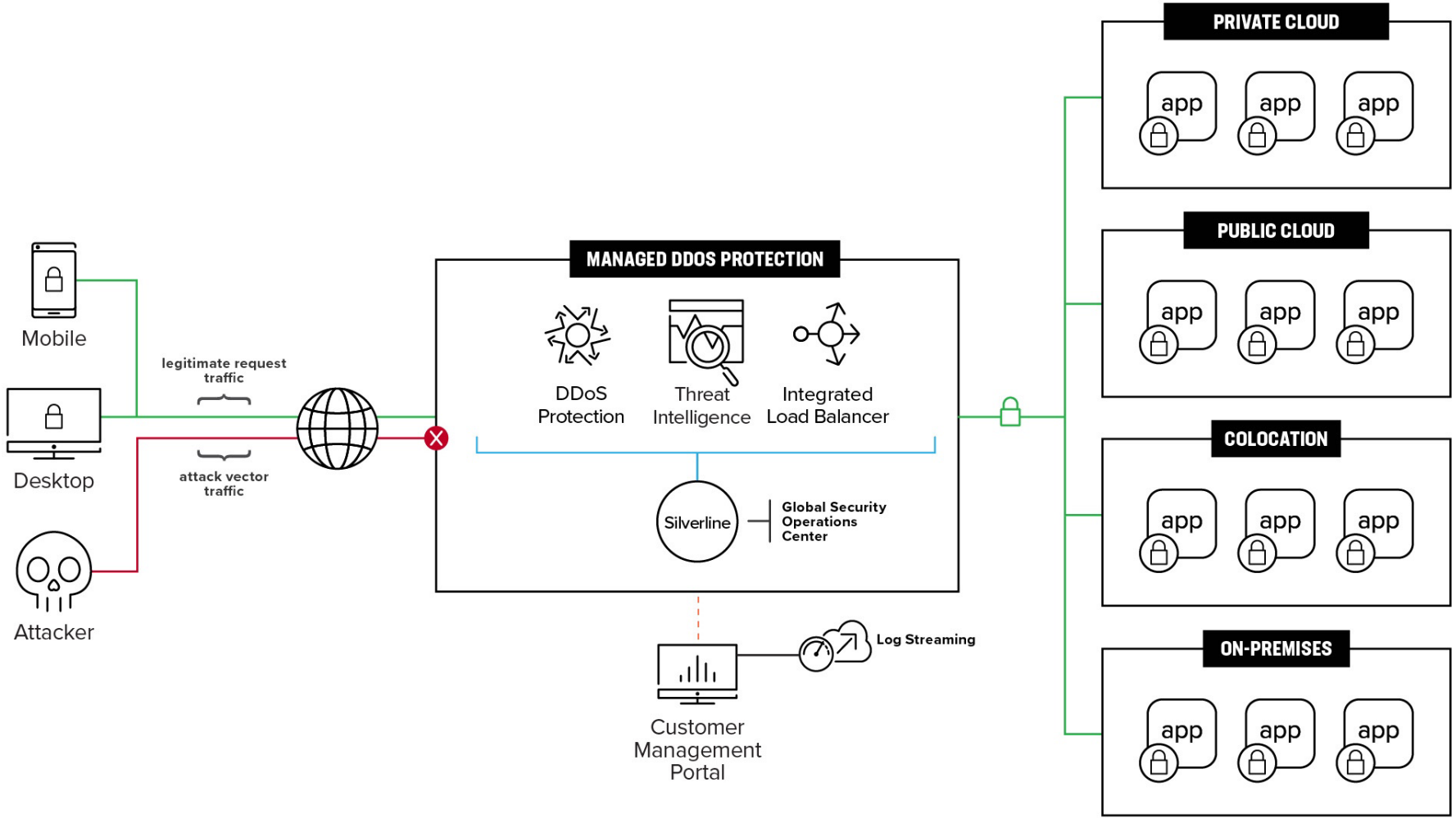
Layer 7 defense to identify transactional or stress-based attacks against an application or business logic

INDUSTRY UNIQUE HYBRID DEFENSE

Easily mitigate attacks both on-premises and in the cloud leveraging F5 Hybrid Signaling between BIG-IP and Silverline

F5 Silverline DDoS Protection Platform

LEADING-EDGE TECHNOLOGIES DELIVERING APPS AND DATA WITH GREATER AGILITY, SECURITY, AVAILABILITY, PERFORMANCE, AND SCALE



F5 Silverline: Service Options

CHOOSE FROM TWO SERVICE OPTIONS FOR DDOS PROTECTION

ALWAYS ON:

Primary protection
as the first line of defense

The Always On subscription is configured to continuously route and process your traffic through F5 Silverline, allowing only legitimate traffic to reach your apps.

- Lowest “Time to Mitigate”
- Maximum visibility for attack trends and detected threats
- Consistent, reliable service delivery metrics and awareness
- Zero activation tasks
- Ideal for complex, dispersed customer application infrastructure

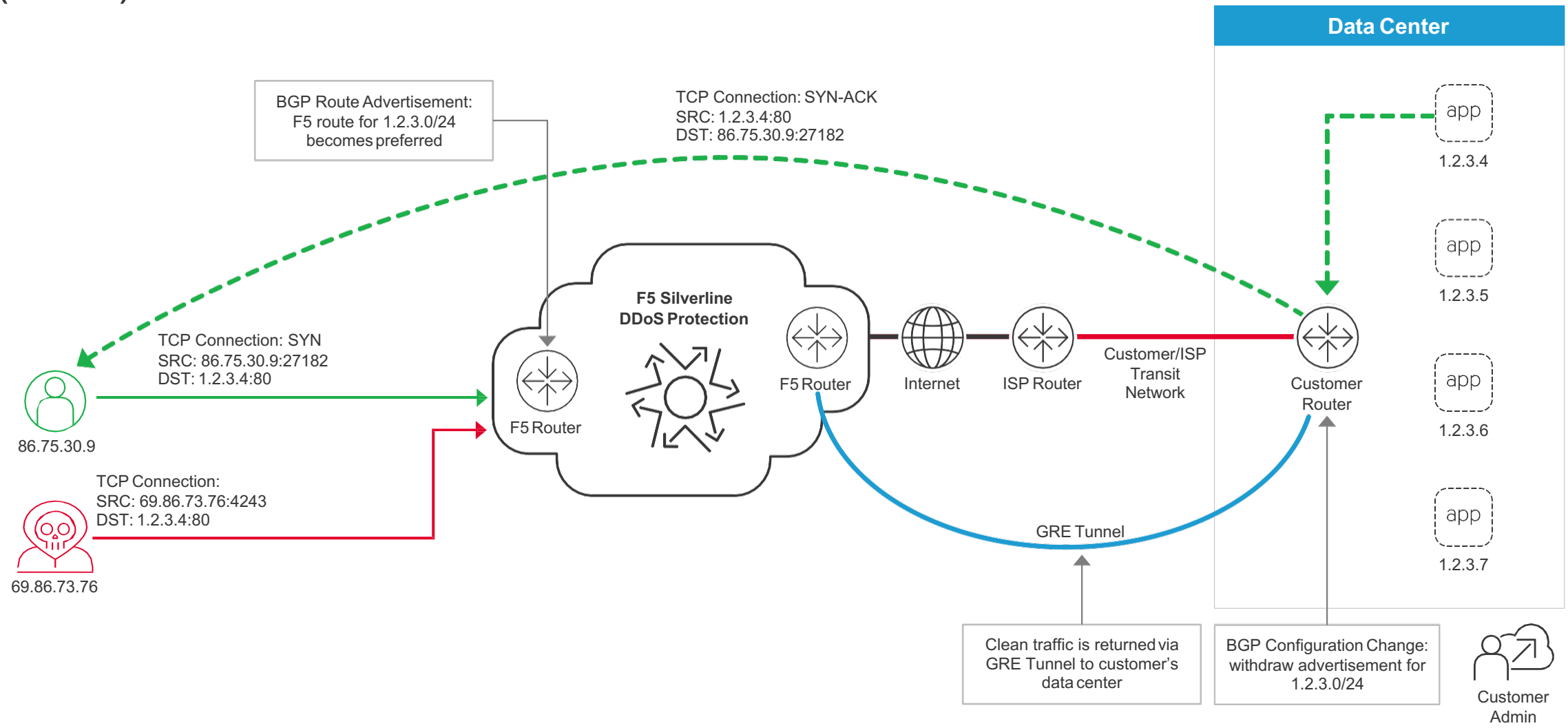
ALWAYS AVAILABLE:

Primary protection
available on-demand

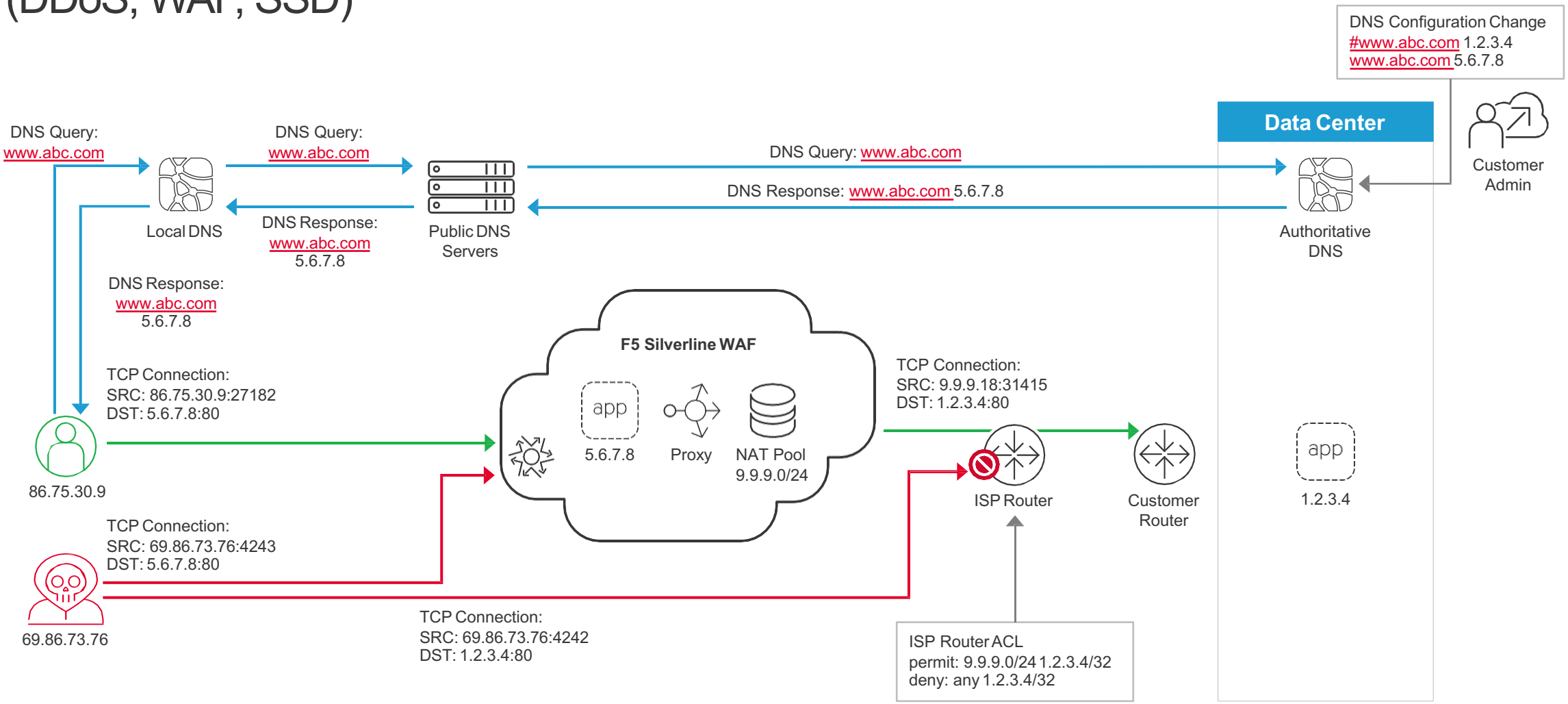
The Always Available subscription is pre-configured for your systems, runs on standby, and can be initiated when under attack.

- On-Demand Service Activation by BGP or DNS Redirection
- No limit to the number of mitigation events or service activations
- Can be combined with Router Monitoring to provide detection and notification of DDoS events
- On-premises signaling functionality to accelerate attack detection and notification

F5 Silverline Routed Configuration
(DDoS)

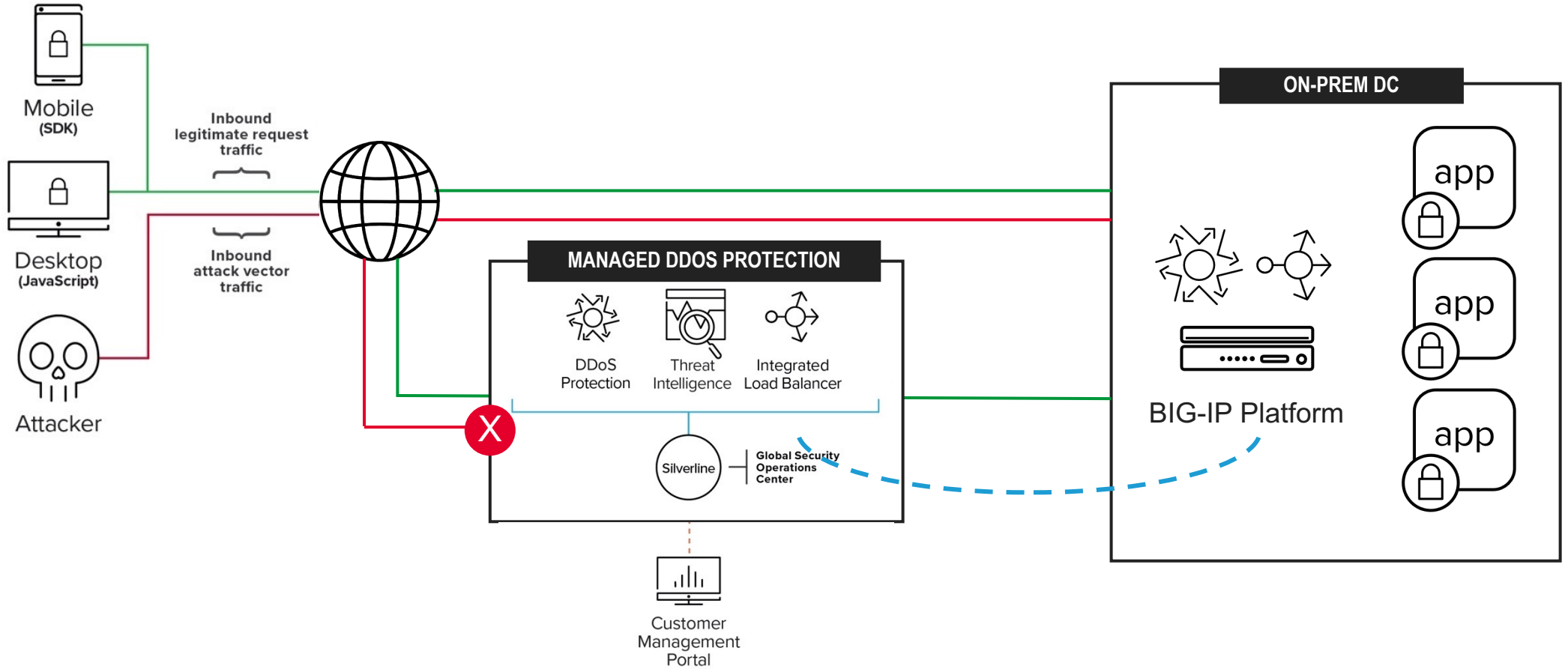


F5 Silverline Proxy Configuration
(DDoS, WAF, SSD)



F5 Silverline: Hybrid DDoS Deployment

LEADING-EDGE TECHNOLOGIES DELIVERING APPS AND DATA WITH GREATER AGILITY, SECURITY, AVAILABILITY, PERFORMANCE, AND SCALE



F5 Silverline DDoS Protection iApp Deployment

SUPPLIED AS OUT-OF-THE-BOX READY AND AS AN IAPP

LTM

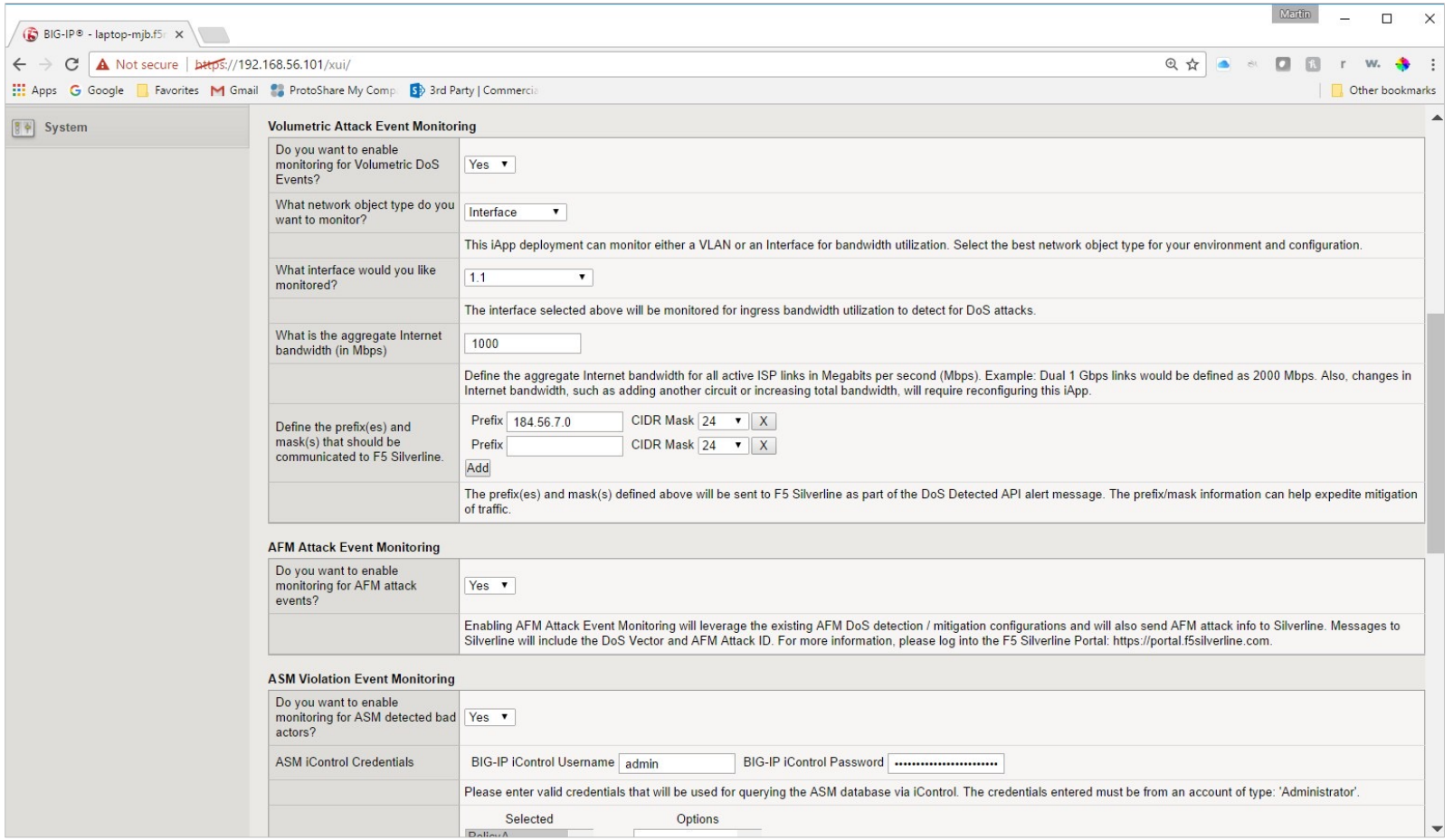
Detects volumetric attacks

AFM

Able to supply attack vector data to Silverline including Bad Actors

ASM

Any client blacklist of learned behavioral DDoS attackers supplied to Silverline



F5 Silverline

Silverline DDoS Protection – The Service

F5 Silverline: The Difference

WHAT MAKES SILVERLINE UNIQUE

PEOPLE

SOC experts have an unrivalled breadth and depth of industry experience

F5 cyber security experts on-hand 24x7

Agile DevOps methodologies across product development teams

PLATFORM

Built on industry leading proven security technology

Flexible multi-layered application security stack

Cloud-based platform built with the highest levels of regulatory compliance & continuity in mind

PORTAL

Globally available and easy to use portal with integrated online chat services

Instant visibility & situational awareness for all application traffic

Rich contextual dashboards for analysis before, during and after attack mitigation

F5 Silverline: The People

AUGMENT IT SECURITY STAFF WITH F5 CYBER SECURITY EXPERTS ON HAND 24X7

SECURITY OPERATIONS CENTER (SOC)

F5 SOC experts are at your service 24x7. Whether that means constantly evolving fraud-prevention services, shutting down malicious sites, or layering protections with Silverline application services, we're here for you.

BENEFITS:

A Managed Service like no other, F5 Native SOC
Dedicated cyber security professionals focused on the F5 Silverline Services. Benefit from integrated support, operations and engineering professionals with direct lines of communication to F5 Product Development.

Specialized Security Experts
SOC experts have an unrivalled breadth and depth of industry experience with no resource limits on leveraging their capabilities, skills and interactions.

Monitoring and Reporting
SOC services include access to the F5 Silverline customer portal so you can securely manage your services, chat online with F5 experts, and review traffic, policies, and attack mitigation reports.

F5 Silverline DDoS: The Portal

GAIN ATTACK INSIGHTS AND THREAT INTELLIGENCE

Rich Contextual Dashboard and Reporting:

- Easy to use service configuration
- Attack mitigation insights
- In-depth violation data & analysis
- Situational awareness of DDoS attacks
- Direct collaboration with the SOC

F5 Silverline: The Portal

EASY TO USE AND FULLY CUSTOMIZABLE SELF-SERVICE PORTAL

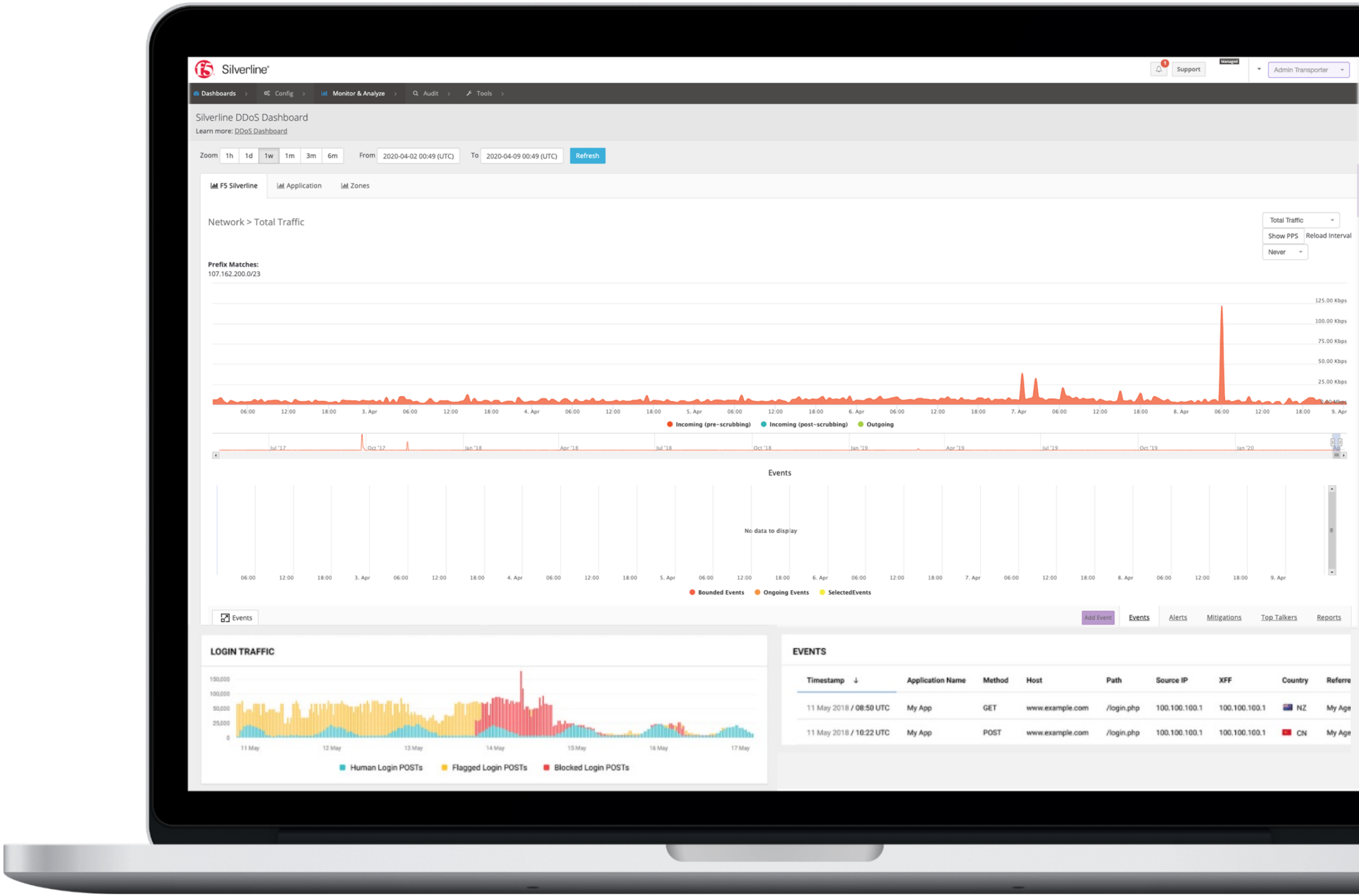
1	CHOOSE TOPOLOGY	Ingress traffic via Routed or Proxy mode, with either Always On or Always Available service design
2	PROVISION NETWORK	Configure traffic routing options for either BGP or DNS based on Topology. Option to provision global Firewall Rule Set
3	SELECT LOCATIONS	Select appreciated scrubbing centers to achieve business continuity, compliance and performance
4	DEFINE INCIDENT PROCEDURES	Define how you want the SOC to support and notify you during a real-time incident or DDoS attack

PORTAL CONFIGURATION BENEFITS

- ✓ Zero Impact Deployments
- ✓ App Infrastructure & Location Agnostic
- ✓ Comprehensive Knowledge Base
- ✓ Immediate Effect

Demo

SILVERLINE SERVICES



F5 Silverline

Silverline DDoS Protection – The Outcome

F5 Silverline DDoS Protection: Use Cases

MANAGED DDoS PROTECTION FOR YOUR MULTI-CLOUD INFRASTRUCTURE

Protect Brand Reputation

Ensure your digital presence stays online during an attack with real-time DDoS attack detection and mitigation in the Cloud

Defend against Volumetric Attacks

Globally available architecture with multi-terabit capacity across high performant Tier 1 carriers with direct public cloud peering

L7 DDoS Protection

Stop bad actors consuming resources and impacting application performance. Mitigations that adapt to user interactions.

Defend your DNS

DNS is a key foundation to your digital presence. Defend it from DNS Flood, reflection and amplification attacks.

Attack Mitigation Insights

Transparent attack mitigation visibility from before, during and after attack with complete awareness of mitigation implemented.

Industry Unique Hybrid Deployments

Integrate on-premises BIG-IP with Silverline cloud-based DDoS mitigation, through threshold-based automated signaling

F5 Silverline: Simple, Flexible Consumption Model

COST-EFFICIENT, FLEXIBLE SECURITY SERVICES, WITH SUBSCRIPTION BASED CONSUMPTION

DDoS:

- ✓ Number of data centers to be protected
- ✓ Clean Bandwidth (95th percentile)
- ✓ Optional router monitoring service

  based on number of edge routers to be monitored
- ✓ Deployment fee

Add-On Services:

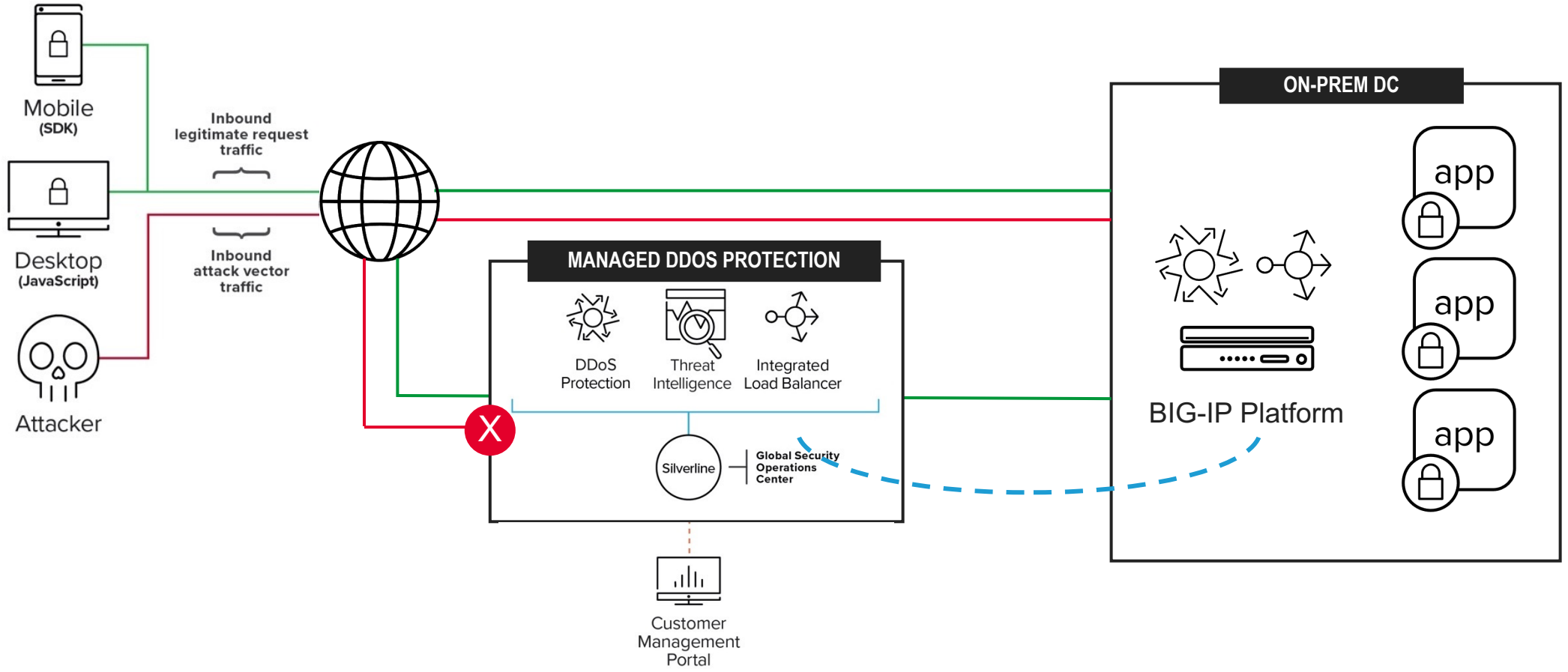
- ✓ Threat Intelligence
- ✓ Silverline Shape Defense
- ✓ Silverline Web Application Firewall

ALWAYS ON:
Primary protection
as the first line of defense

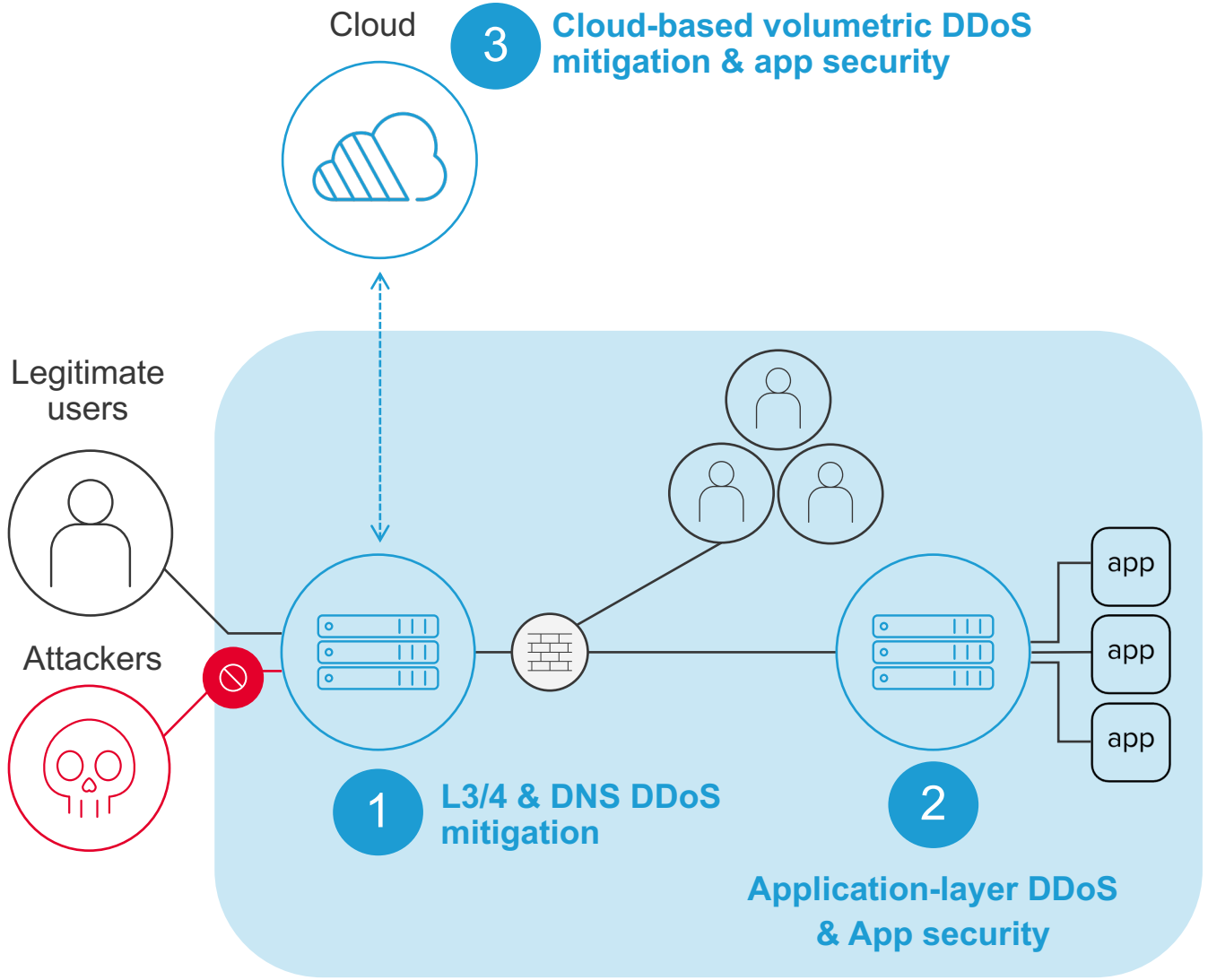
ALWAYS AVAILABLE:
Primary protection
available on-demand

F5 Silverline: Hybrid DDoS Deployment

LEADING-EDGE TECHNOLOGIES DELIVERING APPS AND DATA WITH GREATER AGILITY, SECURITY, AVAILABILITY, PERFORMANCE, AND SCALE



DDoS Mitigation – F5 Multi-Layered Architecture



1 – Protect the Perimeter

- L3/4 floods and scans
- DNS targeted attacks

AFM

2 – Protect the Applications

- Low and Slow attacks
- SSL targeted attacks
- Bots detection techniques

AWAF

3 – Cloud Scrubbing

- Prevent ”Full Pipe” problem
- L3-7 managed DDoS protection

Silverline

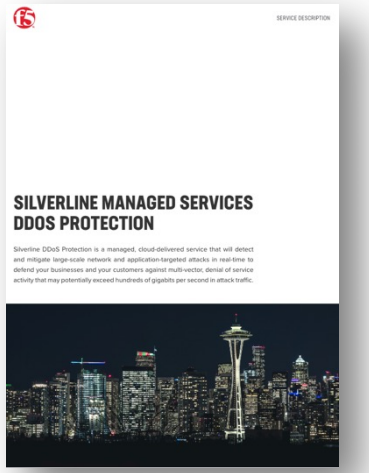
DHD

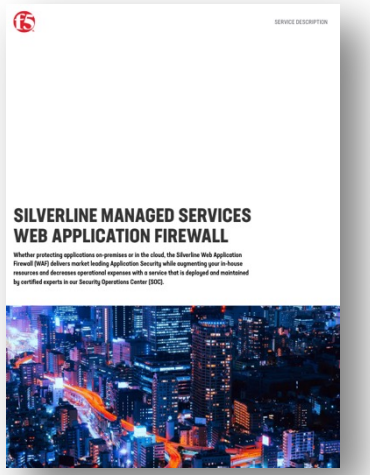
SILVERLINE

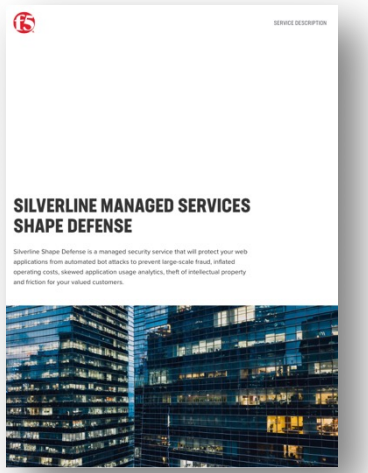
F5 Silverline Resources

WHERE TO GO FOR FURTHER INFORMATION

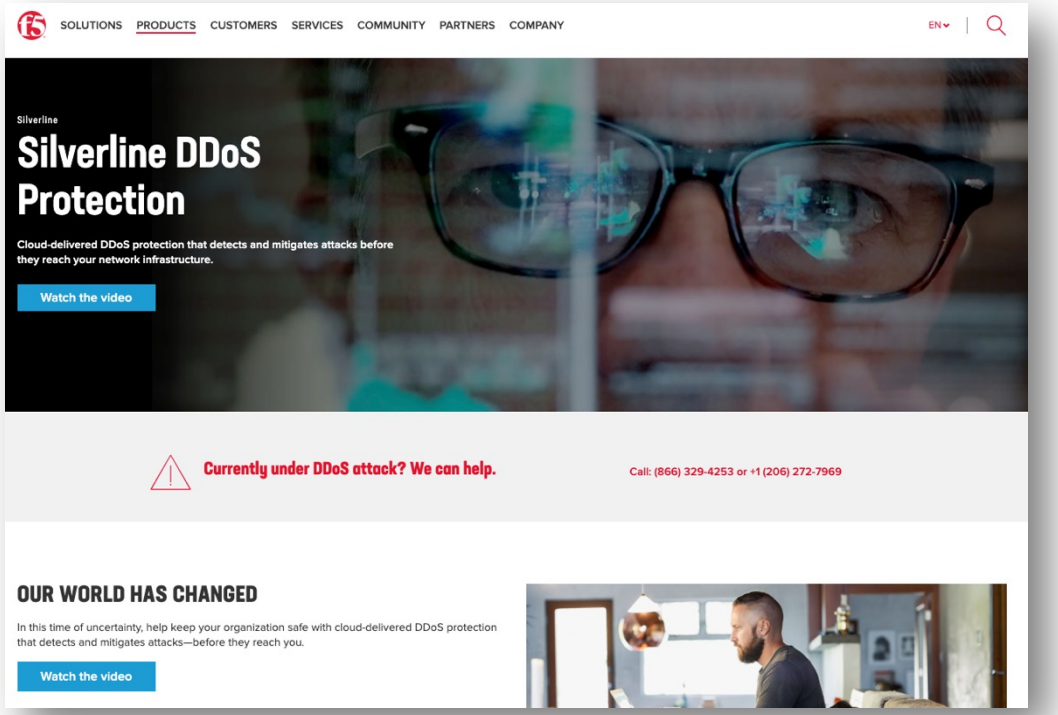
SERVICE DESCRIPTIONS:







SILVERLINE DDoS PROTECTION ON F5.com:



https://www.f5.com/products/security/silverline/ddos-protection

F5.COM

https://www.f5.com/products/security/silverline

Currently under DDoS attack? We can help.

Call: (866) 329-4253 or +1 (206) 272-7969