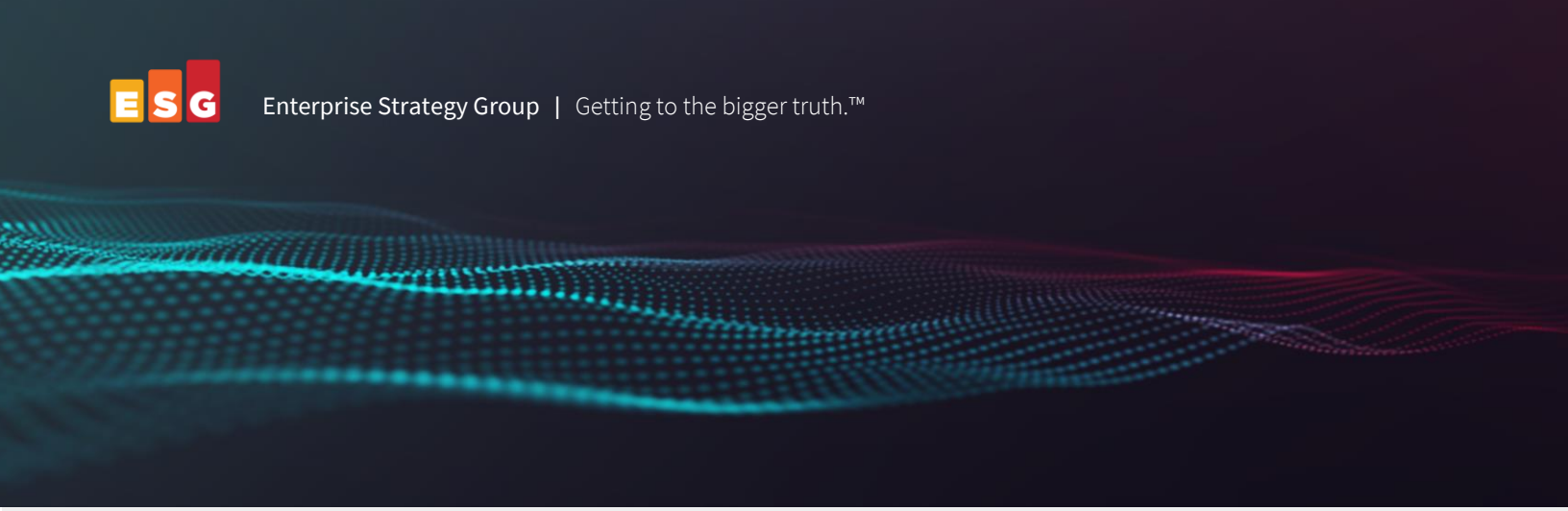


ESG WHITE PAPER

Key Attributes of Network Modernization

Modern Networks Better Position Businesses for Success

By Bob Laliberte, ESG Senior Analyst; and Leah Matuson, Research Analyst

November 2020

This ESG White Paper was commissioned by VMware and is distributed under license from ESG.

Contents

The Transformation to Modern Environments Is Underway

Digital transformation across industries is driving change, encompassing people, processes, and technology. According to ESG research, nearly one-fifth (19%) of organizations view themselves as mature in terms of digital transformation status, having implemented and optimized several digital transformation initiatives, while more than half (57%) are in the process or starting implementation—indicating a major shift toward embracing digital transformation. In addition, of all organizations undergoing digital transformation, 55% said that one of the most important objectives of digital transformation is to become more operationally efficient, while nearly half (49%) said delivering a better and more differentiated customer experience.[1]

One of the best ways to improve experiences is to rapidly iterate application features, functions, and even bug fixes. The transformation to modern application architectures enables organizations to do just that. In fact, modern application environments (often referred to as cloud-native) are core to enabling digital transformation.

The Evolution of Modern Applications

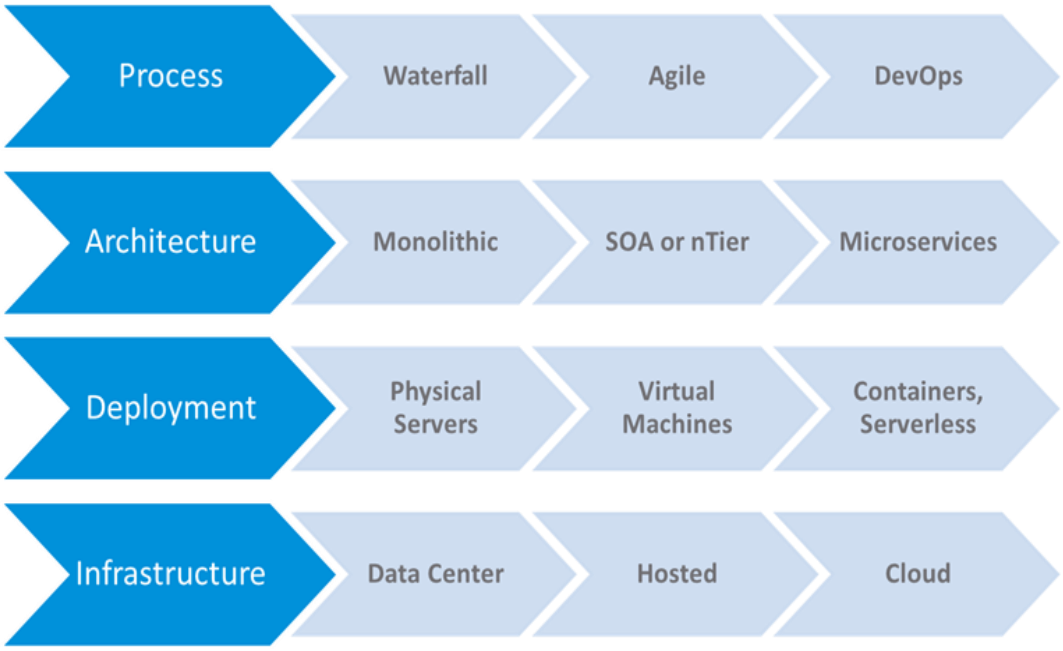
The evolution to modern applications has been marked by substantial development steps, which include new processes and technologies. Earlier stages were characterized by monolithic application architectures and time-consuming waterfall processes. In this stage, new applications usually took years to develop and were frequently situated on physical servers hosted in corporate data centers—and only updated with a single major release and one or two minor releases per year (see Figure 1).

As organizations grasped the necessity of streamlining application development, they began adopting additional agile processes and taking advantage of service-oriented architectures (SOAs) and virtual machines (VMs) to accelerate deployment and promote quicker, more frequent releases.

Today, applications are built on a microservices architecture, separating applications into many smaller pieces, and applications are hosted in cloud-based, container environments using DevOps methodologies. While microservices and containers enable development teams to iterate application updates and new functionality at a faster pace, DevOps practices ensure software developers and IT operations teams are tightly integrated to optimize application delivery in a production environment. With these modern technologies and processes, the business ultimately benefits by becoming more responsive to changing market conditions, with dramatically improved products.

[1] Source: ESG Research Report, *2020 Technology Spending Intentions Survey*, February 2020.

Figure 1. Evolution of Modern Applications



Source: Enterprise Strategy Group

Modernization Drives Significant Infrastructure Changes

As new processes have evolved (e.g., DevOps), so too have the roles of IT staff. Application developers and site reliability engineers (SREs) play significant roles in driving positive end-user experiences. Together, these new roles, architectures, and processes require the support of a far more agile and application-centric IT environment.

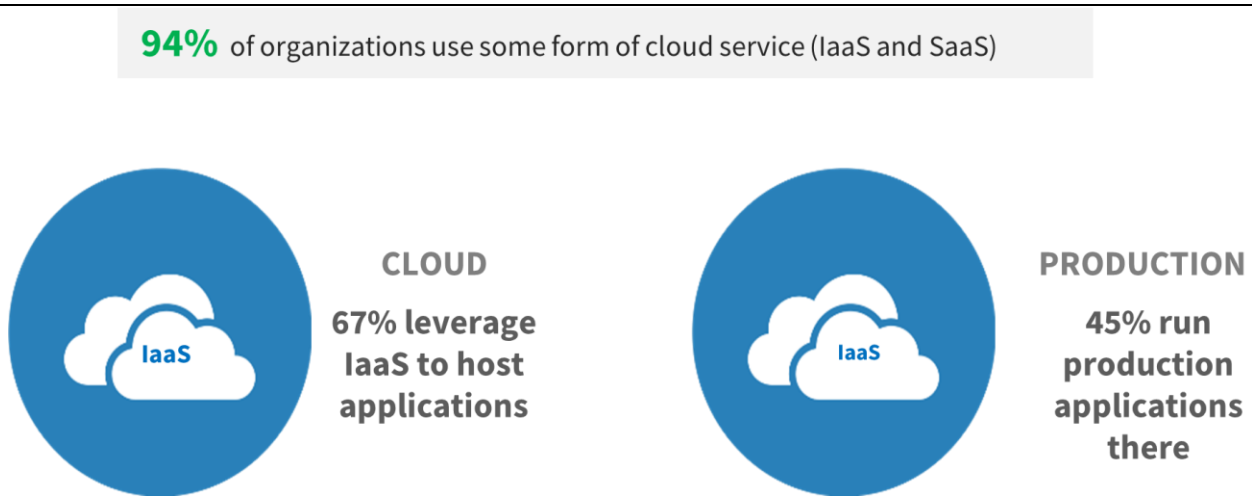
This is because organizations are under increasing pressure to quickly deliver modern applications and new services. ESG research reveals that of those organizations deploying modern applications, 86% report being under pressure to deliver new products and services faster[2] to their end-users to ensure a better, more consistent experience—resulting in increased user satisfaction.

To accomplish this goal, growing numbers of organizations are leveraging cloud environments. According to ESG research, cloud usage is virtually ubiquitous (see Figure 1), with 94% of organizations stating that they use a public cloud service (IaaS or SaaS) and with more than two-thirds (67%) leveraging IaaS public cloud services[3]—purpose-built to help accelerate modern applications. And many organizations will leverage multiple public cloud services.

To illustrate the growing importance of the cloud when running new applications, 45% of respondents report running production applications using public cloud infrastructure services (IaaS), and 38% report having a cloud-first policy for new applications. Another 53% consider both on-premises technology resources and public cloud services equally.[4] It is important to note, however, that cloud-native does not mean public cloud *only*. Based on ESG research, 70% of organizations have or will deploy their modern application environments in a combination of public cloud platforms and private data centers.

[2] Source: ESG Master Survey Results, *Trends in Modern Application Environments*, December 2019. All ESG research references and charts in this white paper have been taken from this master survey results set unless otherwise noted.
[3] Source: ESG Research Report, *2020 Technology Spending Intentions Survey*, February 2020.
[4] Ibid.

Figure 2. Modern Cloud Use



Source: Enterprise Strategy Group

The Role of the Network

Since organizations must contend with highly distributed environments (deploying both on-premises and public cloud-based applications), an efficient application-centric modern network is more important than ever to the business, the end-user, and the bottom line. Consequently, it is critical that organizations create a highly virtualized and software-defined network (SDN) environment that ensures application developers and SREs can rapidly spin up services when and where they are needed, helping to accelerate all phases of an application lifecycle.

Although compute and storage have advanced to support these dynamic application environments, it is essential for organizations to modernize the network—especially given the fact that these applications are deployed in highly distributed, hybrid, and multi-cloud environments. That said, this scenario is not without challenges.

Challenges in Modernizing the Network

Given the transformation associated with modernizing an organization's environment, it should come as no surprise that there are a multitude of challenges in modernizing the network. These challenges span people, processes, and technology—from security, through scale, to performance—including:

General IT complexity. Highly distributed IT environments create more complexity. According to ESG research, 64% of organizations say IT is more complex compared with two years ago. Those organizations with mature digital transformation efforts are 3x more likely to report IT is significantly more complex (29% versus 9%) than those with no digital transformation initiatives.[5]

The question remains: How can organizations keep pace with increased IT complexity using only existing (think flat) staff?

Existing (i.e., legacy and status quo) culture impeding progress. The new paradigm for developing modern applications requires tight alignment and collaboration between application developers, SREs, and operations (DevOps) teams—as well as coordination with adjacent functions including line-of-business (BizDevOps) or security teams (DevSecOps). Organizations that remain highly siloed and isolated will struggle to create modern network environments.

[5] Source: ESG Research Report, *2020 Technology Spending Intentions Survey*, February 2020.

Lack of training and skills development. Many organizations employ staff who may have years of general training in the current tasks they are performing—but architecting a modern application-centric network requires specific skills and specialized knowledge. Without additional skills development, it will be difficult for the network team to transform the network to support modern application environments.

Further, the organization must be willing to invest in the appropriate certifications and training so that all relevant staff possess a common foundation for working in an application-centric network. Based on ESG research, more than one-quarter (27%) of organizations were challenged with setting up and configuring network services for modern application environments.

Highly distributed environments creating performance and end-user experience obstacles. Modern applications span on-premises and cloud environments, which means organizations can't rely on legacy network architectures (i.e., hub and spoke) to ensure adequate performance or prioritize applications based on their criticality to the business and end-users.

Siloed, legacy network architectures create latency issues for end-users when accessing applications (i.e., any distance between the user and the application generates latency, degrading the user experience). In fact, ESG research shows that more than one-third (36%) of organizations cited an inability to meet performance requirements as a top networking challenge in modern application environments.

The ephemeral nature of container environment placing more pressure on the network. Modern application environments require network connections and services to be spun up—and down—in just a few seconds. Legacy networks have limited visibility into applications, and even simple changes can take weeks. ESG research shows that nearly one-third of organizations (32%) indicate that keeping up with the dynamic environment was a top network challenge.

Ability to scale the environment. A significant part of delivering services in the modern economy is the ability to quickly scale services. This was evidenced in the recent surge to enable employees to work from home that required networks to rapidly scale to accommodate a dramatic increase in network traffic to data centers, clouds, and collaboration applications. Yet, ESG research illustrates that 38% of organizations are concerned about their ability to properly scale the network and network services to meet demand.

Security and the visibility gap. For organizations transforming their IT environments, security is a top concern—and for those deploying modern applications, more than half of organizations surveyed (52%) cited network security as a top challenge.

Essentially, organizations will struggle to provide users with a positive experience using modern applications and highly distributed IT environments without deploying a modern network environment.

The Key Characteristics of a Modern Network Environment

As a result of the efforts to modernize the IT environment (and the challenges it has created), organizations must acknowledge the fact that the network environment must transform. With this transformation, there also needs to be a tight alignment between application developers and site reliability engineers (SREs). Additionally, organizations must provide network, security, and virtualization administrators (VIs) with the proper tools that allow them to deliver expected levels of performance to end-users.

With a number of personas working in modern network environments (think application developers, SREs, network security professionals, VIs, and end-users), each role has a number of distinct requirements to effectively perform their functions.

Supply the Proper Network Environment for Application Developers and SREs

- Abstract the infrastructure. It is imperative that a modern network environment abstracts the underlying infrastructure for application developers and SREs. Network teams must enable application developers and SREs to quickly and easily make changes with full confidence that the network will quickly align to the new demands of the application environment. This requires the network team to put in place the appropriate guard rails (policies) to ensure any changes will not impact availability, security, or customer experience (performance). In addition, the abstraction should cover on-premises and any public cloud network—as well as the connectivity between on-premises and any public cloud network—regardless of the type of network used (e.g., public leased line, broadband, MPLS, or cellular).

- Employ extensive automation. Subsequently, the modern network environment must be highly automated. Organizations require sophisticated solutions to overcome highly distributed and complex environments. Given the nature of modern applications and the associated network complexity, it is vital to automate as much of the environment as possible. This automation is not just for the benefit of network teams, but also enables application developers and SREs to more easily implement changes in a timely manner. Essentially, this automation should help to abstract the network, but ensure all relevant policies are followed.

- Support container environments. For the network to enable modern application environments—and ensure a positive user experience—organizations must support and have visibility into container service mesh environments. This should include the ability to integrate with continuous integration/continuous delivery (CI/CD) solutions that accelerate application development and deployment, enabling the infrastructure to continuously deliver better software to production.

Ensure an Enhanced Experience for End-users

It is critical for organizations to provide end-users with a seamless, enhanced experience; thus, organizations must take the necessary steps to ensure this occurs by providing staff with the following:

- Application-centric network environment. In a highly distributed environment, modern networks must ensure all users can seamlessly gain access to any approved applications, regardless of where the applications are located (on-premises data center, edge location, or the cloud) or where the users are located (the office, home, or the road), at any time, and still have a positive experience each time they connect.

- Unified policy and visibility from data center through edge to home. The "new normal" dictates that organizations must support employees regardless of their location. Creating a modern network means more than ensuring data centers and edge locations can connect to one another and public cloud services. A modern network must extend the same corporate network and secure access policies to those working from home or remote locations.

- Highly available network. IT must not only bring up new applications faster but keep them up as well. While rapidly bringing up new applications and services is useful, keeping them up is even more important. Consequently, modern networks should possess:

    - *Self-healing capabilities*, including closed-loop systems that can instantly recognize a potential network issue and self-correct to ensure continued availability. Organizations may want to get comfortable with this technology in a semi-automatic mode before opting for a fully automatic state.

- *Ability to automatically perform patch management without any downtime*. This is important to ensure a secure environment and that the team has the ability to take advantage of the most advanced capabilities.
- *Sufficient capacity to meet network demand within approved guardrails (policies)*. The ability to self-scale should take into account seasonal spikes.

Give Network, Security, and Virtual Infrastructure Administrators Better Management Capabilities

Modern networks will play an increasingly important role in highly distributed IT environments. As a result, the substantial value in the network data and insights gained from the network need to be accessible by other teams. In addition to the network teams, security and virtual infrastructure operations teams will require visibility. To help these groups, a modern network should provide:

- Unified network management for both modern and legacy application environments. For most organizations, there will be a mix of legacy and cloud-native modern applications for some time to come. Therefore, to ensure operational efficiencies, it is vital that organizations have consistent network management for physical, virtual, and container environments. This unified view will aid all operations teams (development, security, networking, and virtual) in troubleshooting, capacity planning, and lifecycle management. Additionally, central management will be required to enforce consistent policies across all these environments.
- Deep visibility and understanding of the overlay/underlay network environment. The introduction of overlay networks has greatly accelerated development cycles and workflows. However, to properly manage these environments and ensure a right-sized physical underlay, network teams must have comprehensive visibility into the environment (both physical and virtual).
- Consumption-based models where they make sense. Cloud services and applications are influencing how IT services are consumed. As organizations build out private clouds that leverage modern network environments, they will expect to have the option of purchasing solutions via traditional CapEx models as well as modern pay-as-you-go subscription or consumption-based models.
- Better application level security. For security purposes, organizations must be able to segment application traffic on the network to eliminate bad actors from accessing restricted, business-critical, or personally identifiable information (PII) data. Employing segmentation (and micro-segmentation) is a significant step to protect application traffic from the outside world. Note that this capability should extend to east-west traffic and not just north-south. For greater defense, zero-trust models should also be employed to only allow authorized users access to the network.

  Given the complexity and ever-changing nature of security attacks, organizations need to take advantage of AI/ML solutions to detect anomalous activity, automatically quarantine traffic, and notify all relevant parties when abnormal activity is detected. This process would typically involve understanding and benchmarking application traffic flows, including east-west traffic between virtual machines located within a physical server and, potentially, containers, to provide organizations with a complete and granular level of visibility and protection. A modern network environment with centralized management and AI/ML capabilities will also enable organizations to ensure compliance can be met, with audits conducted in a timely fashion.

The Value of Implementing Modern Networks

Organizations should not be deploying a modern network because it's the latest marketing phenomenon, or the technology of the month. Instead, deploying a modern network should be the thoughtful evolution of an organization's

network environment, implemented to support highly dynamic (ephemeral) and distributed modern application environments and remote users. Organizations that invest in a modern network will gain a variety of benefits:

Faster time to market. With a modern network, application developers and SREs will no longer have to wait on network teams to manually provision physical network connectivity, thereby enabling higher levels of developer productivity as well as increased employee satisfaction. Implementing a modern network allows organizations to significantly enhance agility, in turn accelerating revenue, and providing competitive differentiation as applications and services achieve faster time to market.

ESG research indicates that 37% of organizations with modern application environments in production report being ahead or significantly ahead of application deployments compared with those organizations using containers in test and development only (13%).

37%

Of organizations with modern application environments in production report being ahead or significantly ahead of application deployments compared with those organizations using containers in test and development only (13%)

Greater operational efficiency—through simplification. Modern networks will enable organizations to effectively manage highly distributed application and user environments. These complex network environments therefore must have easy-to-use management interfaces and be able to simplify complex tasks. This would include the ability to centrally provision policies and ensure distributed enforcement of them will enhance both security and productivity, while empowering DevOps and SRE teams to operate with greater autonomy. According to ESG research, 44% of organizations using containers report the environment has enabled DevOps methodologies in their company helping to drive operational efficiency. On the remote worker side, the use of automation to simplify the network (e.g., zero touch provisioning) will empower organizations to rapidly turn up and support thousands of remote worker environments in a short amount of time, while enabling staff to eliminate repetitive, manual processes, affording them more time to focus on value-added or strategic projects.

Better end-user experiences. Ultimately, modern networks enable end-users to gain a reliable, seamless application experience. As stated earlier, nearly half (49%) of IT professionals said delivering a differentiated user experience was one of the top goals of digital transformation initiatives. In a digital economy, ensuring consistent positive experiences will be a critical factor to determining success or failure. It is important to note that the enhanced user experience is required for virtually every application, regardless of the location of user or application.

Higher levels of availability. Modern networks that take advantage of self-healing and self-scaling technologies will deliver higher levels of application availability. While the impact of downtime will vary by application, one of the primary goals should be to ensure zero downtime. This a lofty goal in an IT culture that always casts blame on the network first. Automated lifecycle management allows patches and upgrades to be completed automatically without rebooting systems (i.e., without taking them offline), further contributing to higher levels of availability and increased security.

Seamless connectivity. Organizations must ensure connectivity beyond corporate locations, such as data center, campus, and edge locations, to any public cloud service (IaaS and SaaS). In addition, given the "new normal" requirement to enable employees to work remotely, seamless, secure, and optimized connectivity for employees working from home or the road is mandatory. This essentially creates a network to support a true hybrid, multi-cloud environment.

In fact, ESG research shows that the top reasons organizations must deploy modern applications in hybrid cloud environments include increased performance (51%), improved security (48%), and reduced IT infrastructure costs (45%) (see Figure 3).

Figure 3. Top Five Reasons It's Important to Run Applications in a Hybrid Cloud Environment

Source: Enterprise Strategy Group

Greater job satisfaction across the organization. With a modern network environment, application developers and SREs are no longer restricted by infrastructure (i.e., network) and can be more productive; it also means applications will come to market faster without any frustrating delays waiting for infrastructure to be provisioned. Network teams will get the opportunity to learn new skills and transform the network by working with new technologies and having more time to focus on strategic initiatives and not repetitive manual tasks, thus increasing their value to the company. Remote workers are included as part of the modern network architecture and can be more productive, enjoy better user experiences when working remotely, and benefit from a more secure remote environment.

More secure environment. A modern environment allows the network team to easily enforce governance and compliance using centralized policies. This allows organizations to better protect users, the applications they access, and the data traversing the network. Taking advantage of solutions that offer segmentation and micro-segmentation capabilities mitigates the threat of a network breach that can access sensitive or personally identifiable information (e.g., a single data breach could result in millions of dollars lost to notifications, monitoring, and brand impact). In addition, automated patching and updates remove potential risk due to human error—helping to eliminate downtime, improve agility, and enhance productivity. Essentially, security must be an integral part of highly distributed modern networks to deliver a true digital experience.

The Bigger Truth

To maintain a competitive edge, organizations must deliver modern applications and services more efficiently. But this isn't quite so simple due to underlying IT environments becoming far more complex, which is especially true for the network.

Modern network environments must be highly virtualized and software-defined to become tightly integrated to development processes, understanding and anticipating the requirements of application developers and SREs to enable them to automatically deliver the requisite network services—regardless of application location—on-premises, in the cloud, or at the edge. Network administrators must be focused on driving innovative new services—not performing repetitive manual tasks.

As digital transformation initiatives continue to mature, organizations will need to ensure their networks can keep pace. To enjoy continued business success, while delivering differentiated user experiences, organizations require a truly modern network environment—one that can match the end-user journey and provide the appropriate capabilities.

VMware has established an architectural framework to enable organizations to evolve to a modern network. VMware understands that a modern network must deliver a seamless user experience regardless of where the applications or users are located. To accomplish this, the network environment has to be software-defined and simple to operate and must deliver the requisite flexibility, performance, and scale that align with both technical objectives and business outcomes.

To better understand VMware's vision for a modern network solution and how it can enhance your existing IT environment, visit the VMware website.

Enterprise Strategy Group is an IT analyst, research, validation, and strategy firm that provides market intelligence and actionable insight to the global IT community.

www.esg-global.com contact@esg-global.com 508.482.0188