CompuCom

Technology Solutions for the Digital Workplace

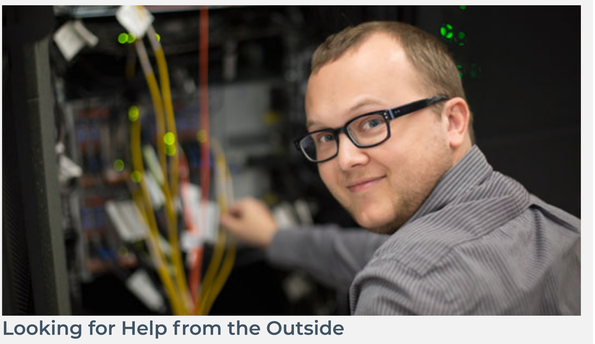
NETWORK SOLUTIONS

Stopping the Vendor Blame Game

When problems pop up on your network, answers can be hard to come by. The circuit provider blames the router manufacturer. The router manufacturer points the finger back at the circuit provider. Meanwhile, your business sits at a standstill with a downed network.

CompuCom® Network Solutions end the blame game. We proactively monitor your entire network and respond to alerts in real time — identifying the source of the problem, and then rapidly resolving it. Our only priority is making sure your business is fully functional as quickly as possible.

Contact us to learn more about CompuCom Network Solutions.



Looking for Help from the Outside

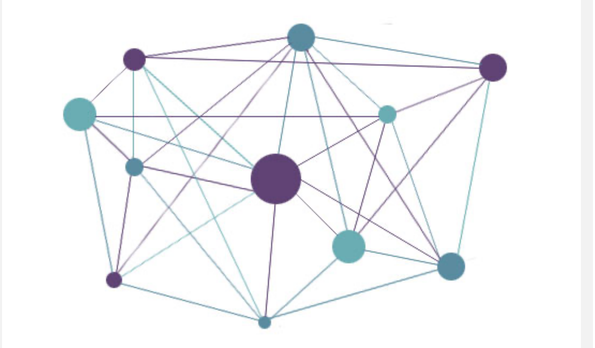
Addressing network problems isn't easy; it takes a deep and thorough understanding of complex systems. Equally challenging, network outages don't always happen between 9 and 5, so having round-the-clock coverage to quickly address issues as they arise is critical.

Telecommunications companies can offer some assistance, but they can't handle your entire network. Managed service providers? While they can help determine where issues lie, they lack the field staff and expertise to repair or replace hardware if needed.

Ready to Respond, 24/7

The CompuCom Managed Network Services team includes network professionals with all the necessary skills to address your network's problems. When your network has an issue, we'll give you immediate attention and coordinate all the specialists required to resolve it successfully.

View More



How Our Network Operations Centers Benefit You

When you hand off your network management to CompuCom, you can count on:

- Improved network utilization and capacity to avoid network congestion
- Increased end-user productivity with a consistent service experience
- Rapid response to network issues, regardless of the problem source
- Transport bandwidth from leading carriers
- A service package that fits your budget and service-level needs

CompuCom®

Technology Solutions for the Digital Workplace

CLOUD, ON PREMISES OR HYBRID: WHAT'S BEST FOR YOUR WORKLOADS?

Since the dawn of cloud computing, companies have had to determine which workloads to put in the cloud and which to keep on premises. In the excitement of the early days, it seemed that everything should be in the cloud. These days, IT teams are taking a more strategic approach.

Choosing the optimal place for your applications takes time and careful thought. Different configurations work for different needs. Here are four key issues to consider.

1. Compliance

Compliance is a big driver for many businesses, especially in highly regulated industries such as healthcare and financial services. It's also critical for companies with global operations, which must deal with data sovereignty issues. For example, privacy laws in the European Union differ from those in the United States. If you're storing information from your French division on U.S. servers, are you complying with the appropriate laws?

When compliance needs are complex or a cloud solution won't stand up to an audit, look to storing that data on premises.

2. Security

It's important to understand how the cloud solution fits with your security guidelines. What's the provider's security policy? How is it split among involved stakeholders — data center owner, provider and your own enterprise?

If you can't figure out who is responsible for each element of security, or the security level doesn't meet your requirements, you need to keep that data or application on premises.

3. Performance

When using shared infrastructure, you don't have any way of knowing what other applications are on the network or how their performance requirements impact service. What kind of performance do your applications and data require? Consider that the biggest technology companies around (like Google) don't use the public cloud because it would degrade performance for their critical applications.

For applications that need optimized or real-time performance, the best option is an on-premises solution. Public-facing applications (like portals or e-commerce sites) are well-suited to the cloud because traffic is dynamic and the cloud enables infinite scaling and easy access.

4. Costs

The cloud can be cost-effective for storing some kinds of data or for applications that don't need much processing power. However, cloud prices are dynamic — based on the storage and processing you need — so be sure to consider your usage patterns.

For applications that require a lot of processing power, on the other hand, it may be cheaper to invest in an on-premises solution.

Hybrid Solutions

Keep in mind, though, that the choice for workload placement isn't simply between cloud and on premises. The third option is a hybrid solution — one that uses the best both have to offer.

When trying to decide, ask yourself questions like these:

- What does the application do?
- What dependencies does it have — e.g. are there other data or applications it links to?
- How will this workload perform best and minimize latency with the applications it uses most?

Where to put workloads isn't a one-time decision. To keep your entire network running optimally, you have to revisit the mix on a regular basis — prices, storage options and performance change all the time. Factoring all this in requires time, effort and continual analysis.

Tackling this challenge isn't always a smart use of your resources. As you think about the best distribution for your workloads, consider working with a third-party IT services provider to help make the decisions. The right vendor can scan critical workloads and ensure optimal placement for your applications. That way, you can focus on strategy and optimizing your company's value proposition.

If you would like to learn more, about the challenges that are top-of-mind for IT leaders in the cloud era, watch our Hybrid Cloud Exploration Webinar series with Frost & Sullivan.

5 CHALLENGES IN MANAGING A HYBRID OR MULTI-CLOUD ENVIRONMENT

If you think managing a hybrid or multi-cloud environment will be easy, you may be in for an unpleasant surprise.

Given the significant shortage of knowledgeable cloud workers out there, many businesses are lacking in-house cloud expertise. As a result, deploying a successful cloud strategy is often a complex undertaking.

Here's a look at five of the most common challenges businesses face in managing a hybrid or multi-cloud environment.

1. Unauthorized Access to Data Applications

Security is always a top concern for IT organizations, and the issue is magnified when deploying a hybrid or multi-cloud environment. Why? Because security is so often tied to the infrastructure, and you can't always be certain that you have consistent levels of security across your various deployment options.

Furthermore, you can't just "set it and forget it" in these cases. You need to figure out how each deployment element works, what the parameters are, what you need to pay extra for, what you have to overlay, what's baked in, etc. Plus, you can't always tell whether things will stay the way you want them to when splitting a workload or migrating to a new environment.

2. Poor or Inconsistent Application Performance

When assessing a hybrid or multi-cloud environment, many businesses neglect to consider application performance. But that should be a huge consideration, especially with sensitive workloads.

There are many reasons why businesses put applications in the cloud. The top reason businesses pull them back? Latency. Applications need to run fast. When you put something in the cloud, however, it adds latency because data has to travel over a network to get wherever it's going.

And if the public cloud is part of the equation, other companies will be on the same machine as you. So your application's performance could be affected based on what's going on with their workload at a particular moment (e.g. if their traffic spikes, you're going to feel it). For performance-sensitive applications — and what applications aren't these days? — the inconsistency is a big issue.

3. Inability to Meet Compliance Requirements

Businesses have a distinct lack of confidence about controlling compliance assurance in a cloud or multi-cloud environment.

In a public cloud environment, for instance, you may not know where your data is or where your applications are. You also may not be able to confirm whether the hardware and data centers are compliant or if you have the right tools in place to support PCI. Issues like these make it difficult to meet reporting requirements (i.e. not only ensuring compliance, but also being able to prove it).

Data sovereignty is another of many growing concerns in this area — particularly in Europe, where businesses must keep personally identifiable information within the geographic boundaries of countries where customers live.

4. Incomplete Visibility

More enterprises today are measuring the cost and performance of their programs and projects right down to the application level. IT leaders must be able to provide line-of-business (LOB) managers with appropriately granular reports.

Given the nature of hybrid or multi-cloud environments — where standalone applications are a rarity — getting the necessary visibility is a real challenge. Not many platforms can offer that type of visibility without a lot of custom programming. So how can you give the LOB managers what they want?

5. Loss of Control

When cloud technology first emerged, some observers derided cloud resistors as "server huggers." As it turns out, those resistors had a point when it comes to control: In a hybrid environment, and especially in a multi-cloud environment, you do lose some control over your applications.

For some applications, that's no big deal. But for an application that absolutely must run smoothly and with the right combination of cost, security and performance, the public cloud probably isn't the answer. Keeping it on-premises, on the other hand, might well give you the level of control that you need. The trick is knowing which applications belong where.

Third-Party Experts Can Help

If you're struggling to manage a hybrid or multi-cloud environment, you're not alone. Far from it. And you shouldn't hesitate to speak with third-party experts who can help you get on track.

If you would like to learn more, about the challenges that are top-of-mind for IT leaders in the cloud era, watch our Hybrid Cloud Exploration Webinar series with Frost & Sullivan.

CompuCom®

Technology Solutions for the Digital Workplace

MANAGING NETWORKS TO ENSURE CAPACITY AND OPTIMAL PERFORMANCE

Network managers have one job: Keep the network running with enough capacity to deal with whatever comes its way while also maintaining security and optimal performance. This complicated task has gotten even more complicated as the number and type of devices that networks must accommodate has grown.

These days, the biggest challenges for networks come from mobile devices, bring your own device (BYOD) policies and the Internet of Things (IoT). Retail establishments, for example, typically have highly distributed networks and centralized IT departments with few staff. Traditionally, this model worked well since stores used a limited number of stationary point-of-sale devices and wired security cameras. Plus, network traffic was predictable.

The retail landscape has changed, however, especially due to mobile IoT devices. Disruptors like Apple use mobile devices for the point-of-sale, causing the industry in general to move that way to remain competitive. Retailers find themselves needing to support in-store sales differently than before — with mobile devices for quicker service for customers and wireless security cameras. It's now easier to deploy physical infrastructure, but harder for the network to handle.

Three Critical Elements

Retailers that deploy wireless point-of-sale devices have to update the operating systems for those devices. Imagine a store with 20 point-of-sale devices that all need an update. If they all download at the same time and the network isn't equipped to route those requests properly, it can bring down the whole network. Imagine if that happened at noon on a Saturday.

The network has to understand how the devices behave and how they're used. It also has to schedule activities like operating system updates at a time that doesn't interrupt the network or store operations.

What must a network manager do to make sure the network can withstand these varying forces and still perform as the business needs it to? The key is to recognize and deal with the challenges of three critical elements:

- User experience: The network architecture must support mobility overall and BYOD and IoT policies specifically.
- Performance: Networks must meet the latest wireless standards, handle varying user requirements (including remote access) and optimize bandwidth.
- Common management: IT organizations must leverage a single platform to manage and secure disparate network components, such as wired and wireless devices, and to seamlessly integrate third-party applications and platforms.

Understanding User Behavior and Context

The solution lies in creating the right policies for using the network. And that requires understanding user behavior and context — like when it is and isn't appropriate to update an operating system for mobile devices. This enables network administrators to effectively identify risks and secure the network end-to-end.

Associating policies with users eliminates the need to create specific policies for wired and wireless devices or to have to manually deploy security as each device joins the network. By creating a policy that understands context (such as retailers with mobile point-of-sale devices) and unifying how they're managed, IT organizations can ensure the network operates at capacity and performs optimally.

If you would like to learn more, about the challenges that are top-of-mind for IT leaders in the cloud era, watch our Hybrid Cloud Exploration Webinar series with Frost & Sullivan.