Dobson
TECHNOLOGIES

Distributed Security for the Modern WAN

Richard Scott
SVP Engineering & Technology

About

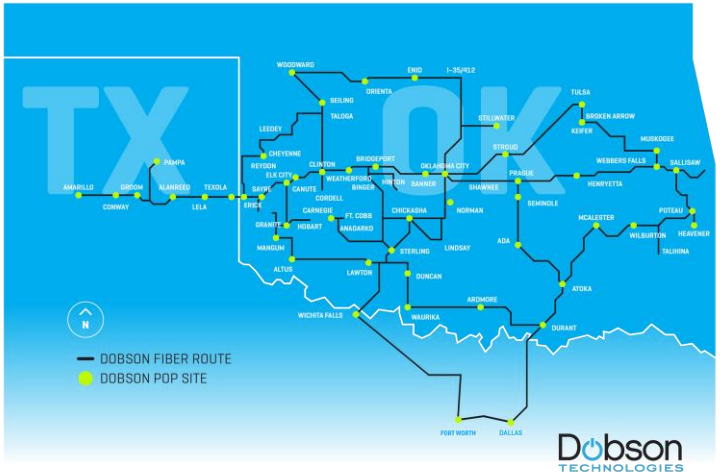
- Richard Scott
  - SVP Engineering & Technology for Dobson Technologies
  - 30 years in Telecom and Managed Services
  - Many hats…

    Software Developer, Network Engineer, CCIE, Entrepreneur, Executive
  - NOT a Security Expert

- About Dobson
  - Formed in 1936 by E.R. Dobson as a telephone service provider in rural Oklahoma
  - Operated primarily as a rural ILEC and middle-mile fiber optic transport provider through 1980's
  - Launched wireless business in 1990, spun-out and

    IPO'd in 2000 and sold to AT&T in 2007 for $5.1B
  - Focused on Fiber Transport since 2011 in Oklahoma

    and northern Texas



Overview

Outline

- Evolution of Networks
- Today's Challenges
- Software Defined – Who/Why/How
- Future

Objectives

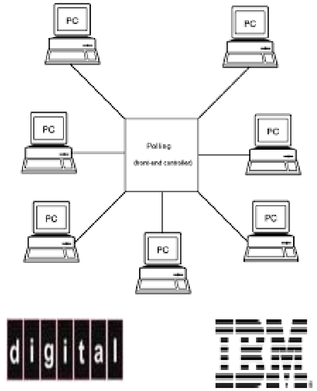
- Few answers
- Questions to consider
- Thought provoking

Disclaimer

This memorandum contains certain ***forward-looking statements****, estimates and projections with respect to anticipated future performance events. Such statements, estimates and projections involve significant elements of* ***subjective*** *judgment and analysis, which* ***may or may not be correct****. Such statements, estimates, and projections reflect various assumptions concerning anticipated results and are subject to significant business, economic, and competitive uncertainties and contingencies. Accordingly, there can be* ***no assurance*** *that such statements, estimates or projections will be realized.*

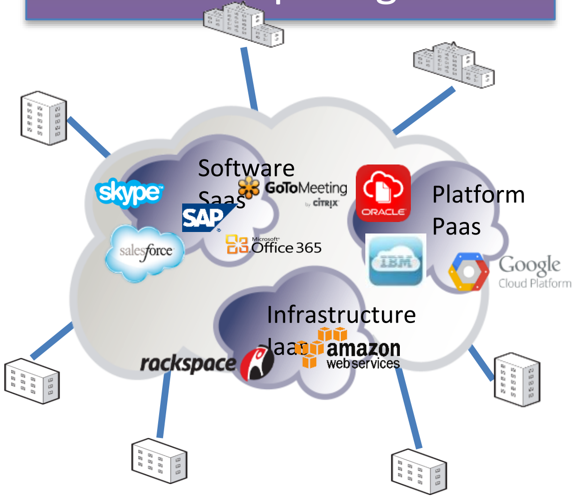
Networks Evolve

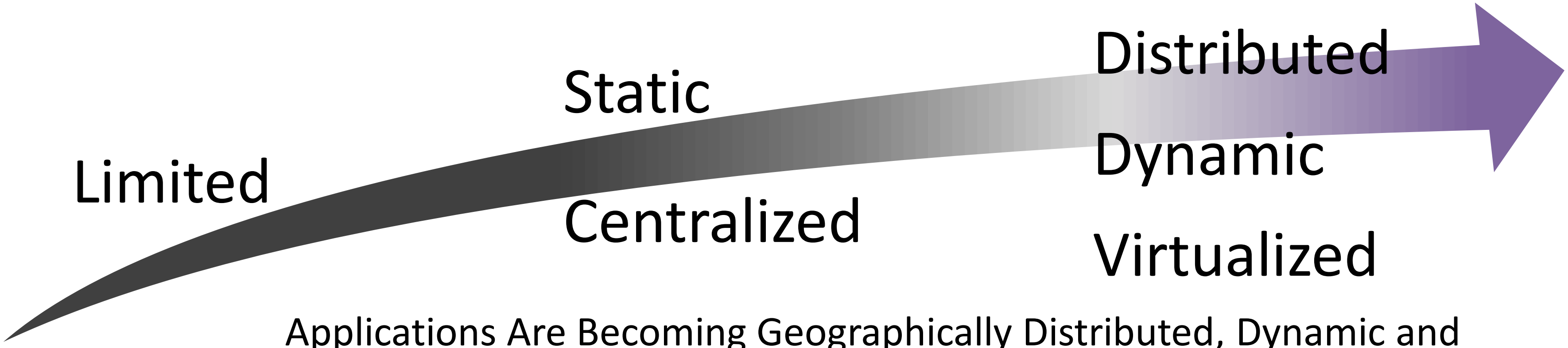
Main Frames



Centralized Applications And WAN's

SaaS and Cloud Computing





Limited

Static

Centralized

Distributed

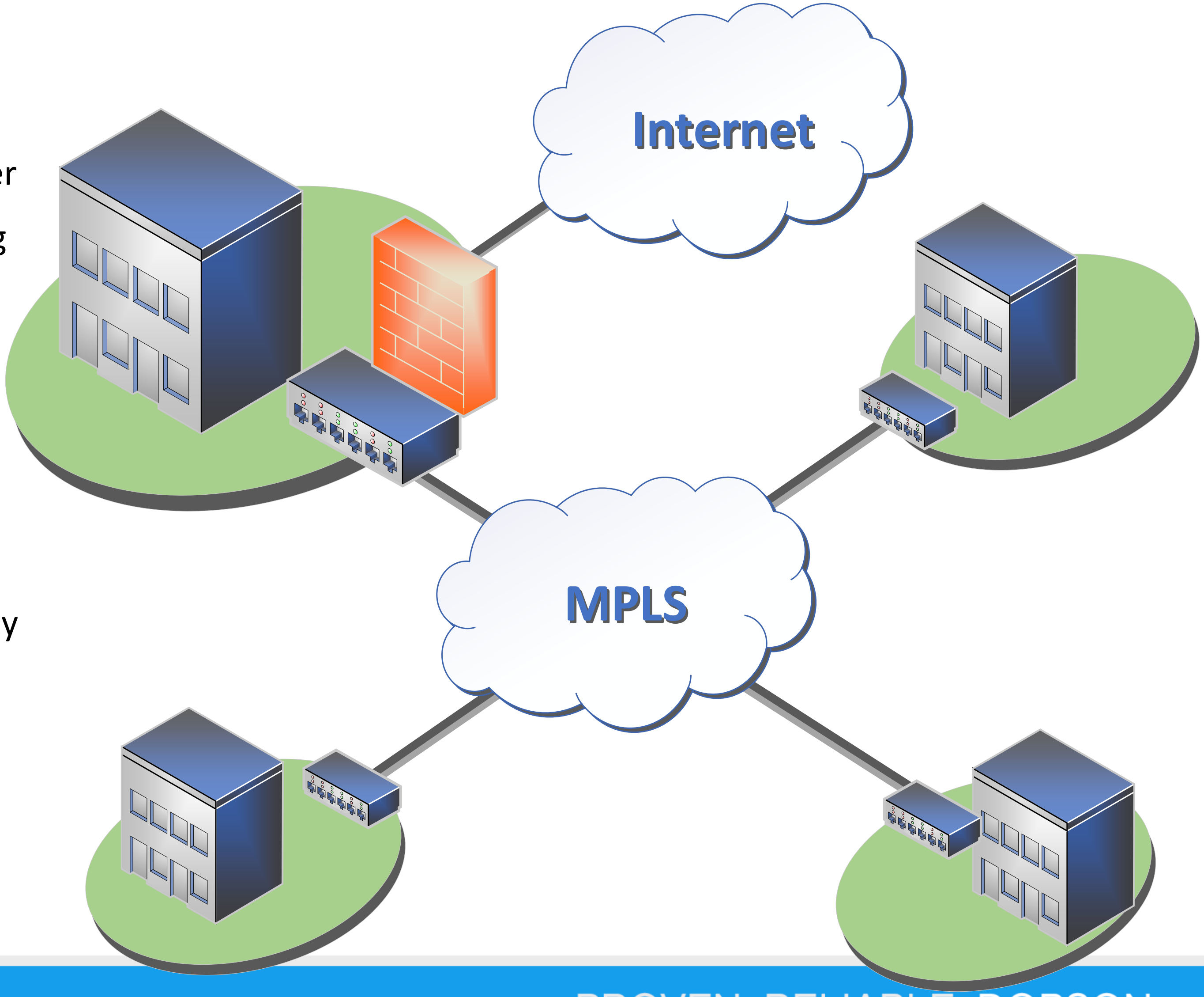
Dynamic

Virtualized

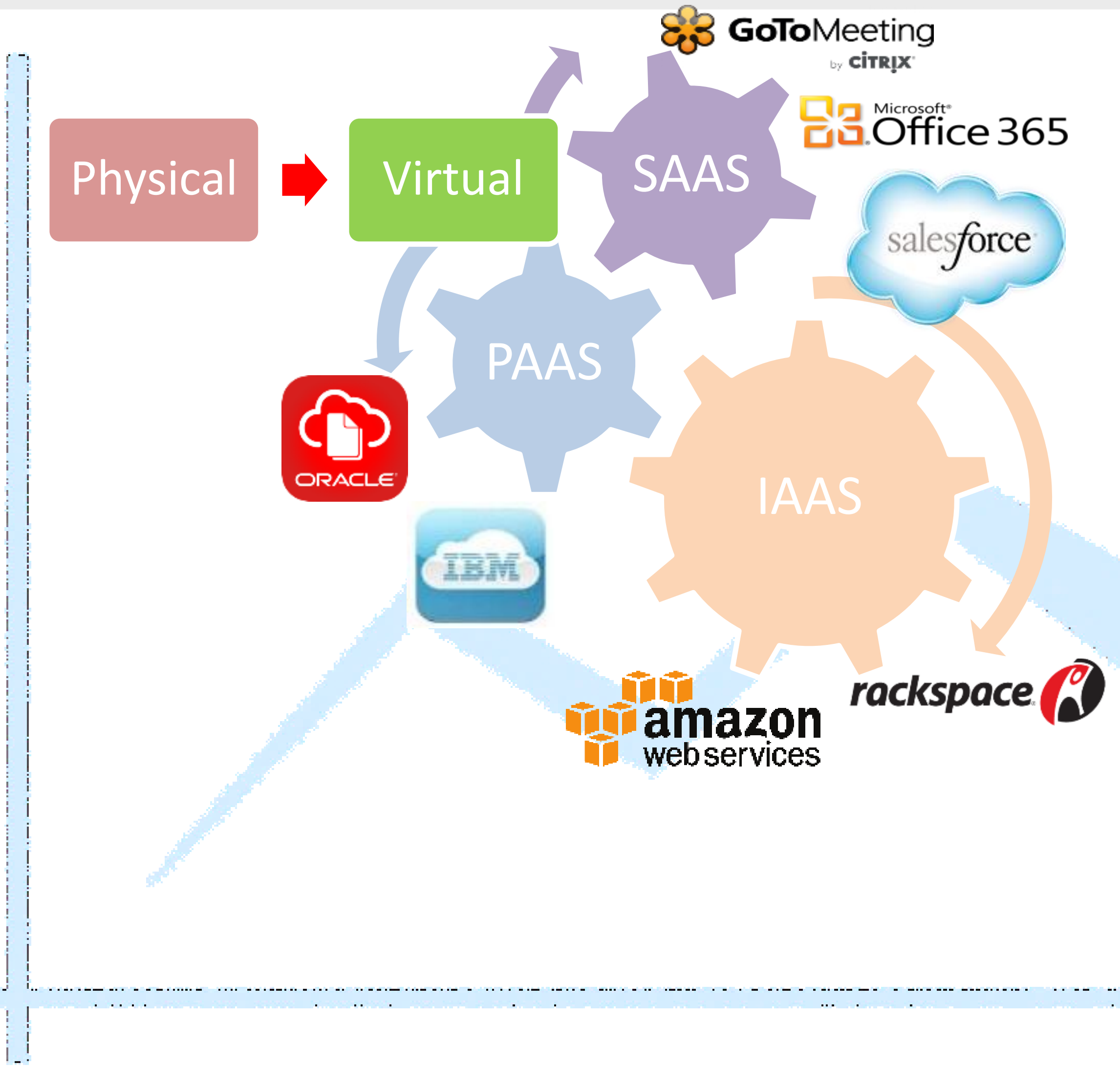
Applications Are Becoming Geographically Distributed, Dynamic and Virtualized Through SaaS, PaaS, IaaS by leveraging Cloud Technologies

Traditional WAN

- All paths via the Datacenter
- Destination Driven Routing
- Monitoring/Visibility
- Branch sprawl
- Expensive MPLS
- Lengthy Provisioning
- Expensive HW
- Over the Top == Complexity
- Policy Management
- Lateral Movement



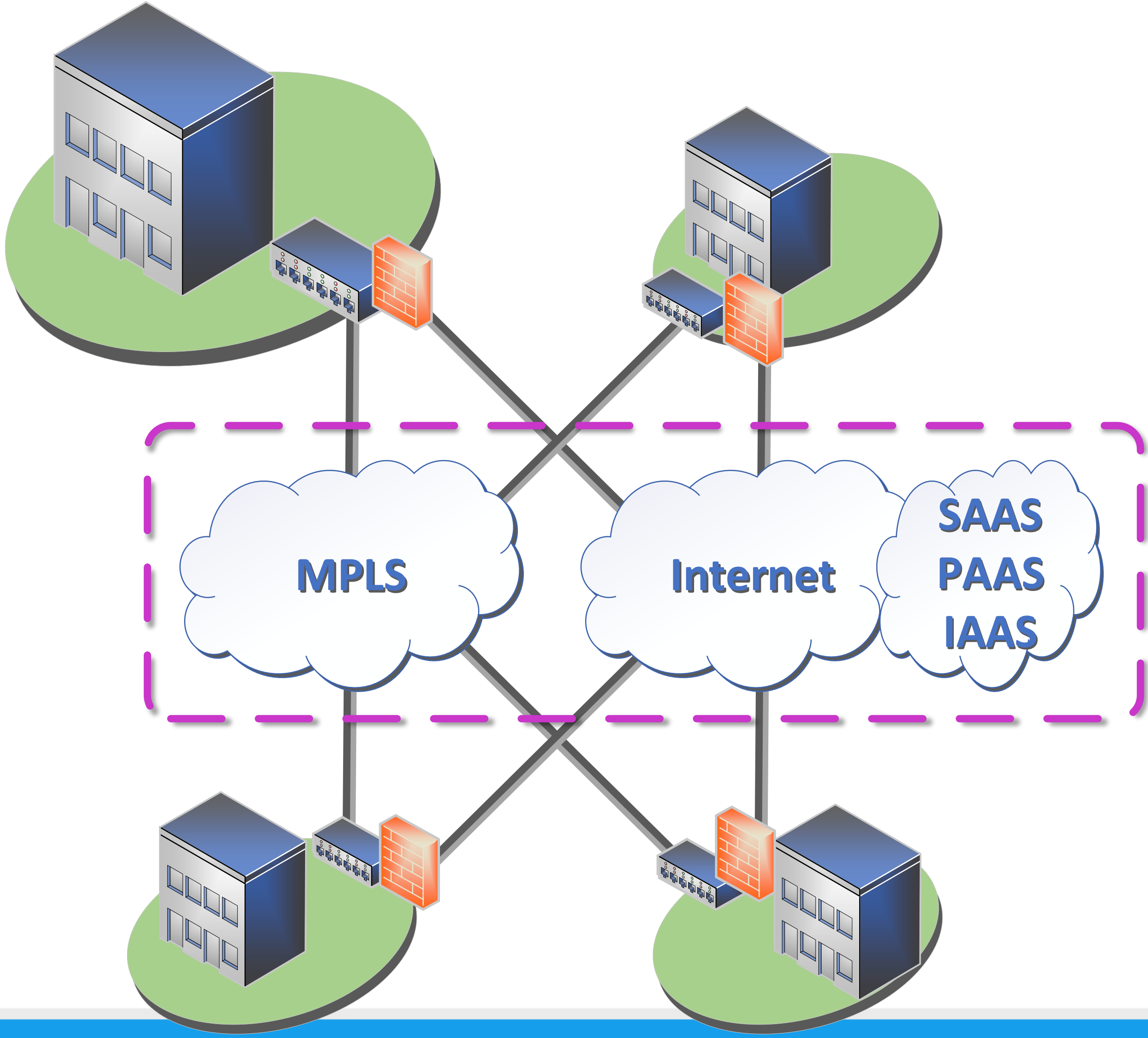
Rapid Movement from Physical to Virtual



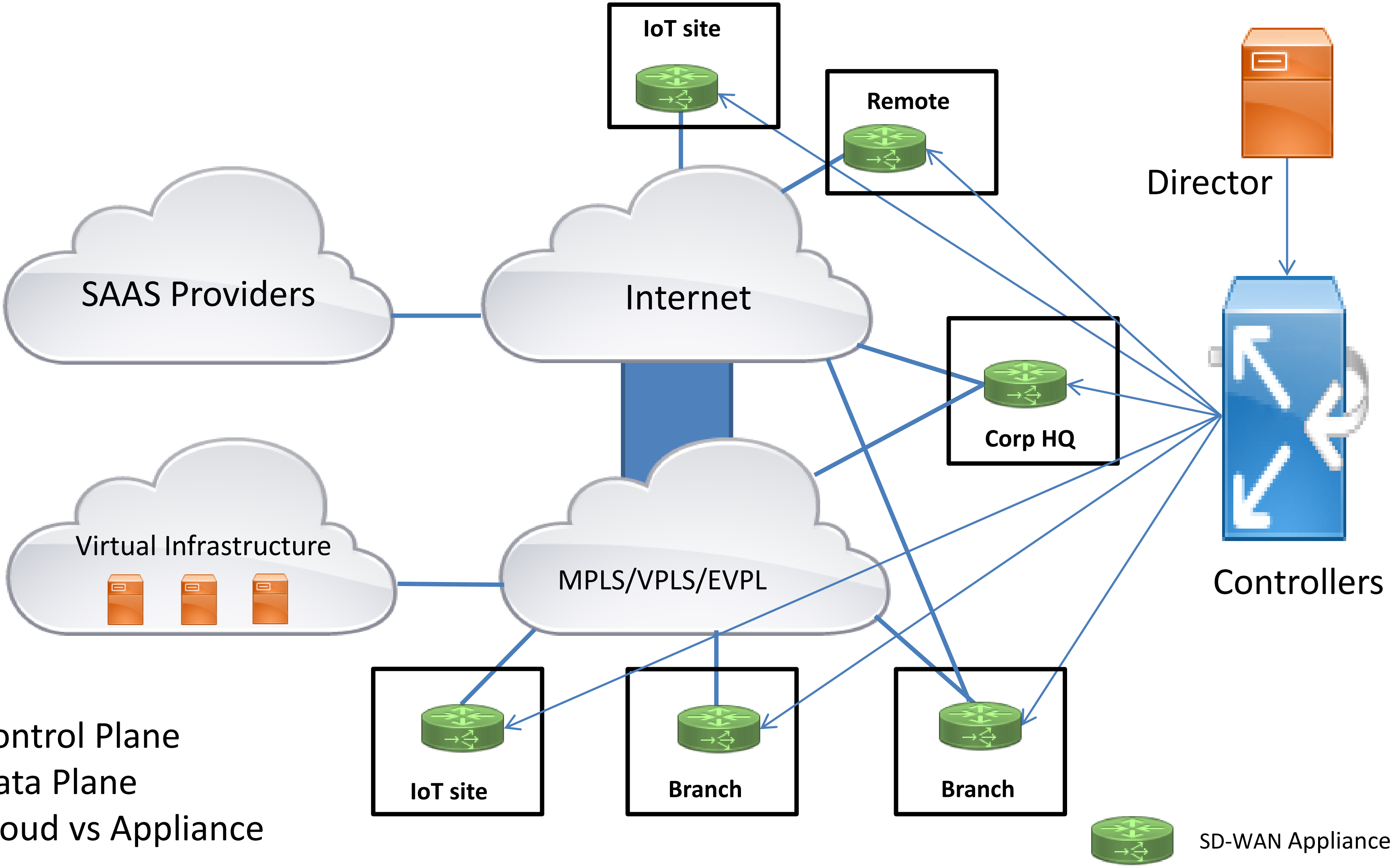
"More than **$1 trillion in IT spending** will be directly or indirectly affected by the shift to cloud during the next five years, said Gartner, Inc. This will make cloud computing one of the **most disruptive forces of IT spending since the early days** of the digital age." [Gartner 2016]

Software Driven

- Single Control Plane
- Encrypted Data Plane
- Policy Management
- Intelligent App Aware Routing
- Layer 7 Analytics
- Network Elasticity
- Service Agility
- Optimize multiple transport
- Leverage Broadband
- Cloud Ready
- Commodity HW + NFV



SD-Wan Network



- Control Plane
- Data Plane
- Cloud vs Appliance

Challenges

- FACT:
  - Migration of customer applications to the cloud (IaaS, PaaS, SaaS)
  - Proliferation of IoT devices/Gateways will increase network nodes (Exposure) exponentially

- Current WAN architecture is Rigid
  - “All roads lead to the data center”
  - Applications are going to the cloud and networks must follow

- In the current WAN remote office/location connectivity is a challenge
  - Terrestrial backhaul private circuits are expensive or not available
  - VPN tunnels through the public internet are un-reliable, complicated to provision and troubleshoot
  - IoT will require remote infrastructure to be integrated into corporate WAN over low cost wireless/wireline where private backhaul is not feasible

- Legacy WAN technology is “one size fits all.” IP/MPLS, VPLS, EVPL….

- Redundancy at remote locations is cost-prohibitive

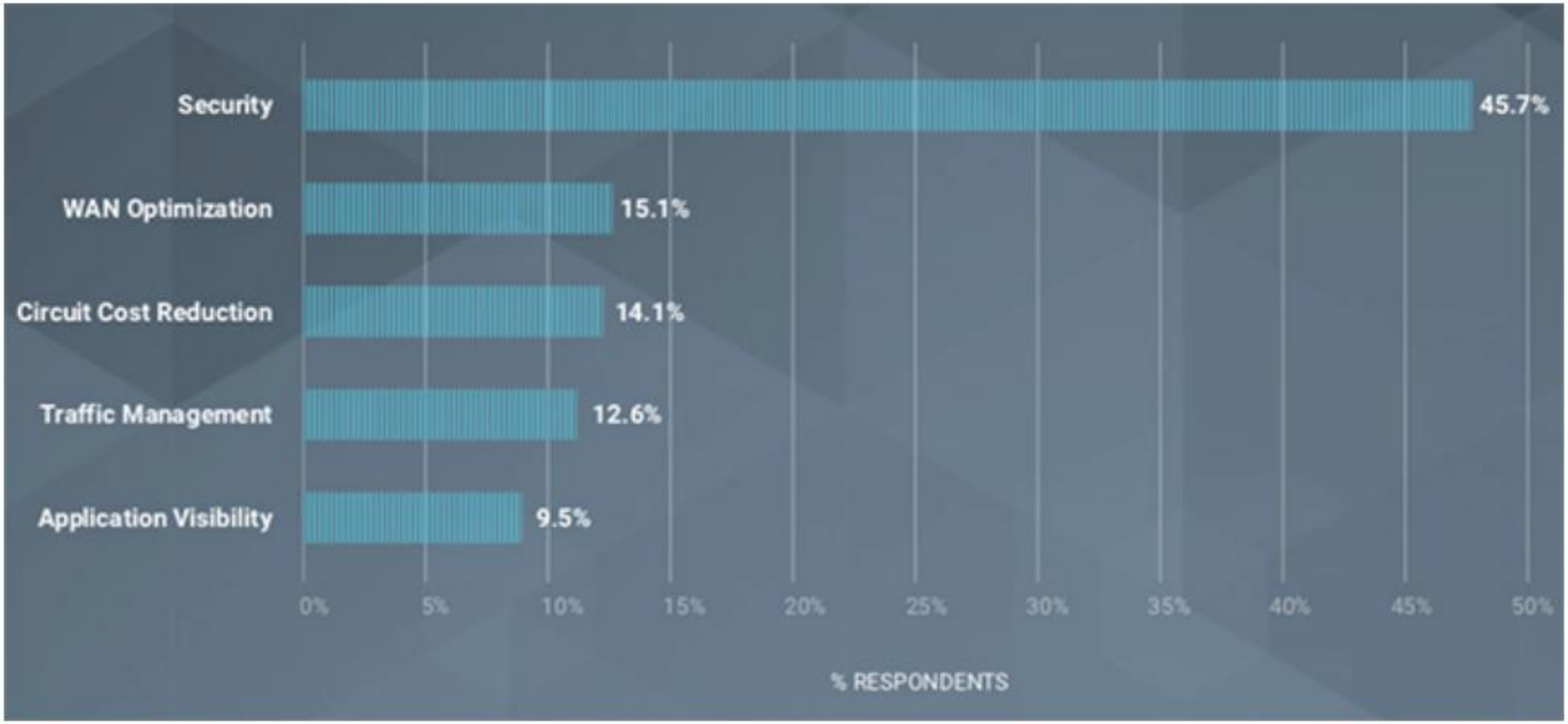
- WAN traffic routing is static and not application aware

- Lack of WAN management

- Inefficient capacity utilization

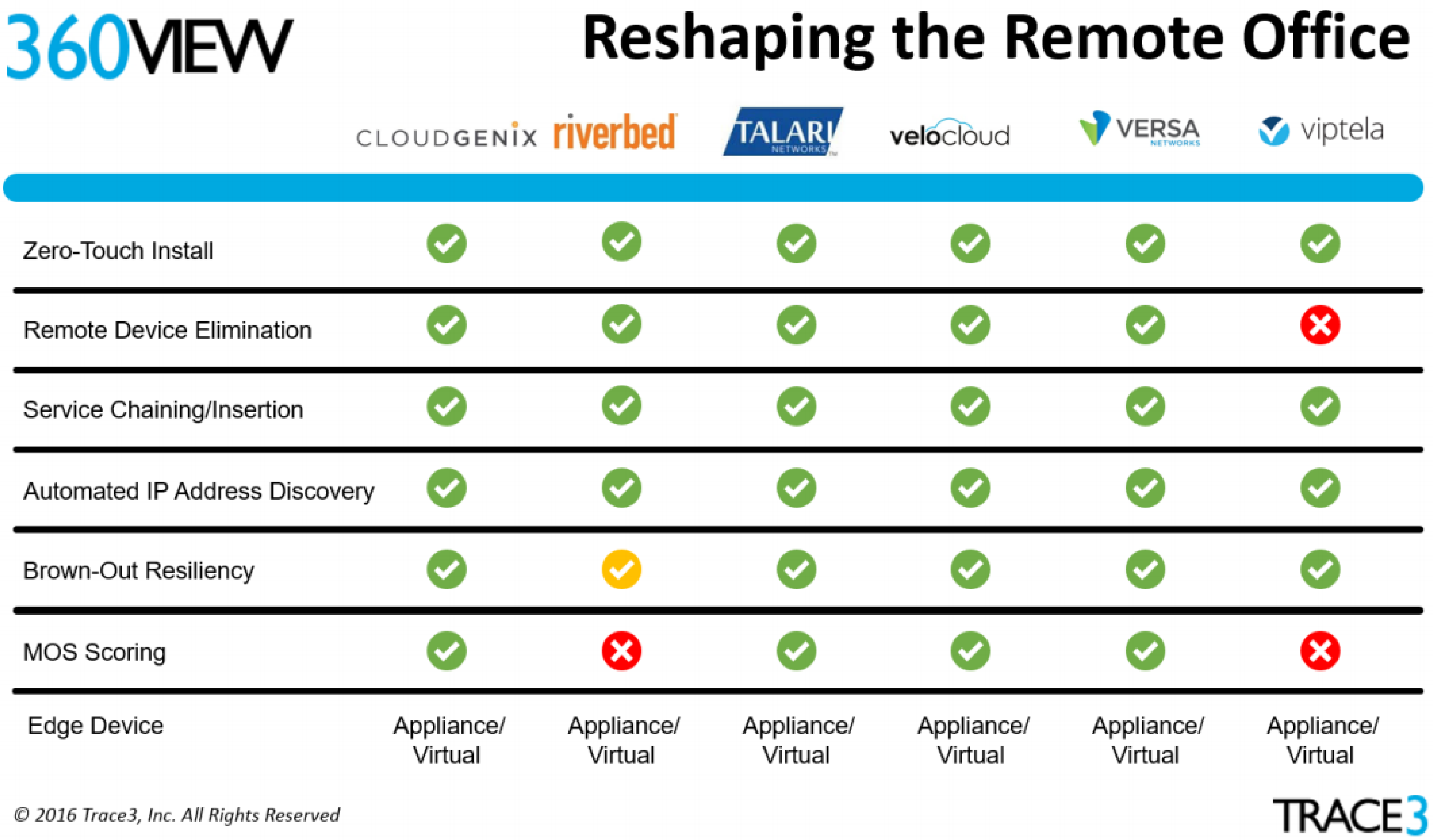
Why SD-Wan?

Adoption of Software Defined Wide Area Network (SD-WAN) has reached an inflection point and nearly every distributed business is deploying, evaluating, or planning to implement an SD-WAN as part of its IT vision.



https://www.helpnetsecurity.com/2018/08/09/tested-sd-wan-products/

Many Solutions…



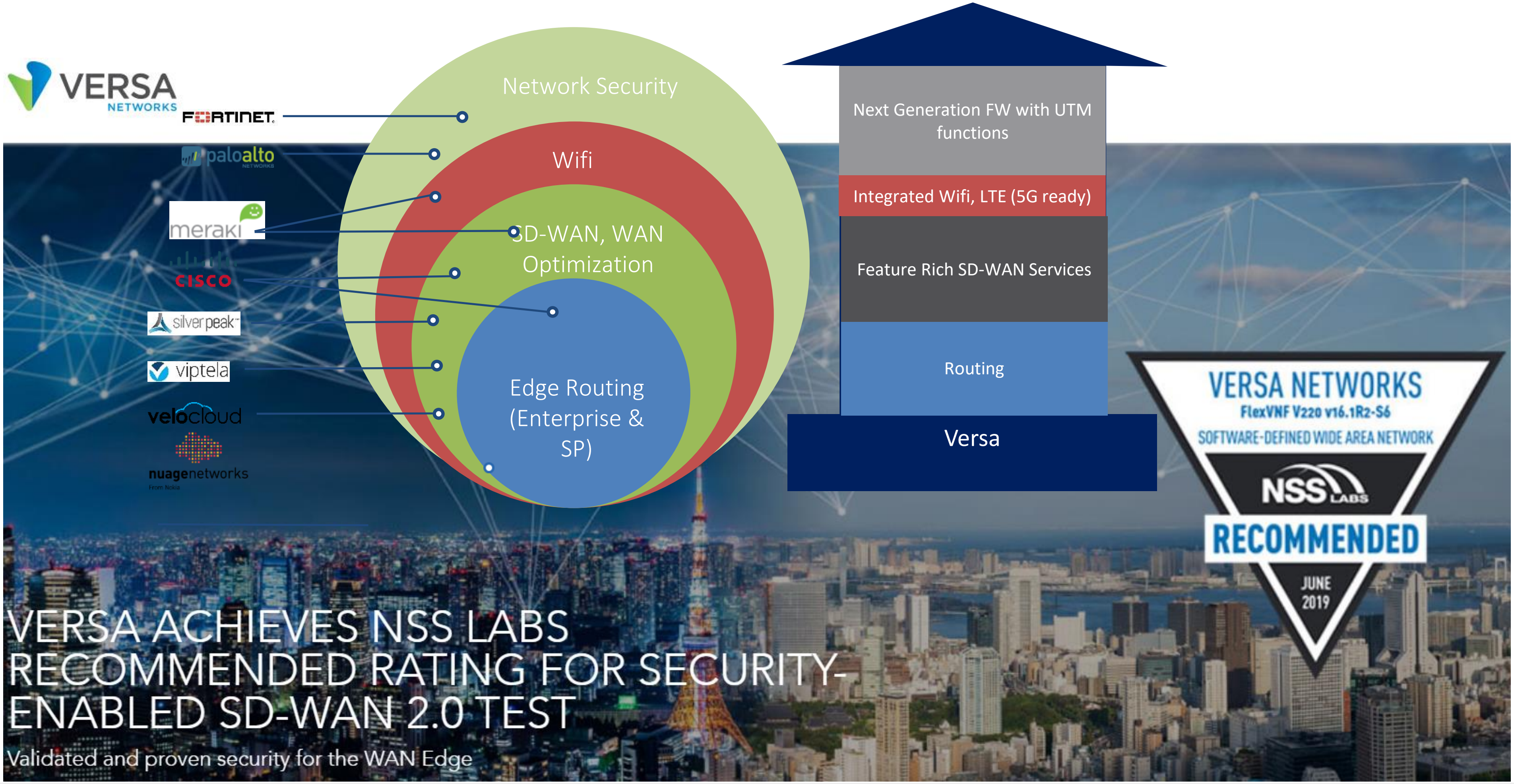
360VIEW

Reshaping the Remote Office

	CLOUDGENIX	riverbed	TALARI NETWORKS	velocloud	VERSA NETWORKS	viptela
Zero-Touch Install	✓	✓	✓	✓	✓	✓
Remote Device Elimination	✓	✓	✓	✓	✓	✗
Service Chaining/Insertion	✓	✓	✓	✓	✓	✓
Automated IP Address Discovery	✓	✓	✓	✓	✓	✓
Brown-Out Resiliency	✓	✓	✓	✓	✓	✓
MOS Scoring	✓	✗	✓	✓	✓	✗
Edge Device	Appliance/ Virtual	Appliance/ Virtual	Appliance/ Virtual	Appliance/ Virtual	Appliance/ Virtual	Appliance/ Virtual

TRACE3

3rd Party Validation



Network Security

Wifi

SD-WAN, WAN Optimization

Edge Routing (Enterprise & SP)

Next Generation FW with UTM functions

Integrated Wifi, LTE (5G ready)

Feature Rich SD-WAN Services

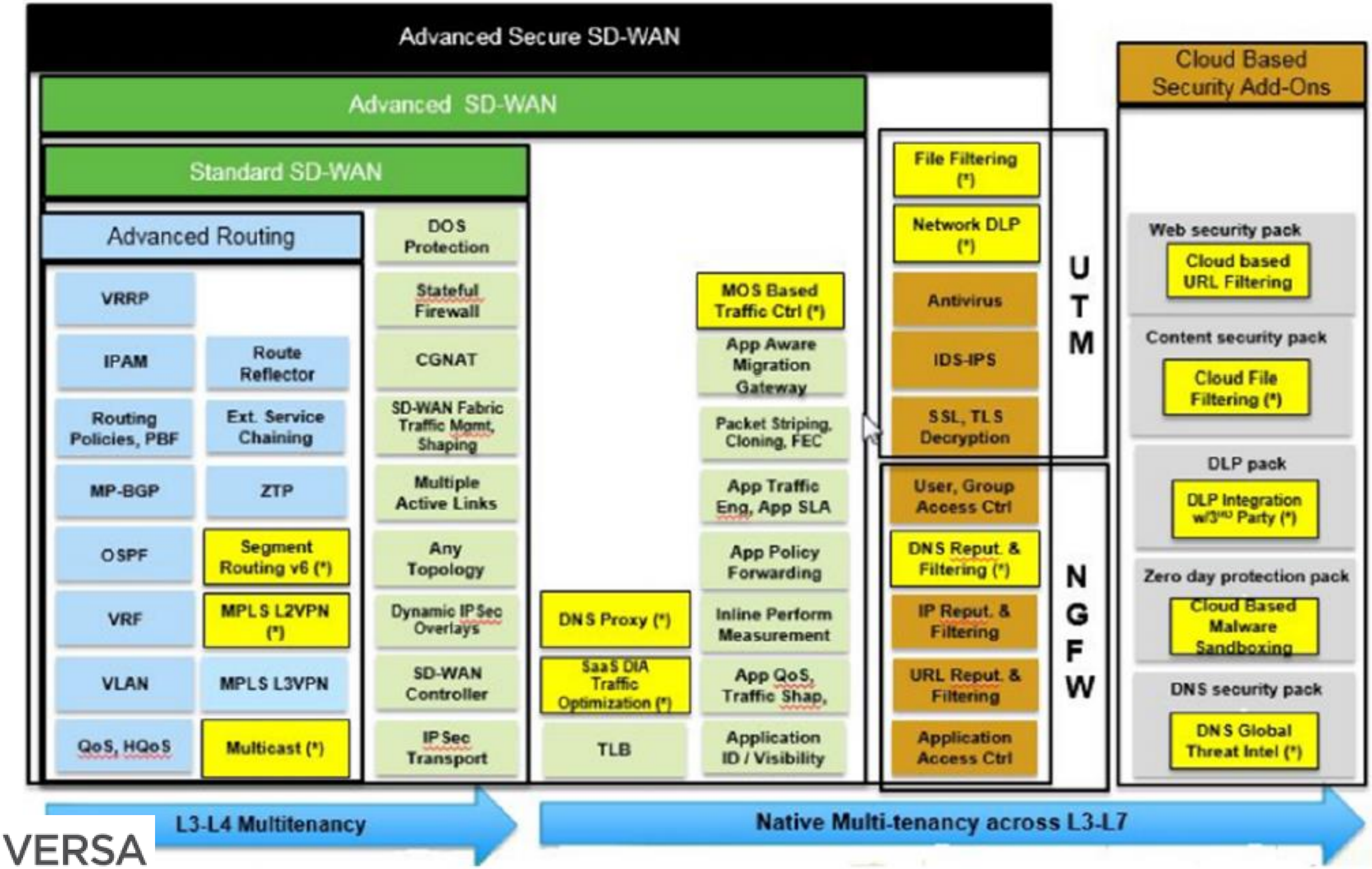
Routing

Versa

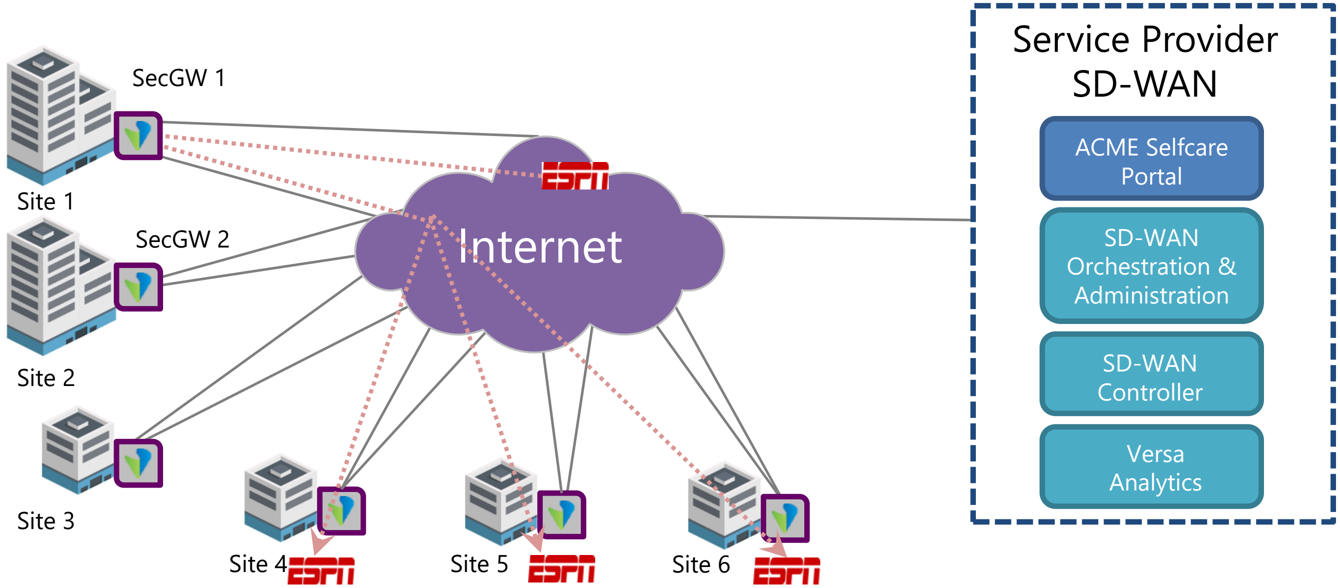
VERSA ACHIEVES NSS LABS RECOMMENDED RATING FOR SECURITY-ENABLED SD-WAN 2.0 TEST

Validated and proven security for the WAN Edge

SDN/NFV

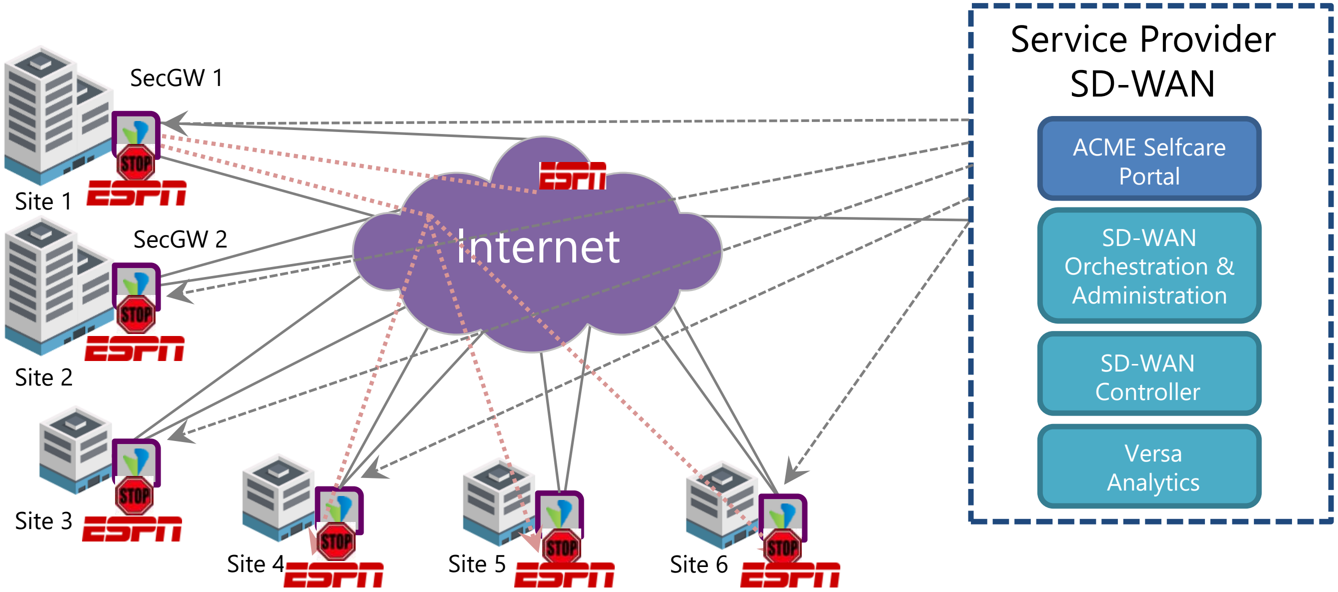

Advanced Secure SD-WAN
Advanced SD-WAN
Standard SD-WAN
Advanced Routing
VRRP
IPAM
Route Reflector
Routing Policies, PBF
Ext. Service Chaining
MP-BGP
ZTP
OSPF
Segment Routing v6 (*)
VRF
MPLS L2VPN (*)
VLAN
MPLS L3VPN
QoS, HQoS
Multicast (*)
DOS Protection
Stateful Firewall
CGNAT
SD-WAN Fabric Traffic Mgmt, Shaping
Multiple Active Links
Any Topology
Dynamic IPSec Overlays
SD-WAN Controller
IPSec Transport
DNS Proxy (*)
SaaS DIA Traffic Optimization (*)
TLB
MOS Based Traffic Ctrl (*)
App Aware Migration Gateway
Packet Striping, Cloning, FEC
App Traffic Eng, App SLA
App Policy Forwarding
Inline Perform Measurement
App QoS, Traffic Shap,
Application ID / Visibility
File Filtering (*)
Network DLP (*)
Antivirus
IDS-IPS
SSL, TLS Decryption
UTM
User, Group Access Ctrl
DNS Reput. & Filtering (*)
IP Reput. & Filtering
URL Reput. & Filtering
Application Access Ctrl
NGFW
Cloud Based Security Add-Ons
Web security pack
Cloud based URL Filtering
Content security pack
Cloud File Filtering (*)
DLP pack
DLP Integration w/3RD Party (*)
Zero day protection pack
Cloud Based Malware Sandboxing
DNS security pack
DNS Global Threat Intel (*)
L3-L4 Multitenancy
Native Multi-tenancy across L3-L7

Global Policy Enforcement



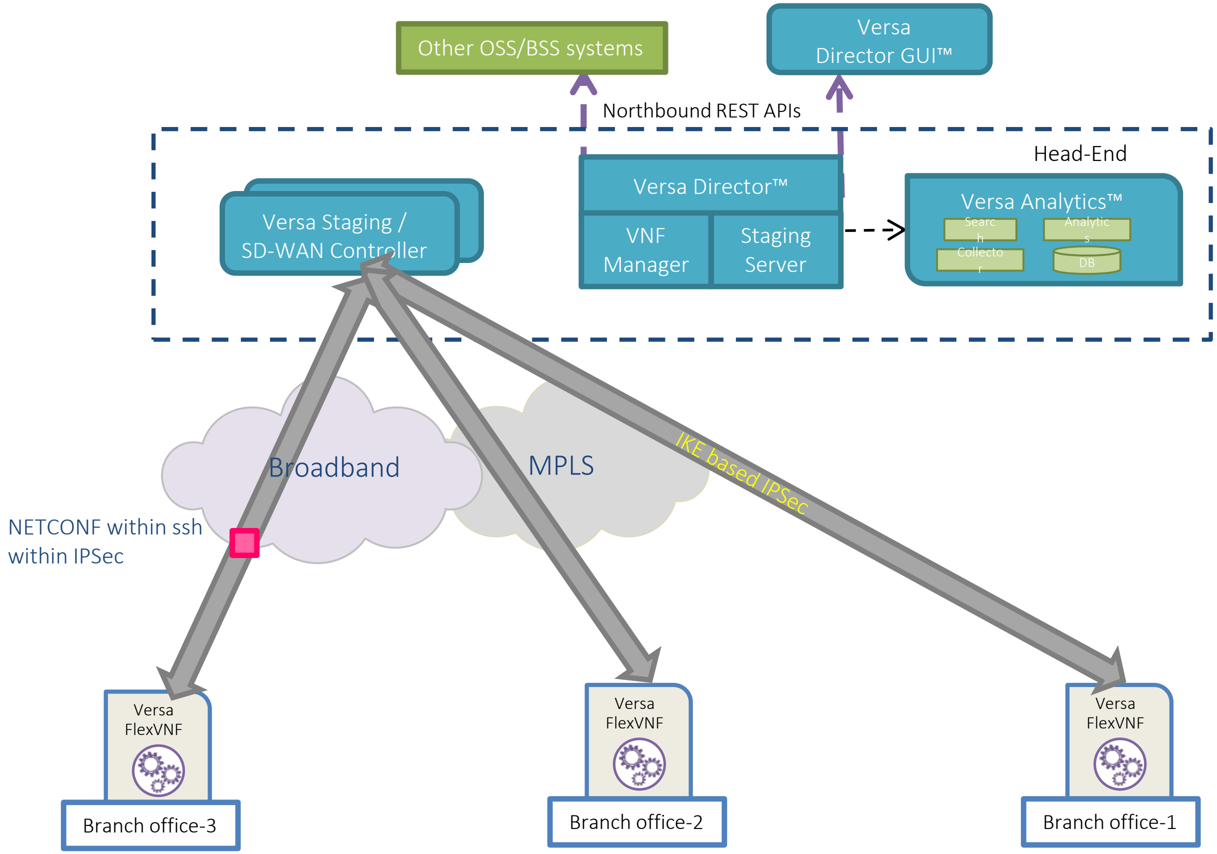
- Versa Analytics Reports a given application 'non compliant' with business practices is being used in some sites
- End customer installs a security policy rule in Versa Director or higher level Orchestration system

Global Policy Enforcement



- SD-WAN Orchestration and Administration (Versa Director) signals to each CPE to block the non business compliant application

Software Driven - API



Security Thumbnail…

Security Functions (all software-defined)				
NG-Firewall (NGFW)	DoS Prevention	Device Authentication	IPSec	User & Group Authentication
CGNAT	HTTP / SSL Proxy	DNS Security	URL Filtering	Web & IP Feeds
Malware Protection	IPS-IDS	Anti-Virus	File Filtering	Visibility & Analytics

- **Visibility & access control**
  - Application, domain & URL
  - User, device & location
- **Layer 7 & content security**
  - SSL decryption
  - App / URL / file filtering
  - Anti-virus
  - IDS-IPS
  - DNS Security

- **Layer 4**
  - Reconnaissance
  - DoS protection (ICMP, UDP, TCP flood)
    - Rate limiting
- **Layer 3**
  - ARP, IP ICMP protocol defense
  - IP spoofing
  - Strict source routing checks
  - Fragment overlaps

Versa Security – Data Sheet

Elastic NG Access Control Policy

- ✓ Application Identification
- ✓ URL and Content Classification
- ✓ DNS Domain
- ✓ Users and Groups
- ✓ Geo-Location
- ✓ Time Of Day

Elastic NG Visibility

- ✓ Logging
- ✓ Traffic Monitoring
- ✓ Packet Capture
- ✓ Flow Mirroring

ALGs

- ✓ FTP SIP DNS PPTP TFTP ICMP

Deployment Options

- ✓ Tap, Virtual wires
- ✓ VLAN
- ✓ L3/Routed Mode
- ✓ Built-in Routing, QoS, CGNAT, IPSec

IP Filtering Profiles

- ✓ Geo-Location Based Actions
- ✓ Reputation Based Actions
- ✓ Whitelists
- ✓ Blacklists

URL Filtering Profiles

- ✓ Category Based Actions
- ✓ Reputation Based Actions
- ✓ Whitelists
- ✓ Blacklists
- ✓ Captive Portal Pages

Anti-Virus Profiles

- ✓ AV Scan Profiles based on Application/File Types

IDS/IPS Profiles

- ✓ Signature/Anomaly Based Detection
- ✓ Coverage for last 10 years' vulnerabilities
- ✓ Support for Custom IDS Rules (in Snort rule format)

HTTP and HTTPS Proxy

- ✓ Certificate checks
- ✓ Transparent
- ✓ Explicit
- ✓ DNS and AD integration

Elastic L3 to L7 Zone/DDoS Protection

- ✓ Anomaly based detection
- ✓ Volumetric DoS detection
- ✓ Multi-layer DoS detection

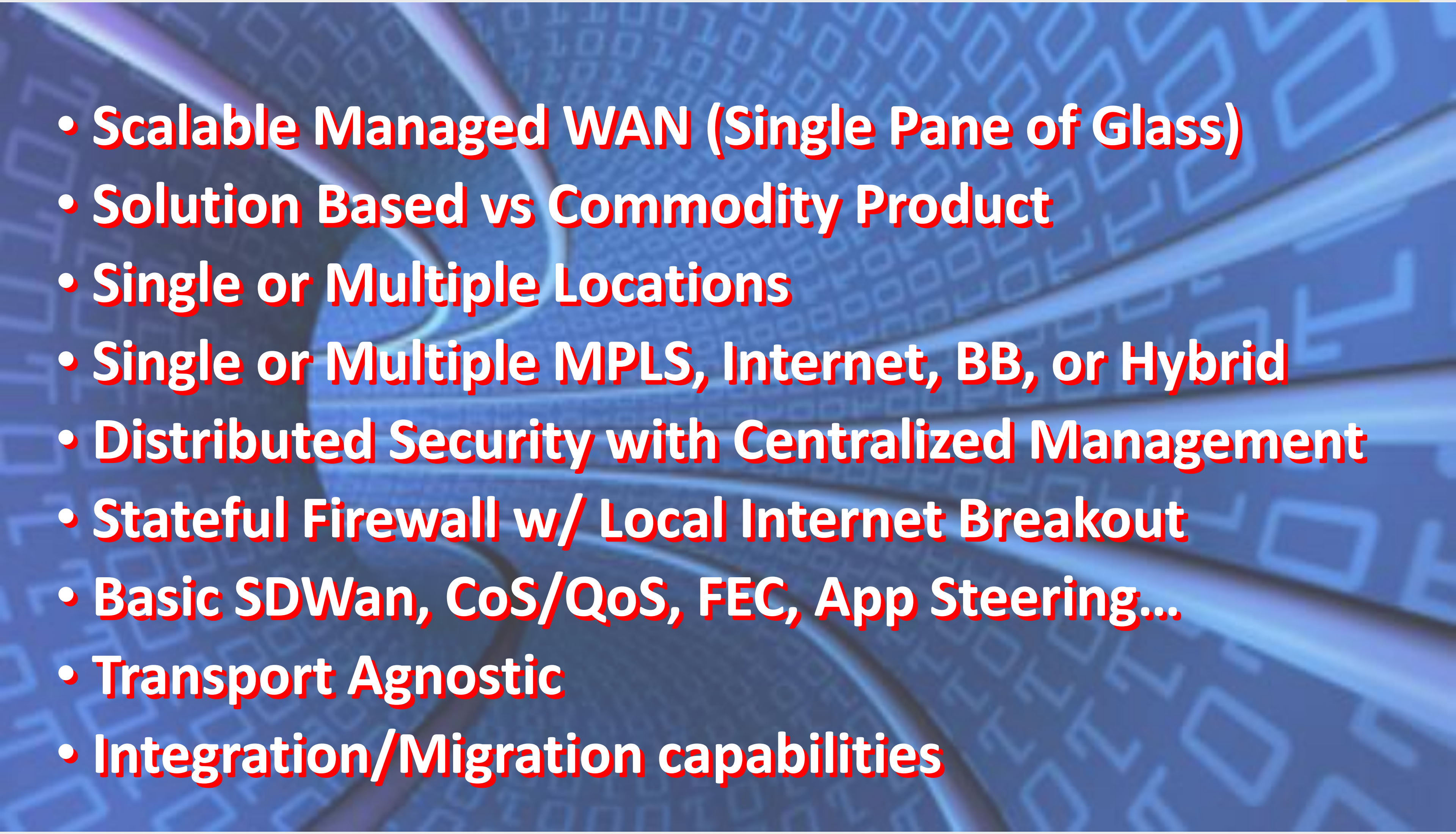
Security Updates

- ✓ Full/Incremental updates daily
- ✓ Real Time Updates several times during the day

Certifications

- ✓ ICSA
- ✓ ONUG
- ✓ NSS (Q4 2017)
- ✓ FIPS, Common Criteria (Q3 2018)

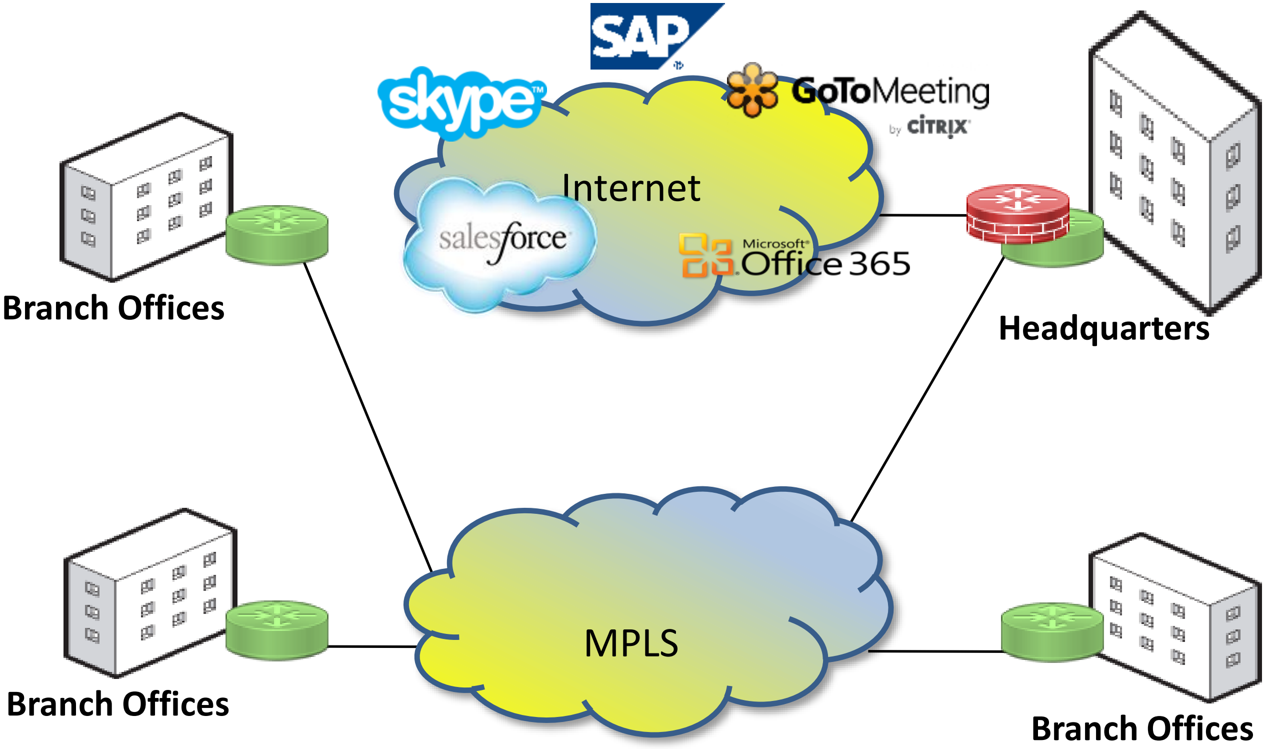
Dobson Phase I – Table Stakes



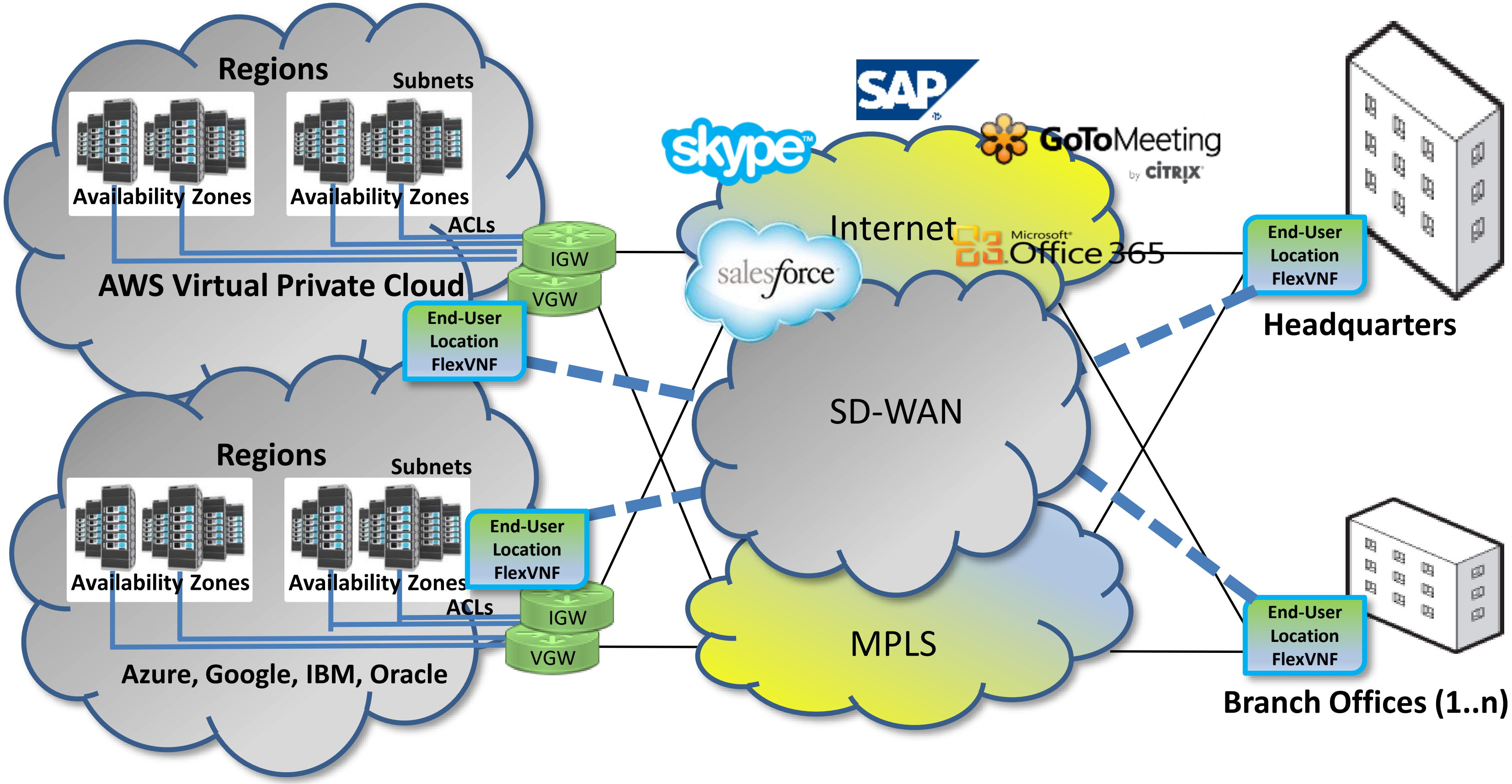
- **Scalable Managed WAN (Single Pane of Glass)**
- **Solution Based vs Commodity Product**
- **Single or Multiple Locations**
- **Single or Multiple MPLS, Internet, BB, or Hybrid**
- **Distributed Security with Centralized Management**
- **Stateful Firewall w/ Local Internet Breakout**
- **Basic SDWan, CoS/QoS, FEC, App Steering…**
- **Transport Agnostic**
- **Integration/Migration capabilities**

Yesterday…

Today…



Tomorrow…



- Cloud Enabled
- Transport Agnostic
- SaaS Optimization
- Distributed Security
- Big Data Analytics
- Artificial Intelligence

Dobson TECHNOLOGIES

Thank you!

Q & A?