BUILD YOUR FUTURE-READY INFRASTRUCTURE

OPTIMIZE, MONETIZE, AND SECURE YOUR NETWORK

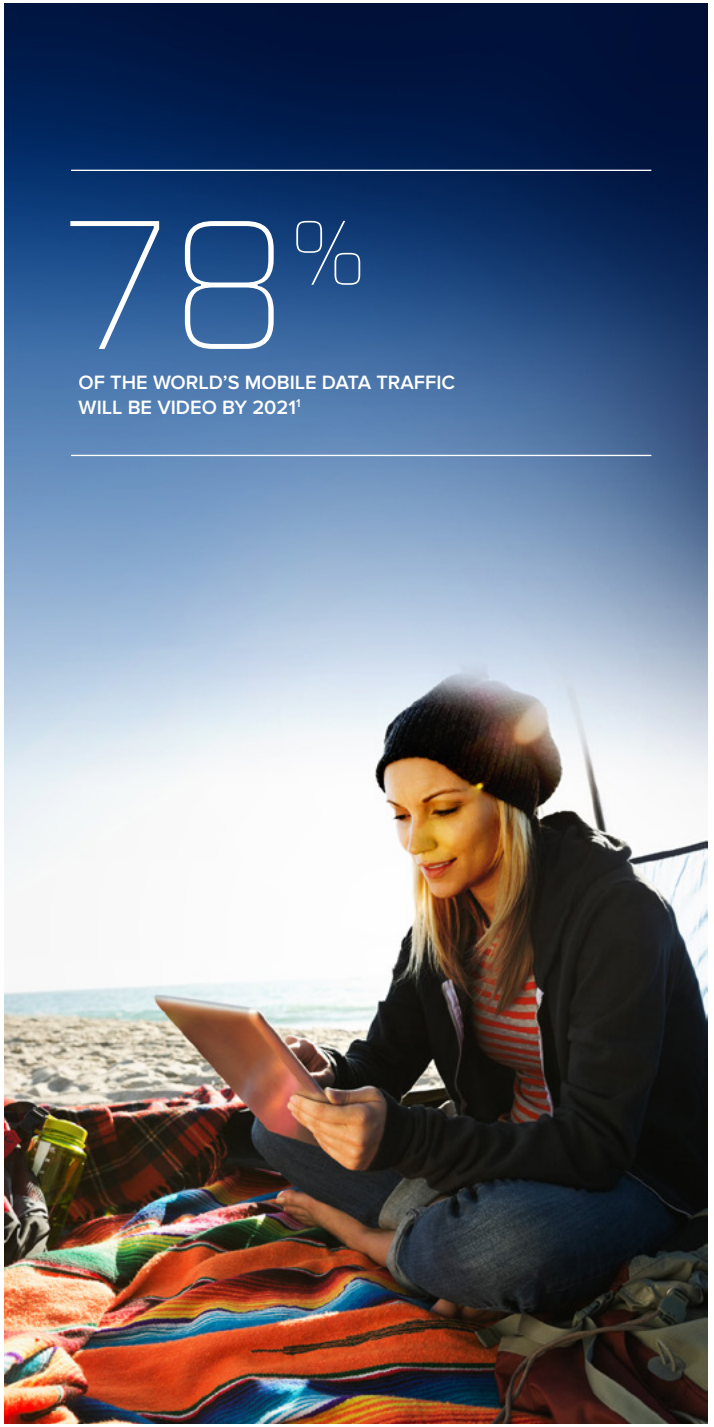
EVOLUTION AND DISRUPTION

The service provider (SP) business landscape is dominated by shifting subscriber requirements and a changing competitive climate. Technology advancements and service-level expectations are disrupting what has long been the principal objective: to nurture the core business and ensure a robust recurring revenue stream. These evolving business dynamics require new strategies to help you achieve sustained success.

The competitive landscape is in flux. Your competitors are scrambling to reposition existing business models as new offerings, and influential providers of cloud services are disrupting the way IT services have traditionally been delivered.

To stay competitive, Service Providers must be future-ready. 5G technology promises 10 times the throughput of current-generation mobile technology and the expectation of lower end-to-end latency (1 millisecond). The Internet of Things (IoT) brings an exponentially increasing number of devices to the web, each of which interact over mobile and fixed networks. This broad attack surface lends itself to unparalleled opportunities for malicious activity. Plus, a massive amount of video traffic floods SP networks—we're talking about zettabytes (10^{21}) of data. By 2021, video could account for as much as three-quarters of all mobile digital traffic.[1] Now is the time to start building your future-ready infrastructure.

YOUR LANDSCAPE IS DOMINATED BY SHIFTING SUBSCRIBER REQUIREMENTS AND A CHANGING COMPETITIVE CLIMATE.



[1] https://www.cisco.com/c/en/us/solutions/collateral/service-provider/visual-networking-index-vni/mobile-white-paper-c11-520862.html

THREE CRITICAL IMPERATIVES

It's a challenging time. Are you ready? Three fundamental concerns drive decision-making when it comes to network expansion: network optimization, services monetization, and data security:

1. **Optimize network investments and reduce total cost of ownership (TCO)**—Long-term survival mandates that you build-in sustainable profitability with your network investments.
2. **Monetize existing and emerging services opportunities**—With slowed subscriber growth and expectations to deliver reliable, secure performance across all existing and projected services, you must find new ways to grow and remain competitive. That growth will come through new service offerings and differentiated features.
3. **Inspire trust by delivering secure connectivity and data protection**—In the face of growing malware, distributed denial-of-service (DDoS), and other intrusive attacks, ensuring subscriber connectivity and protecting hosted data are paramount concerns. Trust goes hand in hand with reliably protected data and unencumbered network availability.

Dealing with these concerns is not a one-dimensional challenge. Get them right and the future is full of opportunity. Stumble and you risk irrelevance.

OPTIMIZE
Build-in profitability with your network investments.

MONETIZE
Deliver new service offerings and differentiate features.

SECURE
Ensure subscriber connectivity and protect hosted customer data.

OPTIMIZE TRAFFIC MANAGEMENT

With IP traffic predicted to grow at a 24 percent compound annual growth rate (CAGR)[2], optimizing your network to improve efficiencies and reduce costs is a top priority. At the same time, creating new revenues to offset rising network costs is imperative.

Consolidation of services, effective traffic management, and policy-driven automation are proven techniques that can help you both maximize network performance and reduce costs. Many optimization strategies help you focus on managing the exponential growth of internet traffic, a significant percentage of which is video.

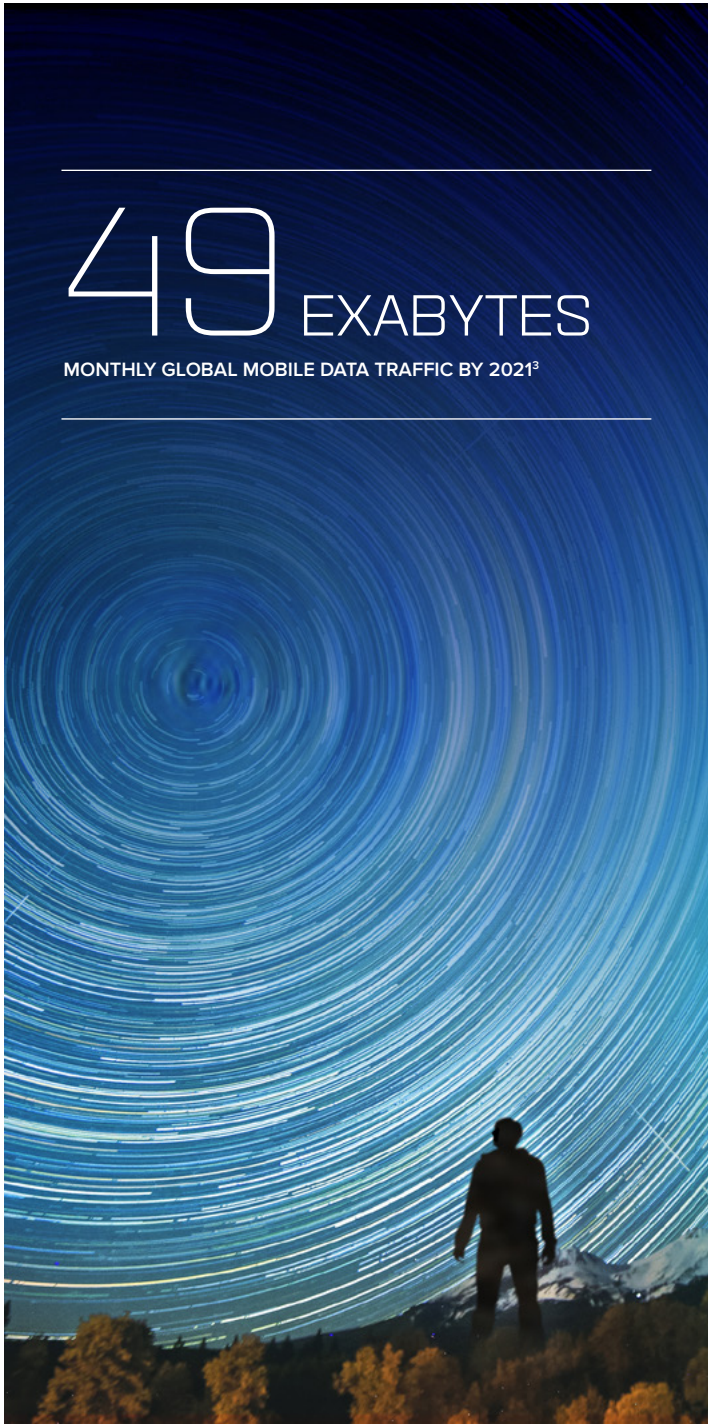
PROVIDE SUBSCRIBERS WITH THE SERVICE LEVELS AND QOE THEY EXPECT.

Network optimization can also help you increase service velocity. Improved traffic management, service function chaining, and detailed network analytics will help you deliver new services based on subscriber plan, location, and devices. These steps will also help you prepare for 5G implementations that require low latency and high throughput.

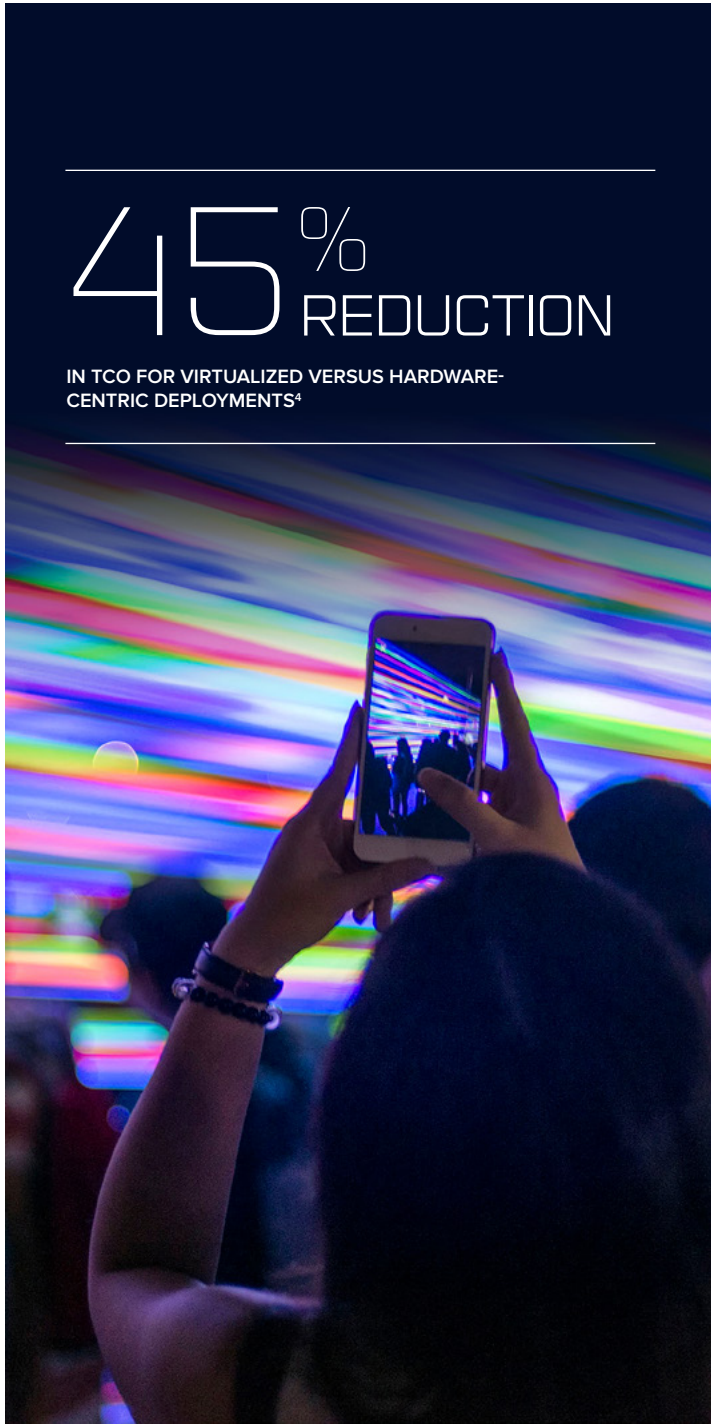
Above all, your networks must provide subscribers with the service levels and quality-of-experience (QoE) they expect, while ensuring end-to-end security. This includes managing and delivering security protection where it is most needed.

Five strategies that can help you optimize traffic management include:

- Consolidating network functionality
- Maximizing traffic throughput
- Increasing service velocity
- Enhancing service value
- Applying analytics to enhance subscriber QoE



[2] https://www.cisco.com/c/m/en_us/solutions/service-provider/vni-forecast-highlights.html
[3] https://www.cisco.com/c/en/us/solutions/collateral/service-provider/visual-networking-index-vni/mobile-white-paper-c11-520862.html



VIRTUALIZE YOUR NETWORK

Over the next five years, global Internet traffic will triple and broadband speeds will nearly double.[5] While much of the demand volume results from growth in video traffic, the IoT will drive an increase in the number of connected devices. The move to 5G and the emergence of new applications (for autonomous vehicles for example) will drive the need for higher bandwidth and lower latency.

It's essential that you scale networks to meet these traffic and bandwidth demands. You must grow efficiently and reduce costs where possible. At the same time, you must generate and deliver new services to offset these costs and remain competitive. Virtualized network functions will be a key to meeting those demands.

Network functions virtualization (NFV) was originally adopted as a means to lower capital expenditure costs and reduce data center overprovisioning. Service providers have discovered that integrating NFV offers many other benefits, including the following:

- **Increased service velocity**—Get to market faster by provisioning new services in hours/days versus months. Easily test services using targeted deployments.
- **Elastic scaling and flexibility**—Quickly scale to meet demand by reusing and repurposing general-purpose hardware, or provisioning in the cloud using commercial, off-the-shelf (COTS) hardware. Port services from one data center to another with whatever network functions you need, wherever you need them.
- **Access to best-of-breed solutions**—Integrate and manage solutions from different vendors that run on common hardware platforms.
- **Simplified service function chaining**—Chain micro services to deliver macro services, dynamically change how traffic is run, and improve traffic flow efficiency.
- **Improved management and orchestration**—Integrate with NFV managers, orchestrators, and SDN controllers from a wide variety of vendors.
- **Lowered TCO**—Reduce or eliminate the need for overprovisioning data centers, run on lower-cost, generic hardware, and increase overall network efficiencies.

GET TO MARKET FASTER BY PROVISIONING NEW SERVICES IN HOURS/DAYS VERSUS MONTHS.

[4] https://www.acgcc.com/creating-agility-efficiency-at-scale-the-economic-advantages-of-open-architecture-platforms-in-nfv-deployments/
[5] https://www.cisco.com/c/m/en_us/solutions/service-provider/vni-forecast-highlights.html

ENSURE SECURITY, ESTABLISH TRUST

Service provider data security focuses on two core issues: maintaining network availability and preventing data loss. Failure in either area can irreparably damage your reputation and directly impact your bottom line.

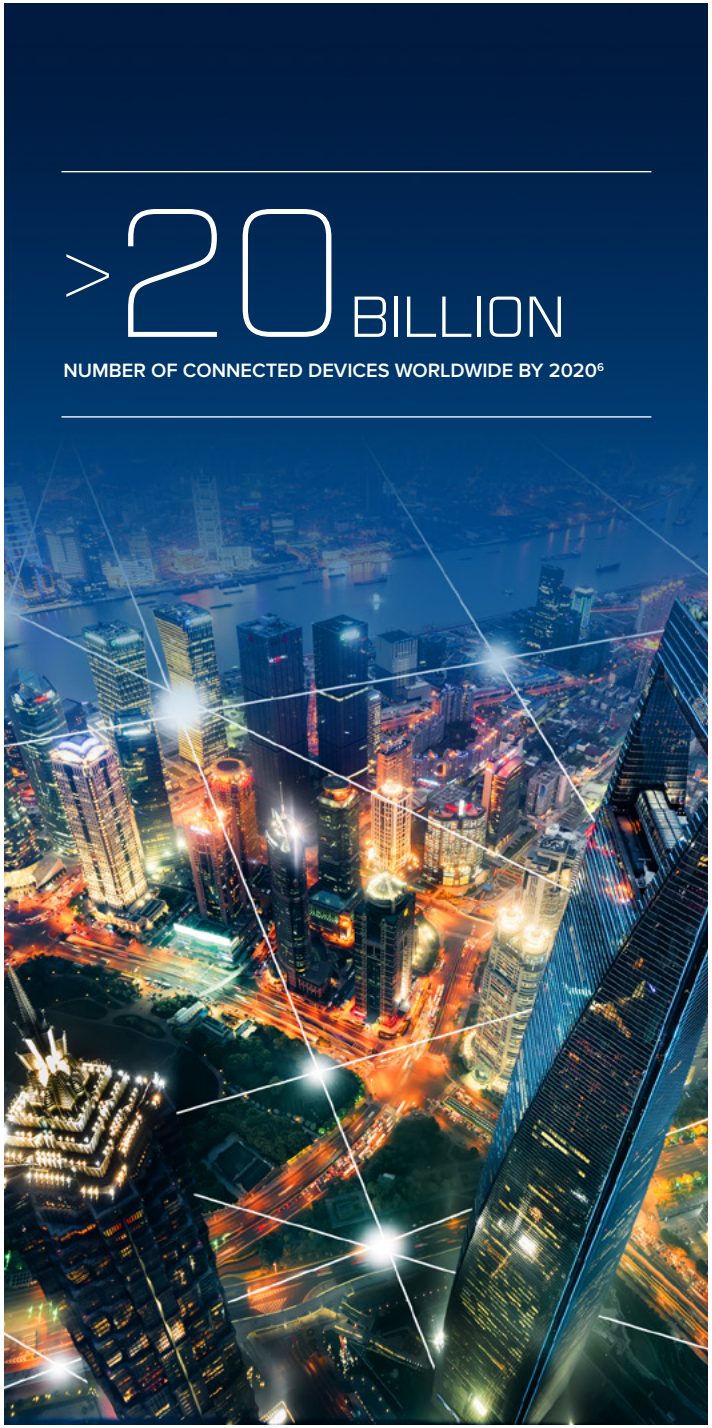
Adopt targeted measures for every vulnerability in your network. The three most effective strategic control points in your network are the data center, the network edge/SGi-LAN, and the roaming interconnect. Each control point plays a complementary role in your security infrastructure.

ADOPT TARGETED MEASURES FOR EVERY VULNERABILITY IN YOUR NETWORK.

Different types of traffic transiting to and through your network might require different security techniques. Stopping a high-volume, DDoS attack does not require the same methods as stopping an intruder trying to gain access to hosted data storage (even though those attacks might occur to, or within, the same network). Being able to quickly identify and handle attacks is paramount to protecting your network. A multi-layered strategy can help make that process more efficient.

Of equal concern are the billions of diverse devices flooding the network with real-time communications. These communications expose network vulnerabilities, but with the emergence of even more advanced mobile and fixed-network capabilities, the volume and variety of attacks will only increase. Every device carries the potential to become a target for hackers and denial-of-service attacks.

A comprehensive approach—strategically overlaid onto your network with measures designed to address specific types of threats at each control point—will give you added versatility to scale your security implementation. The goal is to deliver 24x7 security that will inspire subscriber and customer trust in your infrastructure.



[6] https://www.gartner.com/newsroom/id/3598917

ADAPT TO THRIVE

Emergent technologies, such as real-world artificial intelligence, virtual and augmented reality, and perhaps even drones will converge collectively on both mobile and fixed network infrastructures. They will usher in new technology implementations, including distributed data centers, control- and user-plane separation (CUPS) of EPC nodes, and service-based architectures.

In addition to the onslaught of new technologies, zettabytes of data traffic are being channeled through your networks from over-the-top (OTT) video traffic and technical innovations (such as 4K and Ultra HD video), adding systematic growth to existing traffic-management strains.

To successfully address accelerating bandwidth demands, service providers must adapt existing traffic management, scalability, and security strategies to ensure sustainable delivery of uninterrupted network availability while protecting data integrity. How well you adapt these three key strategies—service velocity, scalability, and security—will determine your ability to thrive in this quickly evolving market.

THREE KEY STRATEGIES WILL DETERMINE YOUR ABILITY TO THRIVE: SERVICE VELOCITY, SCALABILITY, AND SECURITY.

PICK THE RIGHT PARTNERS

Getting your infrastructure future-ready is a multi-stage process. Your first step is to collaborate with vendors, partners, and suppliers that add value to your expansion initiatives.

THREE GUIDELINES WILL MAKE ALL THE DIFFERENCE WHEN ASSESSING POTENTIAL PARTNERS.

There is no shortage of options for products and services purporting to provide secure, reliable infrastructure capabilities. Picking the right partners depends on a myriad of considerations. The following three guidelines will make all the difference when assessing potential partners:

- **Select a proven partner**—Assess the level of experience and expertise demonstrated by your prospective vendors. Choose best-in-class capabilities for every strategic control point in your network. Don't settle.
- **Design for scalability and versatility**—An effective service provider infrastructure must deliver both sustained, reliable resource availability and data integrity across your network. To do that, your environment must be scalable and versatile.
- **Solve today's challenges with future-aware solutions**—Much is made of how 5G and other advanced technologies will impact mobile and fixed network operations, but new dynamics are already bearing down on your network. Find ways to apply next-generation thinking in conjunction with existing products and services to manage today's growing demands.

OUR SERVICE PROVIDER COMMITMENT

F5 has the expertise and experience to help you navigate the uncertainties and demands of your changing landscape. We are driven to provide industry-leading service provider solutions that help you address traffic management, network function virtualization, advanced mobile architectures, cable and fixed networks, and infrastructure security. Our proven ability to deliver high-performance enterprise IT capabilities informs the way in which we address every service provider-focused concern and requirement.

We're here to help you make the best infrastructure choices and to deploy the most cost-effective, secure, and robust solutions possible.

Learn about our 5G solutions at F5.com/serviceprovider.

US Headquarters: 401 Elliott Ave W, Seattle, WA 98119 | 888-882-4447 // Americas: info@f5.com // Asia-Pacific: apacinfo@f5.com // Europe/Middle East/Africa: emeainfo@f5.com // Japan: f5j-info@f5.com