



Under the Hood of “On and Off-Premises” DDoS Mitigation Solutions

Or Yaacov

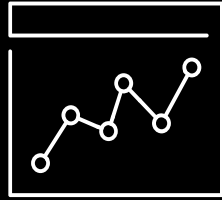
Security Solutions Architect

or@f5.com



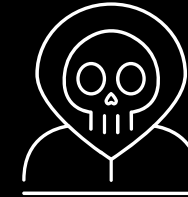
Our **DDoS** World is Complex

Growing



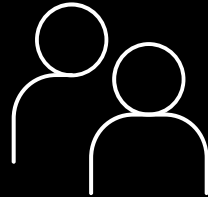
Business

Diverse



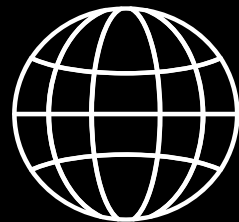
Agenda

Anyone



War tactics

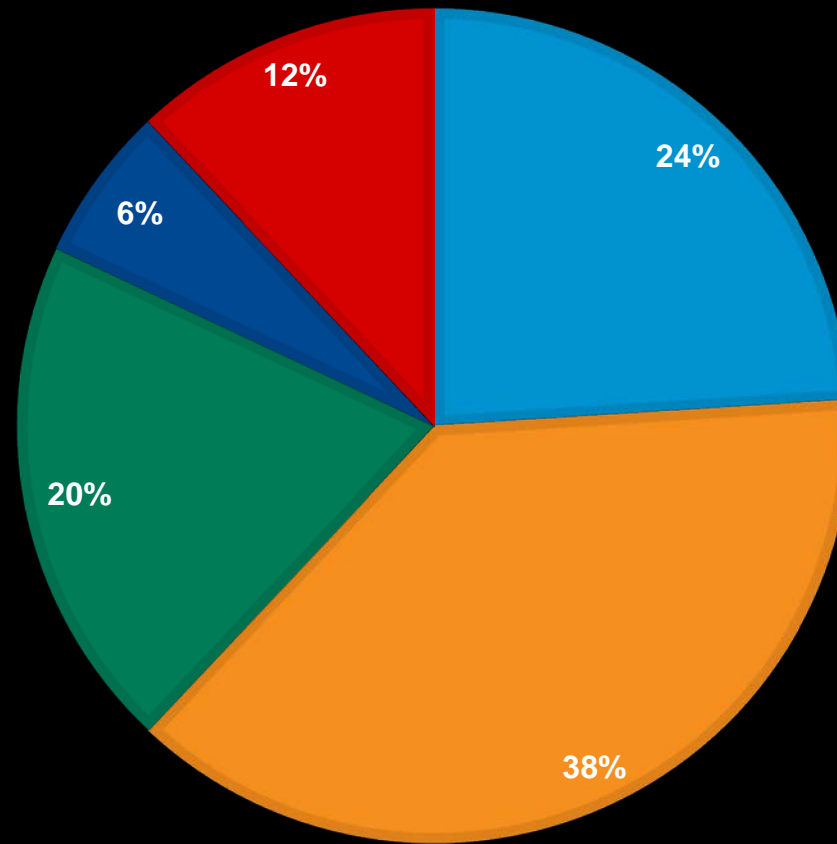
Global



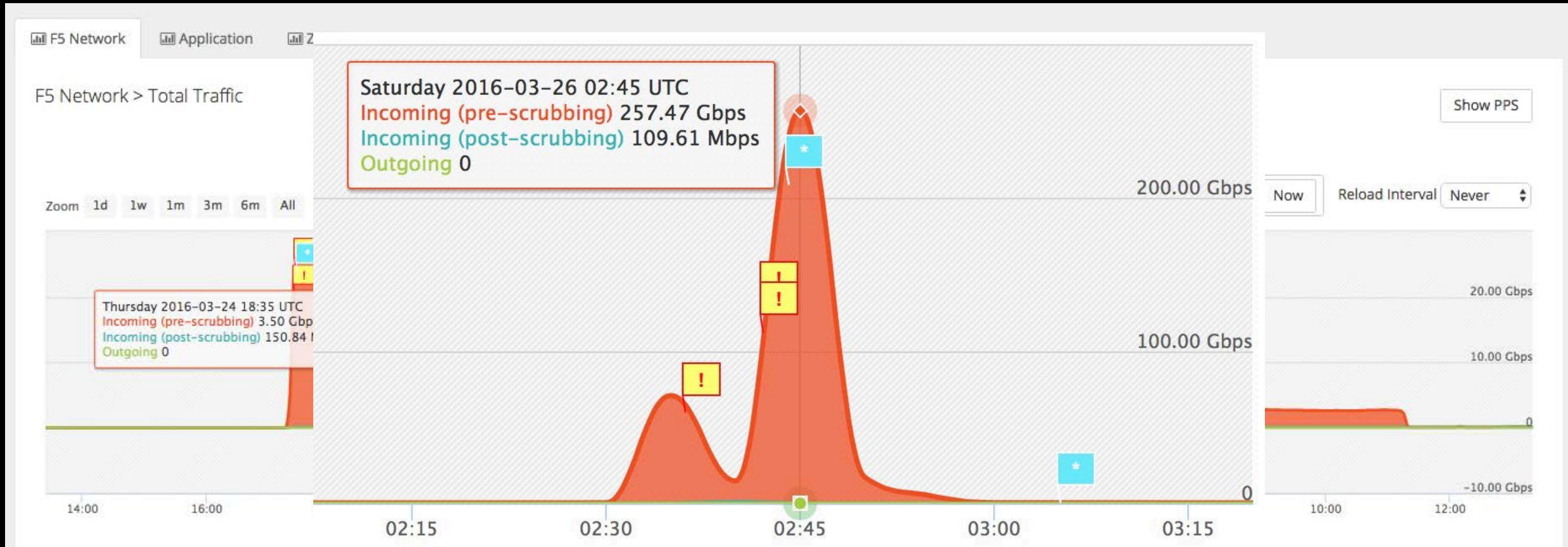
Fun

Attack Size

■ 0.5-1 Gbps ■ 1-10 Gbps ■ 10-50 Gbps ■ Over 50Gbps ■ Unknown



F5 Silverline – Latest Mitigations






“DDoS is becoming normal”



“How to address DDoS?”



F5 Presents: A complete and layered architecture to mitigate DDoS

Effective DDoS Mitigation Architecture

Capabilities

Complete

Global

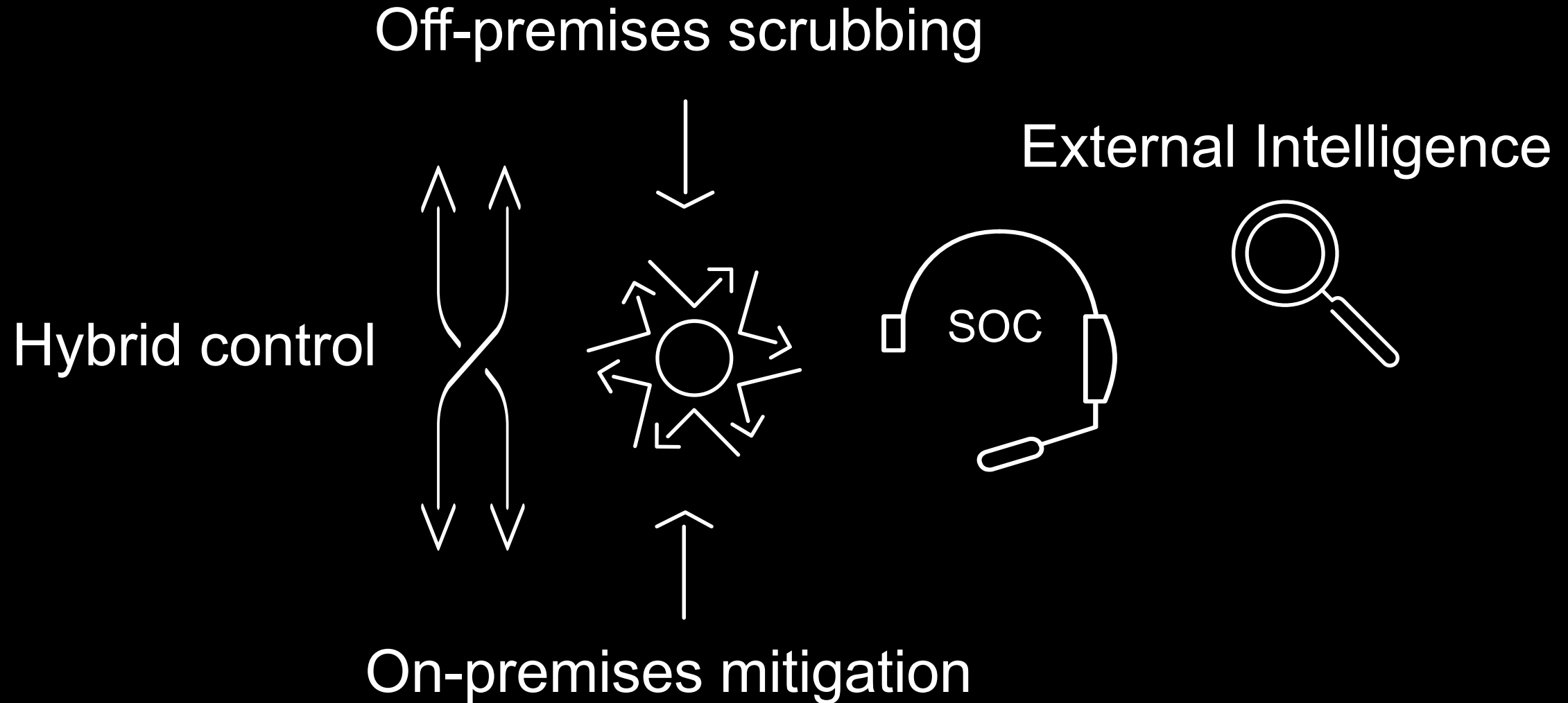
Agile

Visible

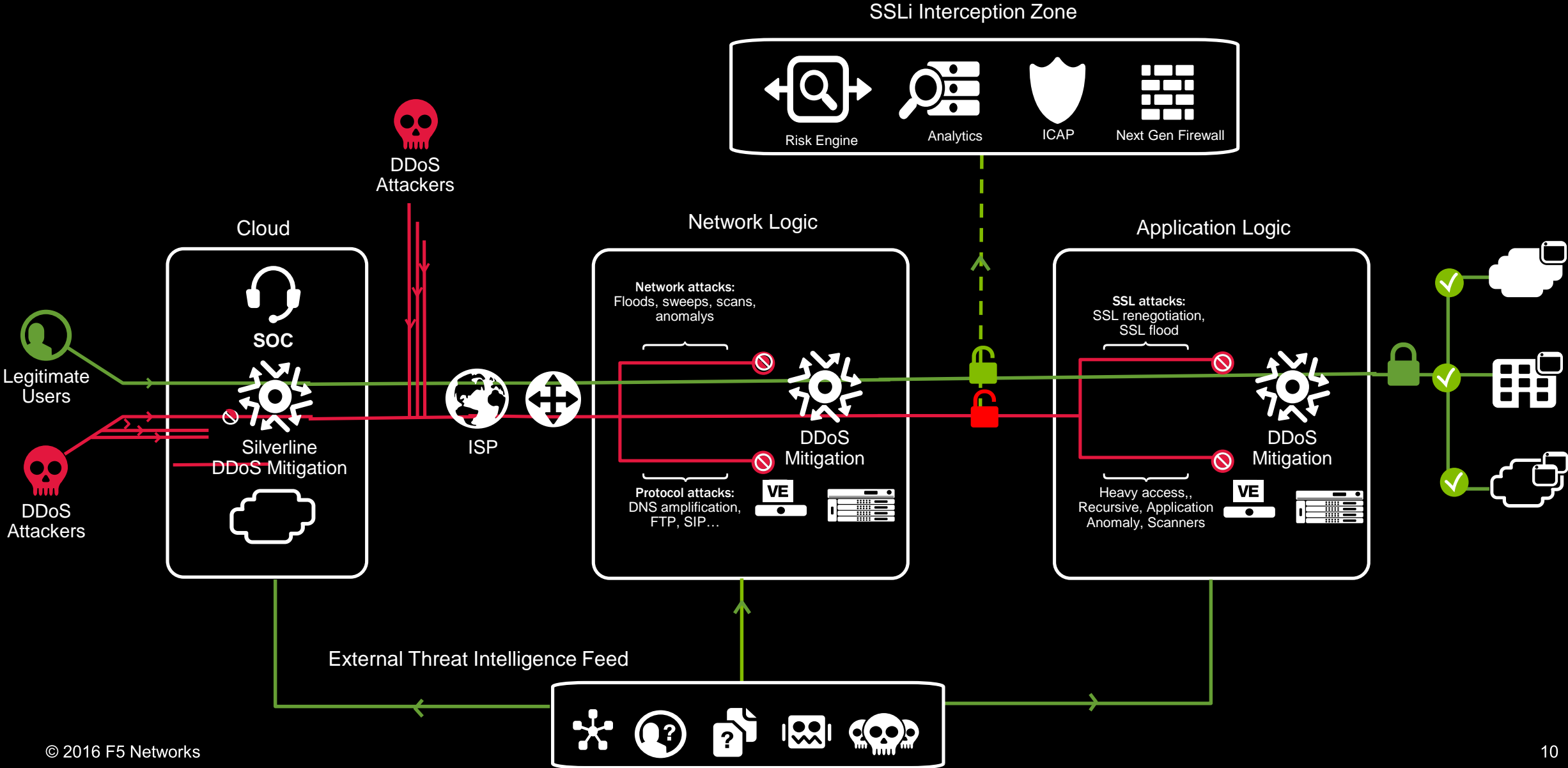
Innovative

Expertise

Building Blocks of DDoS Mitigation



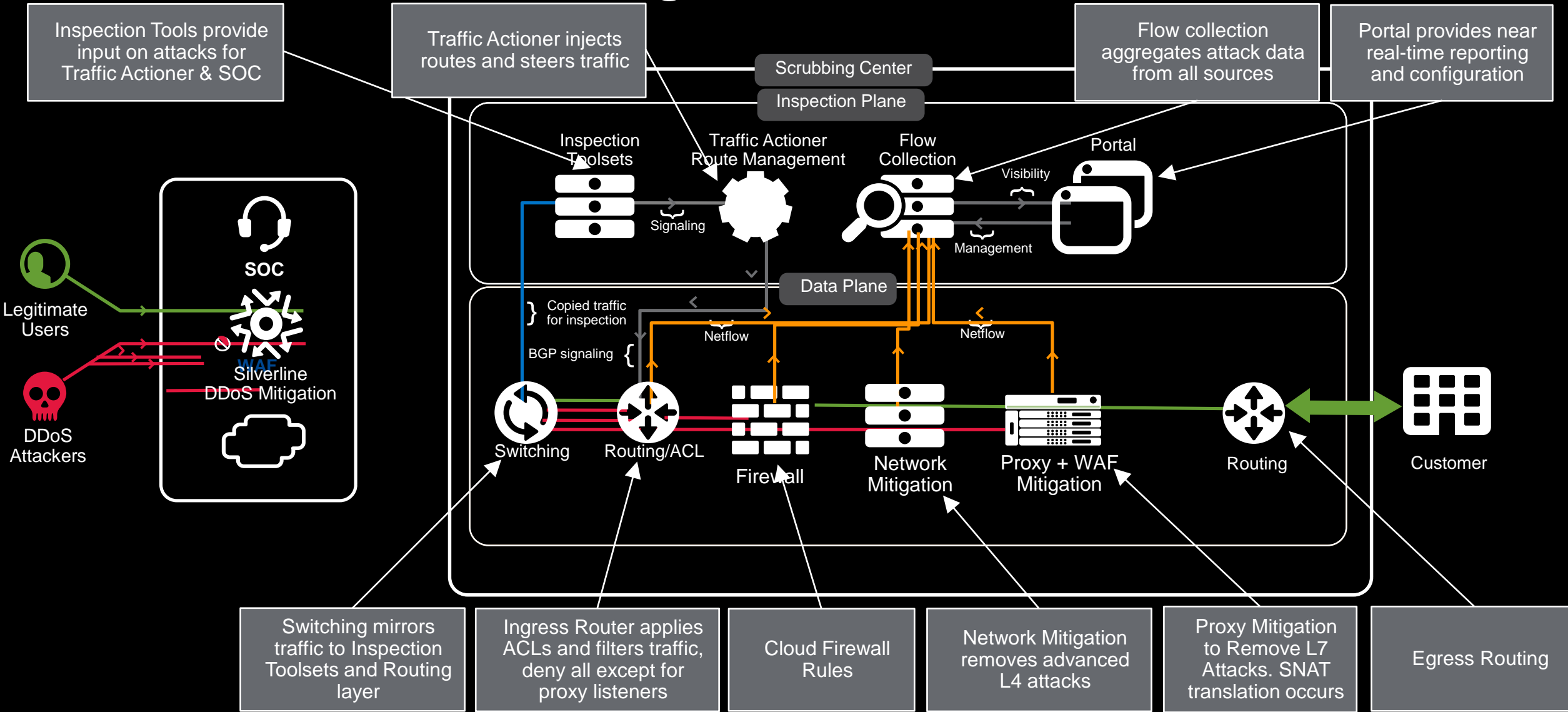
F5 Complete Layered DDoS Mitigation Architecture



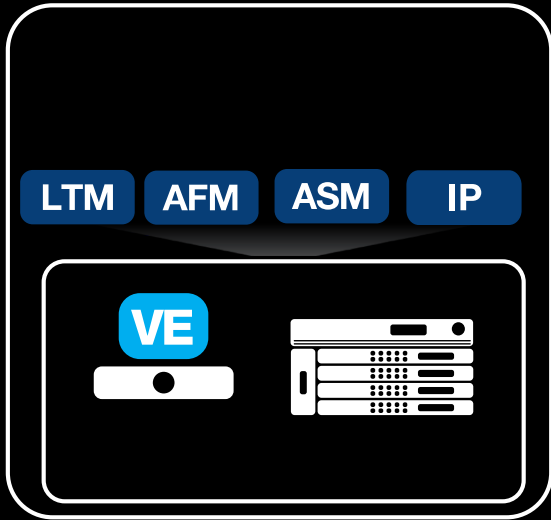
WW SOC and Scrubbing Coverage



F5 Cloud – Scrubbing Center Drill Down



On-Premises Drill Down



120+ DDoS vectors mitigation
Sweep, Scans, Protocol validation
HW/SW mitigation
IP Shunning
RTBH
Firewall
Device ID tracking

Proactive BOT defense
IP threat intelligence
BOT detection
Scraping protection
Behavioral analysis
Anomaly detection
Heavy URL
SSL DDoS protection

Programmability!



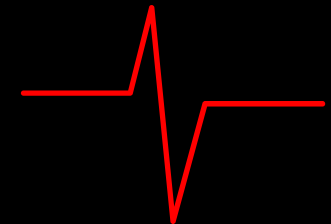
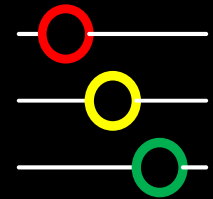
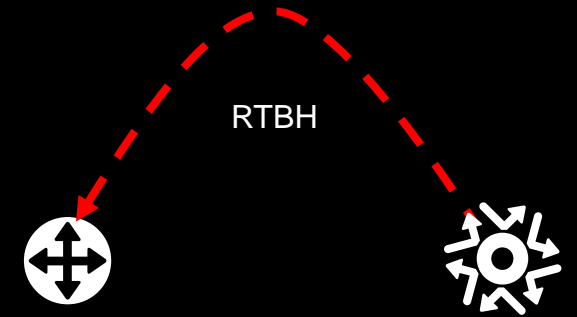
What's next?

12.1 Introduced

BGP Black-Hole DoS protection (RTBH)

Automatic DDoS vectors thresholds

Behavioral analysis DDoS (BADOS)



F5 Introduces: Behavioral DDoS Analysis

Why BADOS?

Today

Configuration

Tune and maintain

Impact leads to mitigate

React to 0-day

Static – automatic

Impacts the good

Uses wisdom of IT

BADOS

Hands free

Unsupervised

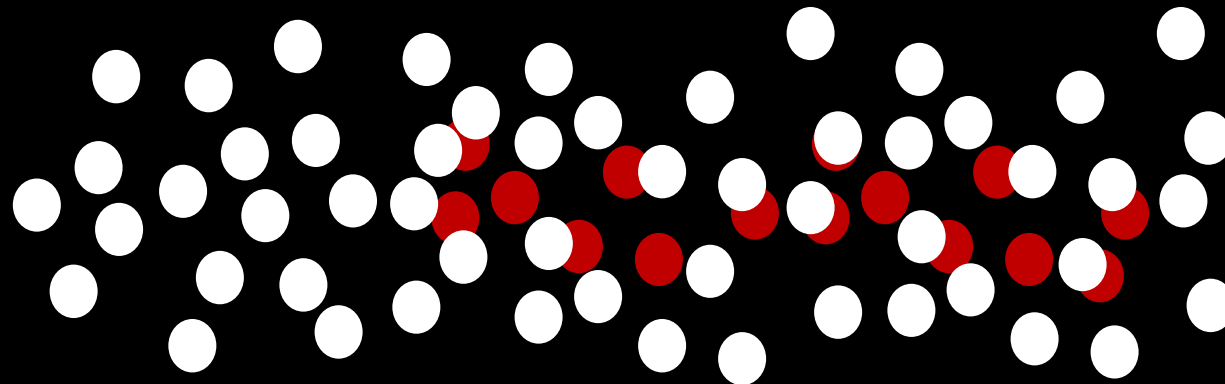
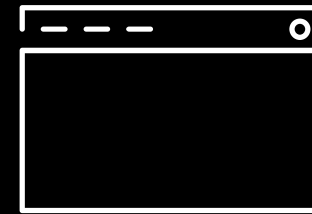
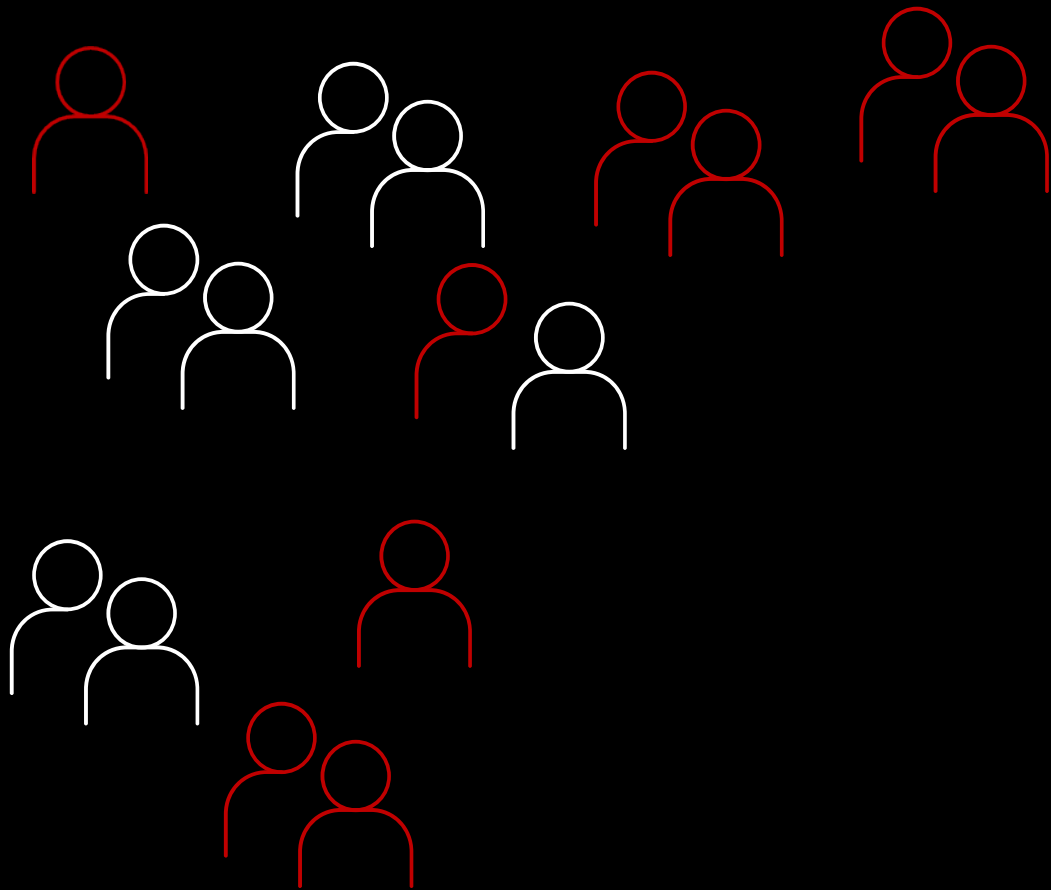
Predictive

0-day capable

Improves with time

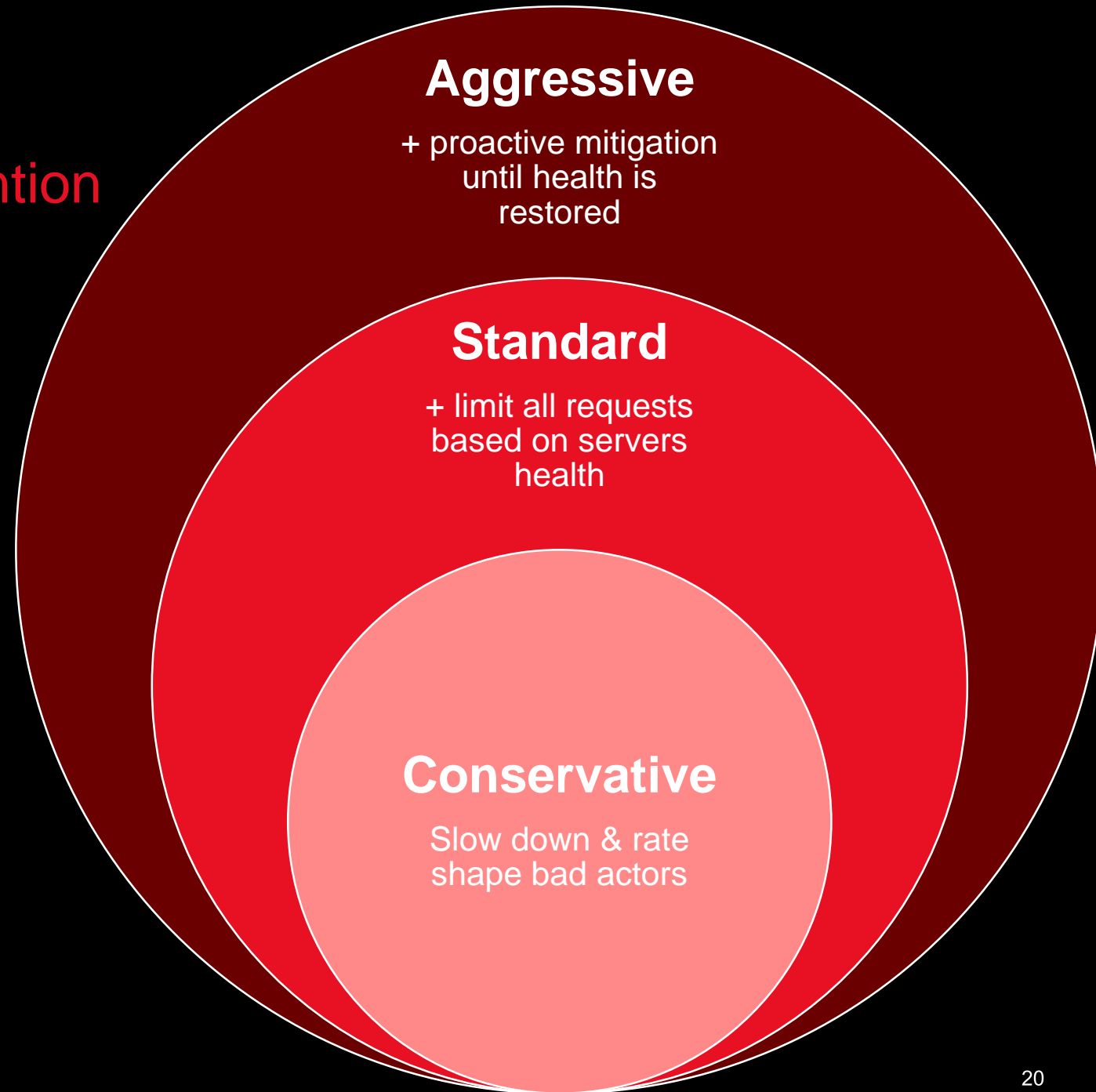
Minimal impact on good guys

Uses wisdom of the crowd



BADOS

3 modes of detection and prevention



BADOS configuration Step 1

The screenshot shows the BADOS configuration interface. The left sidebar contains a navigation menu with categories: Main, Help, About, Statistics, iApps, DNS, Local Traffic, Traffic Intelligence, Acceleration, Device Management, Security, Event Logs, Reporting, Security Updates, Options, Network, and System. The 'Security' category is expanded, showing sub-items: Overview, Application Security, Protocol Security, DoS Protection, Event Logs, Reporting, Security Updates, and Options. The 'DoS Protection' sub-item is selected.

The main content area is titled 'Security » DoS Protection : DoS Profiles » dos'. Below this, there is a 'DoS Profile Properties' section. The 'Profile Information' section shows 'General Settings' as the selected profile. The 'Application Security' section lists several settings: General Settings (checked), Proactive Bot Defense (Off), Bot Signatures (Off), TPS-based Detection (checked), Stress-based Detection (checked), Heavy URL Protection (Off), and Record Traffic (Off).

The 'Application Security » Stress-based DoS Detection' section is highlighted with a red box. It contains the following information:

- Operation Mode:** Specifies how the system reacts when it detects an attack. **Blocking** (Edit)
- How to detect attackers and which mitigation to use:**
 - By Source IP: No mitigation (Edit)
 - By Device ID: No mitigation (Edit)
 - By Geolocation: No mitigation (Edit)
 - By URL: No mitigation (Edit)
 - Site Wide: No mitigation (Edit)
- Behavioral:** ☒ Enabled. Enables traffic behavior, server's capacity learning, and anomaly detection. **Standard protection *** (Close)
- Prevention Duration:** Specifies the time spent in each mitigation step until it is stopped, and the next one is started. Escalation Period: 120 seconds. De-escalation Period: 7200 seconds (Edit)

BADOS configuration Step 2

Apply to an application
(Virtual server profile)

Local Traffic » Virtual Servers : Virtual Server List » **auction_vs**

Properties Resources **Security** Statistics

Policy Settings

Destination	10.1.10.242:80
Service	HTTP
IP Intelligence	Disabled
DoS Protection Profile	Enabled... Profile: dos_bhv
Log Profile	Enabled... Selected: /Common local-dos Available: /Common Log all requests Log illegal requests global-network

Update

DEMO



Q&A





SOLUTIONS FOR AN APPLICATION WORLD