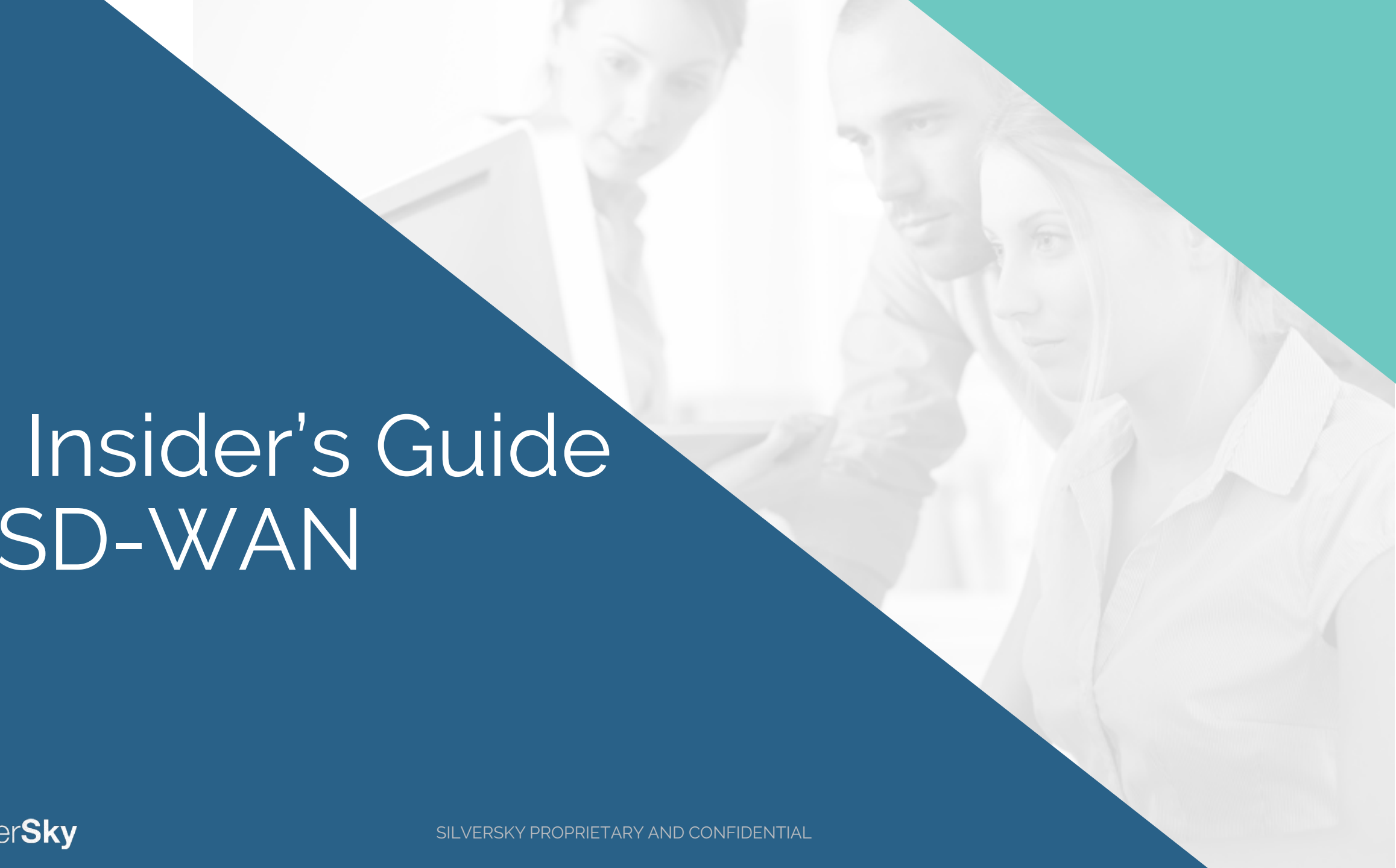


An Insider's Guide to SD-WAN

SilverSky

HOUSEKEEPING

This session is being recorded.

The recording and slides will be emailed to all registrants.

Please submit your questions into the Q&A box.

ABOUT THE SPEAKER

Michael Bacon has over ten years of experience in cybersecurity and over twenty years in IT. His background includes banking, finance, healthcare, government, military and IT companies.
Michael is Senior Product Manager for SilverSky MSS solutions.

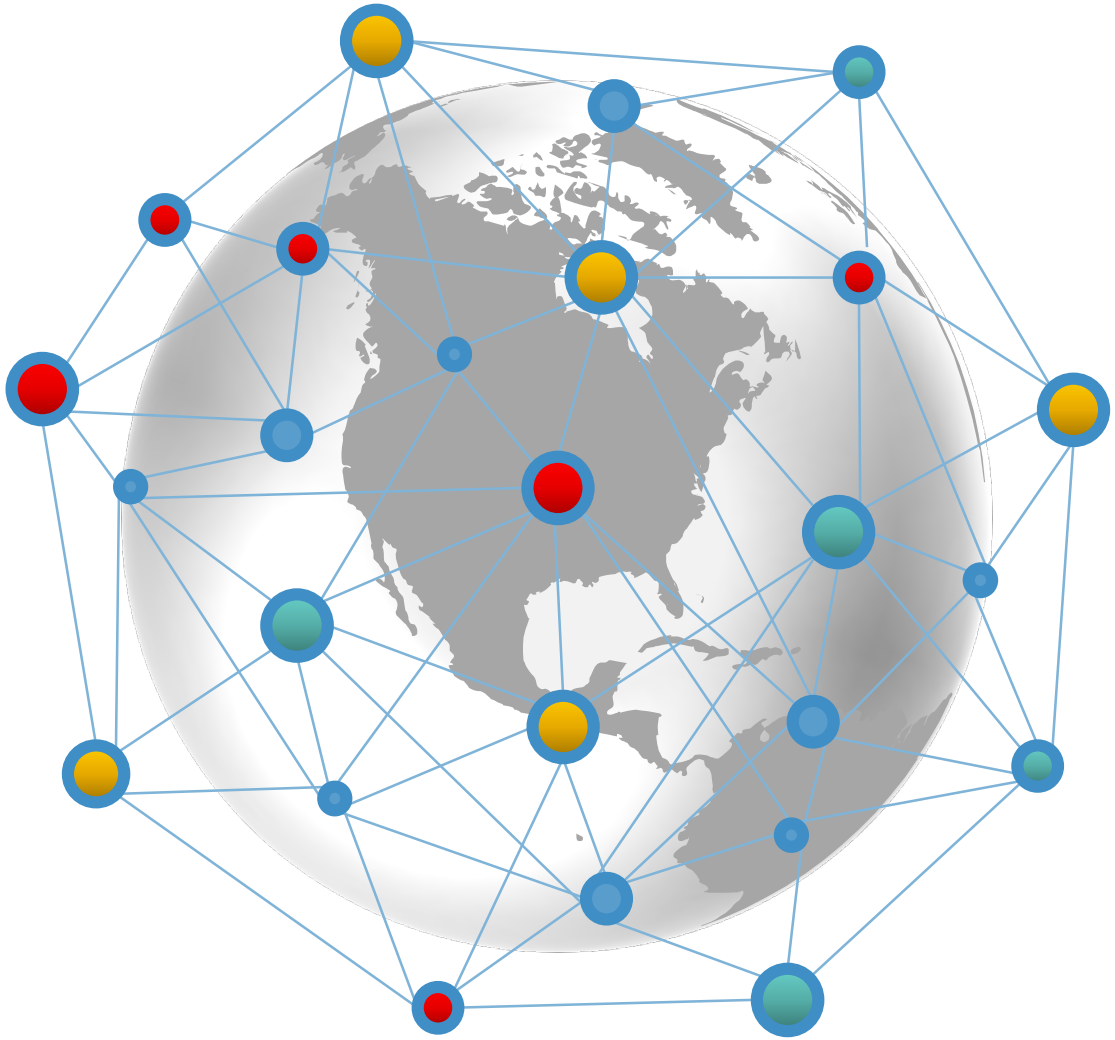
SilverSky

AGENDA

- Introduction
- Transforming traditional WAN
- Pros and Cons
- WAN vs. SD-WAN
- Use Cases
- Risks
- Q&A

SilverSky

INTRODUCTION TO SD-WAN



What is SD-WAN?

A **Software-defined Wide Area Network** (SD-WAN) is a virtual WAN architecture that allows enterprises to leverage any combination of transport services – including MPLS, LTE and broadband internet services – to securely connect users to applications, while reducing costs.

GLOSSARY OF TERMS

- **DIA**: Direct internet access
- **DDoS:** Distributed denial of service – cyber-attack to make resources unavailable
- **Firewall:** Network security system that monitors and controls incoming and outgoing network traffic based on predetermined security rules.
- **Micro-segmentation:** A network security technique that enables security architects to logically divide the data center into distinct security segments down to the individual workload level, and then define security controls and deliver services for each unique segment.
- **MPLS**: A routing technique in telecommunications networks that ensures reliable connections for real-time applications.
- **QoS:** Quality of service
- **Resiliency:** The ability to provide and maintain an acceptable level of service in the face of faults and challenges to normal operation.
- **SLAs**: Service level agreement
- **VNF: Virtual Network Functions**; virtualized network services running on open computing platforms formerly carried out by proprietary, dedicated hardware technology
- **VPN: Virtual Private Network**; connection method used to add security and privacy to private/public networks
- **Zero-touch provisioning**: a switch feature that allows the devices to be provisioned and configured automatically, eliminating most of the manual labor involved with adding them to a network.

NETWORK MANAGEMENT TRANSFORMATION

WAN (Old Way)

- Costly hardware and capex models
- High circuit costs
- Lack of flexibility and scalability
- Long implementation times
- Configuration errors
- Management complexity

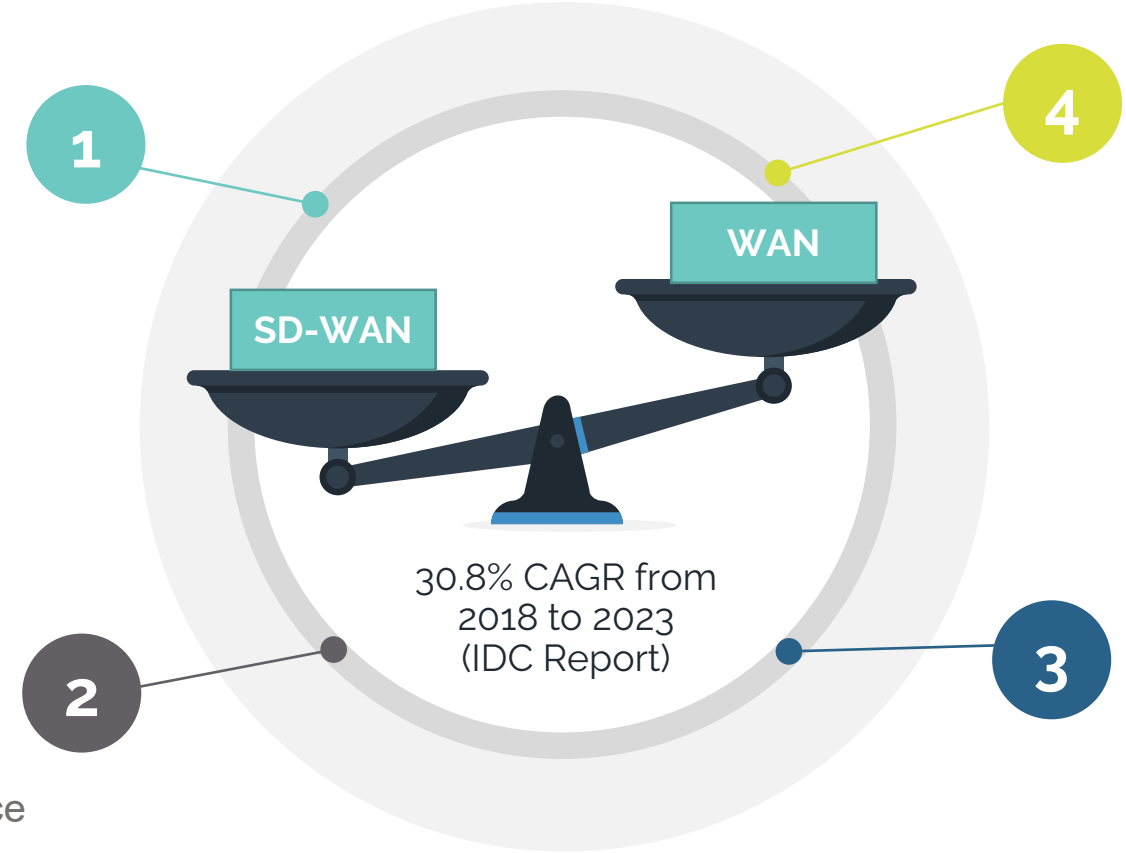
SD-WAN (New Way)

- Increased bandwidth without adding new hardware
- Multiple transport options
- Dynamic provisioning of resources
- Streamlined implementations
- Service templates for repeatability
- Simplified centralized management

SD-WAN IS TRANSFORMING NETWORKS

Reduces Network Costs

- Networks requiring more and more resources to support advanced application needs
- Customers pushing more and more workloads to the public cloud
- Need to reduce MPLS costs



Increasing Network Bandwidth

- Bandwidth on demand
- Maximizing bandwidth with current infrastructure
- Intelligent routing of traffic

Reduces Network Management Complexities

- More automation
- Greater control
- Managing network performance
- Traffic optimization

Addressing Security Gaps

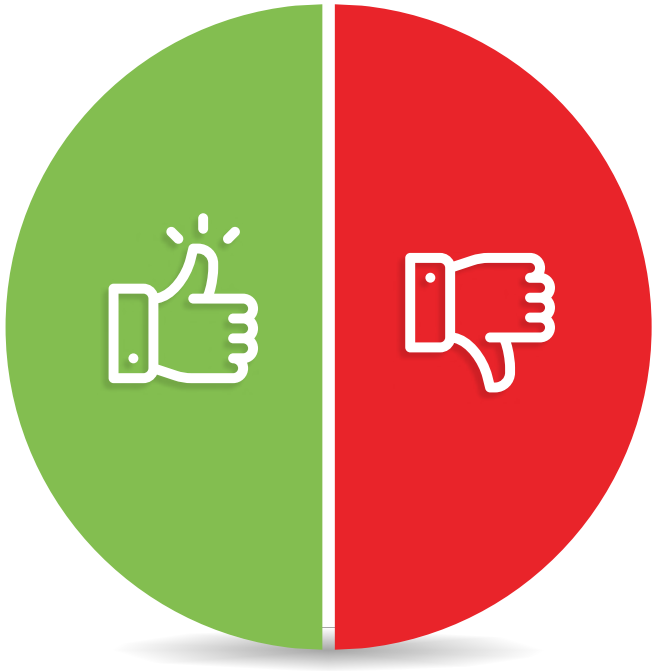
- Build security model into the Network configuration
- Mitigate security events through policies and automation

SilverSky

PROS AND CONS OF TRADITIONAL WAN

PROS

- Centralized IT infrastructure
- Guaranteed uptime because it's on premise
- Increased privacy
- Higher quality of service when running on MPLS



CONS

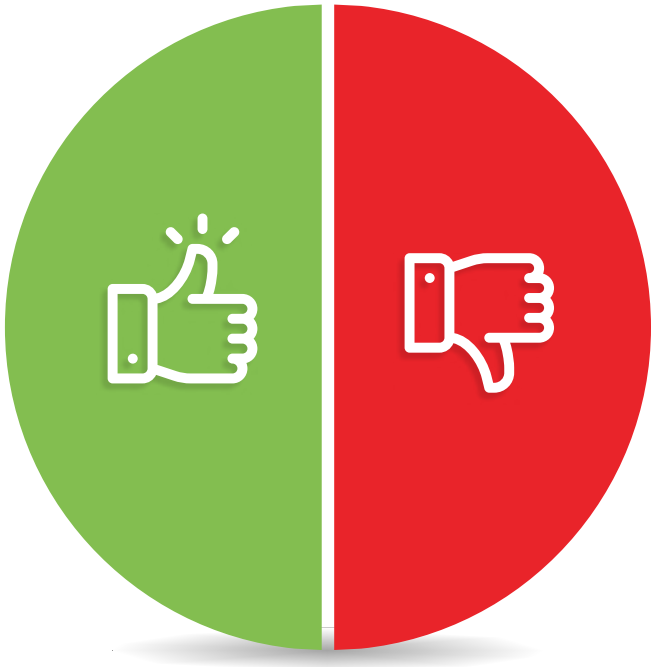
- High cost of setup and increasing bandwidth
- Security gaps within MPLS that frequently causes audit flags
- Management complexity
- Inflexible model that makes it difficult to respond to security threats or add bandwidth to support the business

SilverSky

PROS AND CONS OF SD-WAN

PROS

- Ability to dynamically scale up or scale down bandwidth as needed
- Increased security above what WAN offers such as end to end encryption
- Greater business agility and responsiveness
- Reduces cost by moving traffic off of MPLS



CONS

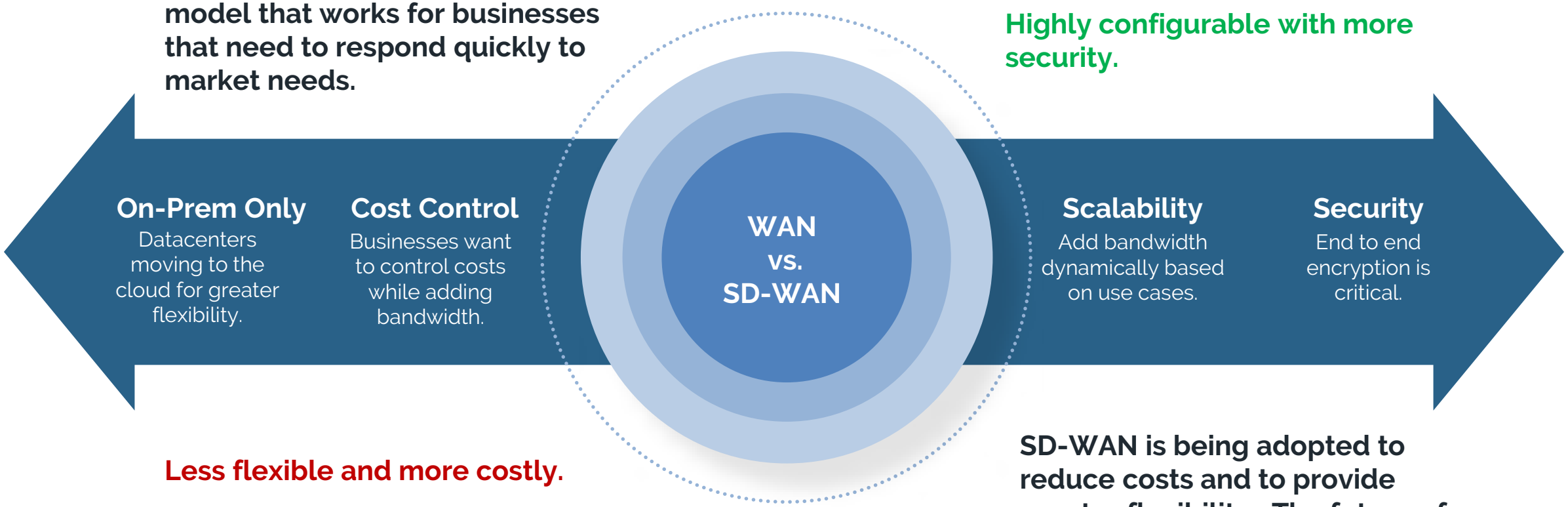
- Primarily a benefit for moving workloads to the cloud versus on premise
- Possible performance or QoS concerns when moving workloads to the cloud
- Could introduce new internal costs if you build and support your own solution
- Initial up front costs, but fuels cost savings long term

SilverSky

WAN VS. SD-WAN

Traditional WAN is no longer a model that works for businesses that need to respond quickly to market needs.

Highly configurable with more security.



Less flexible and more costly.

SD-WAN is being adopted to reduce costs and to provide greater flexibility. The future of SD-WAN is heavily tied to intelligent traffic deployments.

SilverSky

SD-WAN USE CASES

Cost Savings

- Circuit and Hardware Savings
  - Reduced MPLS costs by strategically routing mission critical applications through MPLS, but pushing other traffic to less expensive internet connections
- Ability to add bandwidth as needed without adding new hardware (using internet)

Bandwidth/Performance

- Application performance. Control performance by selectively routing traffic based on QoS or SLAs
- Zero touch provisioning
- Scale by dynamically adding bandwidth on demand.
- Support performance requirements based on user, location, or applications
- WAN resiliency model

Cloud On-Ramp

- Automation to Azure and AWS
- Connect remote sites and branches directly to the internet
- Branch multi-Cloud access
- Regional Cloud multi-hub access

Security

- End to end encryption of WAN traffic to the internet and back
- Secure automated WAN. Create policies that automatically reroute traffic based on security threats such as DDoS attacks.
- Secure, direct internet access (DIA)

SilverSky

SD-WAN IMPACTS SEVERAL INDUSTRIES

RETAIL

- Businesses are able to get stores up and running quickly compared to traditional WAN configurations.
- Reduces resource needs such as amount of hardware, number of engineers, and MPLS bandwidth.
- Less need for hardware upgrades.
- SD-WAN provides auto-provisioning of resources as needed across multiple sites at a time.

MANUFACTURING

- Large number of connected devices require greater control of prioritized traffic flows and connections.
- SD-WAN provides manufacturers flexibility of network segmentation for suppliers etc.
- Provides greater control of QoS requirements.
- Real-time data sharing and predictive maintenance requirements driving factor in the need for SD-WAN.

HEALTHCARE

- Networks for healthcare require a high degree of security to comply with state and federal regulations that SD-WAN can facilitate.
- SD-WAN provides deeper visibility across the network.
- Customers are able to centrally manage their network traffic and even prioritize mission critical applications.
- Healthcare organizations can reduce costs by driving some of their traffic through the internet.

BANKING/FINANCE

- Security is a primary driver for banks and financial institutions moving to SD-WAN. Large amounts of sensitive data is passed through the branch networks every day.
- SD-WAN solutions come with built-in security and protection such as temporary VPN connections and end to end encryption.
- Financial losses can be prevented using SD-WAN.

SilverSky

NOT ALL SD-WAN's ARE THE SAME

Gartner Group classifies SD-WAN products into four different categories:

- SD-WAN with Embedded Firewall
- SD-WAN with 3rd-party NG Firewall
- SD-WAN with Cloud-Based Security
- Firewall with Embedded SD-WAN

Depending on the solution you buy, you will either have richer security or SD-WAN capabilities.

It is good to do your homework. If security is something that is essential, you will want a SD-WAN solution that focuses highly on that.

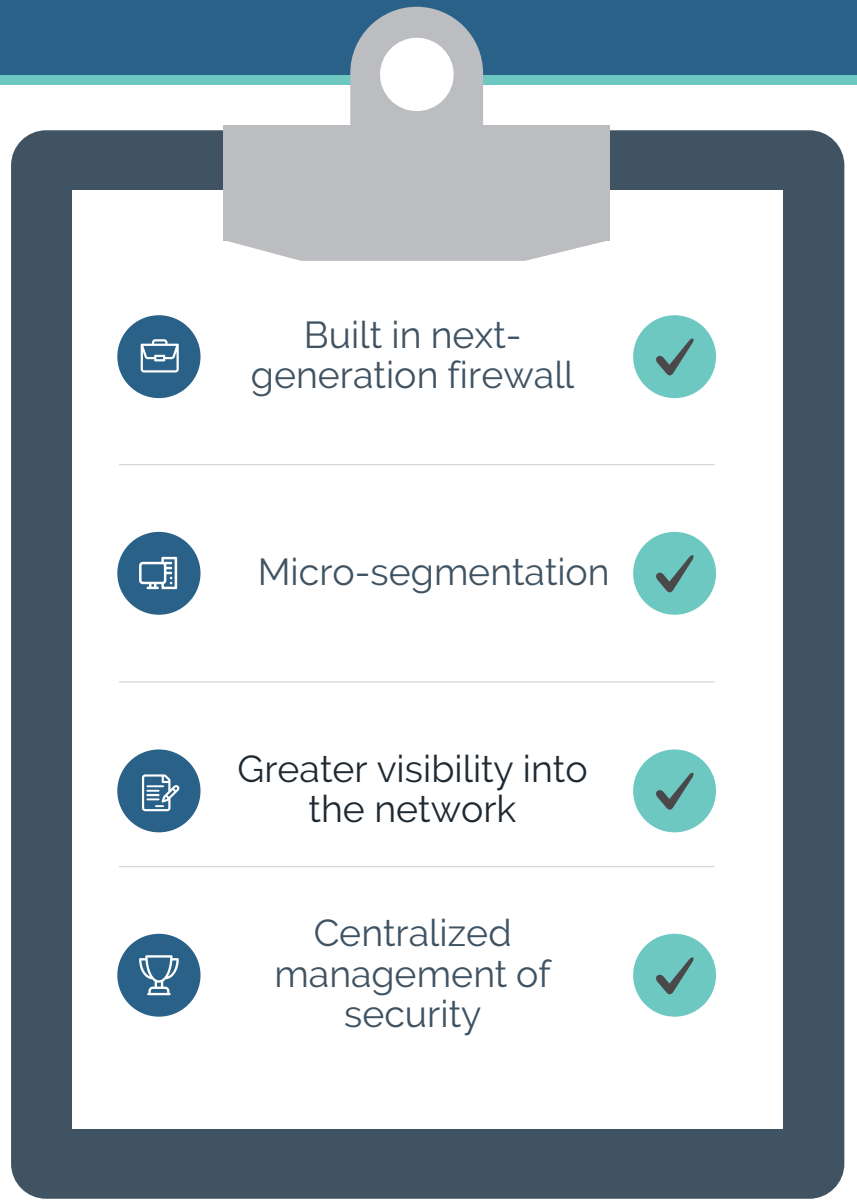
Pricing is also important. There may be a point where it is cost prohibitive and it will eat into your ROI

(Gartner report – "Four Architectures to Secure SD-WAN, October 2017")

SilverSky

SD-WAN SECURITY

- SD-WAN security primarily based on use of IP security, VPN tunnels, next-gen firewalls and micro-segmentation of application traffic with end to end encryption.
- A centralized security model is necessary due to WAN virtualization, and Cloud based applications extending the network perimeter.
- Virtualized next-generation firewall is built into SD-WAN, which gives the ability to run multiple virtual network functions (VNFs) such as application awareness, intrusion detection and prevention, web content filtering, malware detection and antivirus protection.
- Micro-segmentation allows administrators to separate traffic flows based on application characteristics and security policies. This segregation can be down to the workload level.
- Deeper insight into application bandwidth, resource utilization, and performance, gives administrators the ability to put security policies in place that limit user access per IP address or application.

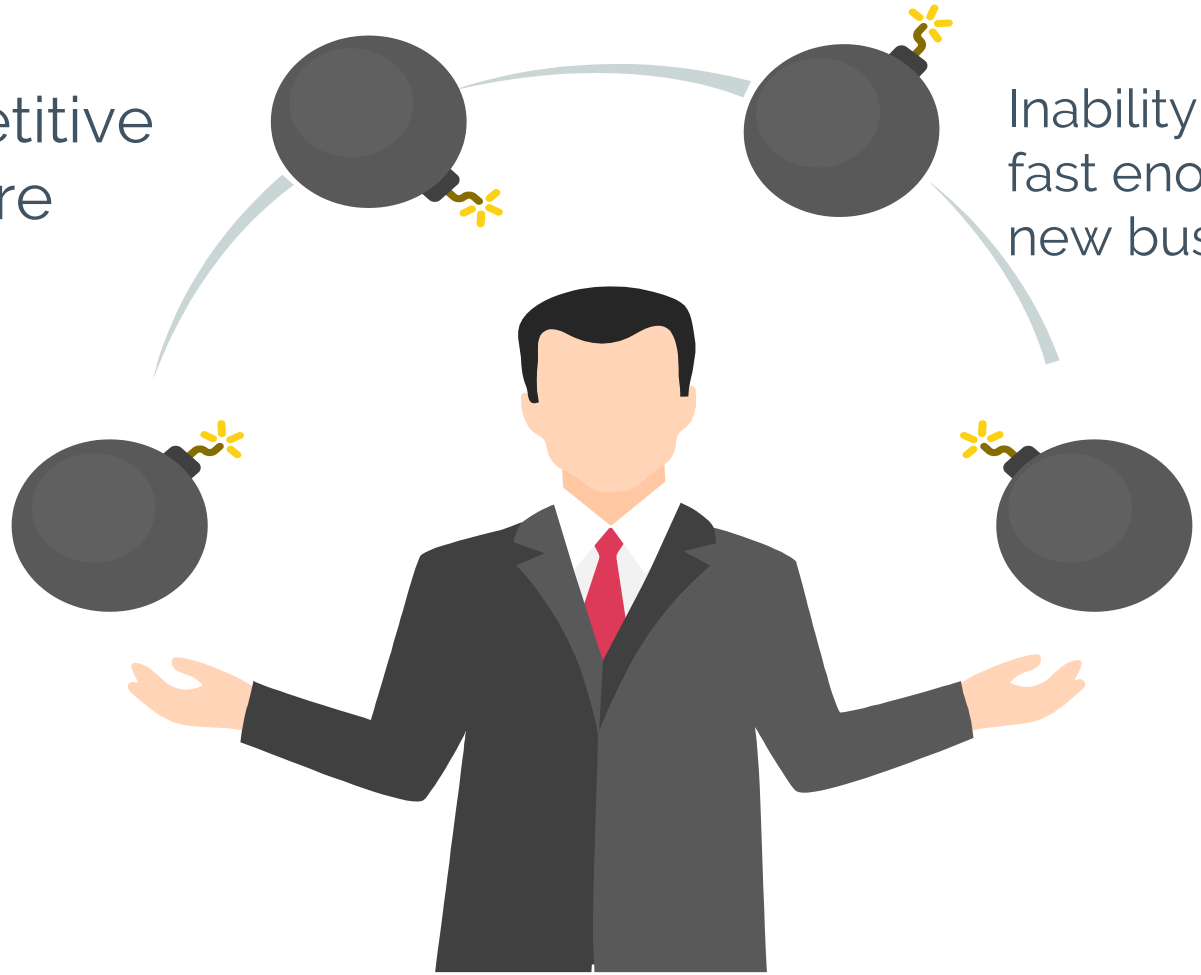


SilverSky

RISKS OF NOT IMPLEMENTING SD-WAN

Competitive Pressure

Inability to scale fast enough for new business



Thinning Margins

One security incident away from a disaster

SilverSky

SILVERSKY SD-WAN SOLUTION

END TO END SECURITY

APPLICATION AWARENESS

MULTI-PATH INTELLIGENCE

WAN RESILENCY

SEGMENTATION

THANK YOU

learn@silversky.com

1-800-234-2175