

The Risks and Rewards of Transitioning to NFV

What CSPs should know in 2018



CSPs

Communications Services Providers (CSPs) provide the networks and connectivity that empower our digital economy – and they are facing unprecedented pressure. Demands from customers and stakeholders are pushing them to:



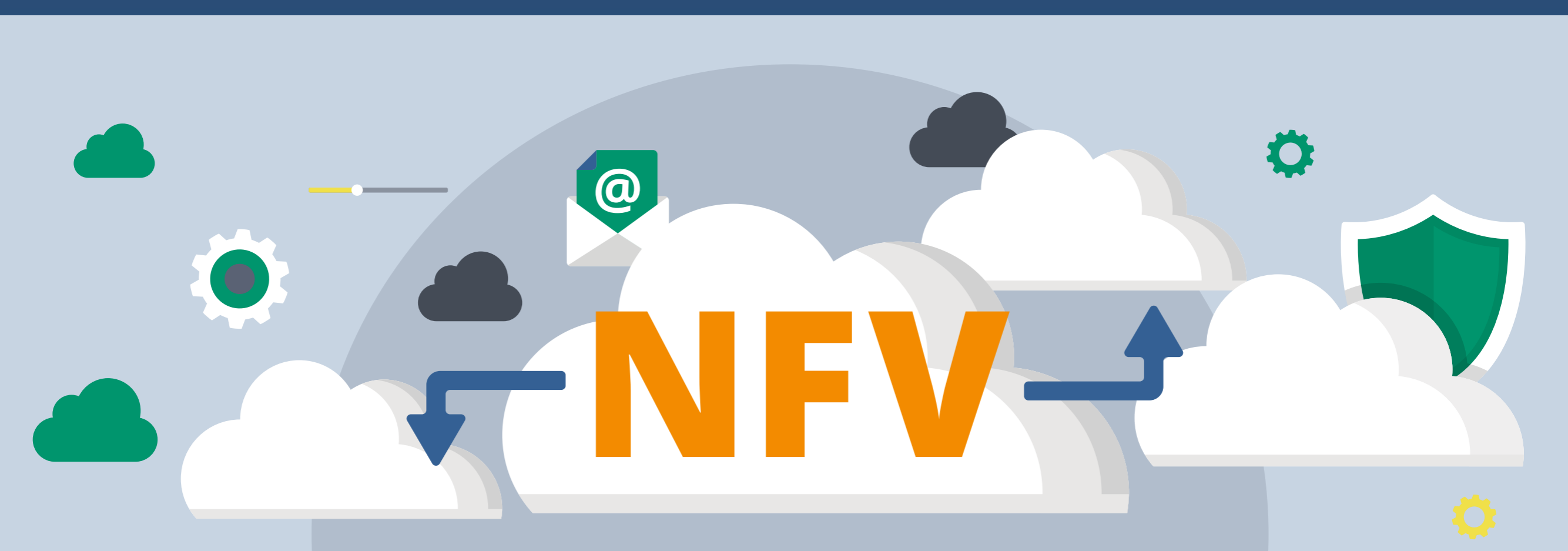
Innovate Faster



Accommodate Disruptive Technologies



Differentiate Their Offerings



Therefore, many are turning to Network Function Virtualization

NFV is the architectural approach of running software-defined network functions independent of any specific hardware platform.

NFV creates 'elasticity' within the infrastructure to dynamically provision network resources, providing agility and efficiency.

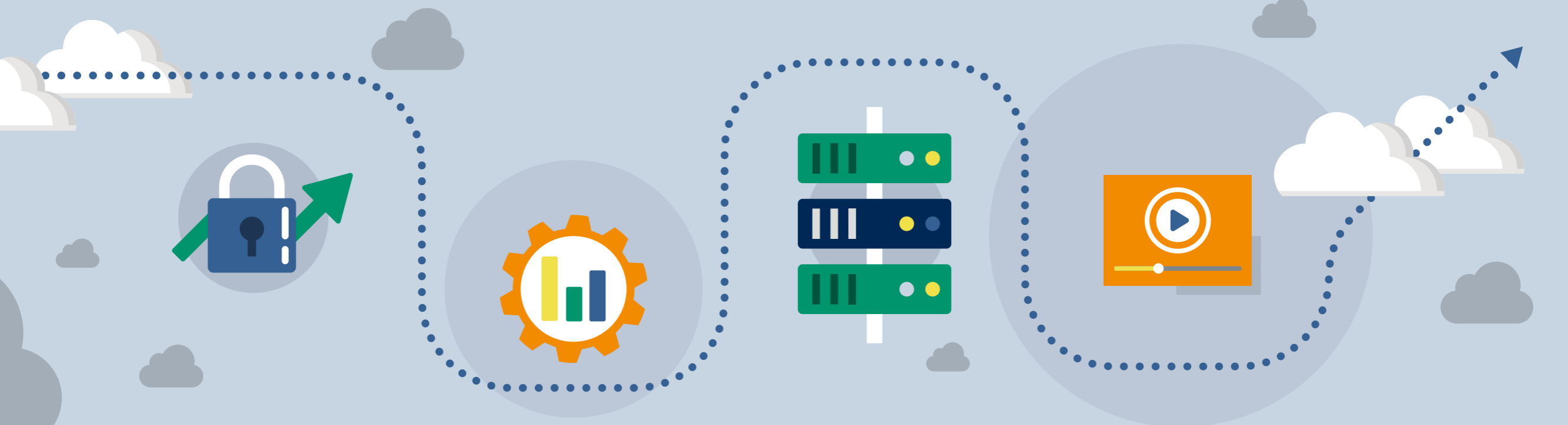


100%

of operators will implement NFV at some point*

82%

plan to extend NFV to customer sites*



NFV provides extensive flexibility for innovation

But given the size of CSPs' networks, many will transition to NFV in phases and, for a period of time, run hardware-oriented and cloud-based networks simultaneously, which can present its own unique set of challenges.

The Potential Risks and Rewards of NFV: A Breakdown

RISKS



Legacy network assurance tools aren't designed to manage virtualized network resources

They can be unstable and aren't optimized to manage multiple environment types.



Managing very different network operations types will be a challenge for network teams

They'll need end-to-end visibility of their operations through a single pane of glass.



Using multiple monitoring tools isn't efficient

It can lead to increased operating costs and higher MTTR when toggling between screens.



NFV brings agility and complexity

This can make it easier for a minor infrastructure performance issue to widen into a service-impacting event.

REWARDS



NFV offers the speed and responsiveness to seize new market opportunities

CSPs can offer compelling new mobile services, including music/video streaming, gaming, IoT and more.



Scalable, flexible provisioning enables automation when managing network services

This provides more efficient ways to meet fluctuating demand.



NFV helps drive efficiencies in network operations

This is due to its cloud-based approach, open systems, and reference architectures.



NFV's automation empowers business agility

CSPs can implement new ideas quickly with less risk and lower costs.

So how do CSPs manage the transition, ensuring visibility across both their legacy and NFV-equipped network environments?

The SevOne NFV Service Assurance Solution gives CSPs the real-time visibility they need to efficiently manage physical and virtual network environments. It is designed to meet the needs of CSPs implementing multi-vendor virtual network functions and service models as part of an OpenStack™-based virtual infrastructure, while also supporting their existing physical network infrastructure.

