CITRIX

Netscaler Connect

Tijl Van den Broeck

Lead Systems Engineer Networking Belux

NOVEMBER 27, 2017

Agenda

- Netscaler 12.0
- Netscaler Managemend and Analytics System (NMAS)
- Netscaler Secure Gateway
- Netscaler SD-WAN
- Brewery Tour & Drink

CITRIX

Netscaler version 12.0

The world is changing.

CITRIX

As I move my business to the Hybrid Cloud…

Apps are moving to the cloud

NetScaler

Reduced CAPEX
Global coverage
Surge capacity

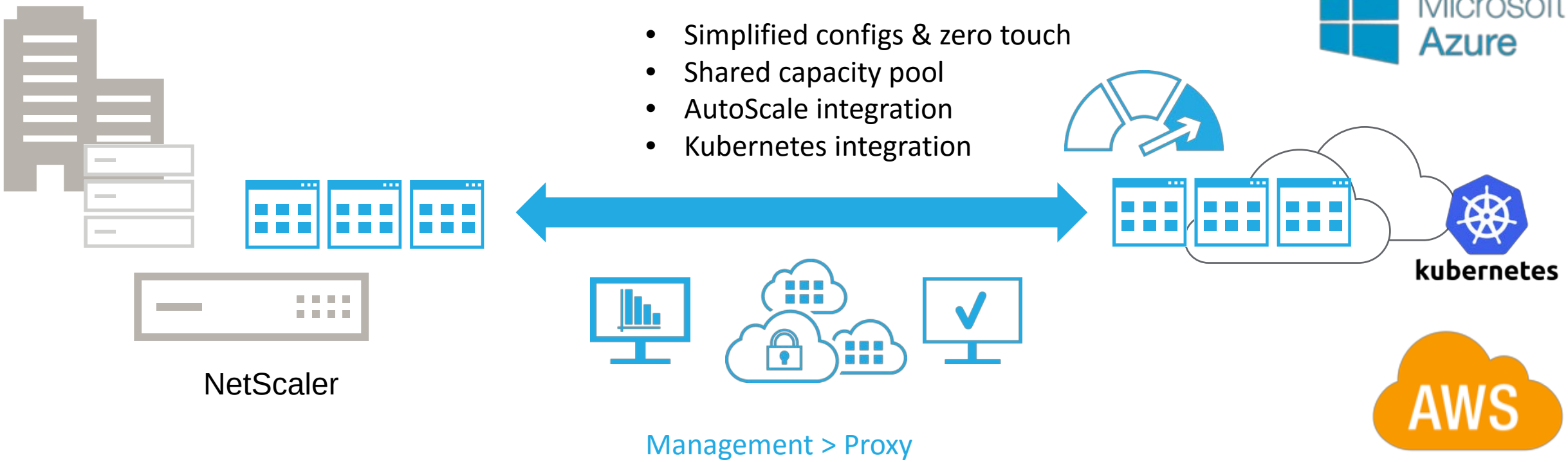
Hybrid requirements
Redundant management processes
Vendor lock in
Risk due to outages
One sided visibility

Microsoft Azure

kubernetes

AWS

Why NetScaler for cloud and SaaS?



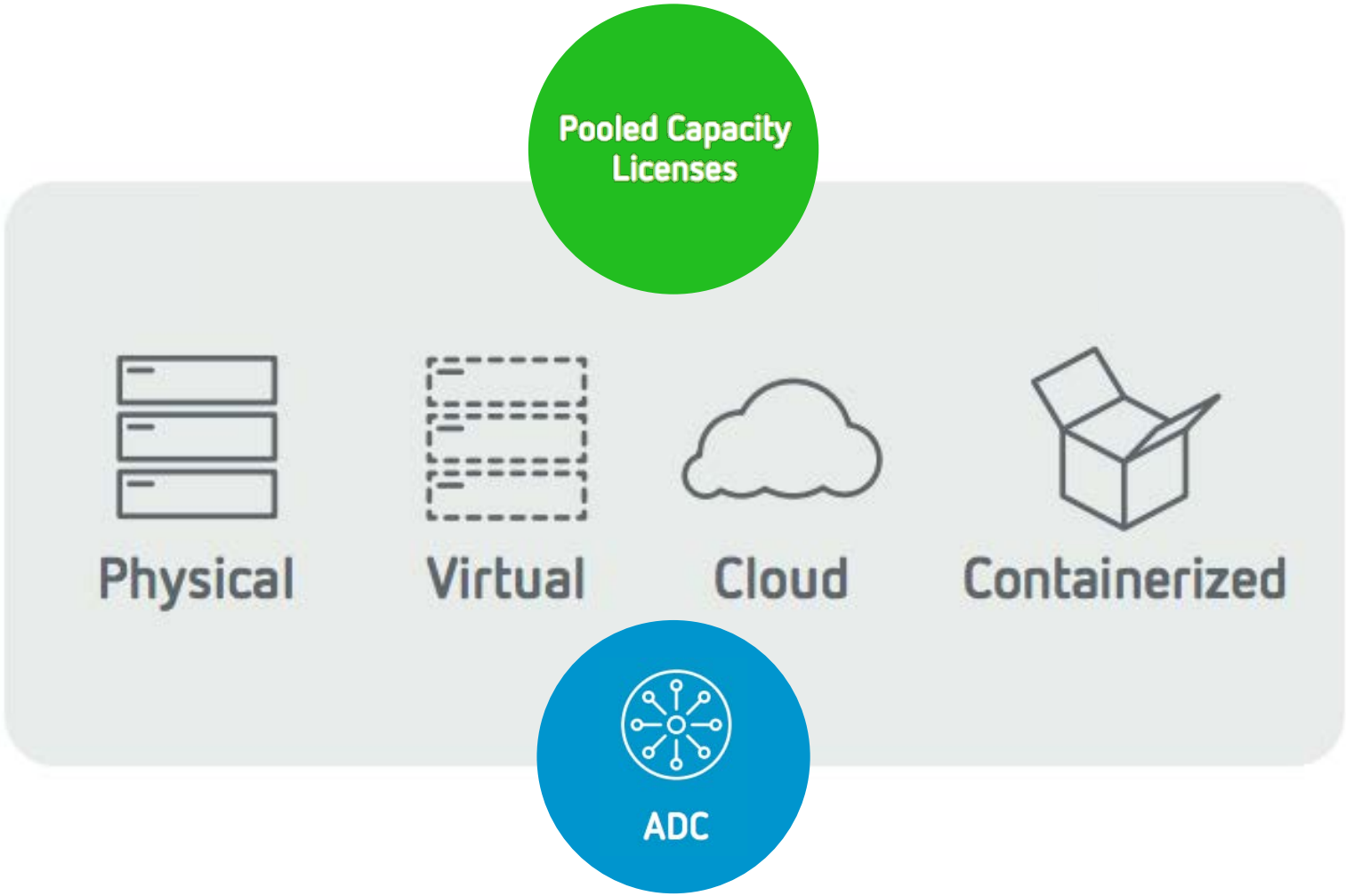
Software first, VPX and CPX

- Simplified configs & zero touch
- Shared capacity pool
- AutoScale integration
- Kubernetes integration

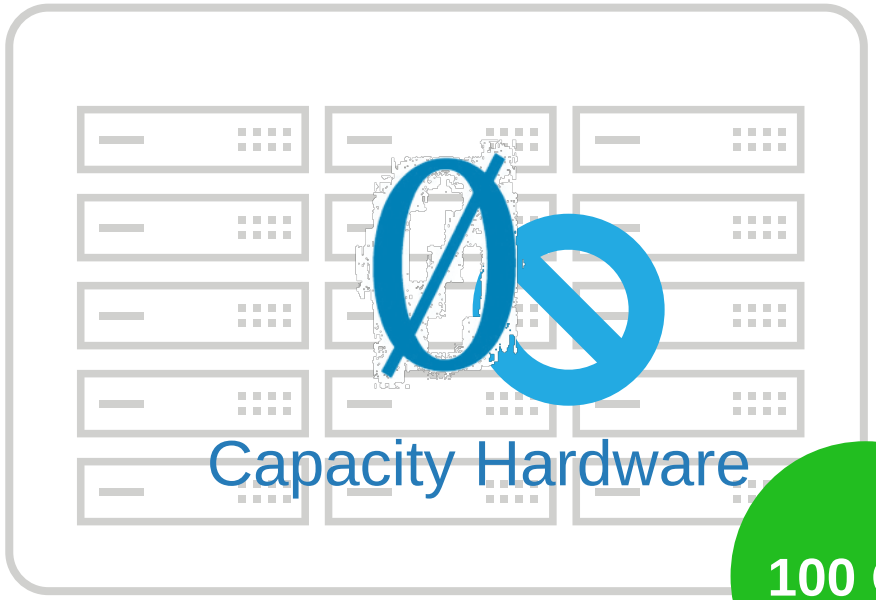
Management > Proxy

- Common management platform
- Multi-cloud availability
- App health scoring
- Application blue prints and templates

Sharing capacity for hybrid environments



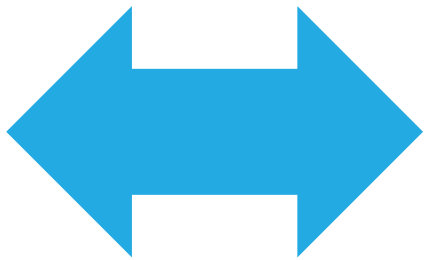
Migrating from hardware to software in the cloud

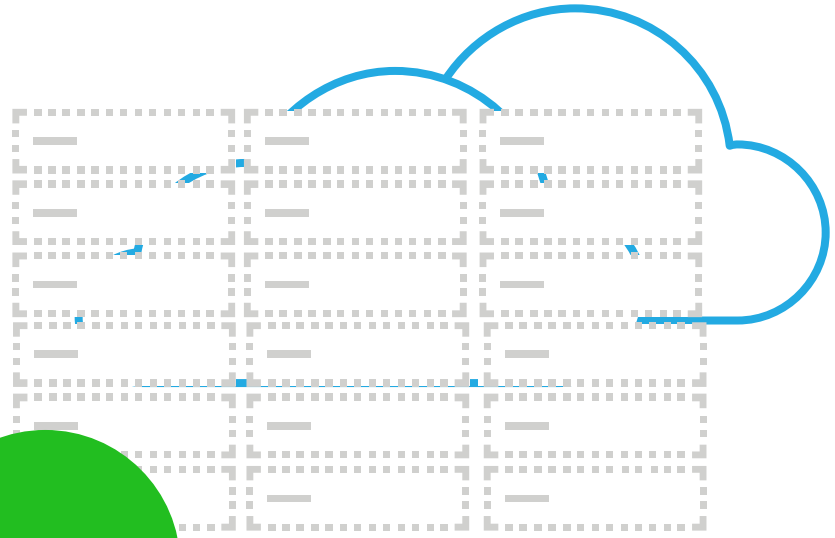


Capacity Hardware

On-Premise

Portability





Cloud

100 Gbps

50 Gbps

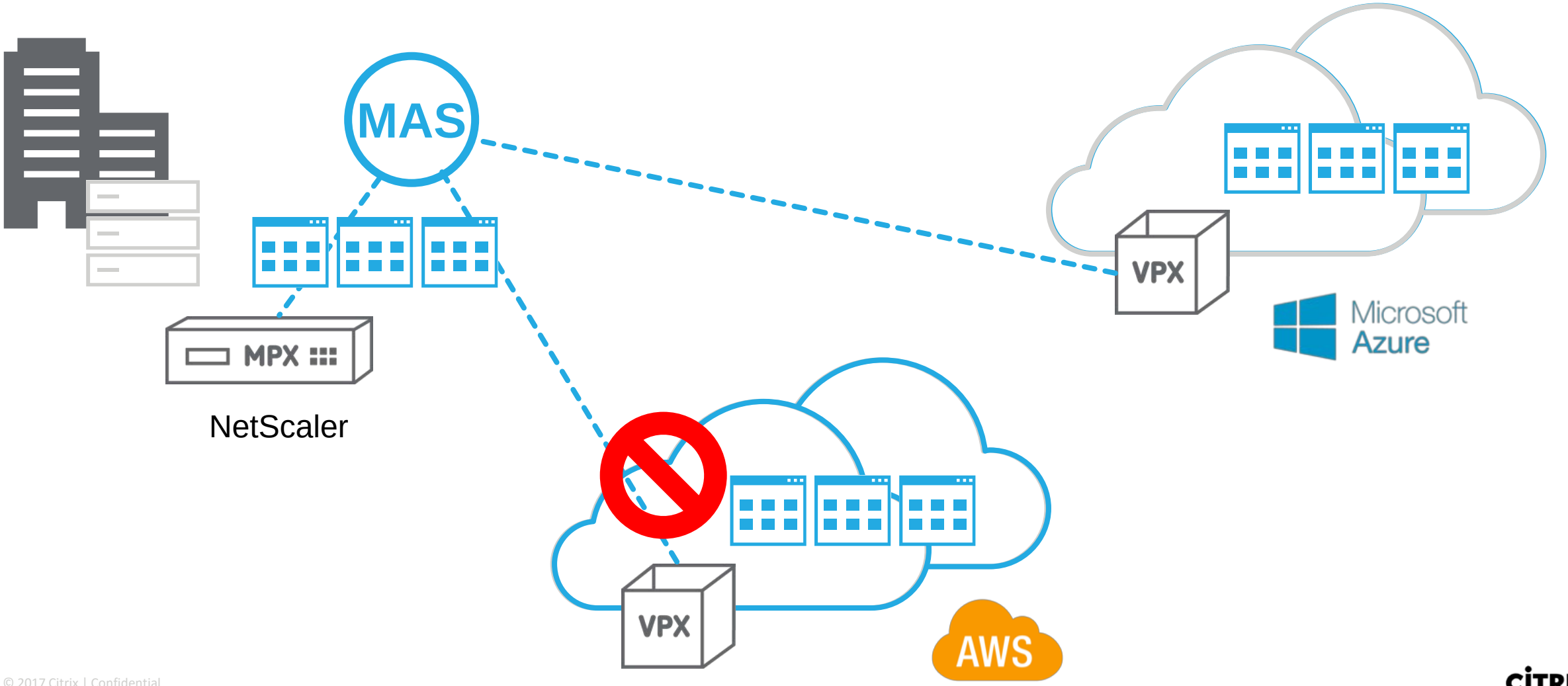
150 Gbps

Pooled Capacity

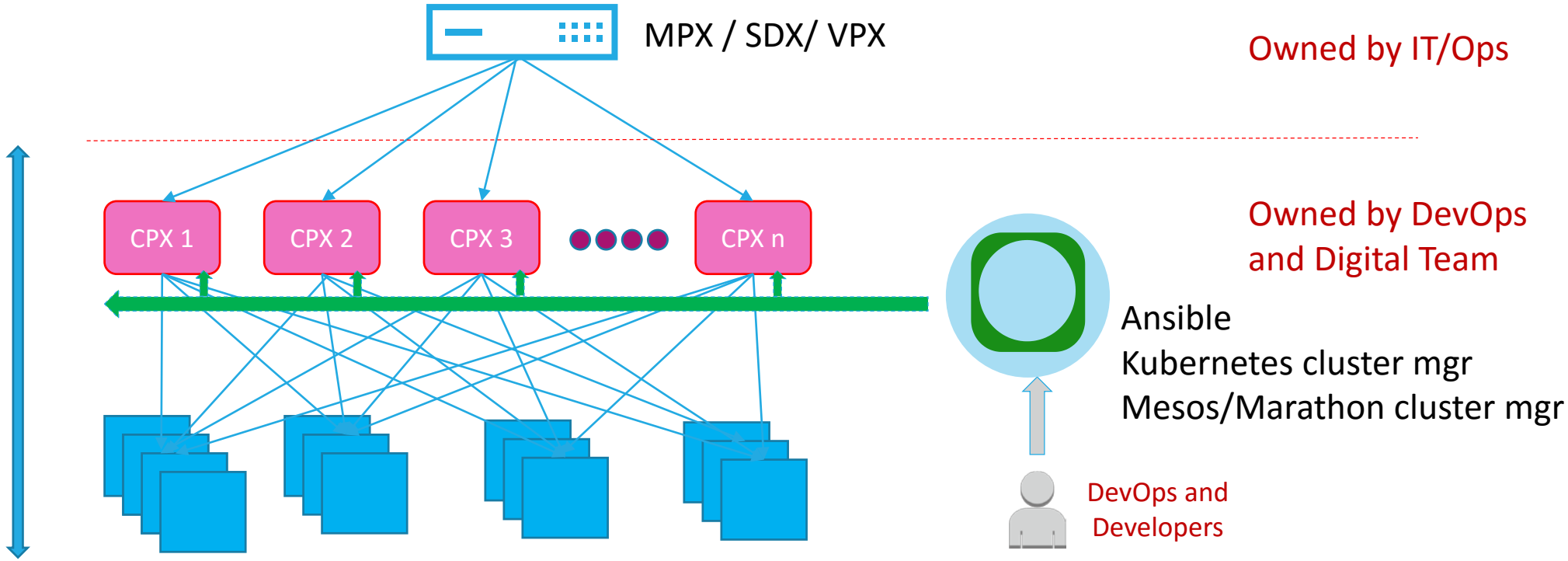
Reduce hardware investment

Lower the barrier to Cloud and virtualization

Hyper availability across clouds

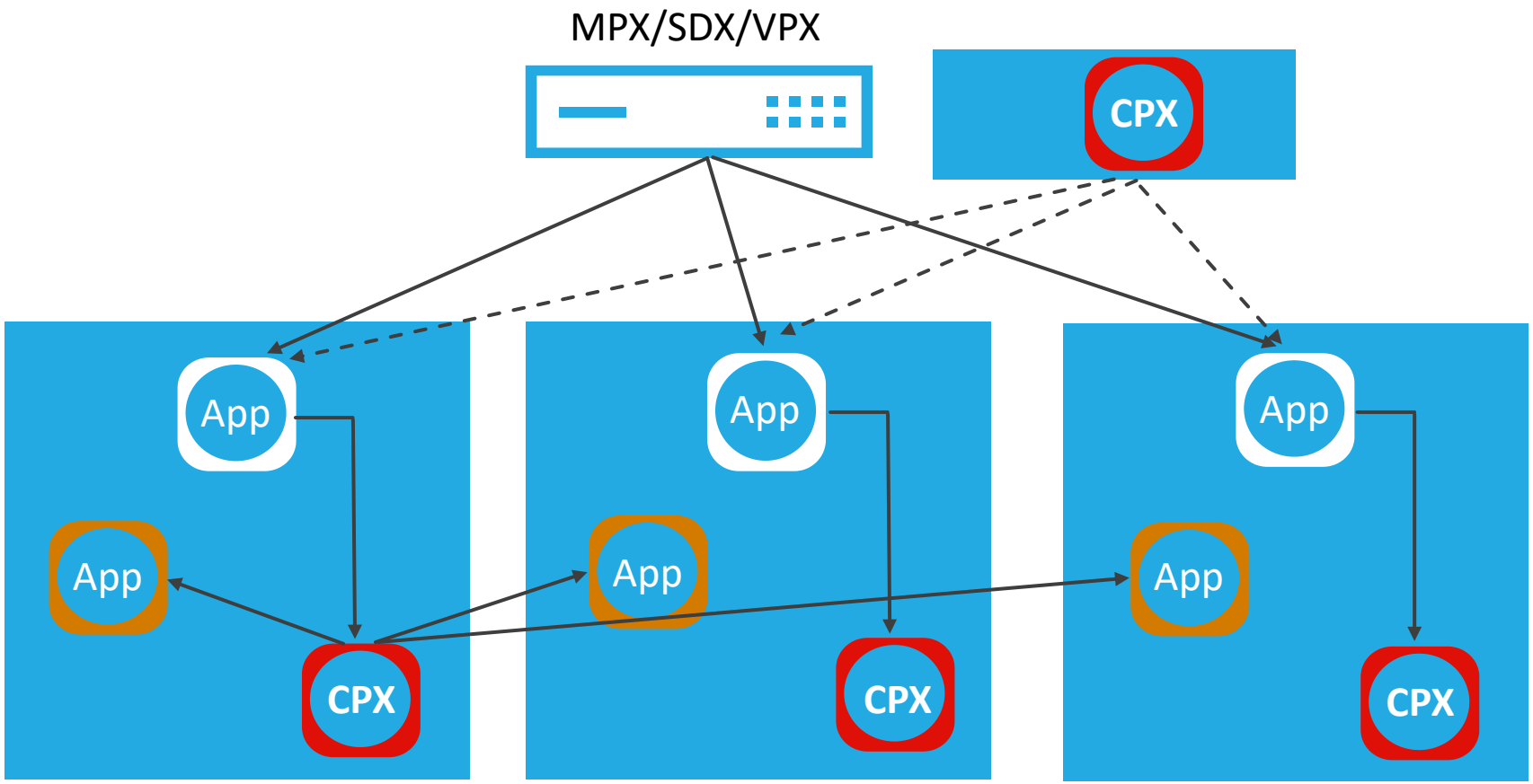


Providing Developers with CPX or VPX



M/V/S/C/PX for North-South and CPX for East West

Kubernetes Ingress Controller and Kube Proxy Replacement



Kube API Server

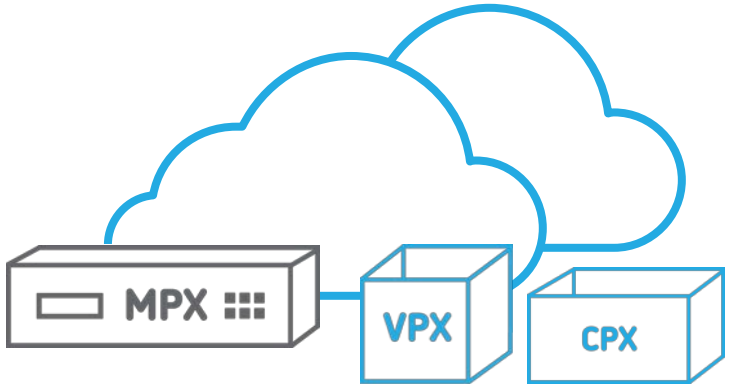
NetScaler MAS

Triton

Managed Apps

StyleBook

NetScaler is cloud ready



NetScaler

Responsive software

Support developer tooling

Secure access for web and SaaS

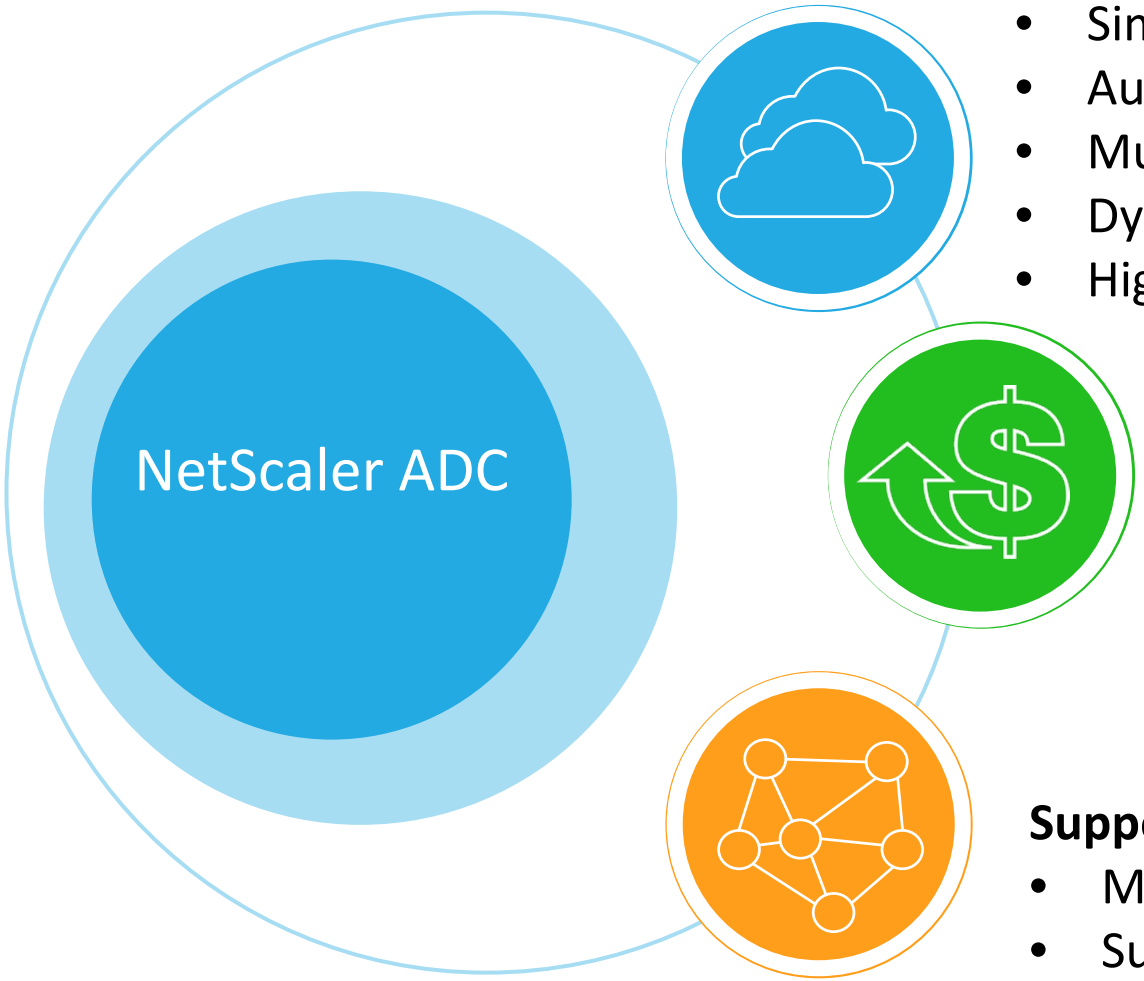
Reliable connection to cloud

One management platform

NetScaler 12.0

V12 - Core ADC Enhancements

NetScaler 12.0 ADC



Deploy in the cloud with ease

- Simplified new instance config in AWS
- AutoScale integration in AWS
- Multi-NIC/IP support for Azure
- Dynamic licensing allocation
- High performance ingress CPX for Kubernetes

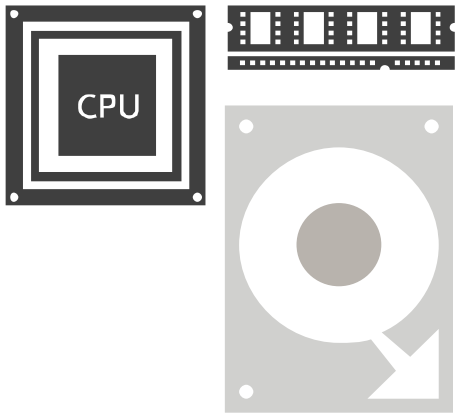
Dramatically improved price performance

- 3x improved VPX performance for SSL
- 3x bulk encryption on MPX/SDX FIPS
- Improved handling for ECDHE

Support IoT initiatives

- MQTT
- Support any protocol

Performance inhibiting factors

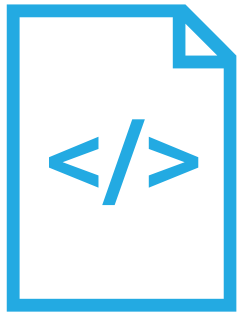


Hardware resources

- Available memory
- CPU utilization
- Custom chip sets

Encryption requirements

- ECC cipher support
- SSL everywhere



Software architecture

- Code efficiency
- Resource dependencies

Start with software…first

VPX SSL/TLS performance significantly improved

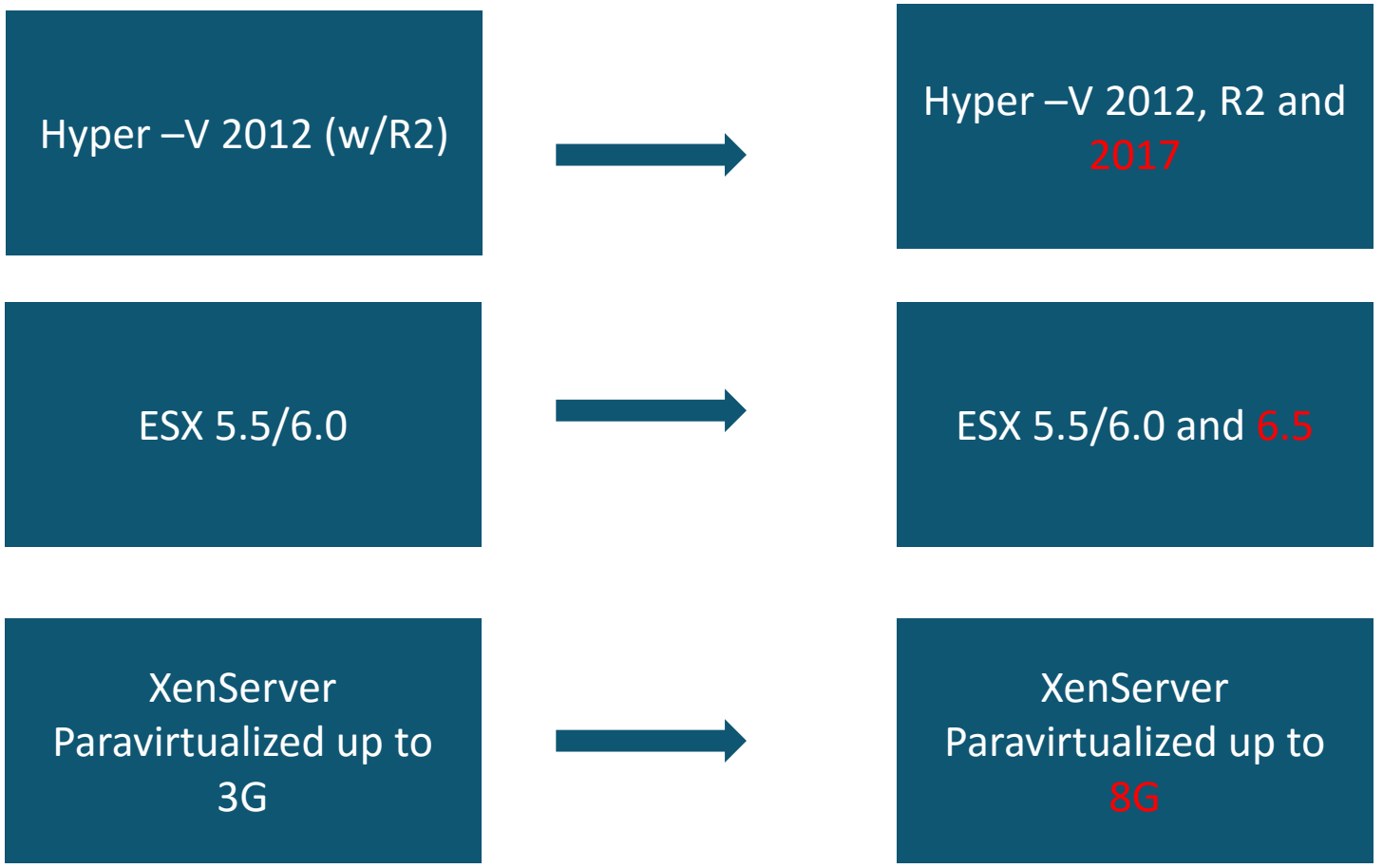
- Advanced vector extension: AVX2 (Intel Haswell onwards)
- Hypervisor: XenServer 7.0 or VMWare vSphere 6.5

New SSL Performance Data with Rel 12.0

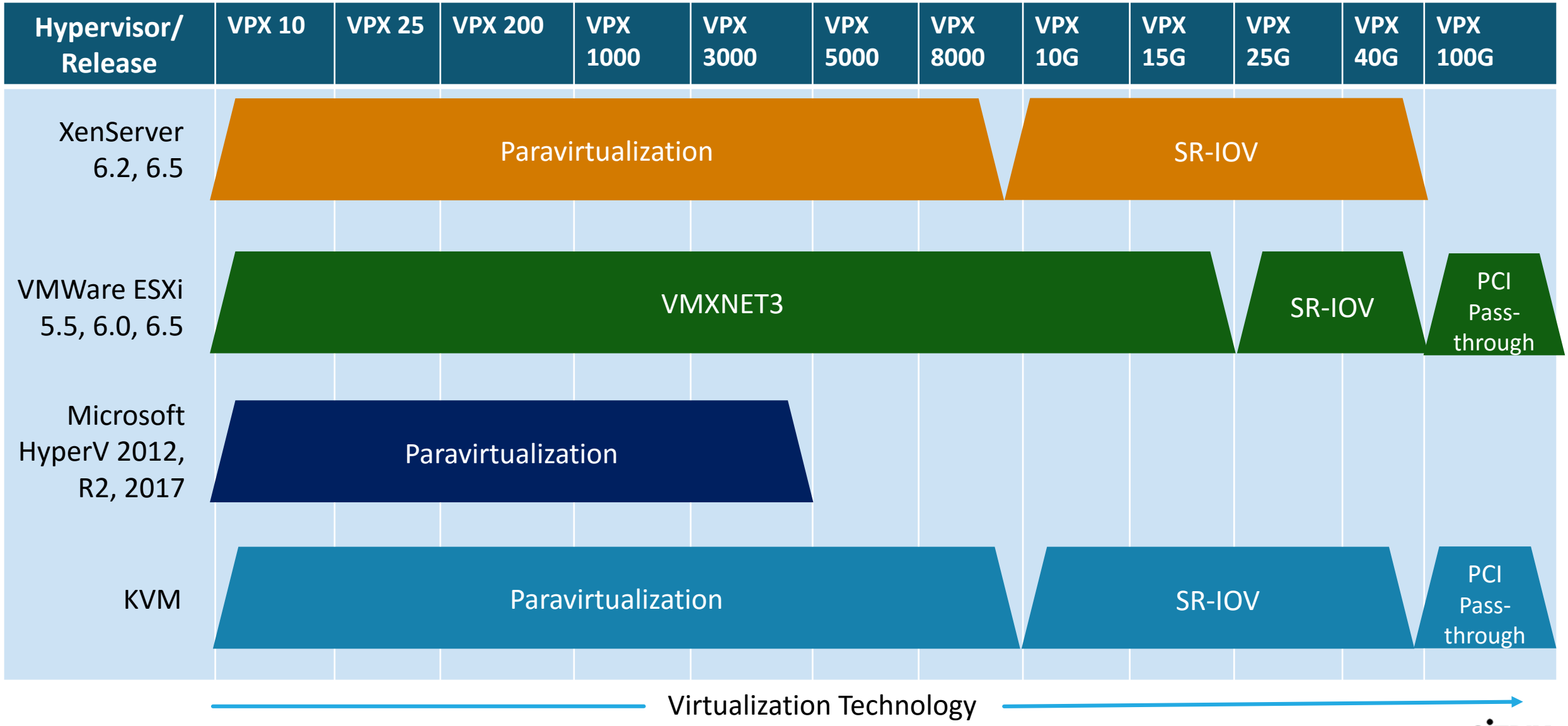
VPX Model	ECDHE - RSA (2K) TPS	RSA (2K key) SSL TPS	Pre-Release 12 RSA (2K key) SSL TPS
VPX 1000 (3 vCPUs)	1300	2,000 ⇧ 2 x	1000
VPX 3000 (3 vCPUs)	2600	3,030 ⇧ 3 x	1000
VPX 5000 (5 vCPUs)	3300	4,100 ⇧ 2.3 x	1800
VPX 8000 (5 vCPUs)	4300	5,200 ⇧ 2.6 x	2000
VPX 10G (9 vCPUs)	7900	9,300 ⇧ 2.6 x	3500
VPX 15G (11 vCPUs)	9600	11,400 ⇧ 2.5 x	4500
VPX 25G (15 vCPUs)	13,230	15,700 ⇧ 2.5 x	6200
VPX 40G (19 vCPUs)	15,000	17,000 ⇧ 2.4 x	7000
VPX 100G (19 vCPUs)	17,280	20,000 ⇧ 2.4 x	8200

- CPU: Intel(R) Xeon(R) CPU E5-2687W v3 @ 3.10GHz, number of sockets: 2, cores per socket: 10
- Advanced vector extension: AVX2
- Hypervisor: XenServer 7.0
- ECC size: 256 bit

New VPX Hypervisor Support



VPX Global Matrix



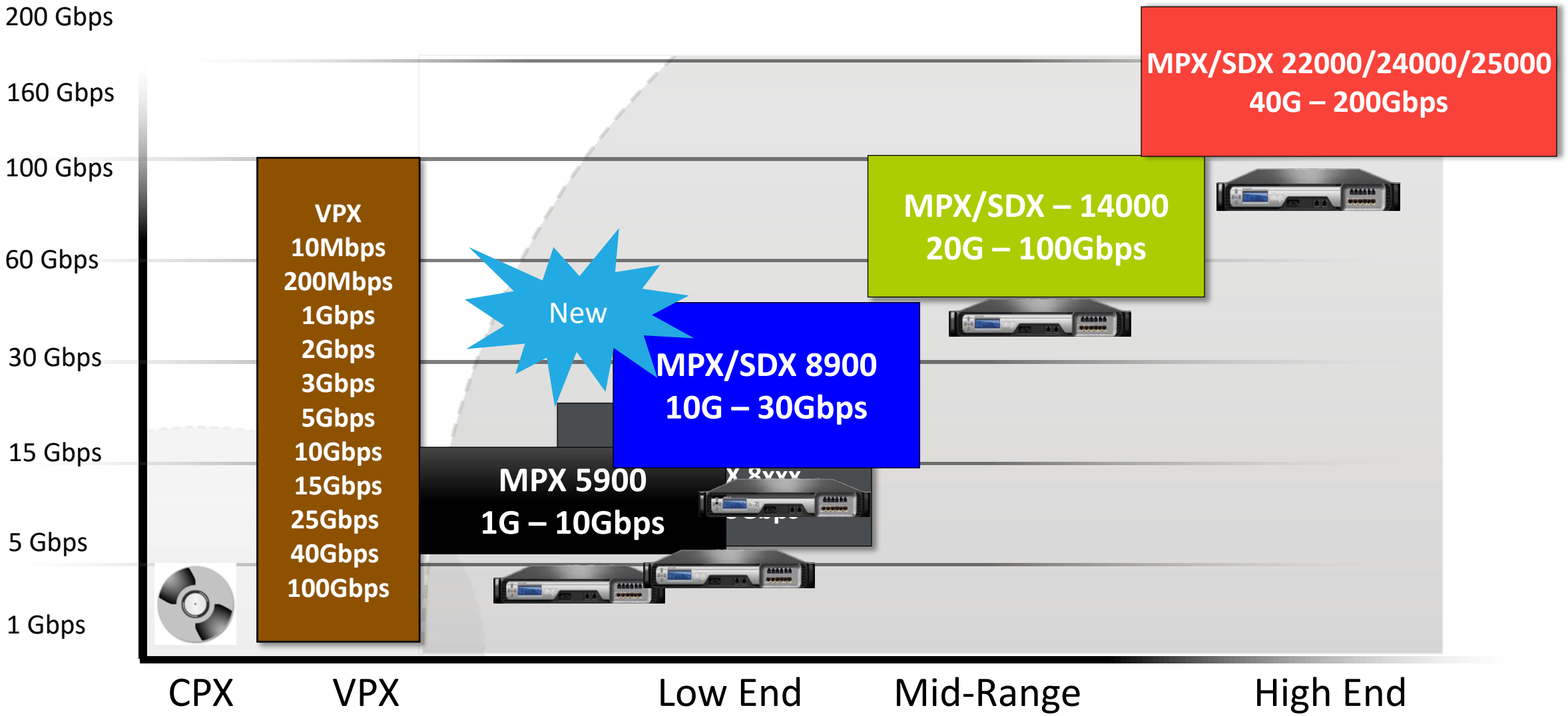
Benefits translate to hardware

Software First

	F5 iSeries i4600	NetScaler 8920
1 Year Asset Cost*	$79,560	**$70,800**
5 Year Asset Cost**	$125,800	**$114,000**
Bandwidth supported	20 Gbps	**20 Gbps**
SSL throughput	10 Gbps	**20 Gbps**
HTTP requests per second	550,000	**1,700,000**
SSL (RSA 2K) transactions per second	10,000	**22,000**
SSL (ECDHE) transactions per second	6,500	**10,000**

* Compared 5-year costs of product and maintenance of F5 iSeries i4600 Best vs. NetScaler 8920 Platinum Edition

NetScaler Platforms



New Low-End Platforms

Platform	MPX 5900	MPX 8900/SDX 8900
Pay-Grow Throughput (L7)	• 1 • 5 • 10	• 5 • 10 • 20 • 30
Port Configuration	2x10G & 6x10/100/1000	4x10G & 6x10/100/1000
Rack Unit	1U	1U
SSL Transactions per second	• Up to 6000 (ECC)	• Up to 15000 (ECC)
# of CPU Cores	8	8
Memory (GB)	8	32
#Instances	N/A	SDX 8910, SDX8920 and SDX 8930 - 2 instances included. Max 7

CITRIX

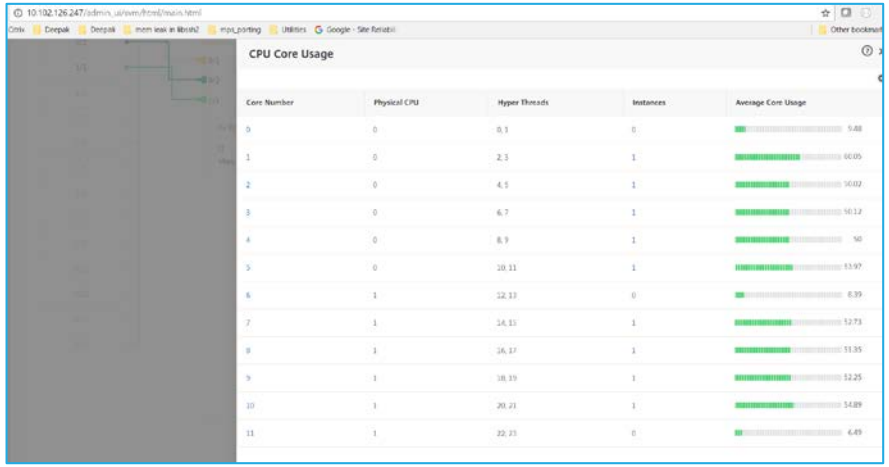
More

Other significant Core ADC Enhancements

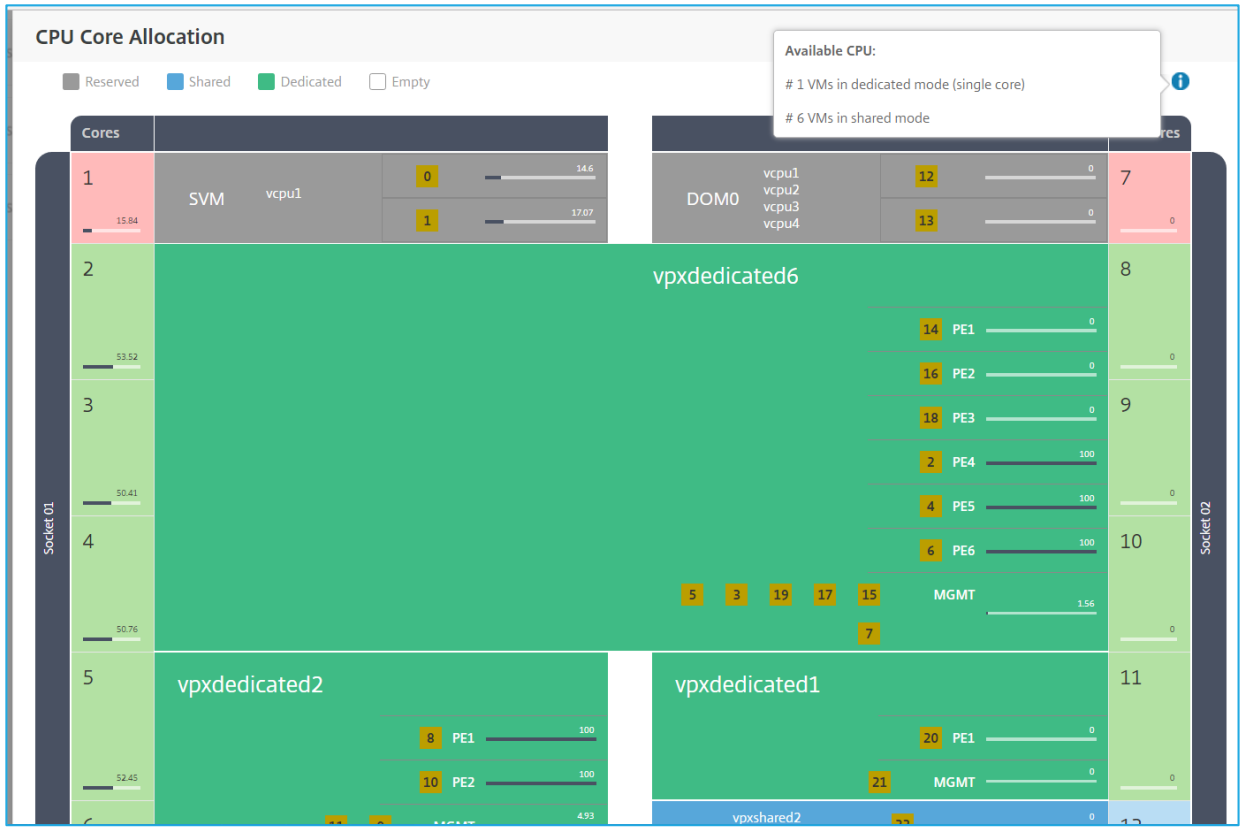
- Persistency groups across multiple vservers
- Vserver accept persistent sessions with TROFS
- GSLB Dashboard
- GSLB Wizard
- GSLB Real-time sync
- Bidirectional Forwarding Session (BFD)
- Cluster:
  - CLAG Support on SDX
  - Static ECMP
  - Graceful Node Join/Leave
- 2nd Management CPU for some models
- 40G series performance improvements
- Upgrade Notification (new version/build)

SDX CPU Visualizer

- CPU layout in dynamic tabular form
- Distinction between committed, shared, reserved or available CPU cores
- Show number of VMs that can be provisioned in dedicated or shared mode
- Show load distribution across CPU sockets



Hyper thread View



By 2020, more than 25 percent of identified attacks in enterprises will involve IoT

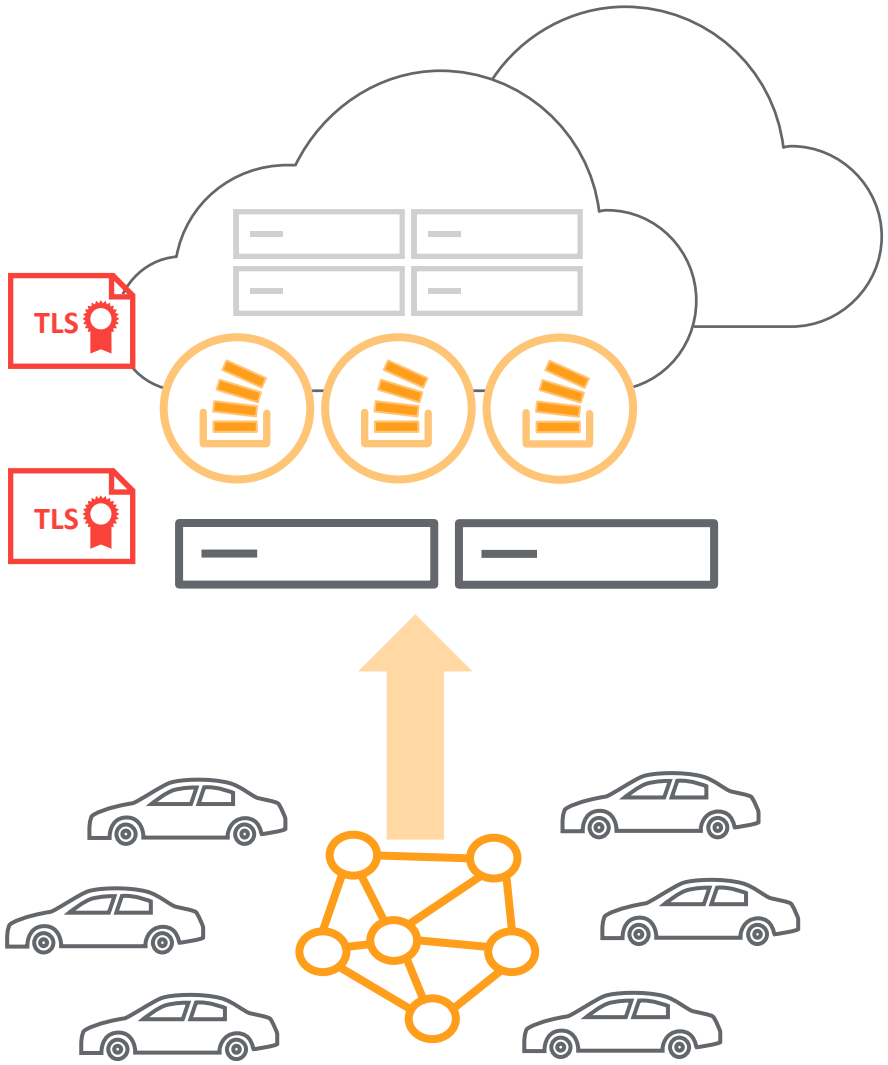
- Gartner

CITRIX

Security and performance risks

Ineffective Perimeter

- Poor scale & performance for TLS termination
- L4 load balancing inefficiency creates inter-broker overload
- Lack of security features: Device auth, DDoS prevention, surge protection
- Poor management & visibility



IoT platforms and applications

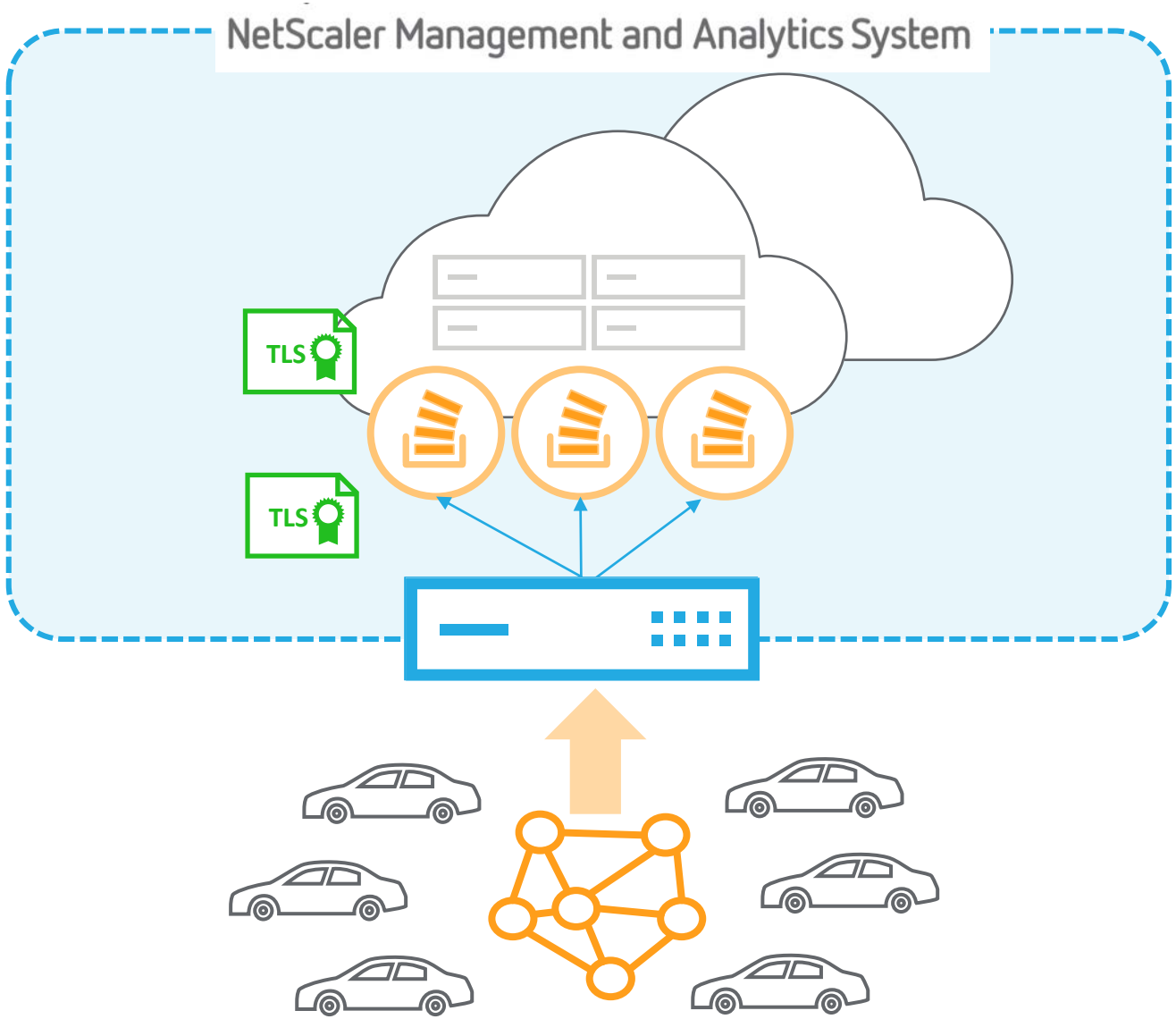
IoT message brokers

L4 load balancers

Secure event delivery

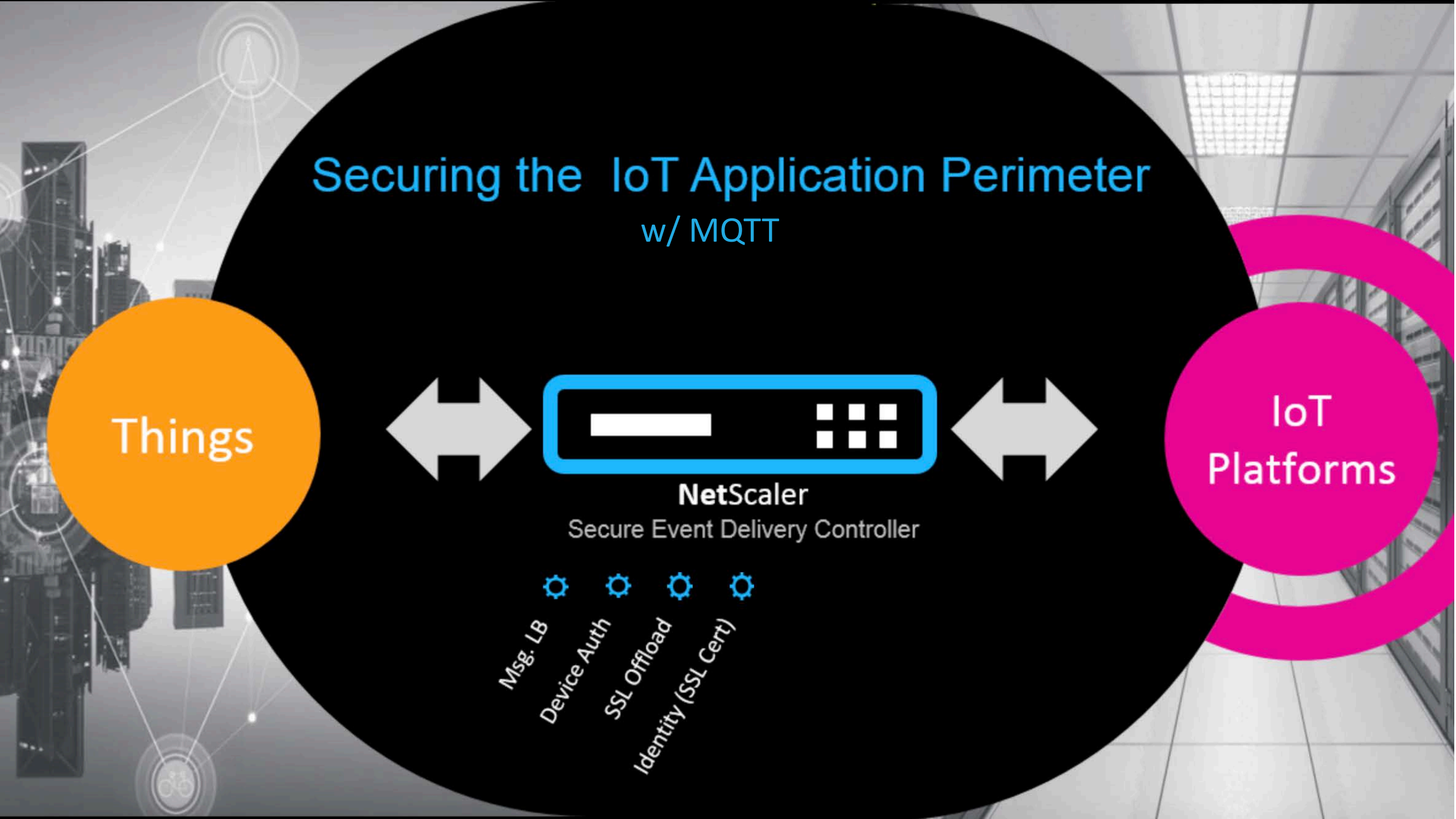
Effective Perimeter:

- Market leading scale & performance for SSL offload
- Connection identity management (SSL Certs.)
- IoT protocol message handling & load balancing
- Scale out hyper availability
- Can be deployed in private, public or hybrid clouds
- Management, visibility & advanced analytics

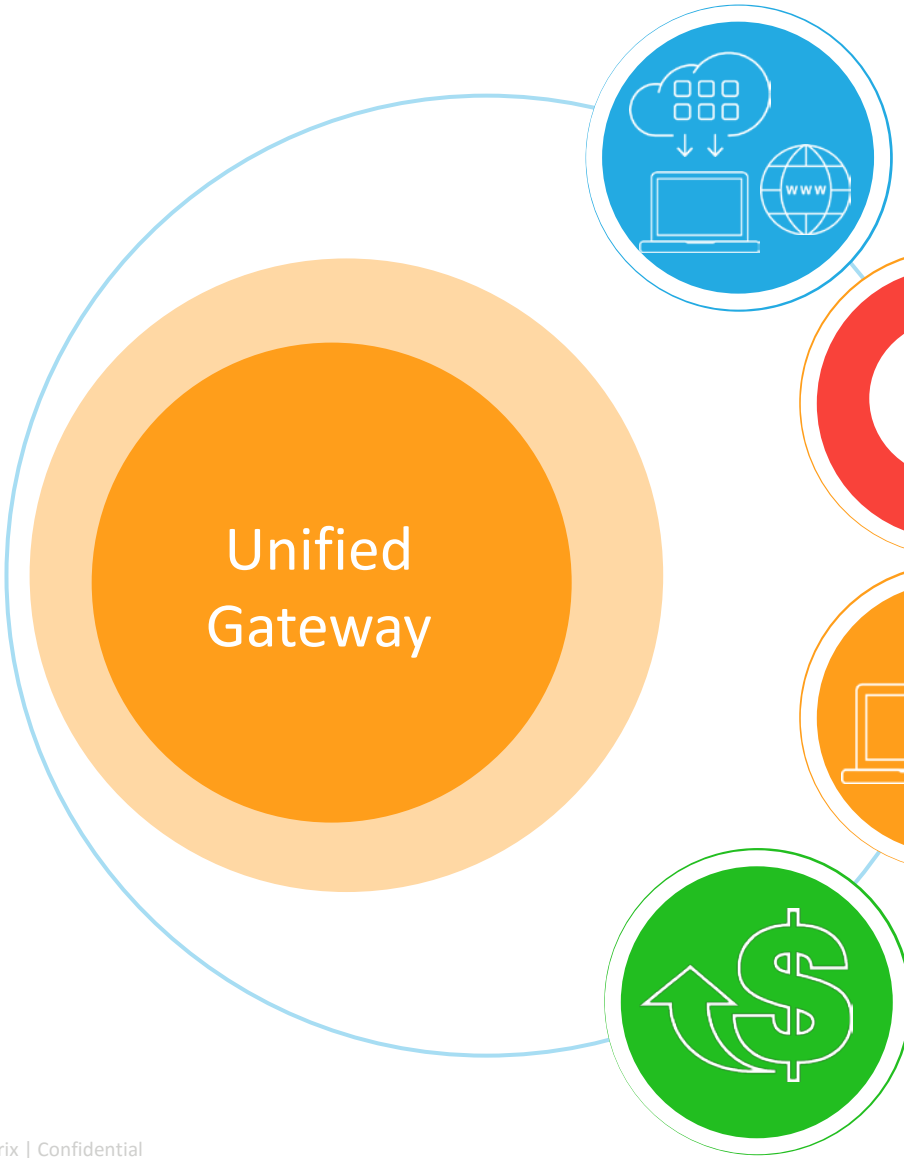


Securing the IoT Application Perimeter

w/ MQTT



NetScaler 12.0 Unified Gateway for Cloud and SaaS



Move to cloud and SaaS

- NGS scalability and user- experience

Secure User Identity

- Native OTP
- Extended support for OAuth and Open-ID

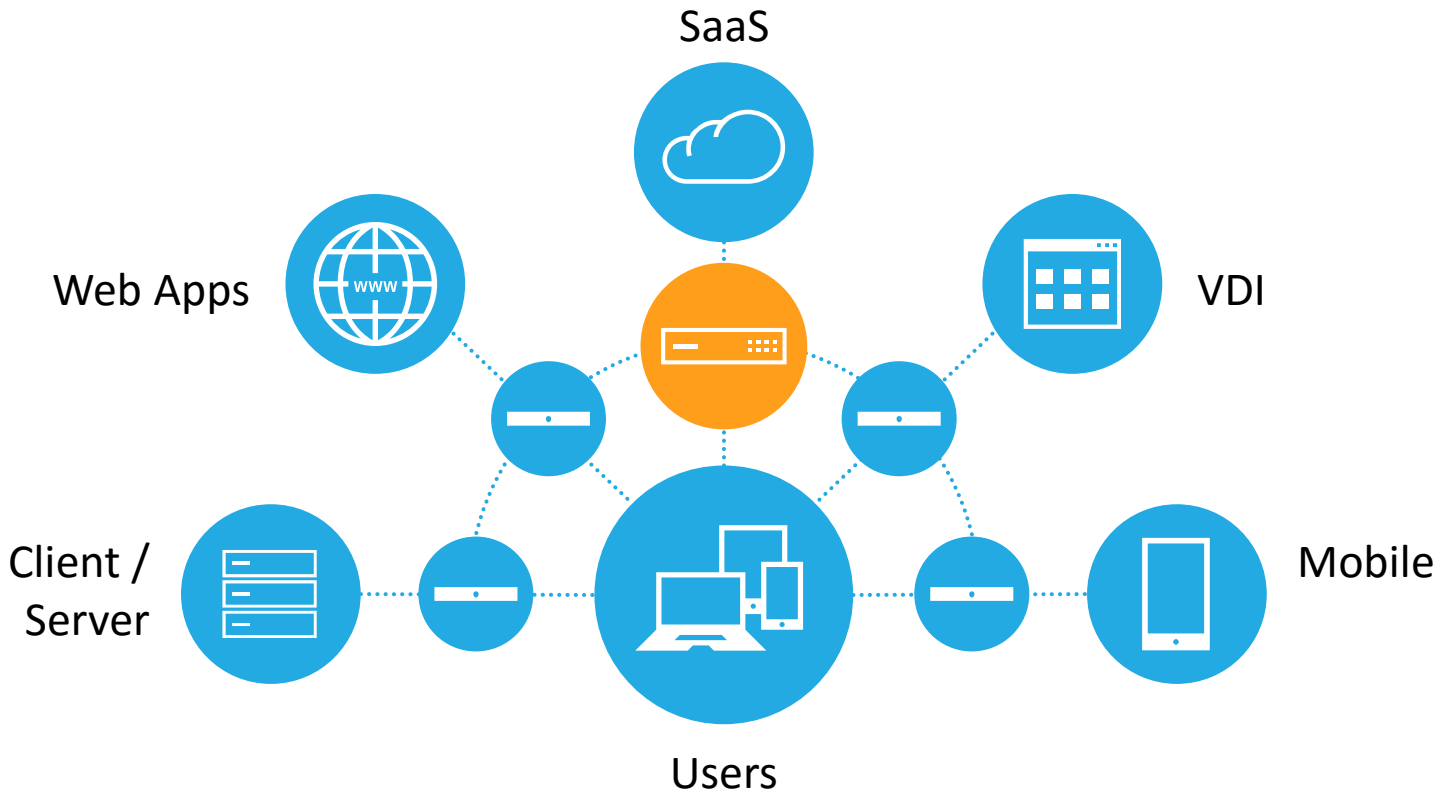
Best solution for XenApp/XenDesktop

- EDT support
- Outbound ICA Proxy
- New Policy Infrastructure
- StoreFront as authentication

Consolidation

- Microsoft Intune MDM/MAM
- PCoIP support (VMWare Horizon View)
- SSLVPN UDP enhancements

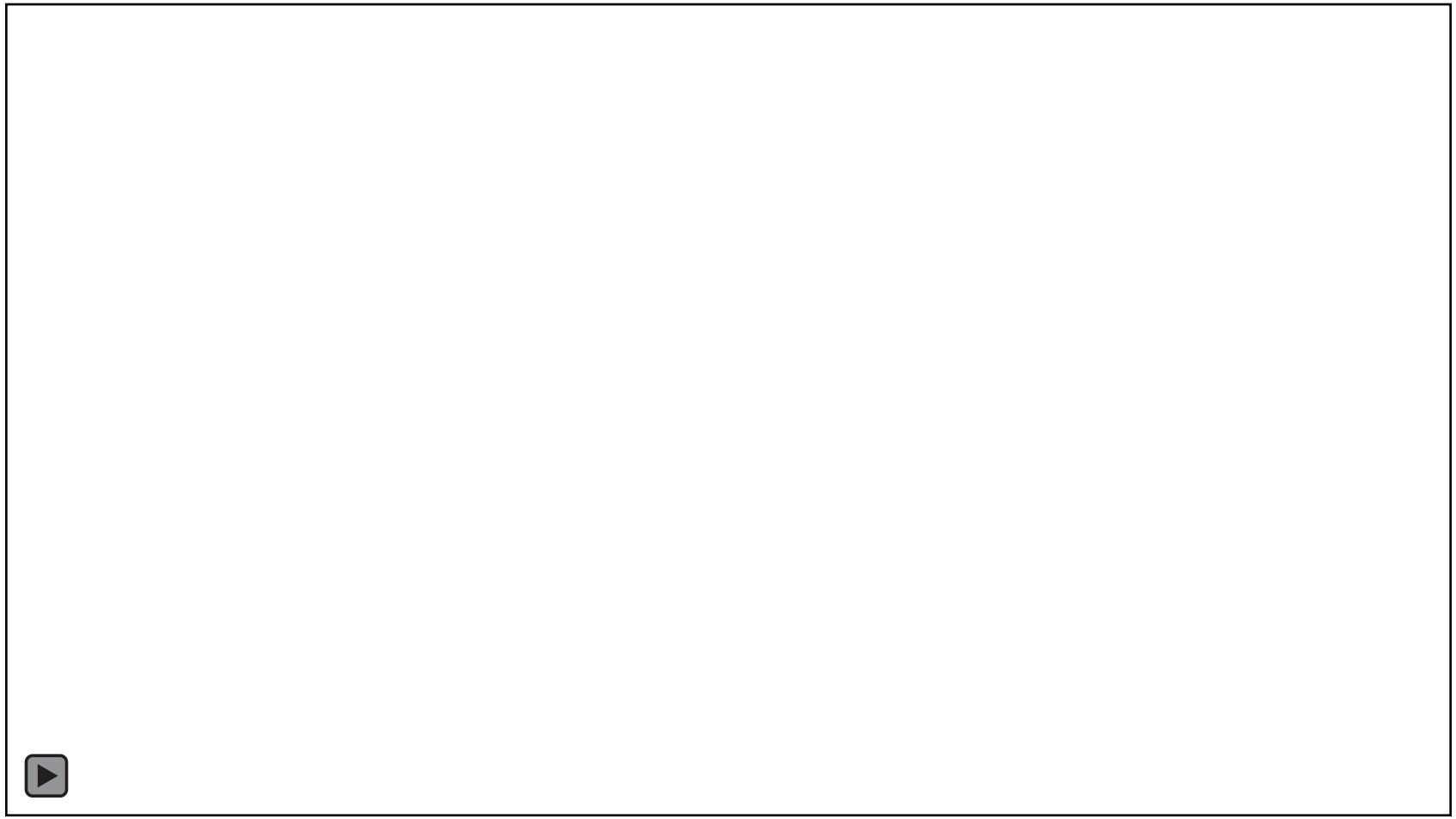
NetScaler Unified Gateway Consolidation – Made better



With 12.0 Release,

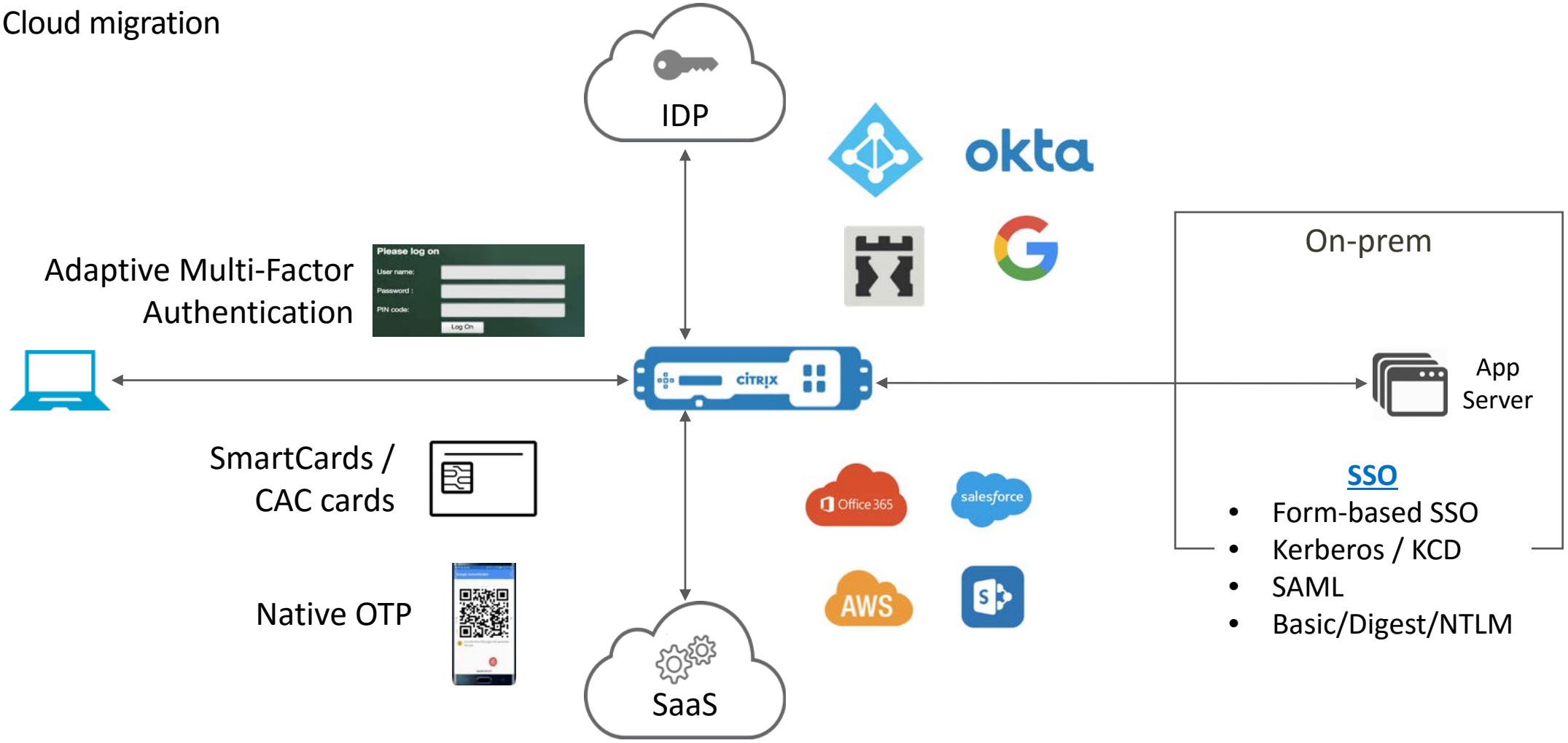
- Stronger with PCoIP & Intune apps consolidation
- Flexible with Advanced Policy support
- Optimal multimedia experience via DTLS based tunneling

Outbound ICA Proxy allows security policies implemented on local NetScaler



NetScaler IDAM

Ideal for Cloud migration



Native OTP – No 3rd party OTP required, reduce cost

- Standards based (RFC 6238) native OTP implementation
- Eg: Google Authenticator app as OTP client
- No 3rd party OTP/Radius servers required

Differences PE to PI

- Binding multiple policies with the same priority to the same bind point is disallowed in PI. In PE, such policy bindings are allowed and these policies are evaluated in the order in which they were bound.

```
bind vpn vserver vpn1 –policy PI_Session_pol1 –priority 1
bind vpn vserver vpn1 –policy PI_Session_pol2 –priority 1 >>Error
```

- Specifying the priority when adding a policy binding is optional in PE, but mandatory in PI. In PE, such policy bindings are added with a priority of 0.

```
bind vpn vserver vpn1 –policy PI_Session_pol
```

- **Binding same type of policy as PE and PI to same or different bind points is not allowed.**

```
bind vpn vserver vpn1 –policy PE_Session_pol
bind vpn vserver vpn2 –policy PI_Session_pol –priority 1
                        Or
bind vpn vserver vpn1 –policy PE_Session_pol
bind aaa user user1 –policy PI_Session_pol –priority 1
```

- Binding different type of policy as PE and PI to same bind point is allowed.

```
bind vpn vserver vpn1 –policy PE_Session_pol
bind vpn vserver vpn1 –policy PI_Traffic_pol –priority 1
```

Differences PE to PI

- Priority space of PI policies is local to a bind point in comparison to the global priority space of PE Policies.

bind vpn global –policyName *PE_Session_pol1 –priority 1 -> Preferred policy*
bind vpn vserver vpn1 –policy *PE_Session_pol2* –priority 2

- Policies bound to aaa groups with higher weight will take preference.

Add aaa group group1 –weight 1 -> *Policies bound to this group takes preference*
Add aaa group group2 –weight 2

GUI Changes for PE to PI

- Default Expression editor for Session, Authorization and Traffic policies is PI editor.
- Only supported PI expressions are shown for each VPN Policy instead of all the PI expressions.
- PI EPA can be configured from this path:
- Security -> AAA-Application Traffic -> Policies -> Authentication -> Advanced Policies -> Actions -> EPA
- In PI EPA configuration one editor combines Non OPSWAT and OPSWAT Expressions.
- In PI EPA, the EPA editor will list expressions supported for each OS type (Windows, Linux, MAC) separately.

NetScaler Gateway Configuration

1. Set up NetScaler and StoreFront interoperability
2. Select **DTLS** to secure datagram protocols
3. Link : https://docs.citrix.com/en-us/netscaler-gateway/11-1/hdx-enlightened-data-transport-support/configuring-netscaler-gateway.html

ICA Connection with UDT (MSI)

ICA Connections

End All ICA Connections | End ICA Connection

Username	Transport Protocol	Domain Name	Client IP	Client Port	XenApp/XenDesktop IP	XenApp/XenDesktop Port
sqladmin	UDP	dnpg-blr.com	10.106.38.28	65465	10.106.38.33	2598
sqladmin	UDP	dnpg-blr.com	10.106.38.28	65466	10.106.38.33	3000
sqladmin	UDP	dnpg-blr.com	10.106.38.28	65468	10.106.38.33	3002
sqladmin	UDP	dnpg-blr.com	10.106.38.28	65467	10.106.38.33	3001

Supported NSG Modes & Features

- **HA, Cluster, Unified Gateway**
- **FULL VPN**
- **CVPN**
- **ICA Proxy**
    1. ICA Proxy deployment
    2. HA
    3. Cluster
    4. MSI
    5. Unified Gateway
    6. GSLB
    7. DUAL STA
    8. CLI & UDT connection Management
    9. ICA Session Timeout
    10. Kill Connection
    11. Framehawk
    12. Client to NSG DTLS

Not Supported with NSG :

- GWAAS/NGS
- IPV6
- Double HOP
- LAN Proxy
- HDX Insight for UDT
- NSG to vda DTLS support
- SOCKS

Receiver Support:

- Windows 4.7
- iOS 7.2
- MAC Receiver 12.5

System test results for UDT

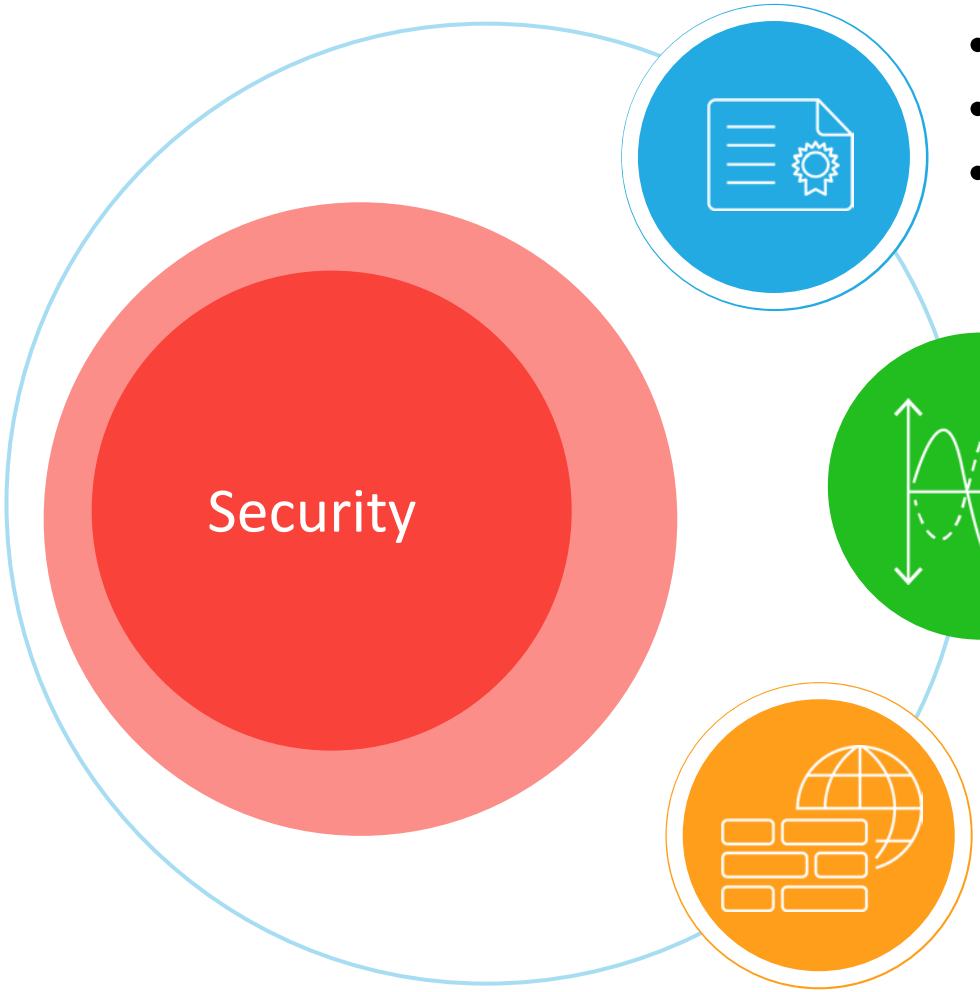
190ms RTL, 0.1% packet loss

- 18% faster interactivity (Thinwire with Adaptive Display)

250ms RTL, 1% packet loss

- 2X smoother interactivity (Thinwire)
  - Even faster on bandwidth limited pipes with Thinwire 7.13 bandwidth reductions
- 10X faster printing
- 5X faster file transfers
  - 10x faster with CDM improvements in Q1 release
- Plays HD 720p server-fetched client-rendered video without transcoding
  - Reduced CPU consumption lowers vCPU requirement from 2 to 1

NetScaler 12.0 Security



SSL Performance

- New Ciphers, Hybrid SSL
- Hybrid FIPS/SDX FIPS
- NetScaler MAS: SSL Insight

DNS Update

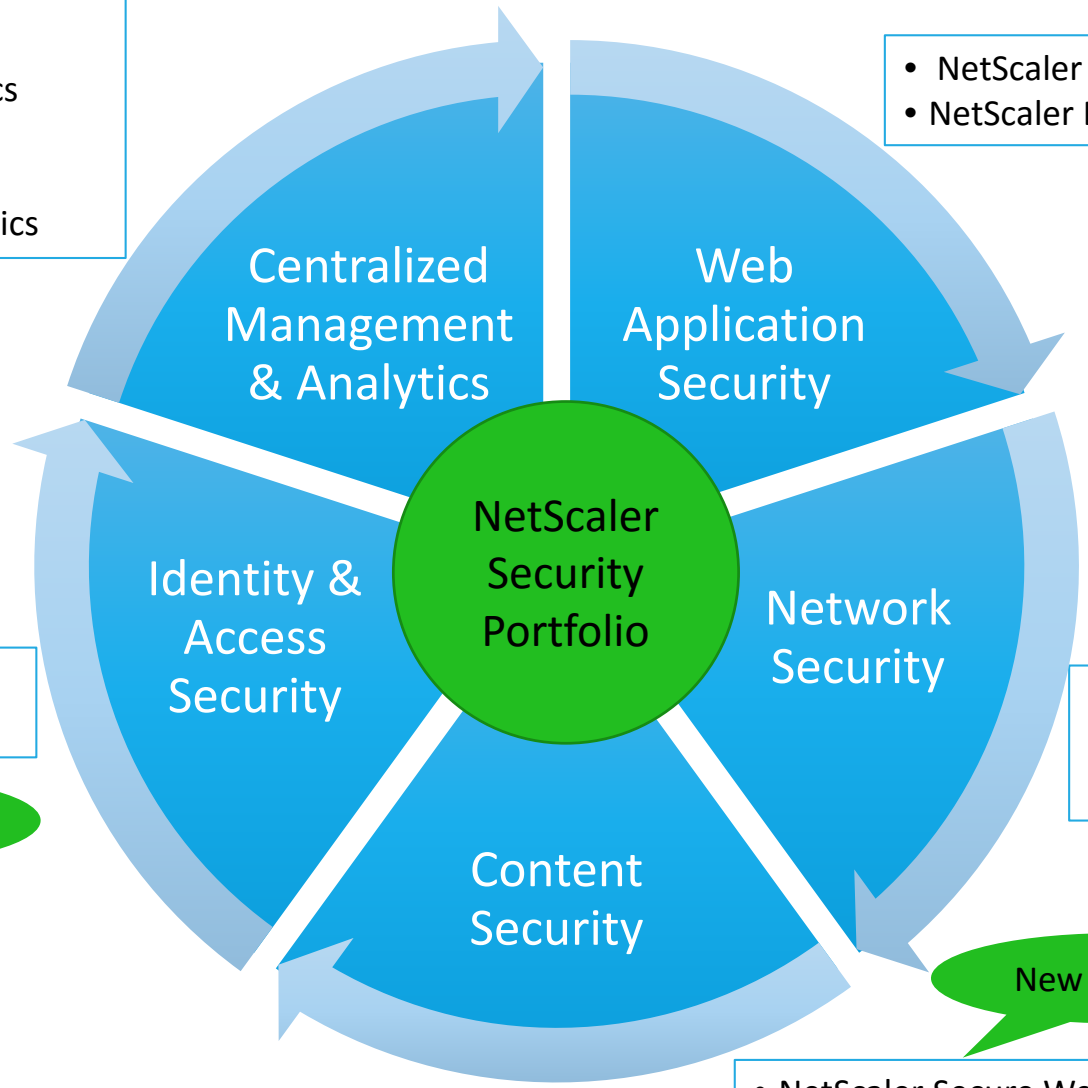
- DDoS Protection
- Reserve System memory
- DNS Security Profile

Secure Web Gateway

- SSL Visibility
- URL Filtering
- NetScaler MAS: User Behavior Analytics

NetScaler Security Portfolio

- NetScaler MAS
  - Security Insight
  - App Security Analytics
  - Gateway Insight
  - SSL Insight
  - User behavior Analytics



- NetScaler AppFirewall
- NetScaler DDoS Protection

- NetScaler Unified Gateway
- AAA

Update

Update

- DNS Protection
- DDoS Protection
- SSL Proxy

Update

New Solution

- NetScaler Secure Web Gateway (NetScaler SWG)

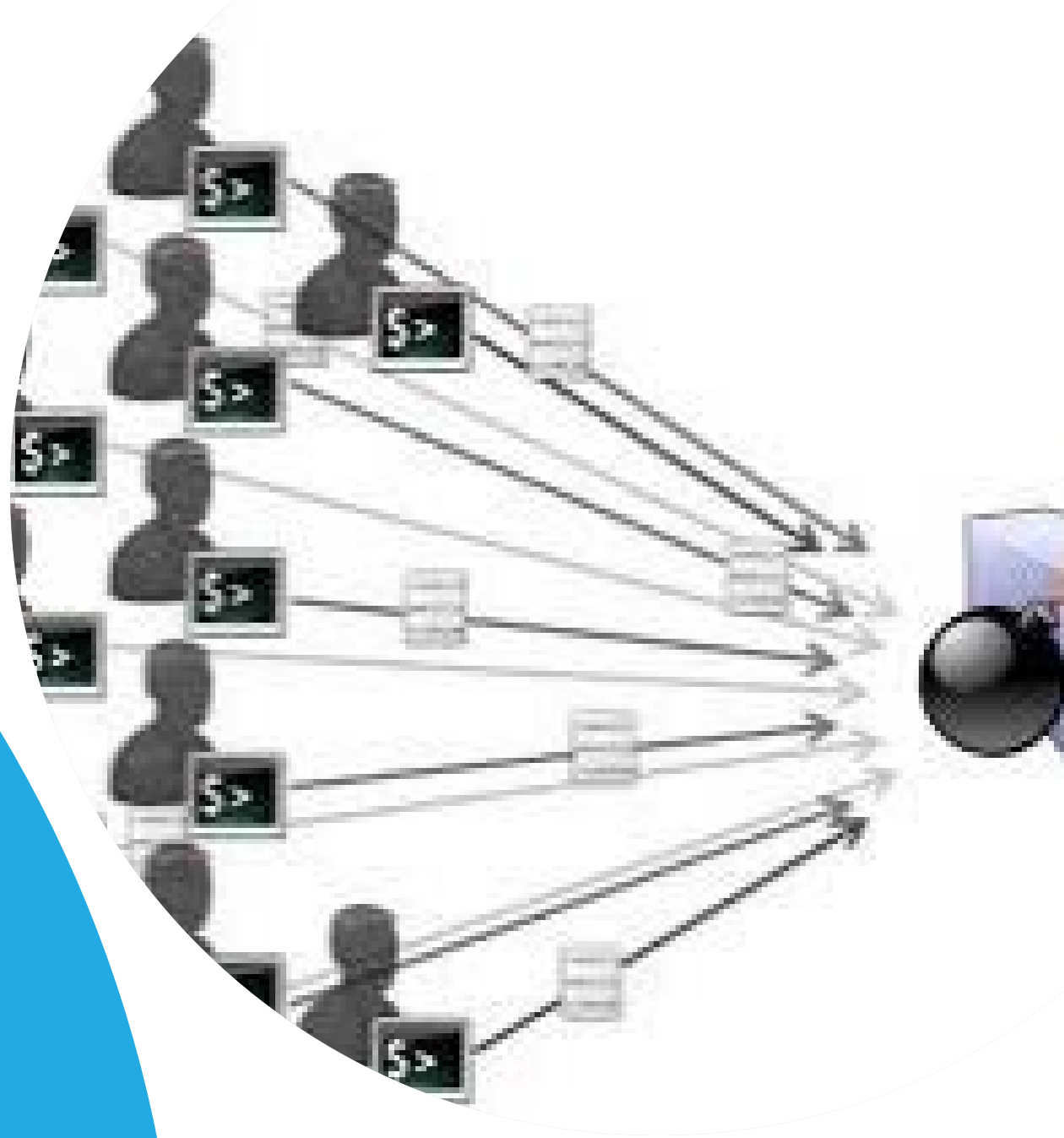
NetScaler SSL Update

More

SSL Enhancements Overview

- SSL Session Sync Support in NetScaler Clusters
- Session Tickets
- 14K FIPS Series (MPX/SDX) and Supported Cipher Details
- Hybrid FIPS Mode on 14000 FIPS Series
- VPX Perf Optimization (RSA, ECDHE)
- OCSP Stapling
- Cluster supported features – SSL Profiles
- Built-in HSTS
- Removal of 3DES ciphers from default cipher group
- Cipher Parity Matrix
- New Signature extensions support
- Updating Intermediate cert without breaking Certlink

NetScaler DNS Security Update

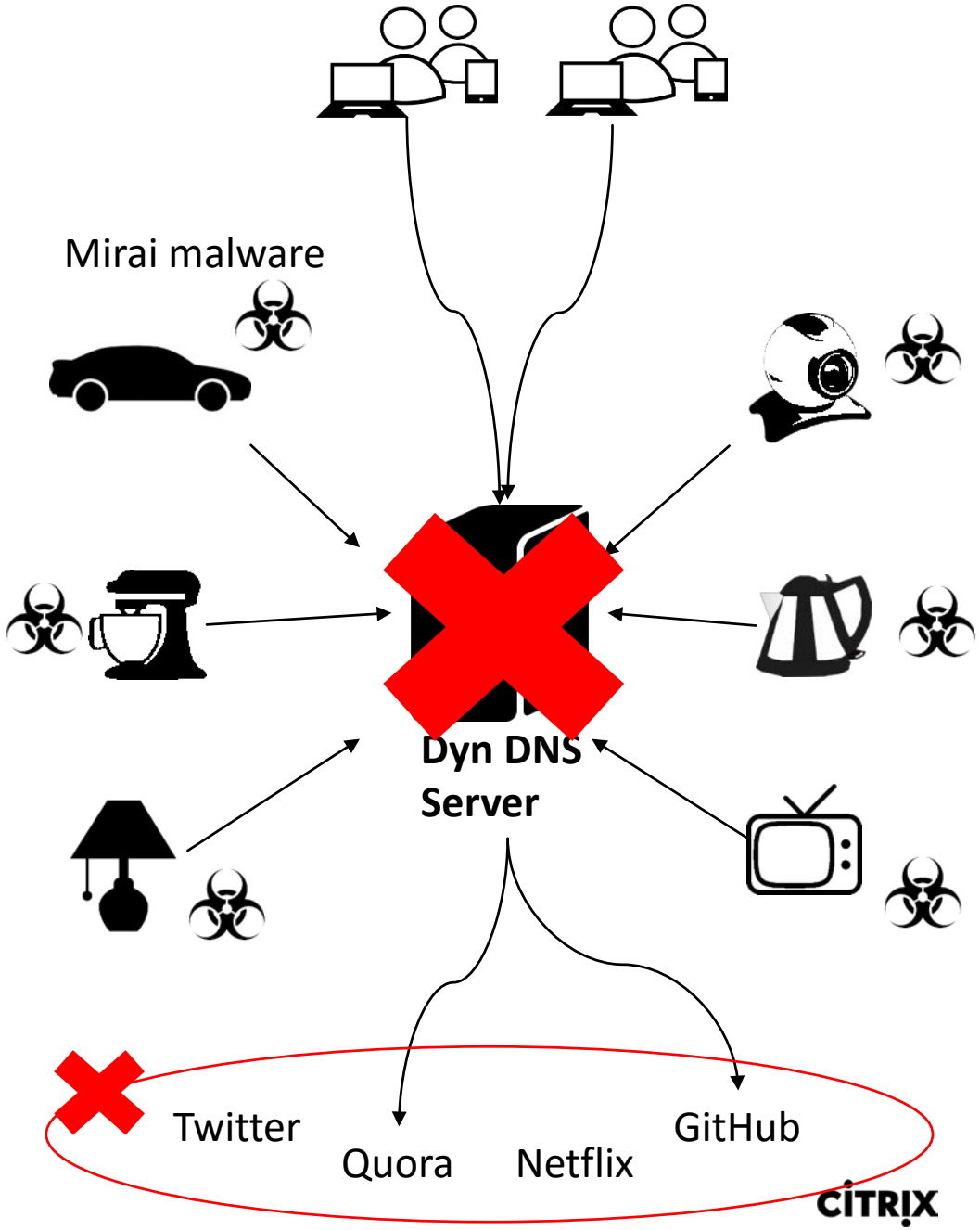


CITRIX

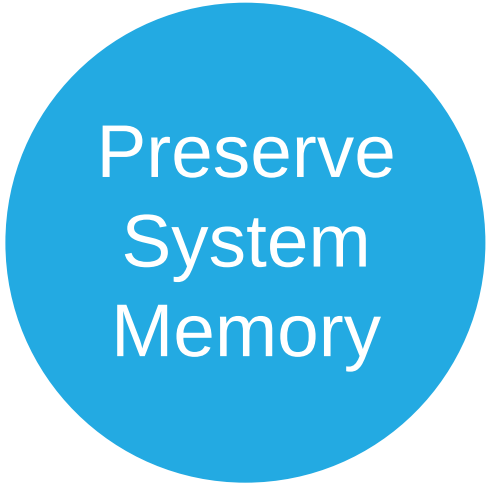
2016 Dyn DDoS Attack

What happened ?

- Largest DDoS attack on record
- High profile services were affected
- Millions of IP addresses went down
- Attack size: 1.2 Tbps

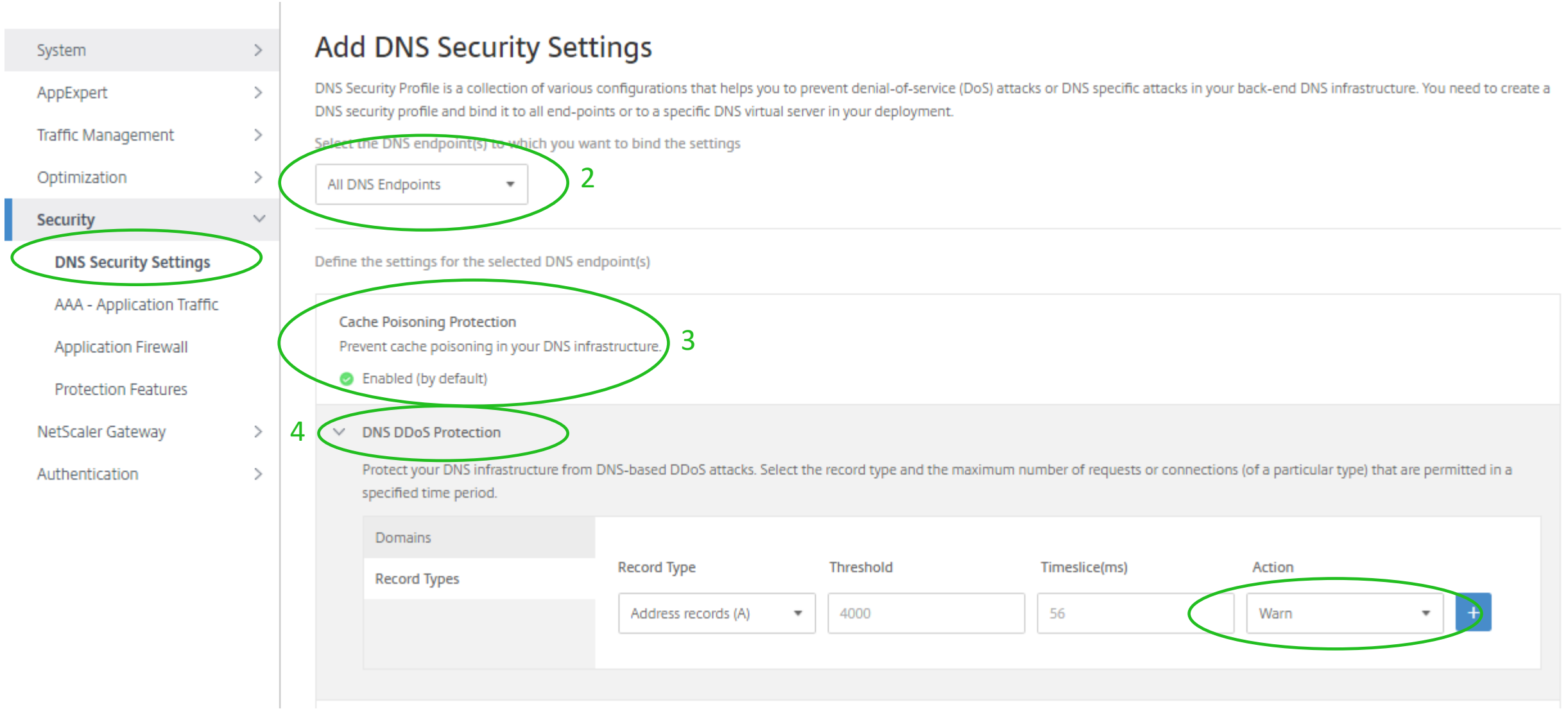


DNS DDoS Protection



During Attack	**Cache Overloading**	**Cache flooding**	**Cache Bypass**
Solution	Allows to restrict DNS cache size	Freeze DNS cache from expiry	Disable bypass cache and respond from cache

NetScaler DNS Security Settings



More

DNS Attack Protection

- DNS Firewall is a security feature which will prevent DoS and DNS specific attacks
  - DoS Protection
  - Exceptions – Whitelist/Blacklist
  - Cache Poisoning Protection
  - Limiting maximum query length
  - Bypass cache settings
  - Setting TC bit
  - DNS root referral
  - EDNS domain name caching + client subnet support
- DNS Firewall options available currently are spread across views
- With DNS Firewall, customers will get a consolidated user-friendly GUI solution for all their DNS security concerns
- Security settings can be on a vserver level or global

Netscaler MAS

NetScaler Secure Web Gateway (SWG)

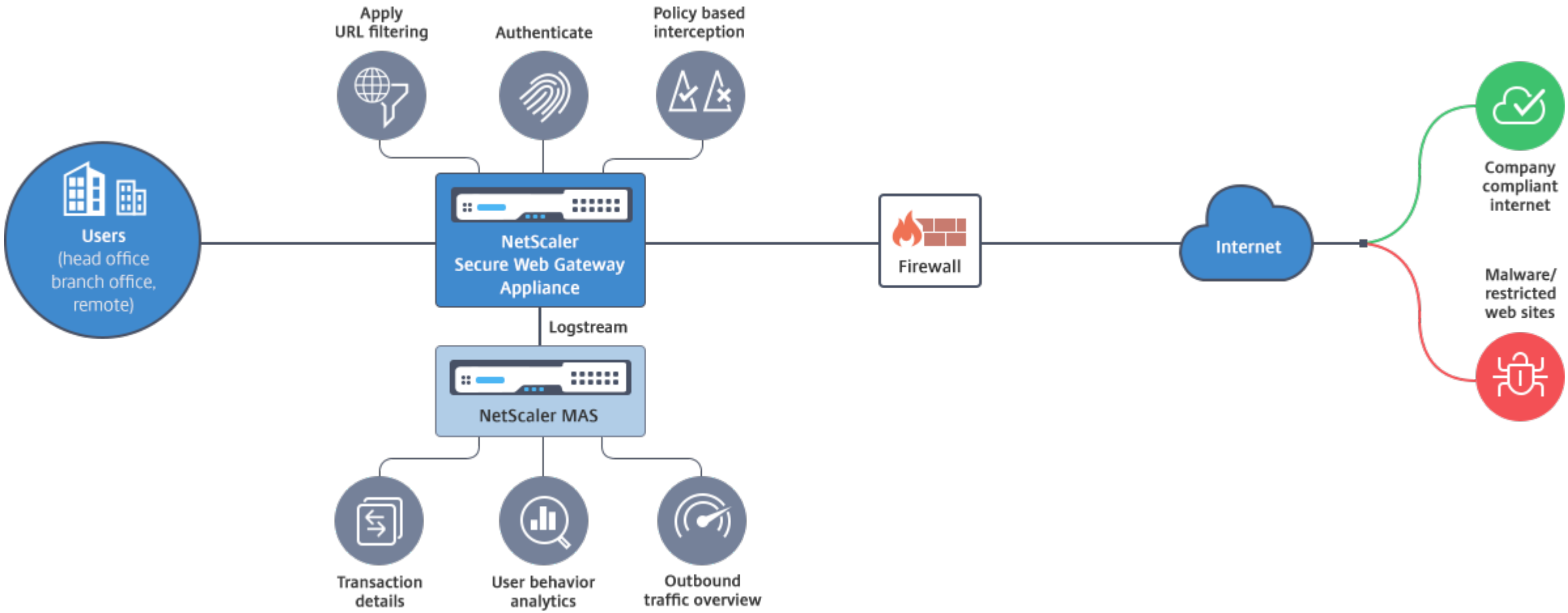
Phase 1

Why SWG?

50 percent of all network attacks will be through SSL encrypted traffic by 2017 -- *Gartner*

Visibility into SSL encrypted traffic is critical to stop potential threats

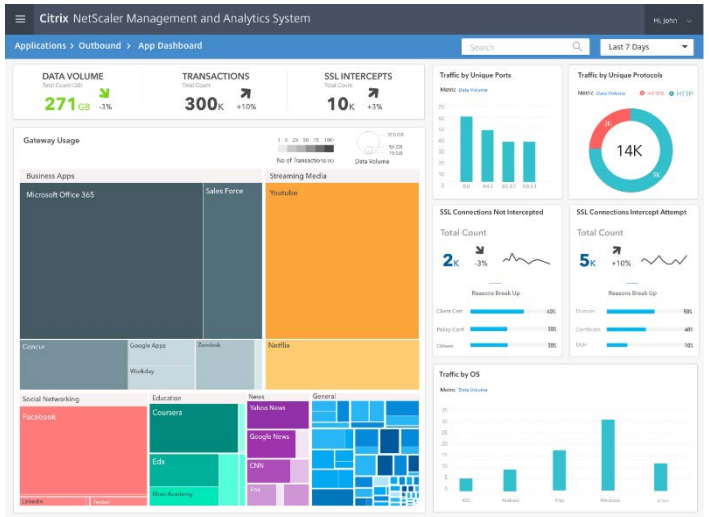
NetScaler Secure Web Gateway



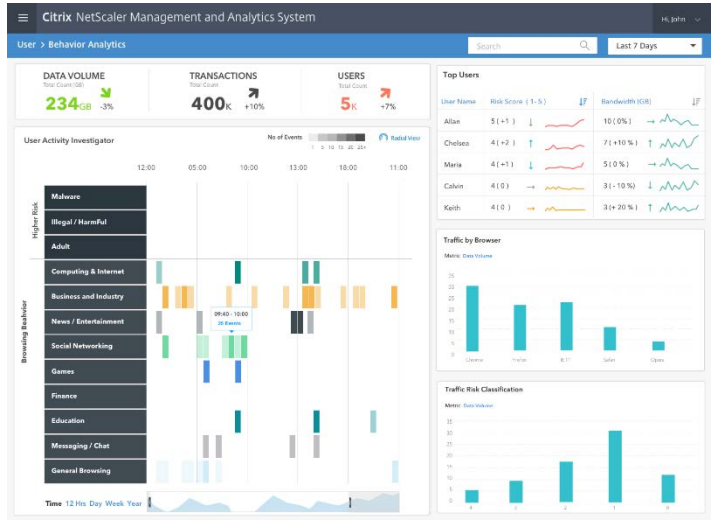
135

SWG App / User Workflow

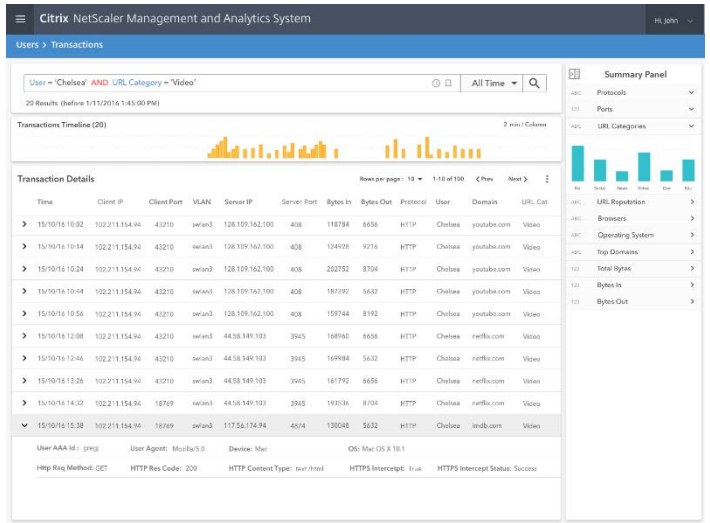
Outbound App Dashboard



User Behavior Analytics with Linear Heatmap



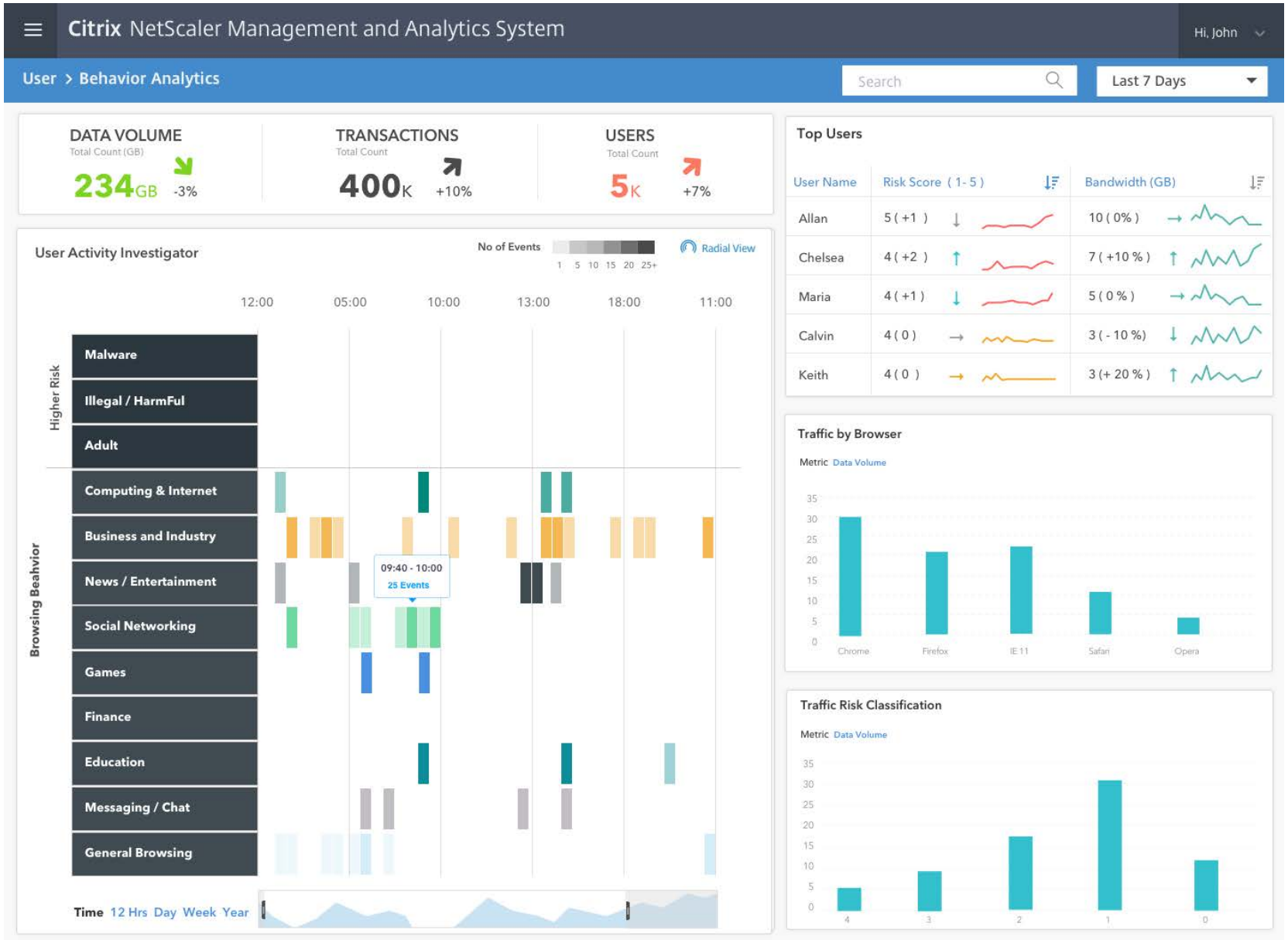
User Details Report



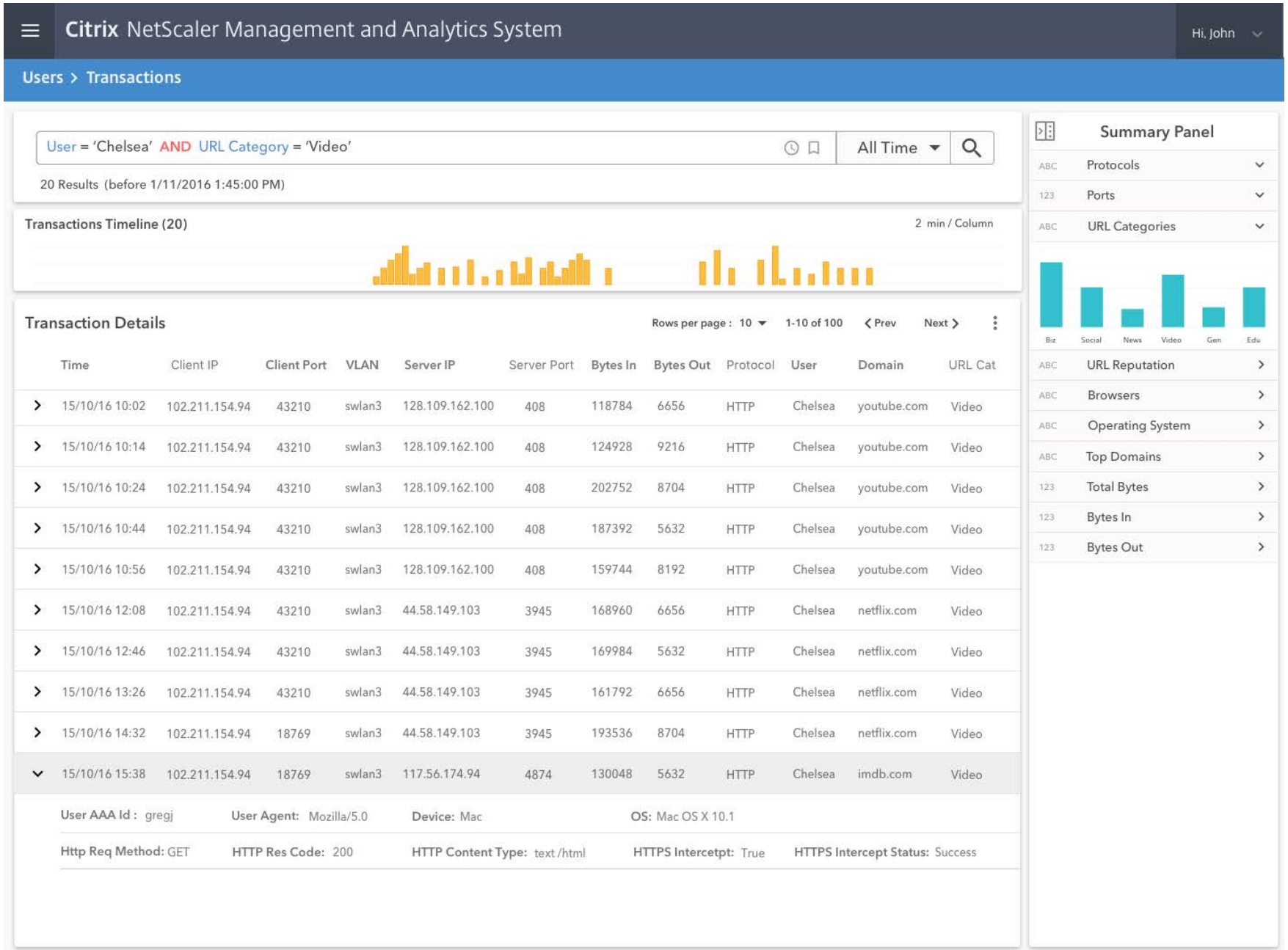
Outbound App Dashboard

User Behavior Analytics

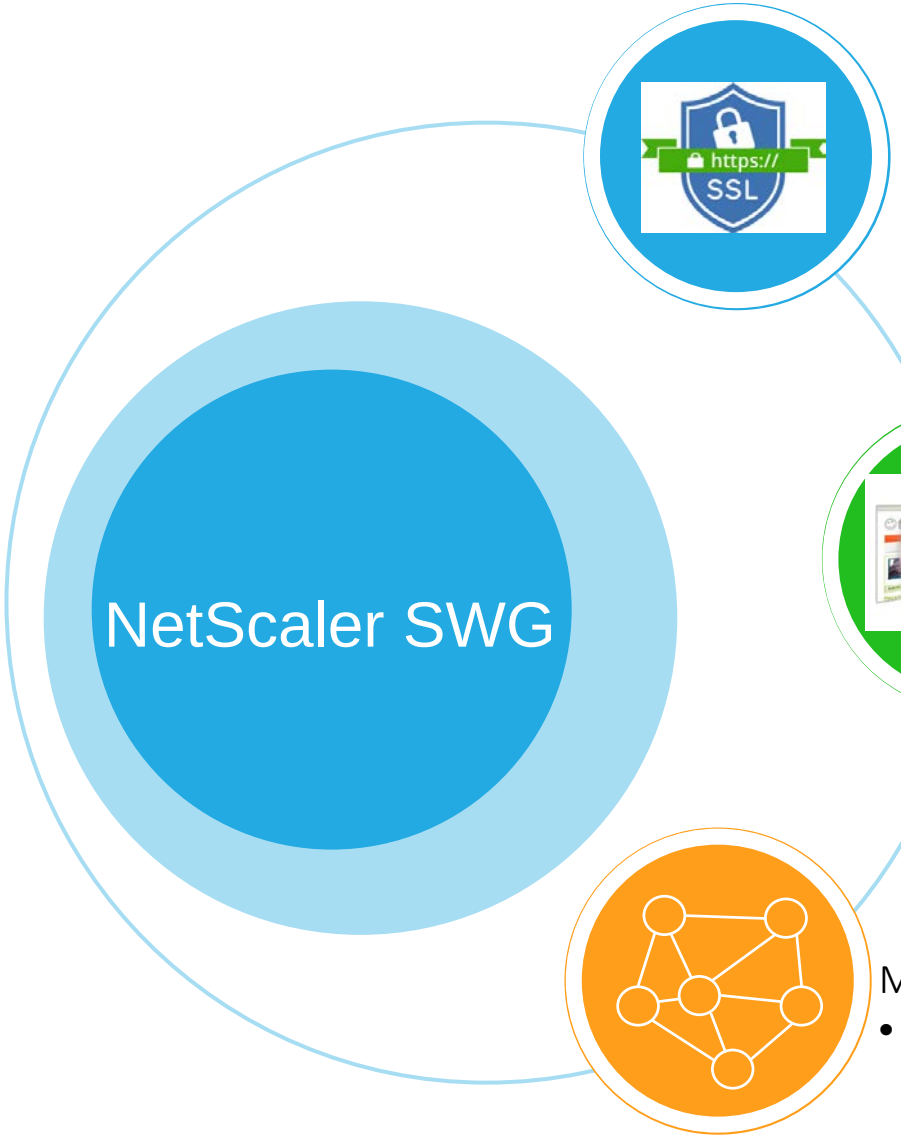
User Activity - Linear Heatmap



User Detail Report



NetScaler SWG Phase I Key Features



Forward Proxy support

- SSL Visibility into encrypted traffic
- Bypass filtering for sensitive traffic

URL Filtering (Prevents malware attacks from bad-reputed sites and blocks certain categories like streaming media, pornography)

MAS Update

- User Behavior Analytics

What Products and Licenses are available?

- Physical device or VPX version
- 14000 series today
  - 5900/8900 later
- Hardware maintenance – Bronze – Gold+
- Software Maintenance
- Pay-Grow philosophy applies
- URL filtering subscription add-on
  - Cloud-based service so no additional Maintenance

Prices

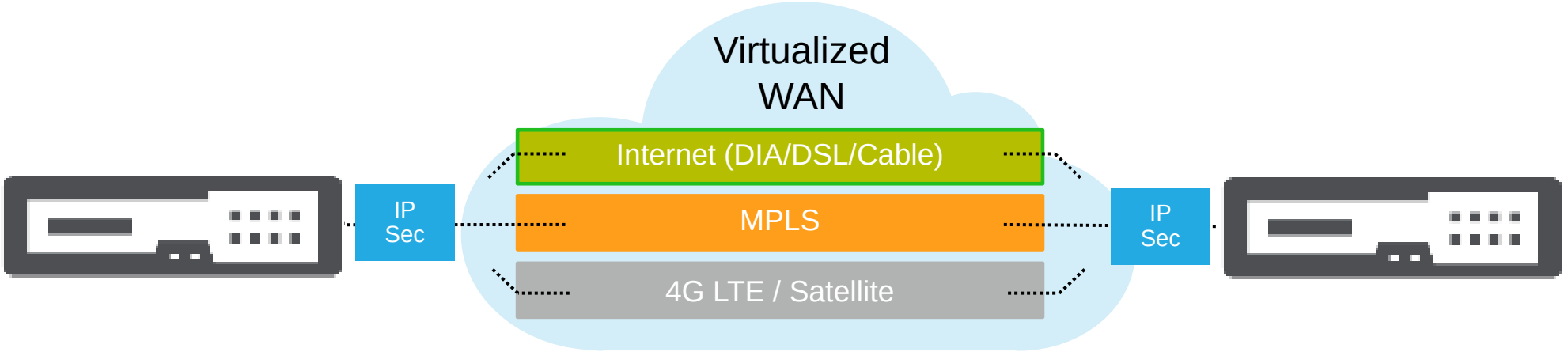
NetScaler URL threat intelligence SKUs	1 year subscription	3 year subscription
Threat Intelligence Subscription, URL for MPX 5901, 5905, 8905 and VPX 200, 1000, 3000, 5000	$3,375	$7,594
Threat Intelligence Subscription, URL for MPX 5910, 8910 VPX 8000, 10G	$6,000	$13,500
Threat Intelligence Subscription, URL for MPX 8920, 8930, 14020, 14030, 14020-40G, MPX-FIPS 14020, 14030, VPX 15G, 25G	$8,250	$18,563
Threat Intelligence Subscription, URL for MPX 14040, 14040-40G, 14040-40S, 14060-40S, MPX-FIPS 14060	$13,500	$30,375
Threat Intelligence Subscription, URL for MPX 14080-40S, MPX-FIPS 14080	$16,500	$37,125
Threat Intelligence Subscription, URL for MPX 14100-40S	$19,500	$43,875

NetScaler SWG Models	SWG edition price
MPX 14020 SWG	$65,000
MPX 14030 SWG	$70,000
MPX 14040 SWG	$80,000
MPX 14020-40G SWG	$85,000
MPX 14030-40G SWG	$90,000
MPX 14040-40G SWG	$110,000
MPX 14060-40G SWG	$120,000
MPX 14080-40G SWG	$135,000
MPX 14100-40G SWG	$150,000

NetScaler SWG Models	SWG edition price
VPX 200 SWG	$10,000
VPX 1000 SWG	$18,750
VPX 3000 SWG	$19,875
VPX 5000 SWG	$21,000
VPX 8000 SWG	$23,250
VPX 10G SWG	$24,750
VPX 15G SWG	$33,000
VPX 25G SWG	$41,250

Netscaler SD-WAN

SD-WAN – WAN Virtualization



- Bonds multiple WAN connections into a single virtual path, **adding up available BW**
- Encrypts data between devices, **providing end-to-end WAN security**
- **Real-time performance measurement** of loss, latency, jitter and congestion and **Per-packet path selection** to ensure high reliability and bandwidth efficiency
- **Sub-second reaction to changing network conditions**, no tcp session loss
- **Centralized management** for simplified operations and troubleshooting

Why Citrix SD-WAN

- Bandwidth Aggregation: More bandwidth for same price (Active-Passive)
- Always-On: < 1 sec failover (Normal routing: 20-30 sec mininum outage)
- Centralized Management: Change Mgmt with Moves, Adds and Changes (Normal Routers/FW's: manual changes per unit – decentralized control plane)
- Visibility: How are links performing & behaving, continuous monitoring, including HDX/ICA
- Application SLA: Quality of Service (QOS) and Application level priorities
- (Cost: doesn't apply to all customers)
- Enterprise Edition: SD-WAN and WANOP in single device
- WAN Edge Consolidation: Firewall, QOS, VPN, …

Change in applications is driving the network architecture

Cloud Delivered

Public cloud is the source of 44% of enterprise traffic

Expanding

The average business in 2016 used 13 cloud applications

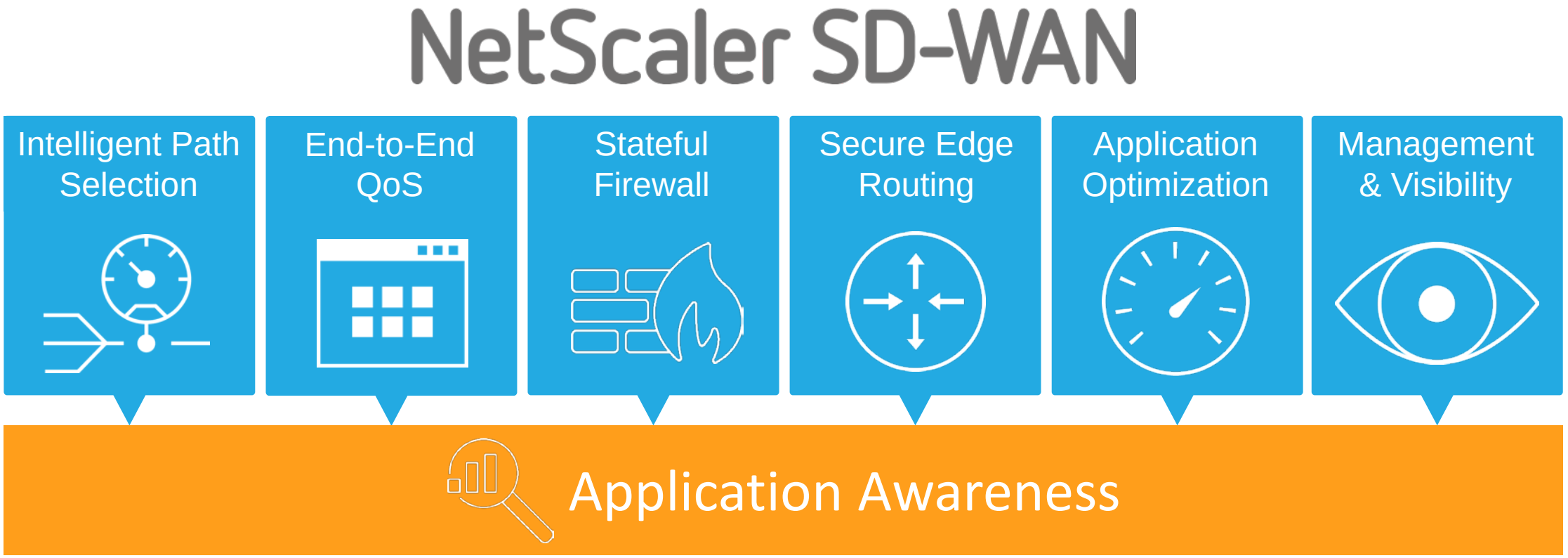
Bandwidth Intensive

IOT is a significant source of traffic in 55% of enterprises

Lots of Endpoints

Network-connected devices in remote sites increasing in 84% of enterprises

Application Intelligence Forms the Core of the Product



NetScaler SD-WAN: An Application Company

Web and SaaS Classification Engine

1. **Known protocols and port numbers**
   Compare port numbers and protocol messages against known applications and application components

2. **Payload Characteristics**
   Search for known binary patterns or packet characteristics in traffic flows

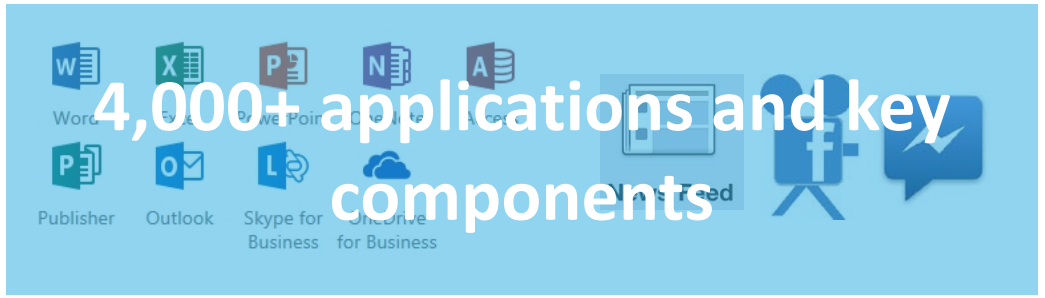
3. **Security Certificate Details**
   Read name of service in SSL/TLS certificate or in Server Name Indication

4. **DNS Matching and Known IP Addresses**
   Inspect DNS queries and session initialization sequences for known IP addresses

What Other's See

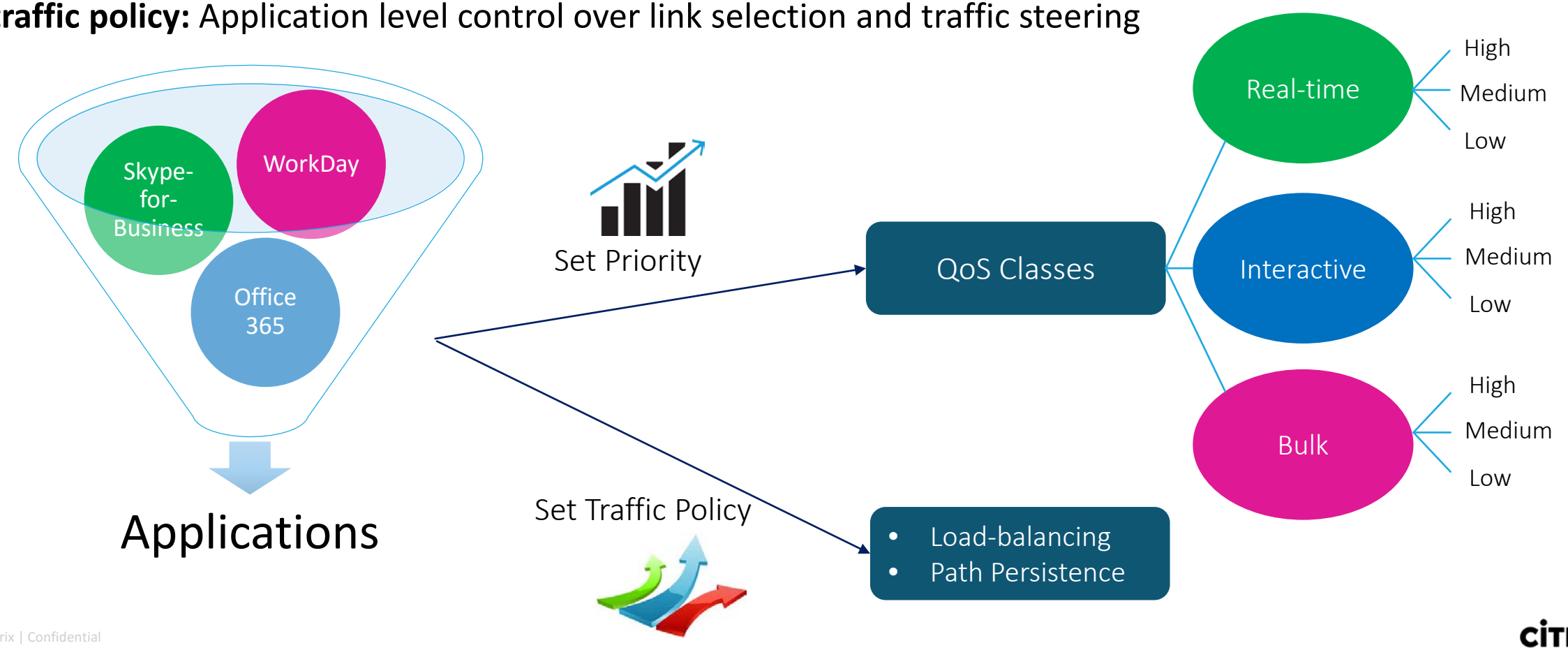
Office 365

With NetScaler SD-WAN

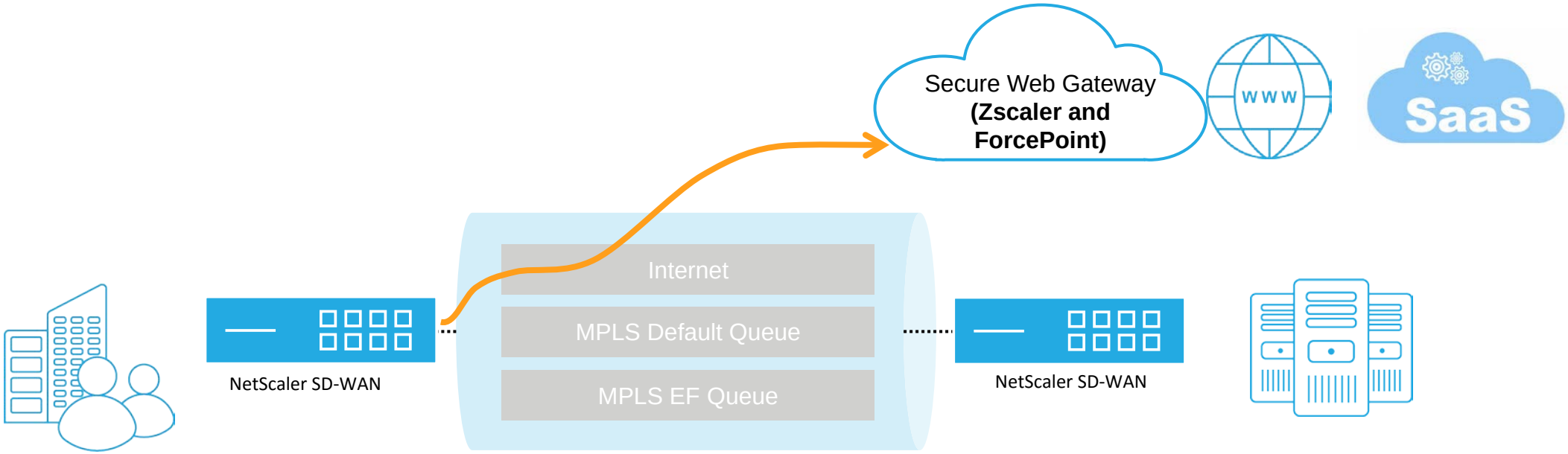


Enhanced Handling for Web and SaaS Applications

Web and SaaS QOS: Class of service can now be assigned for web and SaaS applications
Modify classification: Change classification if the first packet doesn't adequately identify the application.
Classify Optimized applications: Now can be applied to optimized flows in Enterprise Edition
Set priority: Prioritize business critical apps by mapping them to one of the 17 priority traffic classes
Set traffic policy: Application level control over link selection and traffic steering



Secure Internet Breakout Enhancements

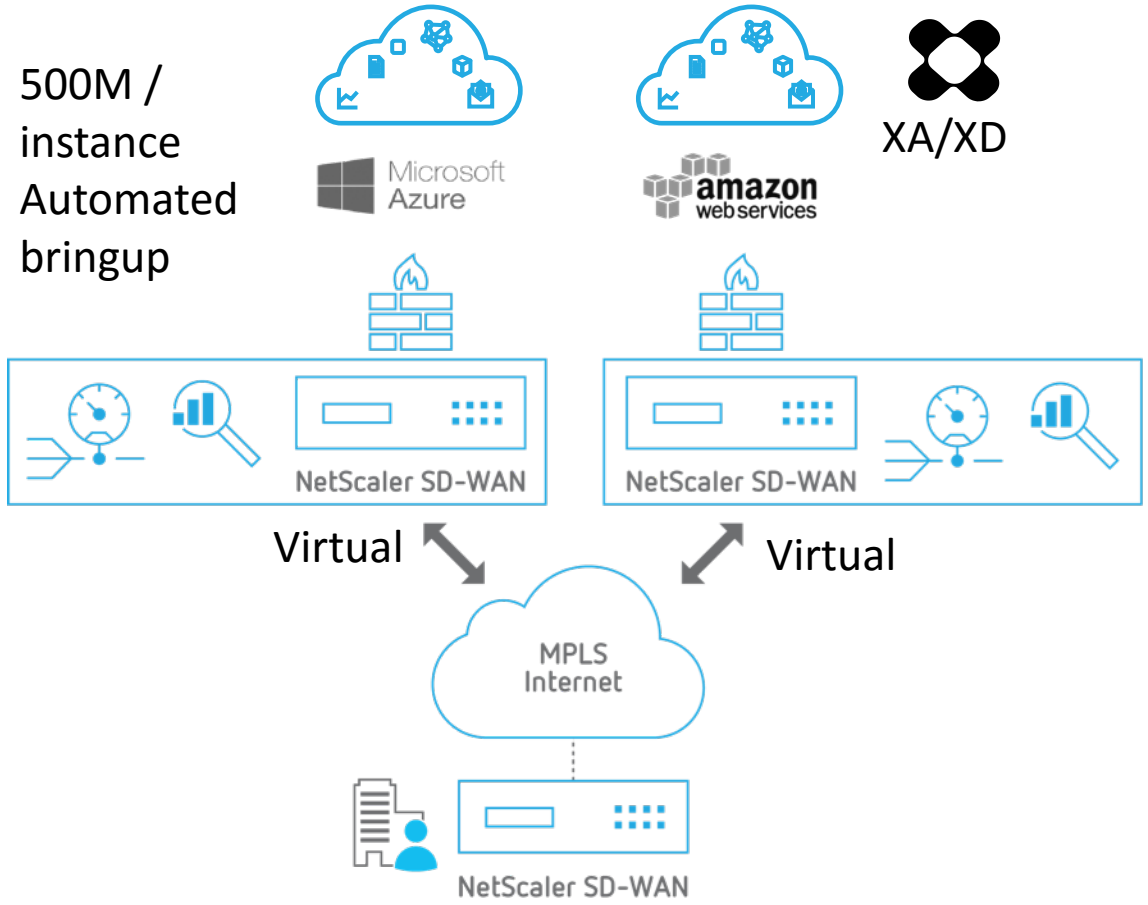


- Forcepoint Integration
  - Connectivity with **IPSec** or GRE tunnels to Zscaler and ForcePoint
  - Forcepoint as a Transparent Proxy

NetScaler SD-WAN Makes Hybrid Cloud Easy

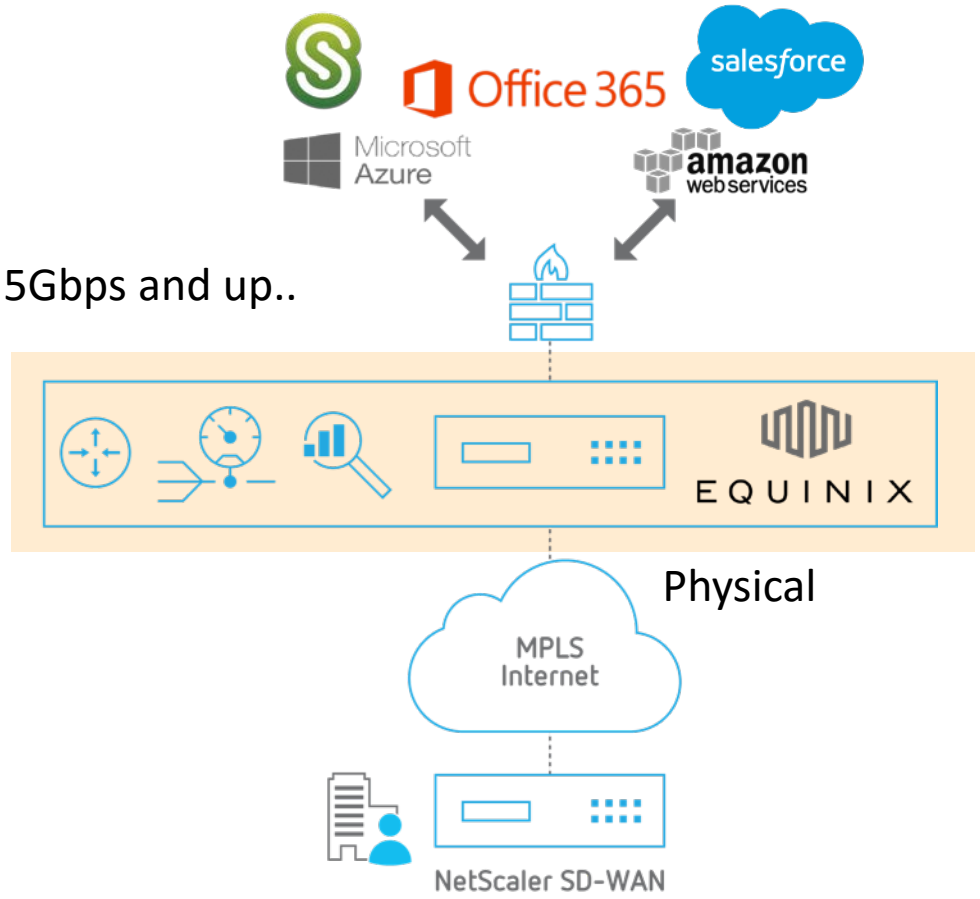
Secure and reliable delivery from cloud to branch

- 500M / instance
- Automated bringup



High performance delivery from multiple clouds to branch

5Gbps and up..

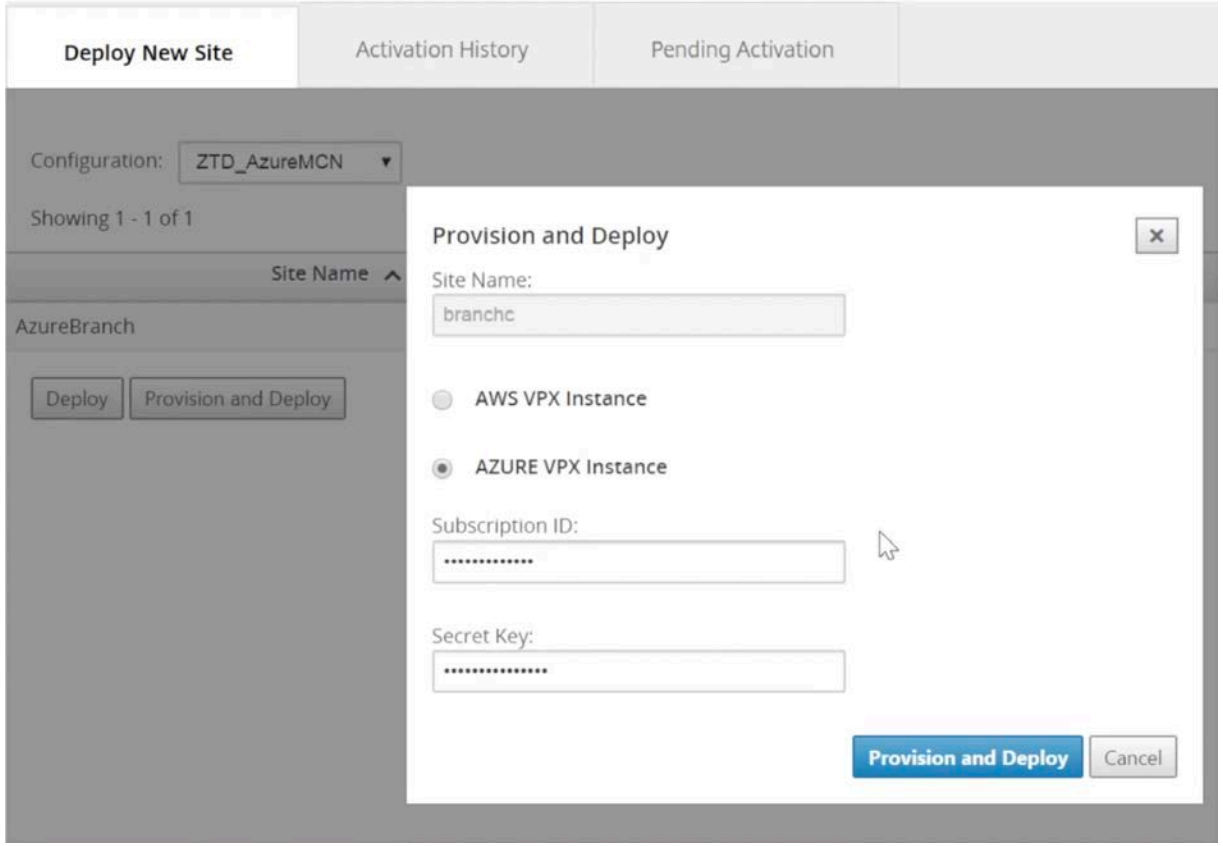


Use AWS and Azure as datacenter

Improving performance, scale, availability, and operations

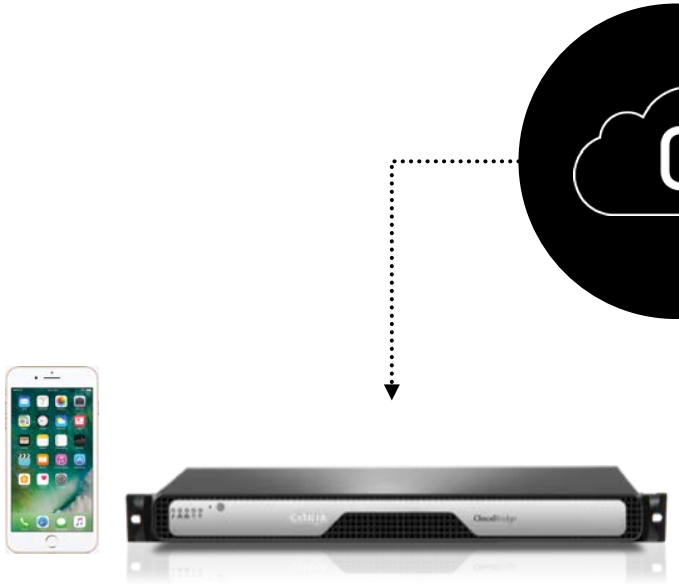
- Cloud appliance can act as Master Control Node or GEO-redundant MCN
- High availability is supported in AWS and Azure so a primary and secondary instance can both be running
- Higher bandwidth in AWS, up to 2 Gbps (1Gbps full duplex)
- Increased number of virtual paths supported for AWS and Azure to 128
- Message:
  - Make it easier for our partners to offer cloud-hosted and cloud-managed service
  - Opens the door for Citrix Solution providers that host their applications in the cloud

Click-to-Launch



- AWS and Azure supported
- Customer provides credentials
- SD-WAN Center launches SD-WAN VPX
- Uses ZTD infrastructure to provision and download the config
- The new VPX automatically connects into MCN and the rest of the network

Simplified Deployment with Zero-Touch Deployment Service



Automated bring-up

Authentication to join Network

Status updates of the deployment process

NetScaler SD-WAN 410, 1000, 2000, 2100, and VPX Appliances

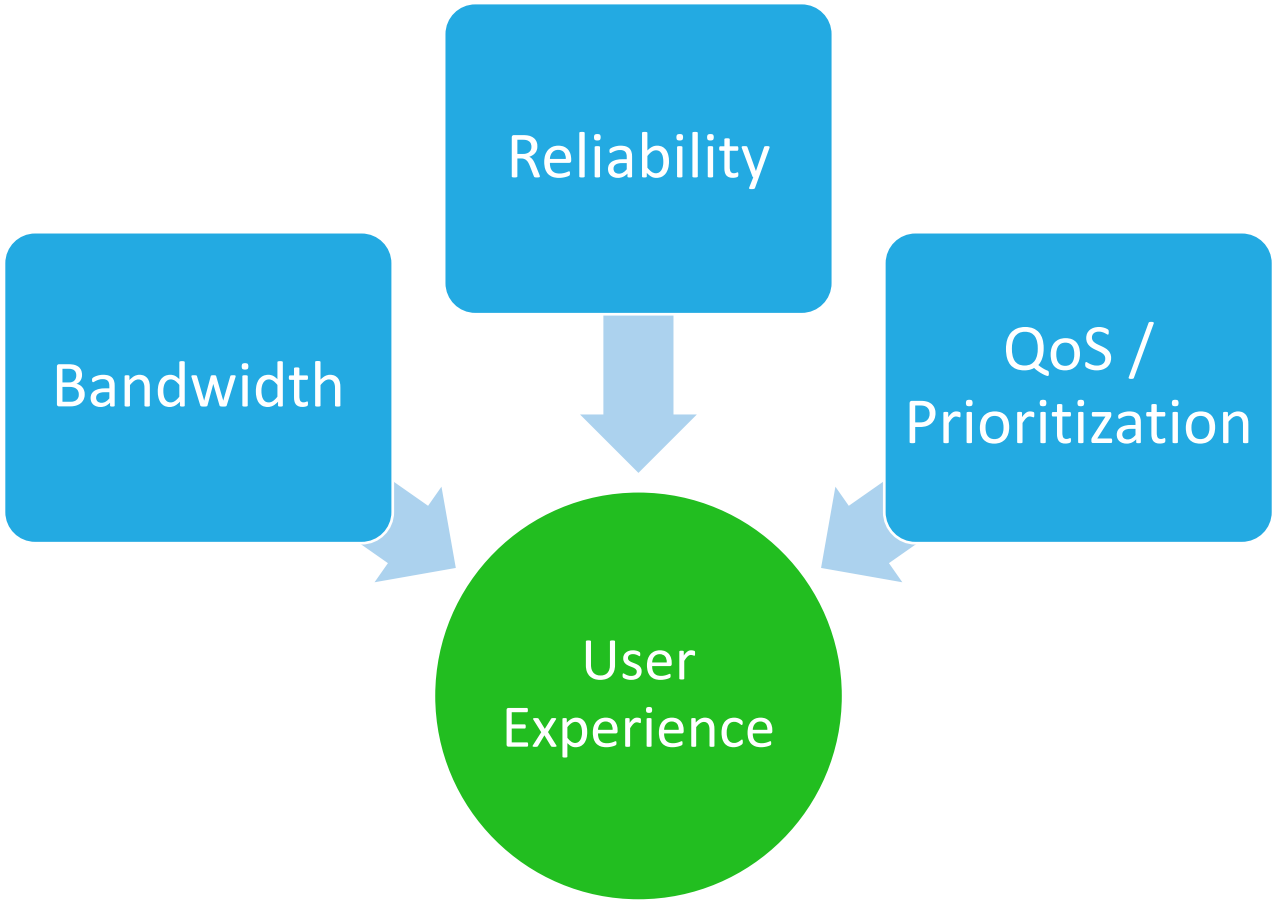
Ideal for large scale deployments, geographically distributed, and those with no technical resources on site

New appliances supported with R9.3

Delivering Best User Experience for HDX

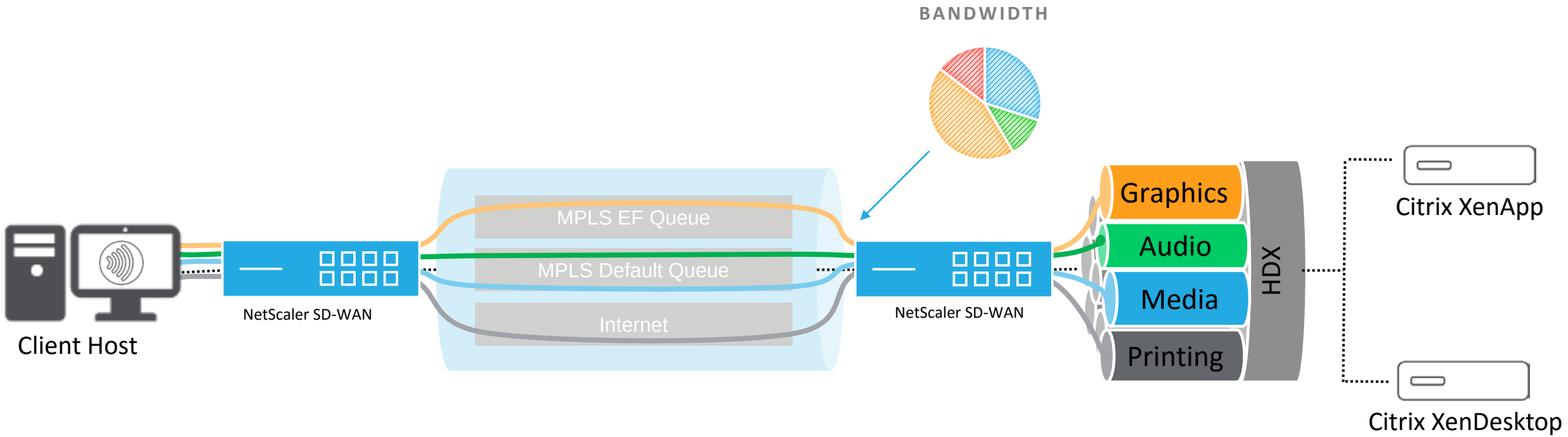
- Constant monitoring and adaptation to network conditions

- Aggregate multiple network links to provide more bandwidth



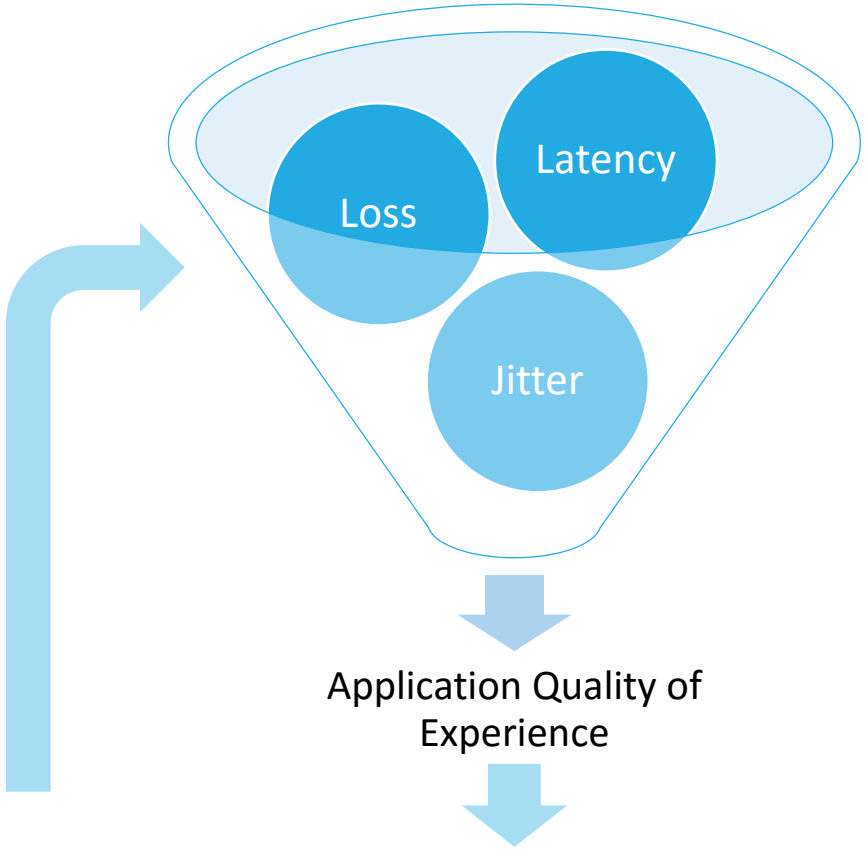
- Identify ICA channels and prioritize interactive and multimedia over bulk
- Optimization as needed

NetScaler SD-WAN Enables Better HDX Delivery



- Recognize HDX in various delivery forms: ICA/CGP/SSL/Websockets etc
- Signal presence to the VDA to enable automatic adjustment of policies
- Automatic switch to multi-stream ICA separates traffic into prioritized connections (Interactive, Multi-media, Bulk etc)
- Adapt to network conditions and deliver each stream with the right quality

NetScaler SD-WAN Ensures the Quality of Experience



Pro-active App Delivery eliminates user complaints

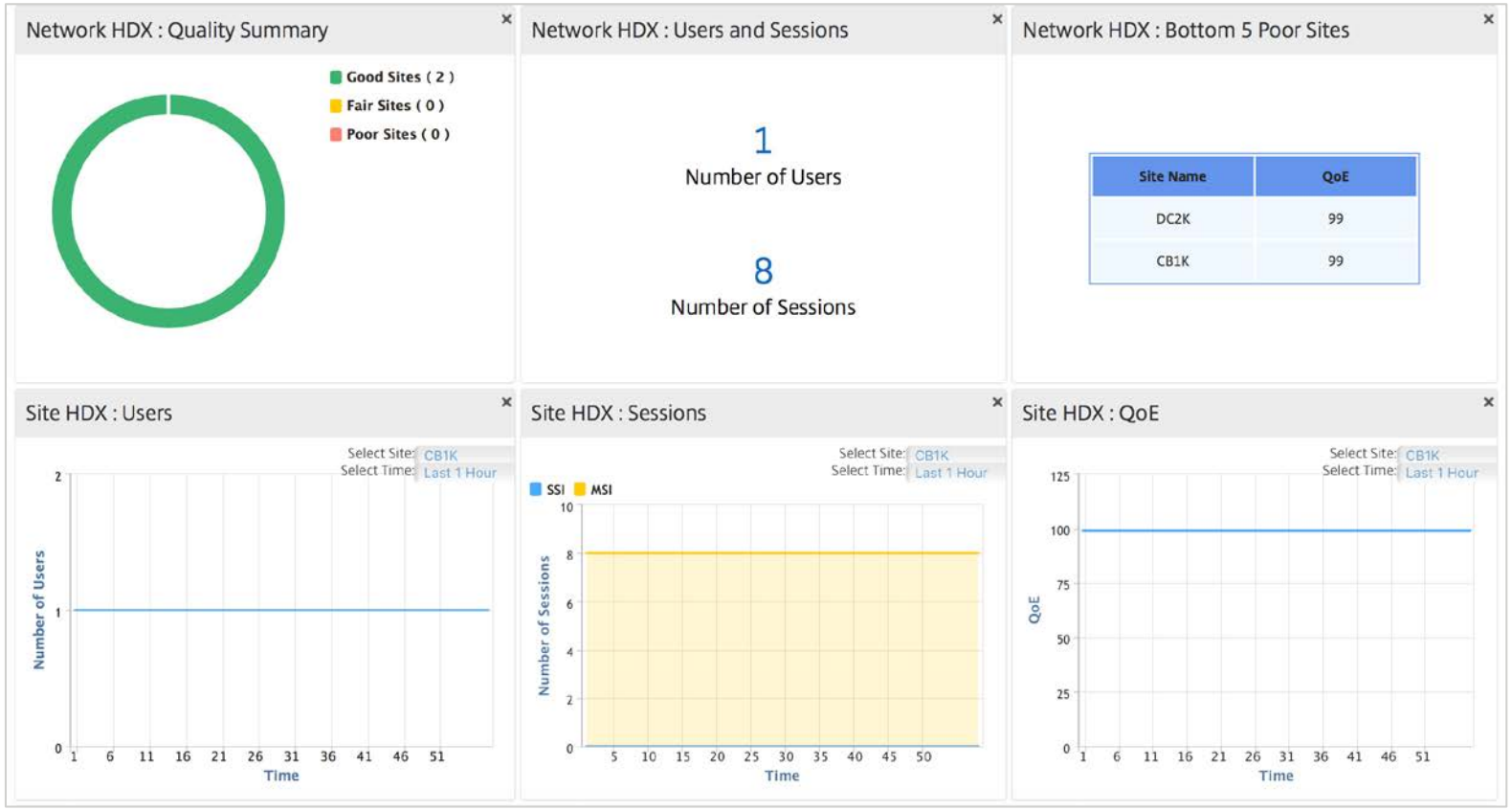
"What Gets Measured Gets Improved"
-Peter Drucker

And Proving It: HDX Quality of Experience

Quality distribution for Various Sites

Current User and Session Count

Bottom 5 Sites



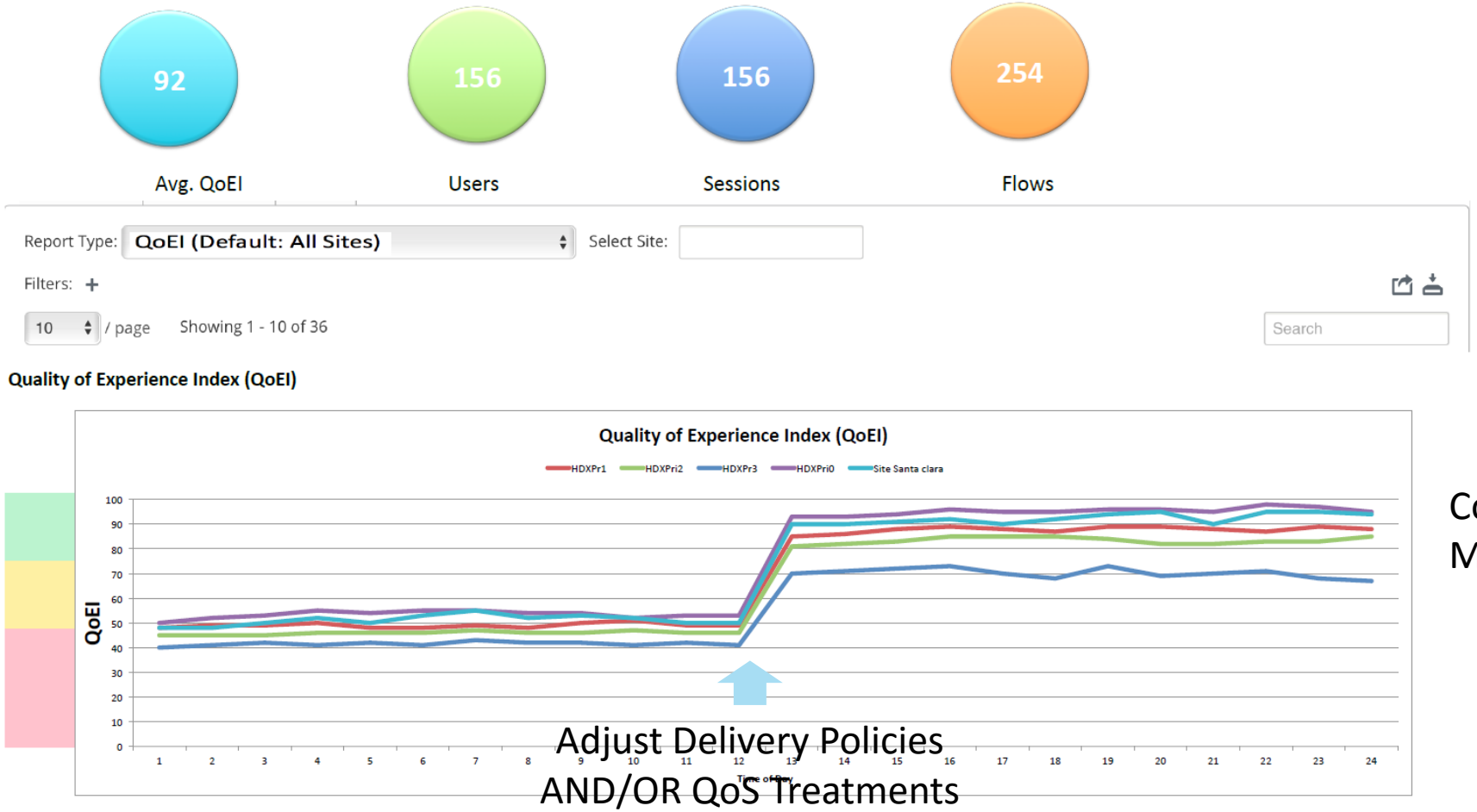
Historical User Count with filters

Historical Session Count with filers

Historical QoE with filters

- HDX QoE provides measure of network performance / HDX user experience across the network and by site
- Developed in conjunction with HDX product team
- SD-WAN Center dashboard provides clickable graphs & charts for detail drill down

HDX-IQ: Tracking Quality of User Experience

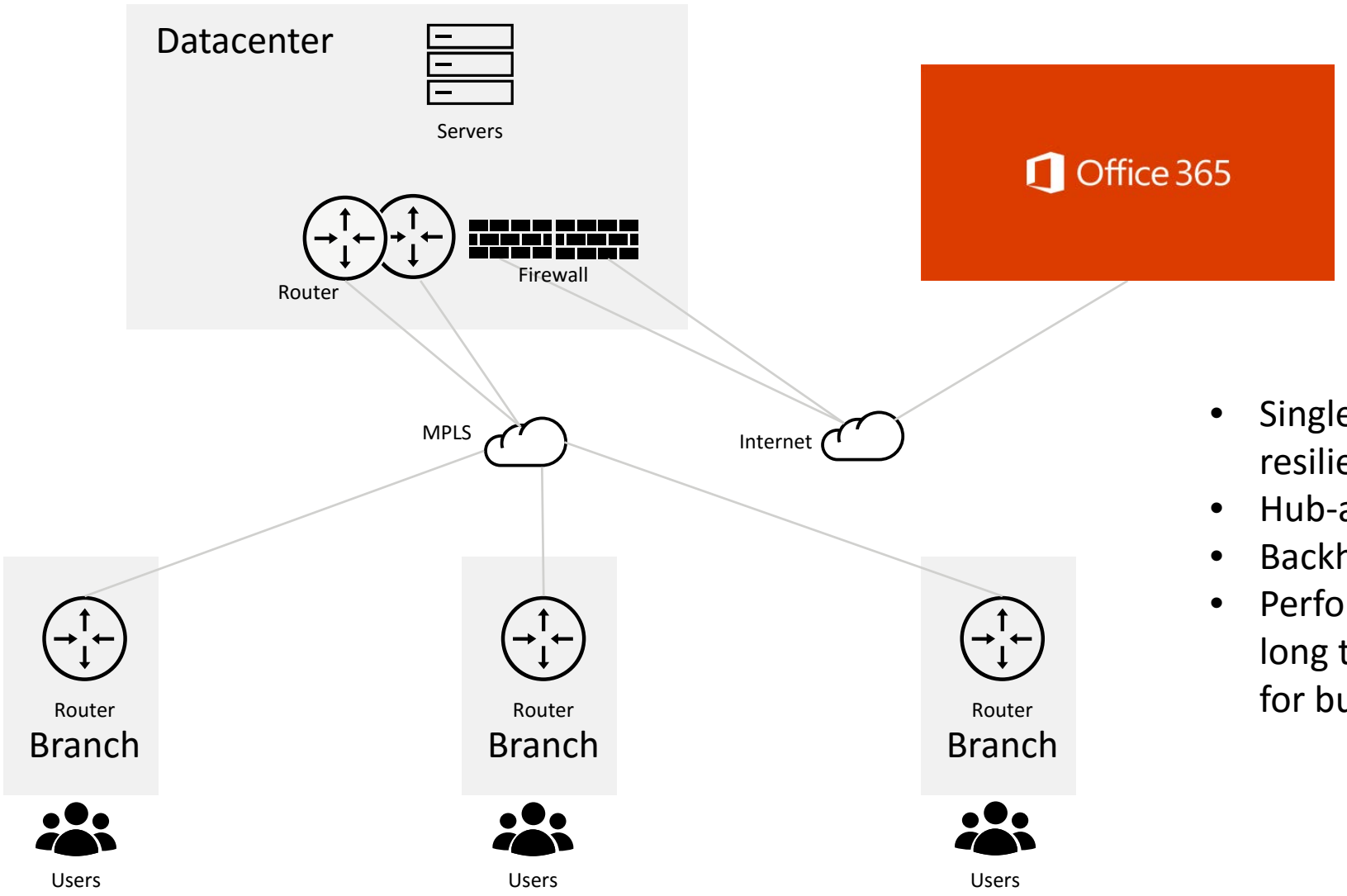


Green, Yellow or Red Zone transitions trigger notifications

Adjust Delivery Policies AND/OR QoS Treatments

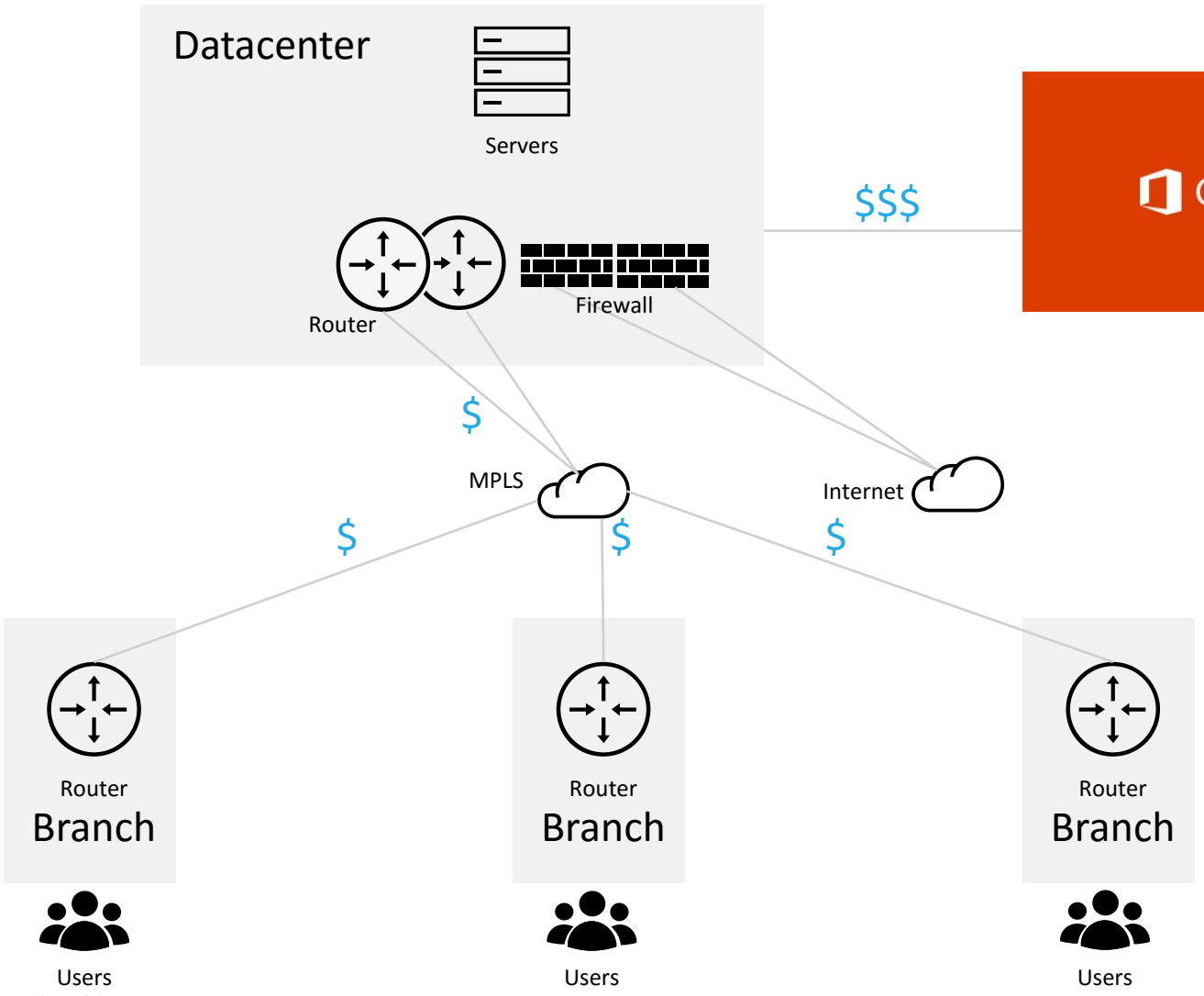
Continuous Monitoring

Common Current Scenario with Office 365



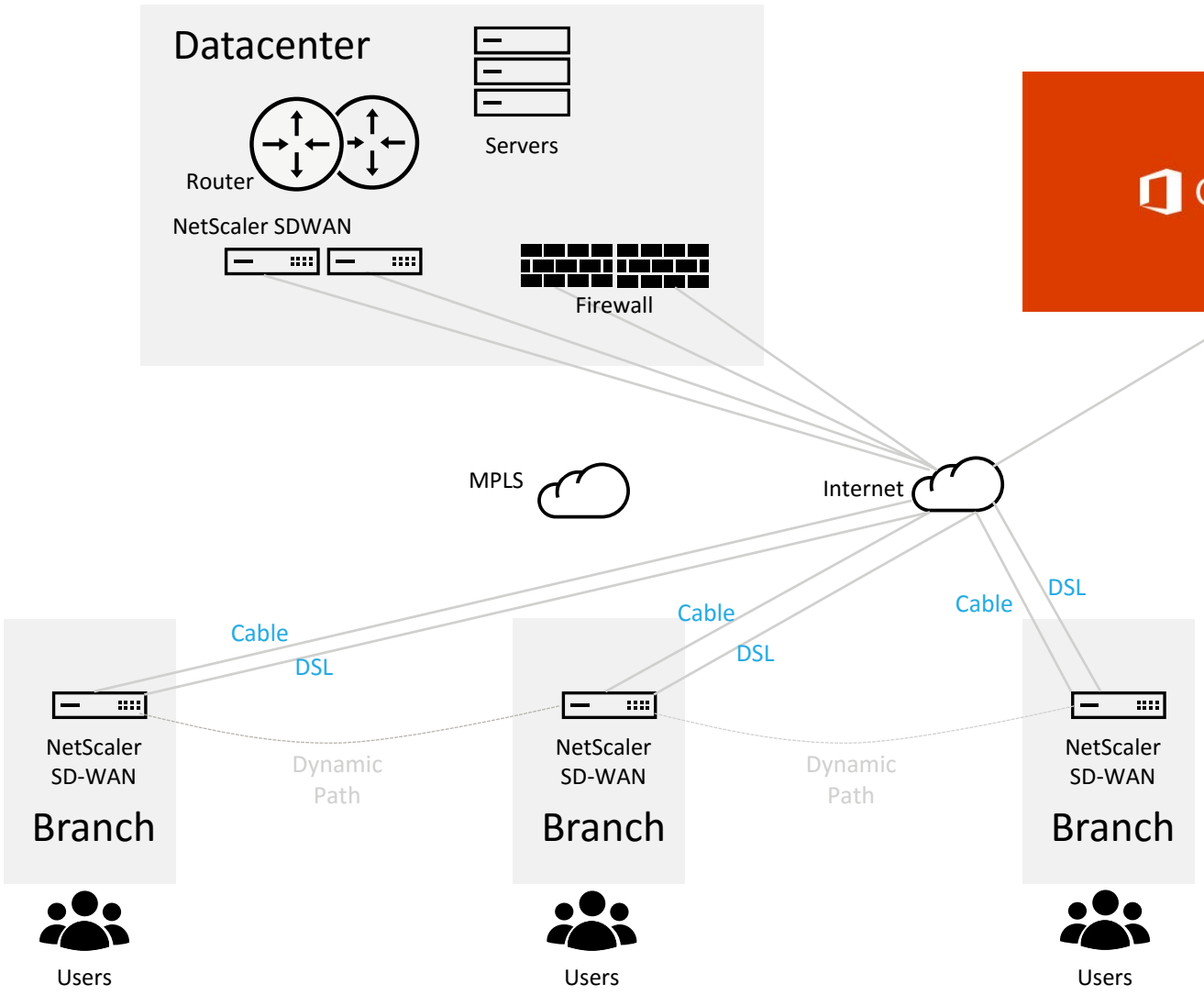
- Single MPLS Connectivity – no resiliency
- Hub-and-Spoke
- Backhaul traffic to reach O365
- Performance issues with O365: takes long time to synch mailboxes, skype for business performance

Common Current Scenario with Express Route solution



- Single MPLS Connectivity – no resiliency
- Hub-and-Spoke
- Backhaul traffic to reach O365
- Increase MPLS capacity and Express Route to solve connectivity problems ($$$)
- Requires manual validation by Microsoft Architect – BGP knowledge Mandatory by customer
- Not possible anymore for O365, only Azure

Introducing Citrix Netscaler SD-WAN



- SD-WAN with Internet Connectivity
  - Higher capacity
  - Active-Active usage of links
  - <1 s change; high resilience
- Mesh Infrastructure:
  - Direct connectivity to O365 without backhaul
  - Skype 4 business with Dynamic Paths
- Reduce/Remove MPLS cost