vmware®

GET STARTED

The Modern Network: Bringing the Public Cloud Experience On-prem

Discover how a modern approach to networking, driven by service objectives and end-user application experience allows business to innovate faster and serve customers better.

Welcome

Companies are under pressure to bring products to market faster. Customer expectations, particularly of digital products and services, leave providers no option but to become more agile and better able to innovate at speed.

Nowhere is this more evident than in the response to the pandemic. In a market shaped by the COVID-19 outbreak, companies are under extreme pressure to assimilate new customer demands and bring new business models to market — all in record time.

To bring new products and services to market, businesses rely on a range of applications, some customer-facing, others that enable the development process. Modern applications are dynamic. They're distributed, and they're often born in the cloud. They are made up of dozens—even hundreds—of micro services.

Such applications can be spun up and scaled quickly to meet evolving user and market demands. To keep pace, infrastructure (computers, storage, network) needs to be software-defined and ephemeral.

Modern applications require a modern network—one that simplifies operations, reduces IT overhead and prioritizes needs—so that organizations can empower users with fast, reliable and secure application access wherever, whenever they do business and regardless of the underlying infrastructure or connectivity. But to realize these benefits, these applications must offer end users a seamless experience of the highest quality.

To make this happen businesses must first identify what an "excellent" user experience looks like. This understanding should then drive and shape what the network and supporting infrastructure looks like and how it is delivered. This is crucial, because only if it has been structured with the application-user experience as its starting point, can the network deliver the performance, availability, and security required from it.

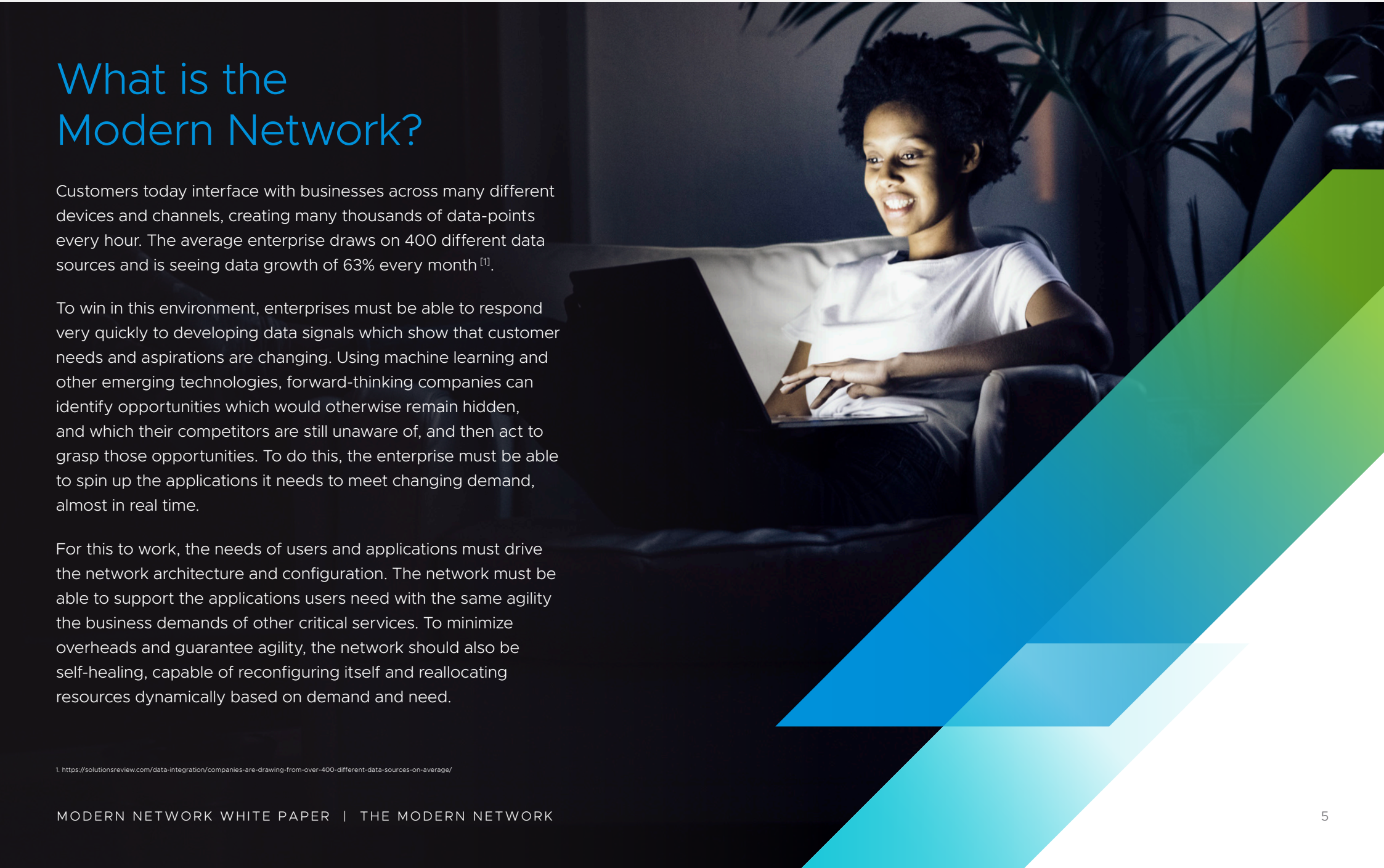
Fortunately, business infrastructure has evolved to meet this challenge. With the right technology, companies can be every bit as agile as the market demands. The key to success is to allow your business needs to drive which applications you build and run and then choose your network infrastructure accordingly. In the past, this dynamic approach wasn't possible, because IT infrastructure was too fixed and scaling it at short notice even using automation involved overheads which were too great.

With the evolution of multi-cloud virtualized networks, these limitations no longer apply. Using virtualized networks and a mixture of private and public cloud infrastructure, enterprises can spin up at short notice not just the apps they need to meet rapidly changing demand but also the network infrastructure required to run those apps.

In this white paper, we look at how this can be achieved and what businesses can do with this turbo-charged ability to innovate at scale and speed. We show how this new approach is relevant not just to the immediate needs of the accelerated post-pandemic market but also to long-term success in the future, hyper-connected environment.

Contents

What is the Modern Network?



Customers today interface with businesses across many different devices and channels, creating many thousands of data-points every hour. The average enterprise draws on 400 different data sources and is seeing data growth of 63% every month [1].

To win in this environment, enterprises must be able to respond very quickly to developing data signals which show that customer needs and aspirations are changing. Using machine learning and other emerging technologies, forward-thinking companies can identify opportunities which would otherwise remain hidden, and which their competitors are still unaware of, and then act to grasp those opportunities. To do this, the enterprise must be able to spin up the applications it needs to meet changing demand, almost in real time.

For this to work, the needs of users and applications must drive the network architecture and configuration. The network must be able to support the applications users need with the same agility the business demands of other critical services. To minimize overheads and guarantee agility, the network should also be self-healing, capable of reconfiguring itself and reallocating resources dynamically based on demand and need.

1. https://solutionsreview.com/data-integration/companies-are-drawing-from-over-400-different-data-sources-on-average/

How the Network Overcame its Physical Limitations

In the past, this process might have taken anything from weeks to months. Now, it can happen in days or even hours. This is possible, because of the changing relationship between line-of-business applications and the networks they run on.

If the DevOps team had to purchase and configure new hardware every time the line-of-business units needed to implement a new application — or install an existing one — then the kind of flexibility we've described would not be possible.

That it is possible, is thanks to the use of state-of-the-art virtualization and public-private cloud technologies. These form an intermediary layer between the physical network and the apps which run on it.

For example, if a new instance of an e-commerce application requires its own network segment, data servers and other infrastructure, the enterprise can create virtual instances of these in as little as just a few hours or even minutes. In this way, the capabilities of the modern network have overcome the physical limitations of the past.

The Physical Layer Still Matters

This does not mean that the physical devices no longer matter. Clearly, to function properly the network must still have reliable hardware with a robust physical architecture capable of running the required apps and the cloud platforms on which those apps run.

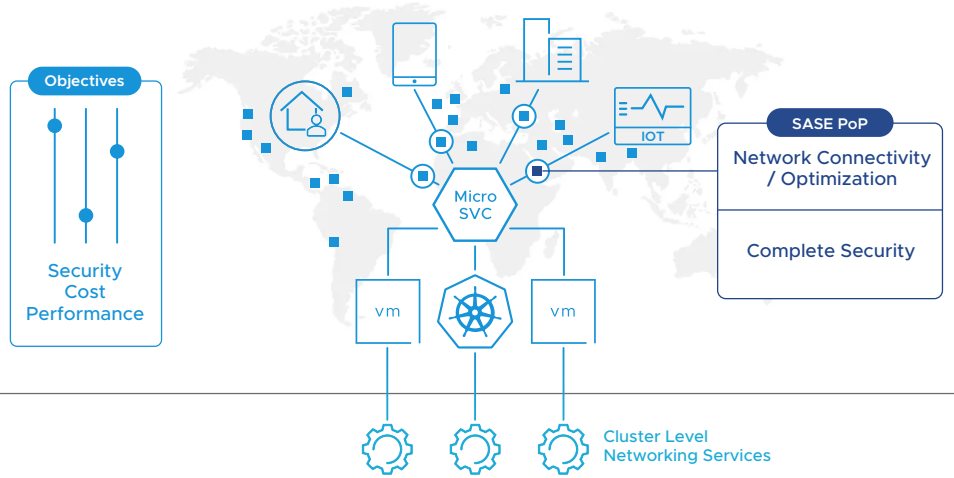
But because much of the network's intelligence resides in virtual devices which often exist on standard servers — much like the servers in a data center — the actual physical network can afford to be less sophisticated and may often be heterogenous, without this limiting the scope, scale or range of functions which the network can run.

The Modern Network

Networking As Code

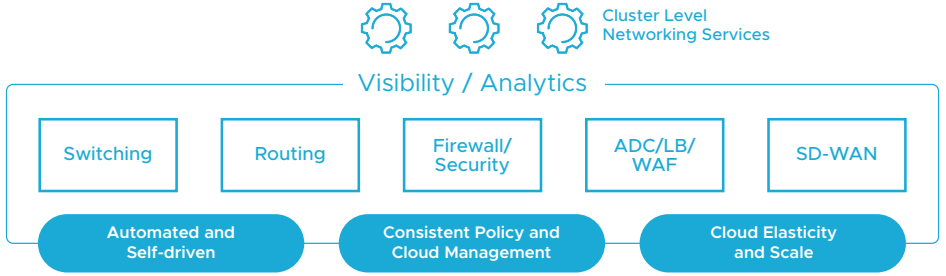
Modern App Connectivity Services

Use service objectives to deliver networking for modern app connectivity.



Multi-cloud Network Virtualization

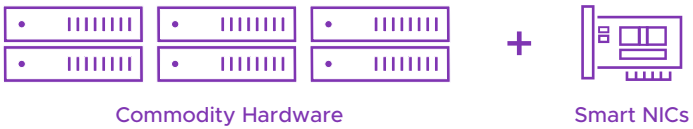
Get massive scale and agility with a self-healing network.



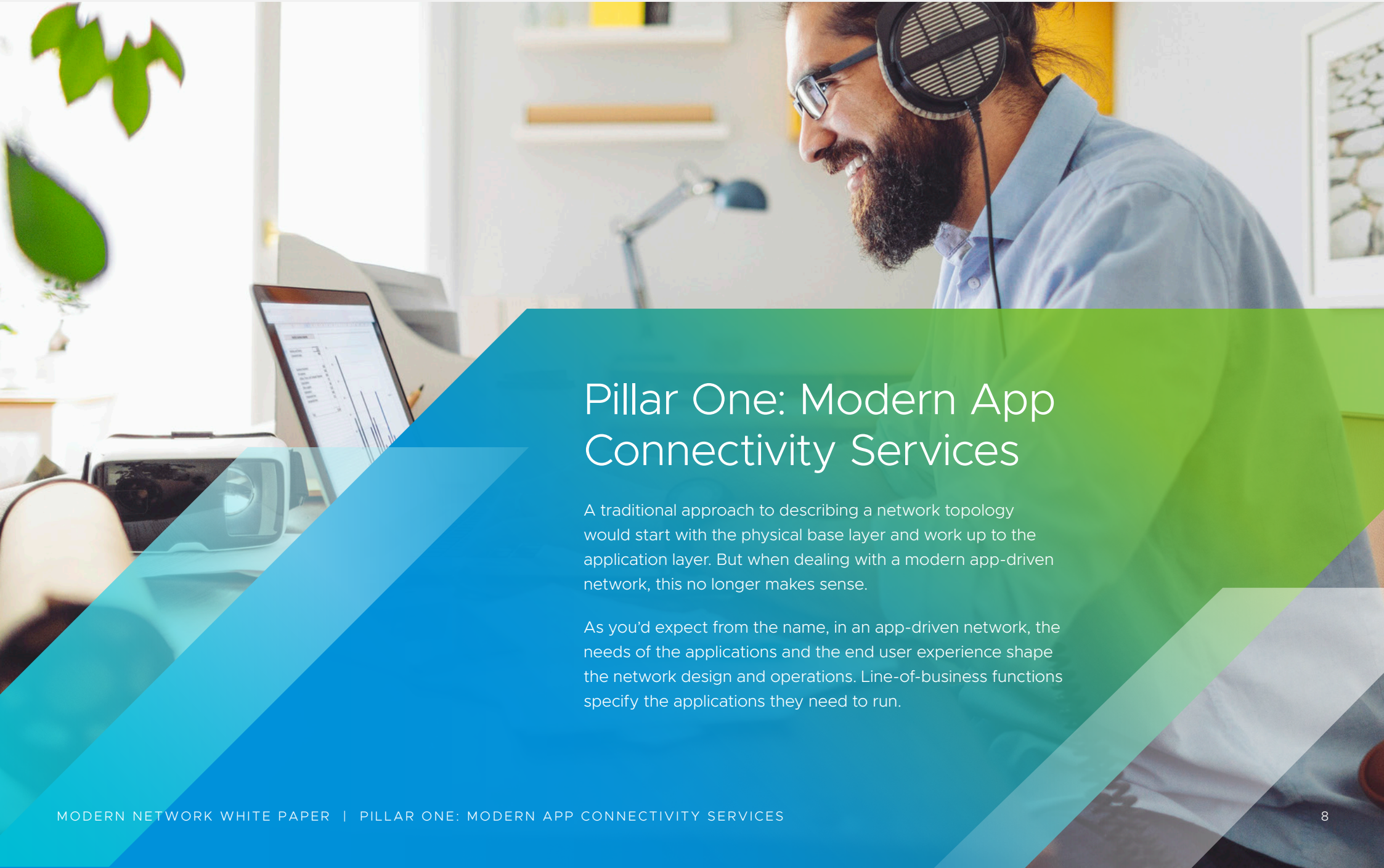
Moving Bits

Physical Network Infrastructure

Focus on app experience with fast, efficient hardware commodities.



End-to-end / Zero trust / Built-in



Pillar One: Modern App Connectivity Services

A traditional approach to describing a network topology would start with the physical base layer and work up to the application layer. But when dealing with a modern app-driven network, this no longer makes sense.

As you'd expect from the name, in an app-driven network, the needs of the applications and the end user experience shape the network design and operations. Line-of-business functions specify the applications they need to run.

There are two tennets which are the core of the modern app-drive network:

1. Deliver a superior user- or device-to-app experience using a automated, intelligent, self-healing network built on a common identity model and end-to-end trust.

2. Use service objectives for user experience, app availability, performance and security as a contract between users and the organization.

This could mean anything from quickly bringing extra e-commerce and payment services online to adding new data analytics and business-intelligence capabilities at short notice. To achieve tasks of this complexity at speed, the user-to-application experience must determine the structure and configuration of the network.

A network user, in this context, is any individual, application or process which draws on network resources and contributes towards the completion of the task at hand and to achieving the goals associated with that task. The job of the modern app-driven network is to deliver the resources required to make this happen.

Service Objectives are the Pressure which Drive Network Evolution

To meet this goal, line-of-business managers define service objectives — specified according to metrics such as latency, uptime and jitter, error rate and response time — that the network and the relevant applications must meet in order to deliver the required user-to-application experience.

Everything else — the structure of the network, the resources and platforms deployed — flows naturally from these service objectives, cascading down through the network from the topmost modern-application layer.

Thanks to the intelligence built into the virtualized-cloud layer that sits between the apps and the physical network infrastructure, the DevOps team is able to quickly and dynamically assign and scale the resources delivered to any application or suite of applications in order to meet the relevant service objectives.

Why is the Time Right for the Modern Network?

In May 2020, US consumers spent $83 billion on e-commerce sites — up 77% year-on-year [2]. Nor is this phenomenon confined to the US. A survey in April 2020 found that global e-commerce had grown by 209% compared to the same month in 2019 [3]. The volume of online payments has also rocked, with one major European payments provider reporting a 74% increase in transactions during lockdown [4].

And research by McKinsey indicates that 75% of people who used digital channels for the first time during lockdown will continue to use them once life returns to normal [5]. Turning to how companies operate internally, one recent report calculated that the COVID-19 pandemic had accelerated corporate digital transformation by as much as six years in global enterprises [6].

The pandemic did not create these trends from nothing. It accelerated what was already happening. But in doing so, it has created entirely new and challenging market conditions. These are marked by hyper-connectivity, as consumers engage with businesses across an unprecedented range of devices and channels.

This new market is also characterized by a disruption to existing brand loyalties, as first-time online shoppers find themselves trying new goods, services and online retailers for the first time. According to one recent survey, two-thirds of customers have tried a new product over lockdown [7].

To thrive in this new market, enterprises must be able to act quickly to forestall threats to their own customer relationships while taking advantage of switchers from other brands. This requires them to be able to adapt quickly, internally and externally. To do this successfully, their network and the applications which run on it must be more flexible, more scalable and more intelligent than ever before.

And that's exactly what the modern network delivers.

2. https://www.mediapost.com/publications/article/352576/adobe-data-shows-online-spending-in-may-exceeds-ho.html
3. https://wwd.com/business-news/business-features/study-reveals-global-e-commerce-retail-sales-are-up-in-april-1203633668
4. https://www.ey.com/en_gl/banking-capital-markets/how-covid-19-is-reshaping-retail-payments-in-europe
5. https://www.mckinsey.com/business-functions/mckinsey-digital/our-insights/the-covid-19-recovery-will-be-digital-a plan-for-the-first-90-days
6. https://www.itproportal.com/news/covid-is-speeding-up-digital-transformation-for-some-uk-firms
7. https://www.alixpartners.com/insights-impact/insights/covid-19-disrupts-brand-loyalties

Pillar Two: The Virtualized Multi-Cloud Network

The multi-cloud virtualized network is the next stage in the evolution of the network. In the last half decade, virtualized networking has become the norm in most enterprises.

Companies are no longer constrained by their physical network infrastructure. Rather than rely on physical devices such as switches, firewalls, DHCP servers and NAT servers, companies use virtual-network solutions — often running on standard data-center servers — to create software versions of these devices, as they need them.

This allows companies to be more flexible in responding to sudden fluctuations in demand or the need for new and innovative capabilities. At very short notice, the IT department can spin up pre-configured and provisioned devices and even whole network segments.

The two tennets which are the core of the virtualized multi-cloud network:

1. Enable network-on-demand for any app, anywhere, using a flexible, software-defined approach to networking in which all the various functions as well as physical and virtual devices work together to achieve the best experience for users.

2. Build self-healing network with cloud elasticity, at scale, by using auto-scaling technology which gives you the flexibility to grow and contract your infrastructure in line with demand, delivering the best possible user experience.

Because the devices are virtual, the company avoids prohibitive hardware costs. The ability to populate devices and network segments with pre-configured operational and security settings similarly saves time and effort while also reducing the scope for human error.

A recent study by analysts at Forrester found that an average enterprise can save up to $8,074,278 on capital expenditure over three years by switching to virtualized networking [8]. Over the same three years, that enterprise would also cut administrator costs by $1,283,724 and boost end-user productivity by up to $1,572,469.

In a fully virtualized network, computing power, storage and networking are all liberated from the limitations of physical hardware. This makes them available as flexible, scalable and configurable resources across the enterprise.

But there are some areas of operations which virtualization alone cannot reach. Many enterprises run their apps on a range of different cloud platforms, each running on different data centers. To simplify and streamline the management of these cloud platforms requires the federation of security policies across sites and cloud platforms.

8. https://www.velocloud.com/sd-wan-resources/white-papers/total-economic-impact-of-virtual-cloud-network

Multi-cloud: the missing piece of the puzzle

According to research by Gartner, 81% of enterprises now use multiple cloud providers: with each application running on the cloud platform that delivers the best balance of features, performance and security for its specific needs [9]. Thanks to virtualized networking, the enterprise can use resources from across its network to spin up and scale each cloud platform, as demand requires.

But to minimize administration overheads and ensure consistent security, the enterprise needs a way to manage all of these cloud platforms through a single dashboard. This is possible, using an advanced multi-cloud network and security solution.

Specifically designed to interface with a broad range of popular cloud platforms, a multi-cloud network and security solution allows IT departments to monitor, administer and update all their cloud platforms from a single dashboard. This includes applying privilege-based security settings — for instance, to determine which users and applications can access data — to all platforms, simultaneously through a single interface.

The most advanced multi-cloud management platforms also come with a high degree of automation built in. Technologists pre-program responses to common network events and failures. This significantly reduces the amount of time IT specialists spend troubleshooting both the underlying network and many issues related to the cloud platforms themselves.

One 2019 study found that on average, an enterprise which has a multi-cloud set-up takes just 29 minutes to resolve a platform outage and restore normal service [10]. For enterprises that don't use multi-cloud, that figure is 1,672 minutes.

9. https://www.gartner.com/smarterwithgartner/why-organizations-choose-a-multicloud-strategy
10. https://www.fintechnews.org/top-3-benefits-of-multi-cloud-strategy/

Pillar Three: The Physical Infrastructure

In a virtualized multi-cloud environment, the physical network continues to be important. But it is no longer the limiting factor it was in the past. Because most network devices can be licensed on demand and then be created as virtual instances, there is no longer the need to buy, configure and maintain the same install-base of physical appliances.

To enable the move to the virtualized cloud, the physical network can be simple — commodity hardware, without complex configuration options, are usually fine — but it must be robust and resilient. In a virtualized network, the physical infrastructure must provide speed, bandwidth, and reliability.

The physical and virtual network capabilities and policies must be aligned so that the network as a whole is able to cope not just with normal levels of traffic but also with unplanned peaks in demand. For instance, using a virtual multi-cloud network, enterprises can easily and quickly spin up cloud instances, network segments and apps in response to unexpected spikes in e-commerce demand.

In theory, this allows the enterprise to respond in an agile manner to rapidly developing business opportunity. But this can only happen if the underlying network has the bandwidth and low-latency required to deliver the extra bandwidth necessary, instantly, and to perform against the service objectives set by line-of-business managers.

Leveraging Heterogenous Infrastructure

Key to the successful configuration of your physical infrastructure is the tennet of leveraging the heterogenous infrastructure to provide the virtual network with a fast, simple and resilient physical underpinning.

Physical infrastructure in the modern network serves as a generic general-purpose platform that can be specialized on demand if necessary and then brought back into the general resource pool.

The modern network can be made up of a hyper-converged infrastructure spanning LTE, 5G, IoT and any service provider. It can be multi-vendor and enables connectivity across all heterogeneous infrastructure.

A Physical-network Checklist for Multi-cloud

Because it's much less reliant on the physical infrastructure, a virtualized network can tolerate a far more heterogenous device mix than a traditional network. However, there are still some health checks that enterprises should make to ensure that their physical and virtual infrastructures will work seamlessly together.

Here are three steps [11] to ensure the physical supports and enables the virtual in your network environment:

1. Ensure that the physical network offers the bandwidth necessary to scale traffic between all locations which will be part of your virtualized multi-cloud setup.

2. Use servers that meet the recommended requirements for running the hypervisor, virtualization software you'll use to virtualize network devices.

3. Hardware must meet specific requirements — for instance, support for large maximum transmission units (MTUs) — required by your virtualization platform.

As you can see, the requirements are minimal. Almost any enterprise will be able to begin the process of network virtualization, and the move to multi-cloud, with the physical infrastructure it has today. And in a very short time, it will see real and measurable benefits. In a recent study by Forrester, companies which made the move to a virtualized network cut the time spent configuring and troubleshooting by 95% [12].

11. https://www.linkedin.com/learning/cert-prep-VMware-certified-professional-6-network-virtualization-2v0-641/describe-physical-infrastructure-requirements-for-a-VMware-nsx-implementation
12. https://www.VMware.com/uk/solutions/virtual-cloud-network.html

NetOps and Security in the Modern Network

The move to virtualized multi-cloud networking makes the role and skills of the NetOps team more important than before.

Modern networks need to be able to deliver business-critical applications rapidly, securely and efficiently. The role of the NetOps team is to make this a reality. And the right multi-app implementation is the most efficient and cost-effective way to make that happen.

Security in the Modern Network

Built on a zero-trust foundation, multi-cloud, app-driven networks give the NetOps team a whole new security toolset. In a zero-trust environment, rather than allowing all traffic within the network perimeter to flow freely, which can create security problems, each application has its own “micro-perimeter”.

Because the applications within the perimeter only trust each other as required to fulfil their function, an attacker who compromises one application is not automatically able to access all the others at will. This zero-trust hardens the network against attack and makes mass breaches of customer or business records less easy for criminals to achieve.

Cloud platforms, and the applications which run on them, no longer run on bare metal but rather on the virtual layer that sits on top of the bare layer. With the right multi-cloud management tools, this virtualization layer comes with security and compliance built in.

Features that support enhanced network security include:

End-to-end encryption: ensure confidentiality and security across and between all cloud platforms and apps.

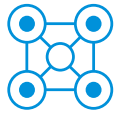
Streamline cloud monitoring: the multi-cloud platform uses cloud-native threat-feeds to monitor and detect threats across all cloud platforms simultaneously.

Total network visibility: see the state of your entire network, across sites and platforms, in one console.

Cut human error: with pre-populated templates for devices and network segments, the chance of security breaches through human error decreases.

At an application level, policies can be applied across the whole network, including different sites and different platforms, from a single console. This increases security within a single segment — for instance by securing traffic between different apps in the same data center — but also across the whole distributed network and the apps which run on it.

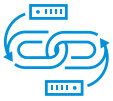
Features that support enhanced application security include:



Common identity model: apply a single identity model across all cloud platforms to deliver a seamless experience built on end-to-end trust.

Apply consistent policies across the cloud: use the multi-cloud management platform to set consistent privileges and security polices across all clouds.

Segment data intelligently: use the multi-cloud platform to set universal rules on which clouds, applications, network segments and users can access data.



Accelerate issue investigation: with alerts unified in one dashboard and monitoring available as part of one workstream, NetOps can track down problems faster.

Those networks which move to a virtualized, multi-cloud architecture that operates on a zero-trust model give their NetOps team the granularity and flexibility it needs to better manage and mitigate risk and to respond faster when something does happen. And the ability to apply policy-based security across all clouds simultaneously removes the problems, and security loopholes, that come with inconsistency and misconfiguration.

The NetOps Benefits of App Modernization

Using the right multi-cloud environment allows the seamless management of the entire network through a single interface. The NetOps team simply specifies the policies it wishes to roll out, and whether it wants those policies to apply globally or only in certain contexts. The intelligent cloud-management layer takes care of applying those policies across different sites and platforms.

NetOps benefits from working with multi-cloud platforms include:

Complete visibility: even operating across physical sites as well as across different cloud platforms, NetOps has total visibility of the whole network, all the time.

Advanced network features: with the right multi-cloud platform, sophisticated network features come built in, even if they're not native to the cloud platform.

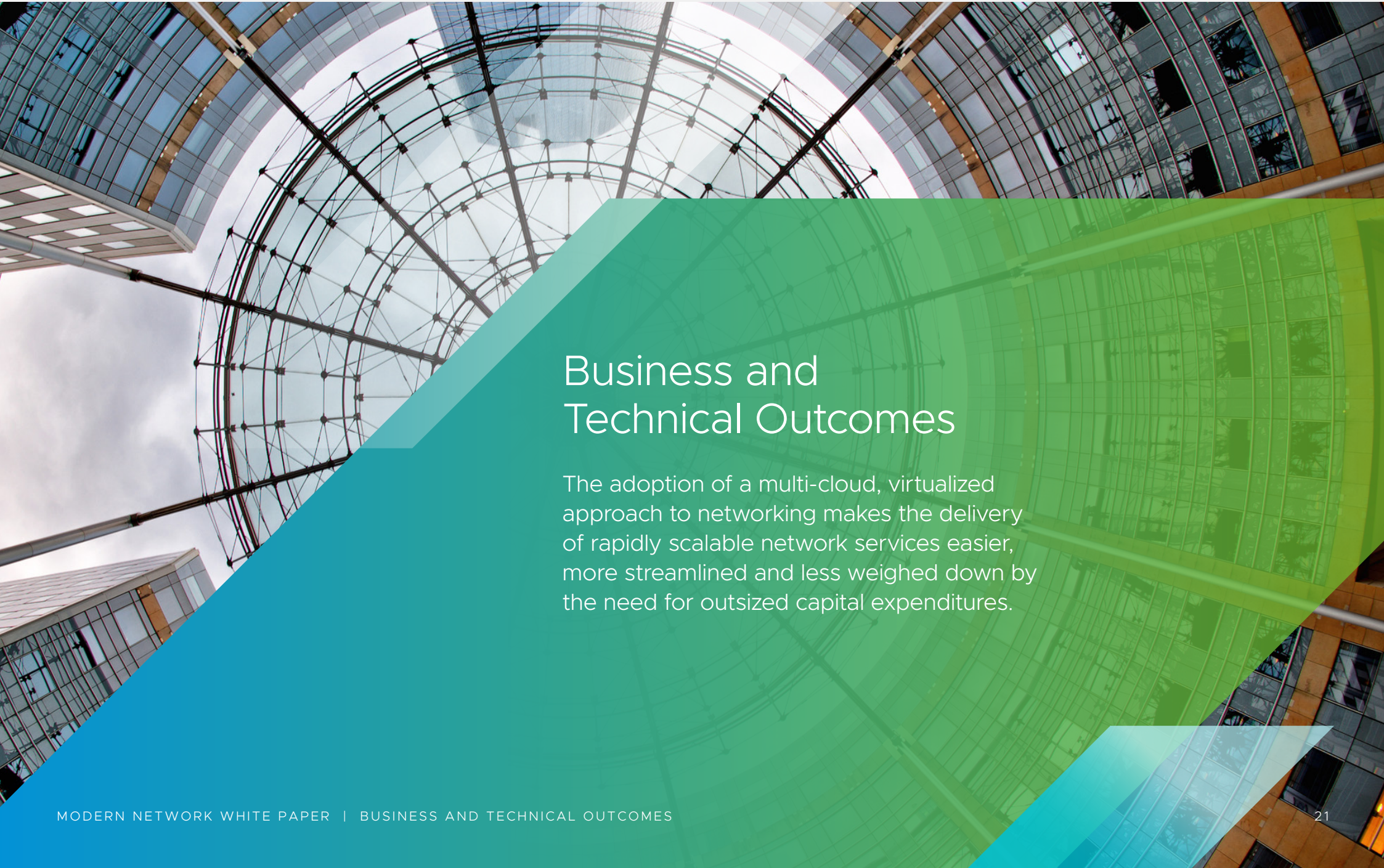
Compliance as standard: advanced data segmentation, policy-based auditing and sophisticated reporting make compliance simple across all cloud platforms.

Simplicity: because the multi-cloud platform provides high levels of control across all clouds, changing policies at any level is quick and simple.

Automation: thanks to built-in automation, the network can self-heal from many types of disruption and NetOps can spend more time on high-value-add work.

Resources allocation: allocate resources and provision new network segments and cloud instances in a fraction of the time it would take to do the same job manually.

The modern app-driven network, built on a virtualized and multi-cloud infrastructure, gives NetOps and other network and cloud specialists within the enterprise the tools they need to meet the demands of a rapidly accelerating marketplace.



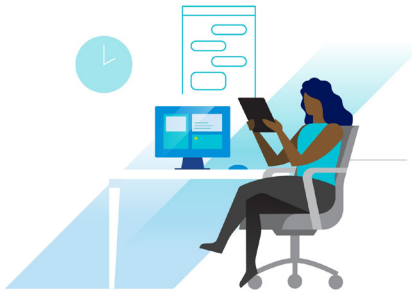
Business and Technical Outcomes

The adoption of a multi-cloud, virtualized approach to networking makes the delivery of rapidly scalable network services easier, more streamlined and less weighed down by the need for outsized capital expenditures.

The benefits and business outcomes an enterprise can expect from moving to an app-driven and multi-cloud model are as follows:

An Outcomes-driven Approach Drives Results

By adopting an approach drive by the needs of business-level applications and their users, expressed as service objectives, enterprises use business needs and metrics to shape their network. This outcomes-based approach fosters an efficient use of resources and the prioritization of business goals.



Improved User Experience

Because the user — and user-to-application — experience is built into the service objectives, it also informs the shape and functioning of the network. With a common identity model, users always have access to the data, services and applications they need, seamlessly. And if users require more computing resources, these can easily and quickly be made available.

Reduce Costs and Overheads

Advanced management, early warning of errors and self-healing are built into virtualized, app-driven networks. This cuts the cost, and time, involved in administering the network and environment. And because key network resources are virtualized, procuring and provisioning new services involves minimal capital outlay.

Be more Agile

When the enterprise needs new network resources or cloud instances, the IT function can deliver these in the shortest possible time. In most cases, no new hardware is required. The enterprise simply acquires the license for new virtual network devices and cloud instances, and then fires these up using existing servers. Thanks to the use of pre-configured templates, provisioning new network segments or services is quick and easy.

Scale Rapidly

Freed from the constraints of a physical network, the virtualized multi-cloud environment makes it possible to add new infrastructure and services rapidly. The enterprise can quickly scale its resources — for instance adding extra e-commerce and payments servers on the go — to meet sudden demand or seize new opportunities.

Embed Security in your Network

Multi-cloud and virtualized networking add a layer of intelligence between the apps you run and the hardware they run. This layer of intelligence allows you to specify how apps, users and services access data. It enables you to set privileges across all apps. And it lets you monitor security events across all cloud platforms and apps from single dashboard.

Measurable Benefits of the App-based Modern Network

Analysts from Forrester studied virtualized app-driven modern networks in 2019 [13]. Among other things, they found that enterprises which made the switch from a primarily physical to a virtual network infrastructure experienced the following benefits:

80% reduction in time spent on flow analysis.

75% reduction in time spent on securing the network.

95% reduction in time spent configuring and troubleshooting.

13. https://www.VMware.com/uk/solutions/virtual-cloud-network.html

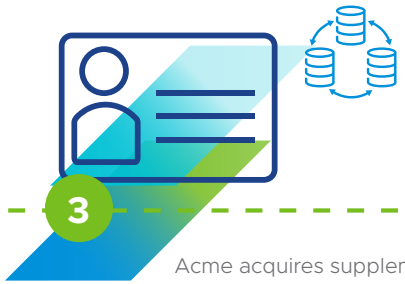
Use Case: Acme E-commerce

Acme E-commerce is a respected and successful online merchant selling a wide range of goods. Since lockdown, the company has experienced a surge in demand, often from entirely new demographics.

If it's going to keep these new customers once things return to normal, it needs to offer them an outstanding user experience. That means eliminating bottlenecks and sources of user frustration.

1. After analyzing cart abandonments and exits from its website, the company identifies the checkout and payment experience as one of the key bottlenecks preventing an optimum user experience. Check-out is too slow and unreliable.

2. The company determines that both the check-out server and the payments server are overloaded. To fix the problem, it needs to spin up new instances of both and then dynamically route traffic to them as required.



3. Acme acquires supplementary licenses for both the checkout- and the payment-server solutions it uses. It also licenses and spins up another instance of Azure and AWS, on which the checkout and payment servers respectively run.

4. Using VMware's Global Namespace function, you can define an application boundary and then connect the resources and workloads that make up the application into one virtual unit to provide consistent traffic routing, connectivity, resiliency, and security.

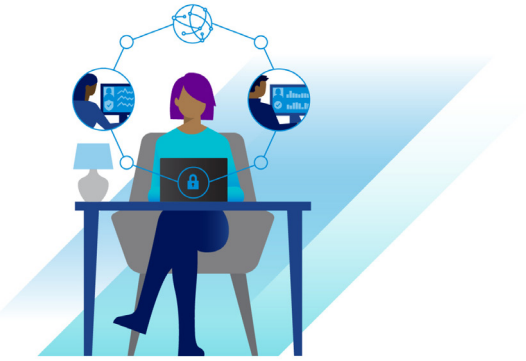
5. Using end-to-end encryption, the existing payment and checkout servers offload traffic onto the new instances of each application, as and when required. Once again, users experience the checkout as seamless, smooth and reliable.

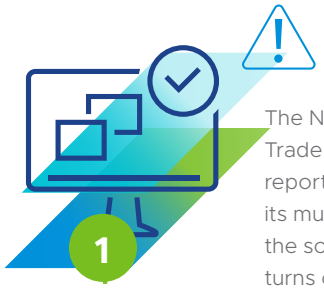
Because it could identify the problem and act quickly, Acme did not alienate its new or existing users. This allowed it to grow its market share by keeping both groups, building loyalty long past the period of lockdown.

Use Case: Trans-Pacific Trade

Trans-Pacific Trade is a world-leading trade finance and brokerage firm. It has offices in almost a hundred countries, from China, through the US and Latin America, to the Congo. To build trust and co-ordinate commodity deals, it makes extensive use of web conferencing.

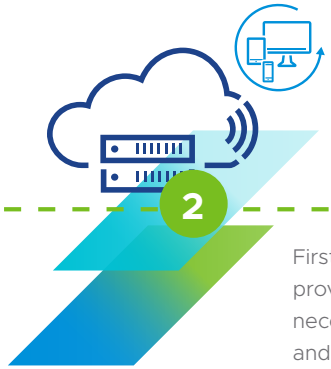
Recently, the quality of conferencing calls has been dropping. Latency, jitter and speed are no longer what they should be. This is impeding communications between colleagues and with customers. The company urgently needs to fix the problem.





1

The NetOps team in Trans-Pacific Trade uses the cross-platform reporting and diagnostic tools in its multi-cloud platform to identify the source of the problem. It turns out that users working from home are overloading the secure video-conferencing server and the available bandwidth.



2

First, the company leases extra bandwidth from its network providers. Using its cloud virtualization solution, it brings the necessary infrastructure online — switches, routers, firewalls and load-balancers — to make use of this bandwidth.

3

The company buys additional licenses for its secure video-conferencing solution and sets up more than one clone of its existing server. Because it works with commercially sensitive data, it uses its multi-cloud platform's end-to-end encryption to secure traffic between servers.

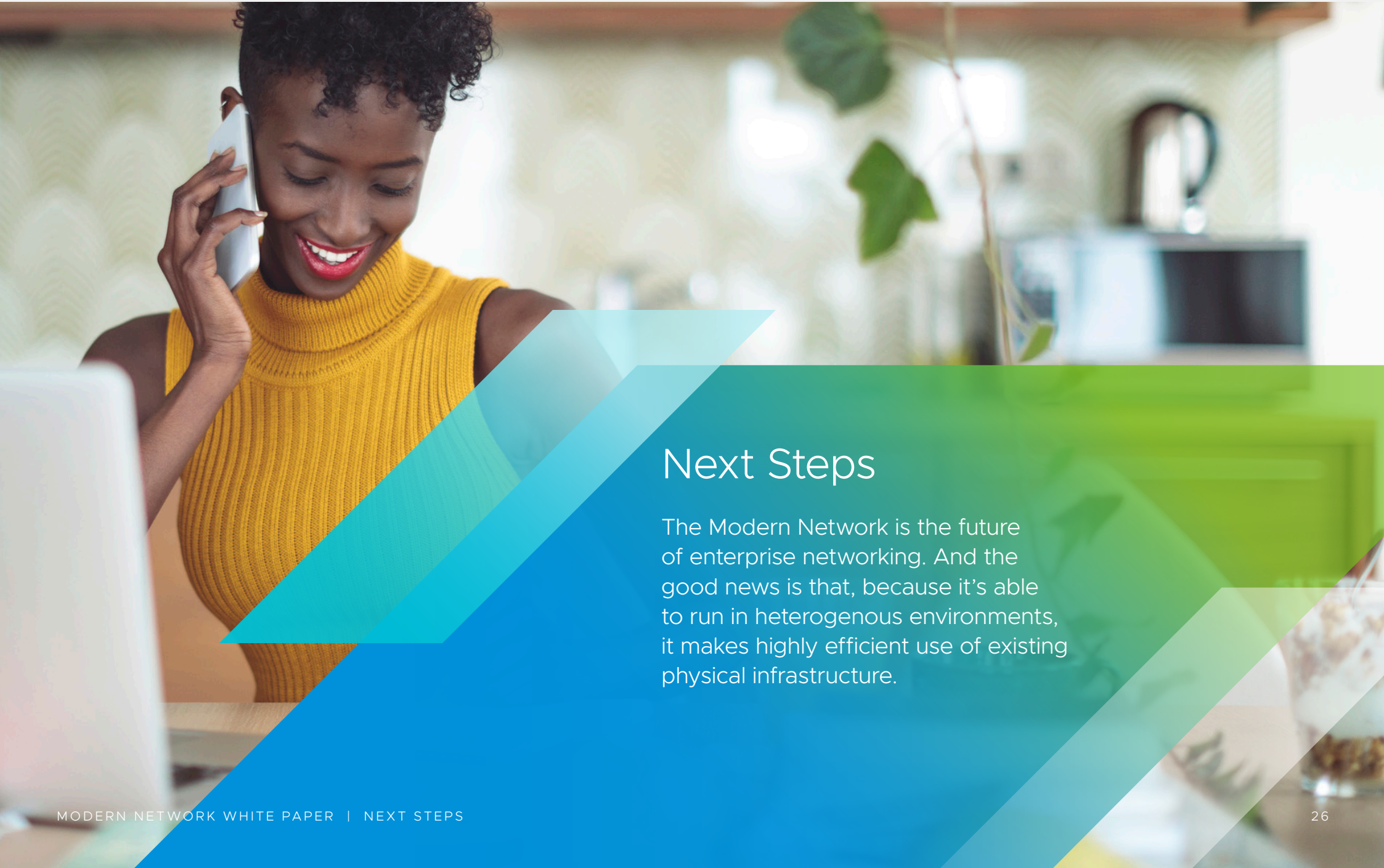
4

Thanks to the common user identity implemented through the multi-cloud platform, the new video conferencing servers are secure by design. And only those users authorized to use the system, and participate in calls, are able to log in.

Both customers and colleagues of Trans-Pacific Trade notice an instant improvement in call quality. This enables the company to continue its important work in brokering trade deals across continents, even as competitors struggle with IT issues and poor consumer experience.

5

Using the extra bandwidth and load-balancing between the video-conferencing servers, the IT team configures different teams within the business to interface with different servers, based on location, eliminating the overload.



Next Steps

The Modern Network is the future of enterprise networking. And the good news is that, because it's able to run in heterogenous environments, it makes highly efficient use of existing physical infrastructure.

Next Steps

That means that no matter what the state of your network is today, there's no reason you can't start your move to an app-driven, enabled future tomorrow. With the right technology, the right skills and the right strategic partnerships, nothing stands in your way.

VMware has over two decades' experience helping Enterprises realize increased business agility. VMware Virtual Cloud Network brings enterprise networking and security architecture into the digital age with solutions including VMware NSX, NSX ALB, VMware SD-WAN, and vRealize Network Insight.

VMware engineers and consultants can help you design the virtualized infrastructure that best meets your businesses needs and supports its ambitions. Working with our experts you can increase your operational efficiency, be more agile and still control and even reduce networking, virtualization and cloud costs.

Resources

Modern Network Website
www.vmware.com/go/modern-network.html

Virtual Cloud Network
https://www.vmware.com/solutions/virtual-cloud-network.html

Secure Access Service Edge – VMware SD-WAN by VeloCloud
https://www.velocloud.com/secure-access-service-edge

VMware Tanzu Service Mesh
https://www.vmware.com/products/tanzu-service-mesh.html

Zero Trust Security for the Digital Workspace
https://www.vmware.com/products/workspace-one/device-security.html

vRealize Network Insight
https://www.vmware.com/products/vrealize-network-insight.html

Contact us

To find out how VMware can help your business become more agile, get in touch today:

- 1-877-486-9273
- sales@vmware.com

www.vmware.com/go/modern-network.html