ManageEngine

SOLVING HYBRID WORKFORCE CHALLENGES TO MEET FUTURE DEMANDS

ITOM

www.manageengine.com/itom.html

INTRODUCTION

COVID-19 has had a lasting impact on the world and on business—especially the IT sector. During the early days of this virus, organizations had to make major changes in how they operated, including shifting to remote operations. Employees and employers struggled equally to replicate an office-like scenario at home with respect to accessing the internal parts of their organizations while ensuring security.

After the initial disruption, focus shifted towards maintaining and adapting businesses to meet customers' changing needs and in providing seamless services. This continued for a while until the employees started partially moving back to office premises, which led to a hybrid workforce set up.

Organizations are now looking for answers on how to address the challenges they overlooked during the different stages of the pandemic and meet the requirements of a hybrid workforce model.

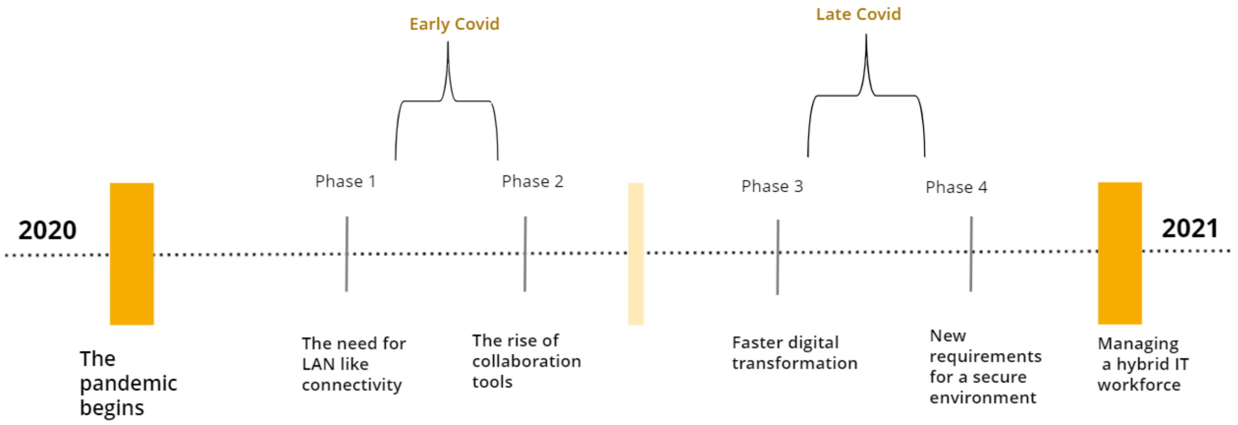
In this e-book, we'll discuss how to manage a hybrid workforce effectively. We will also shed light on how organizations should rethink their strategies and adopt new technologies to sculpt a better future for their businesses.

The past: COVID-19, phases, and IT

The IT industry did not adapt to remote work in a day; it was a slow process. What we are witnessing now was triggered by various factors such as remote access to the internal network, adoption of collaboration tools, digitization, and the shift to the cloud during the transition period. What many organizations have yet to address are the challenges that came along with these factors.

To develop a plan to manage a hybrid work environment, it's crucial to study the different areas that require fixing. We'll now take a look at the various phases IT organizations went through, the challenges faced during every phase, and how to fix the issues in a remote working environment.

> Over the last five years, the remote workforce has **grown by 44%** while over the previous 10 years, it grew by 91%.


Early Covid
Late Covid
Phase 1
Phase 2
Phase 3
Phase 4
2020
2021
The pandemic begins
The need for LAN like connectivity
The rise of collaboration tools
Faster digital transformation
New requirements for a secure environment
Managing a hybrid IT workforce

Phase 1 - Replicating an office setup at home

LAN-like connectivity

Most IT operations were confined within the safe walls of their organization and, due to the work-from-home scenario, these operations had to be accessed by employees from remote regions. Organizations had to protect remote workers and company information from online attacks, since parts of their networks, which were previously accessible only within the office network, had to be opened up to remote employees

That is when virtual private networks (VPNs) came into the picture. A VPN creates what's known as a tunnel: an encrypted link between your device and your organization's network, allowing your data to move in a secure manner as if you were on connected through a LAN cable at your office. VPNs eased the remote access process, since employees could securely access sensitive company information after establishing a VPN connection.

> Use of VPNs in the United States **increased by 124%** during the onset of the corona virus pandemic

The challenges that come with VPNs

1. Adopting a VPN: Although many large organizations were familiar with VPNs before the pandemic, the sudden shift to work from home forced small companies that never invested in VPNs before to adopt this technology. These companies had to start from scratch; this meant that, in order to host their VPNs, they needed to evaluate VPNs, allocate a budget for them, and reconfiguring their firewalls and gateways.

2. Scalability issues: For some organizations, the problem was in scaling. What was once used by 1 out of 100 employees had to now be used by 75 of those 100 employees. Apart from that, the rising load issues and insufficient bandwidth hindered productivity.

3. IT security teams were caught off guard: The IT security teams that rested safely behind their firewalls were shaken up, as they had to bring in more security measures to ensure no private information was stolen by hackers when employees started accessing the network from homes. On top of this, when people started adopting bring your own device (BYOD) policies and using public Wi-Fi to connect to office networks, it became more difficult for IT security admins to prevent cyber mishaps.

4. Trouble from third-party vendors: When businesses work with third-party vendors, those vendors often have complete access to the network, not just the parts involving them. This led to a lot of complications and companies had to implement strict segmentation within firewalls and switches, which made configuration changes grow exponentially.

> In June of 2019, both **LabCorp and Quest Diagnostics** experienced third-party data breaches that exposed 7.7 million and 11.9 million records, respectively.

VPN scenario - Network slowdown

The case: You are connected to a VPN server, and at the same time, 1,000 of your coworkers are trying to access the same VPN server. The server can only handle 300 requests at a time, and due to too many requests, the server becomes overloaded, which causes slow loading times for you and your coworkers. Since you're working on a client's project, you can't afford to waste time waiting for pages to load since your deadline is nearing. How do you tackle this?

The challenge: While being connected to a network through a VPN, internet speed drops drastically. That's because your traffic is being routed through a VPN server, creating one extra step in the data transfer process. In most cases, insufficient bandwidth and server overload can be the major reasons behind slow VPN performance. This can also result in:

- Reduced productivity: Business-critical applications impeded.
- A poor end-user experience: Due to substandard customer service.
- Monetary loss: Failure to meet service-level agreements.
- Increased IT costs: Poor VPN bandwidth capacity forecasting.

The fix: You can improve the speed of your network by:

- Checking the VPN server location and making sure you are connected to the nearest VPN server.
- Choosing a different protocol that has lower encryption standards for projects that do not require tight encryption.
- Making sure your bandwidth is not being consumed for purposes other than work.

How to overcome VPN challenges

1. Monitor VPN activity and usage, identify high bandwidth consumption, track destination URLs, and block unwanted traffic.
2. Keep tabs on the number of active VPN sessions, and measure the VPN session duration and consumption.
3. Identify failed user login attempts, and generate alerts on security attacks, viruses, and other anomalies in your network.
4. Analyze VPN bandwidth trends, and predict and plan bandwidth capacity needs.

By following the above VPN monitoring methods, you can increase VPN performance, improve security, and extract maximum benefits from your VPN.

Phase 2: The rise of collaboration tools

Adoption of collaboration tools

After organizations discovered a way to achieve an office setup and connectivity from remote locations, their focus shifted to adopting online communication and collaboration tools to increase interaction across teams and to maintain relationships with customers, partners, and vendors through the use of these digital channels.

While these collaboration tools certainly have their advantages, they come with issues and security challenges that often make things more difficult than is necessary, especially while working from home.

> **Comscore's data** shows that, comparatively, people in the U.S. spent a total of six billion minutes using top collaboration tools in May 2020.

The challenges

1. Too many tools: Some tools offered online chatting via messages while others provided audio and video conferencing. A lot of organizations face difficulties while juggling between more than one tool while working from home.

2. Improper use and execution along with privacy concerns: If a person is unfamiliar with the platform presented, they may not use it correctly. For example, a user may not know how to add more users to an online video conference, which will cause delays.

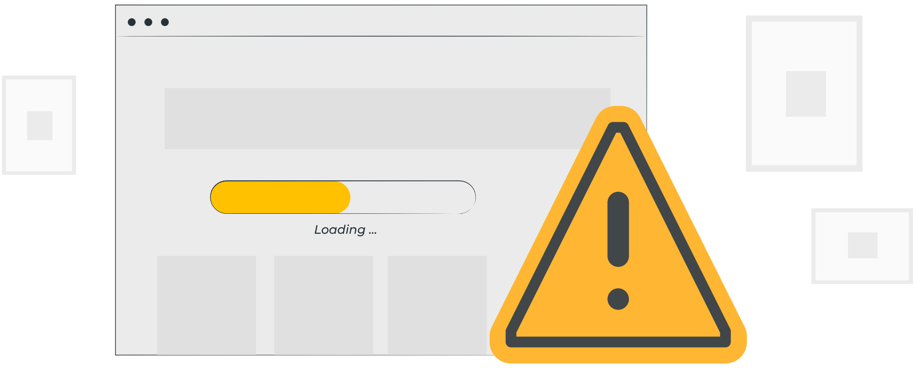
3. VoIP issues: A lot of employees faced chopped audio, lag, and poor video quality while using collaboration tools. This can be attributed to insufficient bandwidth while hosting VoIP services.

4. No single sign-on option: Many collaboration tools that belonged to the same suite of solutions did not provide a single sign-on option. This meant the employees had to provide credentials every time they tried to log in to different tools.

5. Privacy concerns: Since many collaboration tools aspire to make communication among teams easier, they introduce features that allow employees to share data within their tool, which can be a major security concern. For example, if an employee shares critical information in a communication channel that has many other employees, there is a possibility of a data leak. Not just that, downloading files shared across these platforms can be a potential security threat leading to a breach, since a lot of collaboration tools have loose security protocols.

> In a survey by Alfresco, **59% of respondents** revealed that they experienced challenges while working on their collaboration tools.

Scenario: Bandwidth issues with collaboration tools



The case: Daniel is working as a support engineer in an organization. He works the night shift along with 500 other support engineers. Ever since work from home started, Daniel and his 500 coworkers have been finding it difficult to make VoIP calls with customers using collaboration platforms, mainly because they have to connect to their office network via the VPN for every call. Many agitated customers complained of poor video and audio quality, lag, and background noise. What should the organization do to improve the support experience so that it does not lose customers?

The issue: This issue is mainly due to improper bandwidth allocation and increased VPN connectivity.

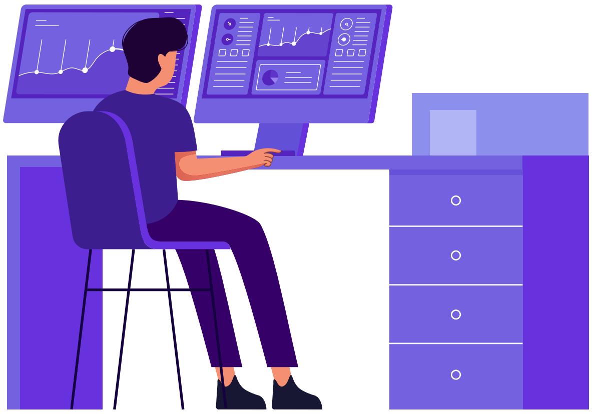
The fix: To improve performance of collaboration tools, the organization should:

- Ensure that there is sufficient bandwidth for the collaboration tools to work properly, especially when support call volume is high during the peak hours.
- Block unwanted incoming and outgoing traffic to prevent unwanted apps and sites consuming bandwidth unnecessarily.
- Predict bandwidth capacity needs for the collaboration tools so that the problem does not persist in the future.

How to avoid bandwith and VoIP issues

1. Monitor network bandwidth and traffic patterns at an interface-specific level.
2. Reconfigure policies with traffic-shaping techniques via quality of sale or access-control lists (ACLs) to gain control over bandwidth-hungry applications.
3. Ensure a high level of data and voice communication quality by keeping tabs on the performance of voice and traffic data.
4. Make informed decisions on your bandwidth growth by measuring your bandwidth growth over time.

Phase 3: Digitization takes a quantum leap



Organizations and digitization

After organizations fulfilled their basic needs like an office-like setup at home and after investing in collaboration tools, they had to resort to adopting digitization techniques like cloud adoption and virtualization to be relevant in the industry.

Although virtualization and the cloud have been IT trends for some time, the pandemic made these trends a necessity; a vast number of organizations migrated to cloud in a short period.

> **Forrester** now predicts that the global public cloud infrastructure market will grow 35% to $120 billion in 2021.

Cloud adoption - The challenges

1. Unhealthy migration: Cloud environments can be significantly different fromin-house on-premises ones on which applications are hosted. An application to be moved to the cloud must be compatible with the OS, and a system reconfiguration may mean an application might not work as expected. These issues were increased in number since the speed of migration affected project deadlines and budgets.

2. Short term fixes: Due to the speed at which cloud adoption was taking place, migration issues were not properly addressed. IT admins relied on short-term fixes due to the pressure of service delivery to the end users and the poor foundation often caused applications issues.

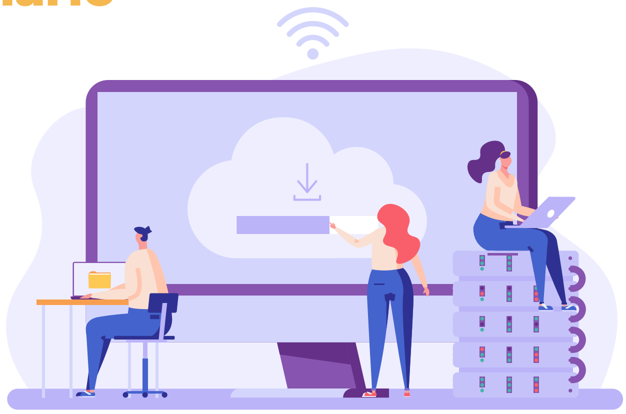
3. Multi-cloud environment: With enterprises adopting a multi-cloud strategy for their digital transformation, the real challenge was in the management of a multi-cloud space. IT admins, operators, and the security engineers had to juggle different consoles and dashboards across the multiple cloud platforms and didn't have enough visibility while managing such an environment.

4. Poor customer experience: When organizations moved to the cloud, it was no longer an internal affair where employees could respond to customer complaints by checking a server hosted within the premises. Mean time to repair increased drastically, since a lot of elements like load balancers, queues, apps, and services had to be reviewed to find a fix. This led to a lot of angry and unsatisfied customers.

5. High operating expense: It's important to note that introducing the cloud into your existing infrastructure is not a cake walk, especially when an array of vendors are involved. To ensure a smooth cloud integration with existing systems, organizations will have to invest in additional resources to derive a desired level of performance. This often results in expensive operating costs.

> In a survey conducted by **Flexera**, respondents estimated that organizations waste 30% on cloud spending.

The cloud scenario



The case: A mid-sized enterprise had to migrate to the cloud when work from home commenced since in-office operations were restricted and it seemed like an affordable alternative. It later found out that cloud migration was not as easy or as cheap as it seemed.

When moving data between the cloud and on-premises systems, it had to open certain firewall gateways, which put tons of customer data at risk. Not just that, the enterprise was not able to move data from its existing software to the cloud without an expensive rewrite of its existing code. This affected the enterprise's existing projects, and it was not able to meet customer deadlines due to migration and security issues.

The issue: The enterprise failed to visualize its cloud architecture and its requirements before migrating from on-premises operations.

The fix: The enterprise should have:

- Prepared itself for a phase-by-phase cloud migration where it understood the requirements of every module.
- Performed data filtering to reduce the transfer of redundant data so that important data required for client projects was transferred first.
- Relied on proxy servers to reduce bandwidth demands by compressing data that had to be transferred.

How to optimize the performance of cloud-based applications

1. Monitor applications, servers services, processes, and cloud components by tracking and troubleshooting the health of your
2. cloud elements.
   Track the capacity and resource utilization of your containers and drill down into specific parts of the cluster with extensive usage stats.

Phase 4: Security issues that spiked during the pandemic

Using collaboration tools, VPNs, and cloud services increased the risk of data breaches and exposed companies' critical IT systems to malicious content. Many organizations also started following a BYOD approach, which opened the door to a new set of security issues.

As the world started witnessing increasing breaches and security attacks, organizations realized that they had to identify potential risks by investing in security solutions before an attack was hurled at their network.

> Global research and advisory firm **Gartner forecasts** that the worldwide cybersecurity market will reach $170.4 billion by 2022.

A security scenario

The case: Peter works in ABC enterprise, which consists of 10,000 employees. The enterprise relied on a third-party VPN service provider during the work-from-home period. One day, Peter and his fellow coworkers woke up to a headline reading, "Russian hacker reveals a list of plaintext usernames and passwords, along with IP addresses for more than 900 enterprise servers of a famous VPN vendor." It was indeed the same

VPN service Peter's enterprise was using, leading to a major dilemma in his organization since important confidential information was threatened.

The issue: The news later revealed that the VPN servers included in the list were running a firmware version vulnerable to the CVE-2019-11510 vulnerability.

The fix: The VPN service provider should have done the following to avoid this massive breach:

- It should have scanned all its VPN servers for vulnerabilities and applied patches.
- It should have supported two-factor authentication to ensure more security.

What are the ways to ensure overall network security?

1. Monitor active VPN users, user-specific VPN usage, sessions, and the bandwidth consumed.
2. Use two-factor VPN authentication to increase VPN security.
3. Invest in Zero Trust solutions, which analyze user behavior based on a user's login time, the location from which they log in, and more to provide access to applications that do not require a VPN.
4. Monitor the list of rules, policies, and ACLs used by the traffic of your enterprise network through the firewall.
5. Go for role-based access control (RBAC) authorization and adhere to compliance standards by conducting security audits once every
6. three months.
   Scan your network for vulnerabilities and apply patches before information is leaked.

The present: The birth of hybrid IT

A year and a half into the pandemic, organizations started reopening partially. However, many organizations realized they were able to reduce operational and functional costs by allowing employees to work from home, so they decided to continue working remotely. Either way, it's clear that the IT industry is not going to go fully remote or operate with 100% office population any time soon. This is when the hybrid workforce model came into the picture.

A hybrid workforce is similar to a remote workforce model where employees work from a location outside of the office. The difference, however, is that hybrid workforce approaches are not entirely remote.

> A survey by **Appolo Technical** reveals that hybrid work models are already used by 63% of high-growth companies.

Hybrid workforce model - Checklist

1. Resolve pending issues you overlooked during the four phases of the pandemic such as VPN, bandwidth, VoIP, cloud adoption, and security issues. Tending to these issues as soon as possible will solve almost 75% of the challenges in a hybrid workforce model.
2. Set up an employee tracking system to ensure that employees are healthy and performing well without facing issues.
3. Regularly have your network audited by your IT security teams to make sure they are running properly and that the most up-to-date patches have been installed. Analyze how vulnerable your devices are by thoroughly monitoring your firewall and VPN on a weekly
4. basis.
   Invest in IT automation tools so that IT admins can automate patch management and reduce the amount of manual effort required to
5. patch the systems of employees who are working from home and the office.
   Deploy new technologies like software-defined wide area networks (SD-WANs) and adopt technologies (AWS VPC) over VPNs to connect to corporate networks.

Let's explore how an SD-WAN can help ease the hassles faced while managing a hybrid workforce.

How can SD-WANs benefit a hybrid workforce model?

Let's say there's an organization that has a single main office in a city and its employees have been working from home ever since COVID-19 hit. Due to wavering lockdowns and relaxations, it opens small office spaces (hub/spoke offices) in remote locations to allow employees to experience a setup similar to the main office.

Now, in order to allow employees to connect to the corporate network in the main office from remote hub office locations, it has to set up site-to-site VPN connections.
However, deploying site-to-site VPN connections is expensive and slowly losing its significance ever since cloud migration started.

This is why an SD-WAN is a better option since it completely eliminates the need to establish expensive site-to-site VPN connections with its centralized approach, which allows communication between devices present in the hub offices and the main office through a central SD-WAN controller.

Example: From the central SD-WAN controller, an IT admin will have the liberty to make configuration changes to a selected network device in a hub office without having the need to establish a VPN connection to the main office.

> According to a **survey**, 52% of respondents view improved management and monitoring as a benefit of SD-WAN technology.

The future: Hybrid operations

The future is undoubtedly going to be hybrid. By establishing a fully functional hybrid environment, organizations can enable the hybrid workforce to deliver uninterrupted, quality service to customers while operating from anywhere.

Gartner vouches for hybrid workforces to take center stage in the future!

"A hybrid workforce is the future of the work, with both remote and on-site part of the same solution to optimize employers' workforce needs," said Ranjit Atwal, senior research director at Gartner.

DC's Asia/Pacific vice president of research practice, **Simon Piff**, has suggested that both the supply-side and buy-side should move to a conscious hybrid working model that provides employees with the same secure access to applications regardless of where they're working.

Following Simon's approach, we can also infer that it is not feasible to rely on band-aid solutions and quick fixes to face the future. It's high time CEOs and CFOs steer their organizational ships in the direction that replaces age-old short term solutions with fresh, sustainable technologies to become future-ready.

The right direction: Remote-first, digital-first approach

Talking about future trends in the IT world, IDC has coined a term called Branch of One, which means the future lies in the connectivity, and organizations must provide efficient, sustainable, and secure ways for remote and in-office communities. The main goals of the Branch of One architecture are to:

- ✓ Enhance the employee experience in a perimeter-less work environment using digital experience monitoring, endpoint analytics, self-service provisioning, and remote troubleshooting tools.
- ✓ Enable employees to be productive during remote support by investing in voice-controlled collaboration tools and by regularly optimizing the performance of the tools.
- ✓ Adopt team structures, processes, skills, and tools to drive business model innovation using a digital-first, location-independent strategy.
- ✓ Invest in distributed cloud and edge technologies that enable the building of a blended workplace to move work environments seamlessly between physical and virtual locations.

Sounds familiar, right? Most of the future trends point towards one concept referred to by different names, and the concept is simple: The future of IT is a hybrid workforce.

The past, the present and the future are all intertwined. The IT industry is like an infinite knot where the actions in the past will directly affect the future. This is why it's important to understand the important elements of managing IT, so you can steer your business in the right direction.

IT operations management (ITOM) solutions, can help you do it. Check out our products!

NetFlow Analyzer

- □ Identify the who, when, and what of excessive bandwidth usage.
- □ Ensure high-quality data and voice communication.
- □ Track the duration of any network issues and bandwidth bottlenecks.
- □ Limit the use of bandwidth-intensive apps by scrutinizing traffic.
- □ Predict future bandwidth capacity needs with capacity planning reports.

Firewall Analyzer

- □ Monitor VPN activity and usage, track destination URLs, and block unwanted traffic.
- □ Analyze the use and efficiency of your firewall rules, logs, and policies.
- □ Identify potential security attacks, viruses, and other anomalies in your network.
- □ View the complete trail of all changes applied to your firewall configurations.
- □ Automate firewall audit reports and ensure continuous compliance.

Applications Manager

- □ Track key performance metrics for apps hosted on-premises and in the cloud.
- □ Identify application issues, including slow response times, memory errors, CPU spikes, and more.
- □ Track the capacity and resource utilization of your containers.
- □ Monitor and measure the end-user experience with your web applications.
- □ Manage servers, databases, VMs, and cloud applications from remote regions.

Network Configuration Manager

- □ Back up configurations of network devices across your infrastructure any time.
- □ Get instant alerts on configuration changes in real time.
- □ Keep a track of the who, what, and when of configuration changes.
- □ Ensure internal compliance and comply with industry standards (HIPAA, SOX, and more).
- □ Control who can make what kind of changes by implementing RBAC.
- □ Scan your network for vulnerabilities and apply suitable patches.

OpManager

- □ Monitor network devices, physical and virtual servers, load balancers, and more for fault and performance.
- □ Get instant notifications about network issues via SMS, email, and SNMP traps.
- □ Automate repetitive tasks through code-free IT workflow automation.
- □ View all your network data in one, central dashboard.
- □ Gain insights on network performance with more than 100 built-in reports.

OpUtils

- □ Enable network admins to wake up machines remotely on demand.
- □ Identify used and available IP addresses and quickly scan switch port locations.
- □ Detect rogue devices quickly and block their access.
- □ Leverage troubleshooting with Cisco, SNMP, network, and address management tools.
- □ Keep track of your network's bandwidth usage and generate reports.

If you'd like to implement all the above solutions in one, try OpManager Plus, our integrated IT operations management tool.

Get Price Quote

Request Demo

Download Free Trial