Technology transformation and readiness assessment

BCG | verizon

White paper

Part two in the *Business as Unusual* white paper series

Authors

Sampath Sowmyanarayan
Jay Venkat
Michael Coden
Val Elbert

Introduction

This is the second in a series of articles discussing the workplace of the future and particularly what businesses need to do to enable remote working as part of business as usual.

The way we work has been transformed by the COVID-19 pandemic, which has made it clear that a remote working model is not a "nice to have" for global businesses, but a prerequisite. The new world that will take shape as we work through the pandemic and beyond—the fourth wave of remote working—will be determined by organizations deploying remote working at scale and extending remote working possibilities with next-generation technologies driving competitive advantage.

The first article discussed the six imperatives that are needed to drive effective remote work, namely:

1. **A scalable network**
2. **Cloud-ready applications**
3. **Strong and secure mobile connectivity**
4. **End-to-end monitoring of performance**
5. **Zero-trust security**
6. **A resilient end-user support model**

But of course, remote working is just one part of the workplace of the future, and you cannot look at the six imperatives outlined above in isolation—you need an overall technology transformation agenda in place.

In our first article, we also asked the question, "Are organizations ready for technology transformation?" The point here is that any organization's transformation agenda will now be radically different from one that was put in place six months or even six weeks ago, especially with the COVID-19 crisis acting as a catalyst.

In fact, enabling the workplace of the future necessitates resolving a unique set of challenges to drive a competitive advantage amidst deployment at scale and extension into next-generation technologies. As such, these six imperatives are all technical building blocks that need to be carefully aligned for organizations to be future-ready for success.

This next article aims to discuss what technology leaders need to do to make the fourth wave a reality from a technology transformation perspective. We'll delineate the high-level imperatives all leaders need to be considering, as well as look at what must be done from a tactical perspective and discuss technology solutions. The objective is to provide a path that all organizations can follow as they enter the new world of "business as unusual."

Reshaping the technology transformation agenda

At the very core, we believe there are four key stages to be undertaken when organizations look to reshape their technology transformation agenda.

1. **Define your transformation vision and goals.**
2. **Focus on future-readying your people building blocks, i.e., workforce and talent.**
3. **Build scalable and adaptable application, IT infrastucture, data and digital platforms (DDP).**
4. **Design in cybersecurity from the beginning of the transformation.**

Four key stages: Reshaping your technology transformation agenda

1. Define your transformation vision and goals.

The COVID-19 pandemic's dramatic drive toward a remote working model offers us many lessons. As we move into the fourth wave of remote working (as referenced in the first article of our series), CIOs need to think about how their IT infrastructure performed during the crisis and really note down their key learnings: What held up? What failed? Was their IT infrastructure resilient enough? Was there any impact on workplace efficiency, process and productivity—and did they still manage to effectively support their customers?

With these reflections made, the first step CIOs should take is to determine their organizational transformation end goal and target operating model across the six imperatives outlined above. This end goal has to be clearly defined and should also create a competitive advantage for the organization. A rule of thumb here is to enlist specific metrics to guide the thinking, which further translate into must-dos within each dimension. For example:

- For scalable networks, what level of flexibility is expected for our network usage? What levels of remote working are anticipated (and which functions, roles, geo-location "hotspots")? How will the network needs change as we flatten the curve and fight out of the economic trough, gradually bringing some of the workforce back to the office?
- For zero-trust security, what amount of threats are expected to be handled annually, and within what time frame are threats expected to be resolved once detected?
- For the end-user support model, the online multichannel customer experience and the supply chain, what is the range of suppliers that could be considered? How much do we want to diversify? How much do we want to consolidate? What are the interdependencies among suppliers in the supply chain?

A rule of thumb for defining your transformation goals and vision is to enlist specific metrics to guide the thinking.

In the same vein, and to wrap this within the context of real-world examples, across hundreds of projects, Boston Consulting Group's (BCG) research puts forth the thesis that the goal is for organizations "to develop world-class technology functions (WCTFs) that create strategic differentiation by enabling new digital capabilities and increasing the enterprise's simplification (to drive cost savings) and resilience." (See graphic on next page.) In view of these goals, the six dimensions have a critical role to play.

Source: "A World-Class Tech Function Is Digital, Simple and Resilient," BCG, September 30, 2019

In a related article, *Managing the Cyber Risks of Remote Work*, BCG has described the full range of cybersecurity actions that a company should apply to a remote workforce.

The next step to take is to define how to reach that goal. What strategy will you adopt? It's important to define that strategy from where you are today, which is most likely a very different place from where you were just a couple of months ago. Different organizations will have radically different technology setups in place, for example, depending on their size, age and geographic spread. We also encourage technical leaders to clearly define the organization's network needs in this new world—e.g., higher flexibility of network usage, increased levels of remote working, digital customer engagement and commerce, digital supply chain, differentiation by "hotspots" globally, etc.—and force a radical "as needed" rethink rather than using a more organic, go-with-the-flow evolution.

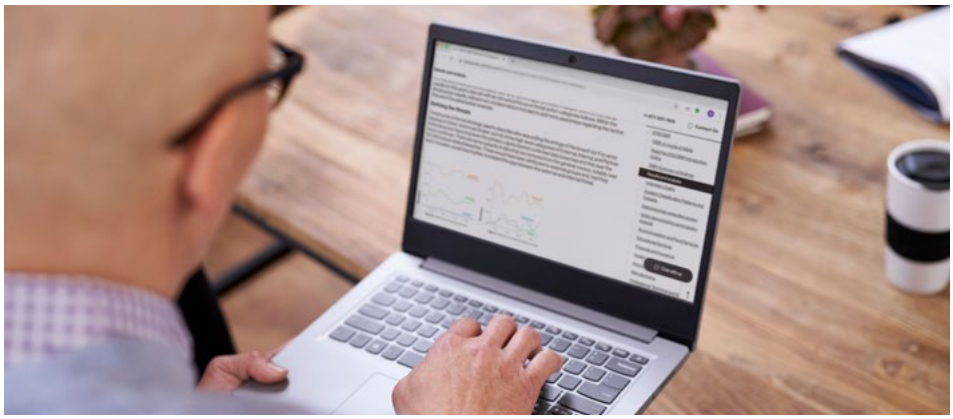
From there, it is critical to conduct a full technology discovery and inventory (functions, architecture, environment) to fully understand your true baseline. Identify your most critical assets—e.g., your business-critical applications and functions. This will enable you to build out use cases that deliver value and are fully aligned with your business objectives. It will also enable you to understand what absolutely needs to change and what does not. From this, you can forge a comprehensive plan that leverages assets that not only matter now, but that may also be critical in the future.

2. Focus on future-readying your people building blocks, i.e., workforce and talent.

This second step is about ensuring that you have the right skills available to deliver on your transformation vision. This might mean retraining existing staff in areas such as AI, machine learning or cybersecurity or hiring in to ensure that you have the right skills to deliver the six imperatives of transformation. Or it could mean identifying a partner who can contribute specialist knowledge. But you need to ensure that you have the right team in place to make transformation happen, or you won't get out of the starting gate.

You need to ensure that you have the right team in place to make transformation happen, or you won't get out of the starting gate.

You also need to ensure that, from the beginning, technology teams and the business are fully integrated and aligned. Technology cannot be developed without a feedback loop from its eventual end users, and if technology does not fit with how people work, then work-arounds will be used. Adopting human-centered design (HCD) and agile methodologies is a good option here, as it enables customer feedback and swift responses through a balance of alignment and autonomy. This is an area that we will focus on in the third article in our series.

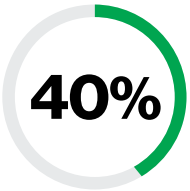


3. Build scalable and adaptable application, IT infrastructure, and data and digital platforms (DDP).

This is where transformation comes to life. The most important part of future-readying your business is to ensure that you have a modular, flexible IT architecture, which can adapt to challenges the future brings. This means simplifying your data and application landscape and establishing application programming interfaces (APIs) and microservices to create more flexibility. It means leveraging private, public and/or hybrid cloud infrastructure, with an opportunity to scale if required. And it means infusing strong cybersecurity elements across the design and implementation of technology, data and platform layers.

4. Design cybersecurity in from the beginning.

Designing cybersecurity into a transformation from the very start helps control development and operation costs, reduce time to implementation and generate revenue earlier. BCG client data analysis has shown that designing cybersecurity into a transformation can reduce rework costs by up to 62%, and time to market by up to 20%. Moreover, by instituting a common cybersecurity framework for all applications (both on-premises and multi-cloud), BCG indicates that operating costs can be reduced by up to 40%.



Instituting a common cybersecurity framework for all applications can reduce operating costs by up to 40%.

Many organizations don't take the time to look in depth at these four factors, and that is a key reason why transformations have cost overruns and fail. Not taking the time to look at your current state, work out how to get your future skill set or build in flexibility from the start of your design can all cause major issues down the line.

What is clear is that to move from theory to reality with these building blocks will require both technology and people upskill investment—and that's why it's important to establish the investment horizon and expected returns as early as possible. And this needs to be a long-term view. It's very easy to think about short-term cost savings rather than the longer-term potential of putting all these building blocks in place. So the best transformation agendas will strike a good balance, where bets are placed carefully across these imperatives in an economically well-planned sequence.

Technical building blocks—transformation imperatives

And so now on to your technical building blocks—the six imperatives outlined in the introduction.

01 A scalable network

In this first building block, the very first must-do is the full environment discovery: a review of baseline architecture and common network functions, as already mentioned as a fundamental in developing a technology transformation plan. You then also need to identify potential future operation modes through tabletop exercises to prepare for at least two to three major event scenarios (e.g., pandemic, natural disaster, disruption in supply chain). This will enable you to build an architectural roadmap that will support your business objectives.

Perhaps the most important considerations for building a scalable network are flexibility and scalability. This is where SDN comes in.

But perhaps the most important considerations in this building block are flexibility and scalability. For organizations to stay relevant and competitive in a global and turbulent market (both during and after COVID-19), organizations of every shape and size require a network that can support the dynamic and on-demand needs of their users and applications—for example, more bandwidth to support seasonal sales requirements, more VPN connections or cloud access to support work-from-home requirements. This is where software-defined networking (SDN) comes in.

Traditionally, companies have purchased different devices to deliver networking functionality—routers, switches, firewalls, load balancers, etc. With SDN, the network is now software based, and these functions are accomplished virtually. SDN enables organizations to gain network flexibility and agility and also makes their network much more elastic, as software can also be used to increase capacity or introduce new functionality. SDN supports innovation in a way that static networks cannot.While one can have an SDN without scale, you can't have a truly scalable network without SDN; SDN is a prerequisite for scalability. A scalable, SDN-enabled network has four clear characteristics:

Application/user awareness built in

Within any organization, inconsistencies exist across importance of applications and users—and so segmentation matters. Not all applications have the same level of importance to an organization (e.g., an enterprise

1 "Market Trends: SD-WAN and NFV for Enterprise Network Services," January 30, 2020

resource planning application versus web browsing), and not all users have the same level of importance to an organization (e.g., doctors in a telemedicine world, traders in finance). Software-defined WAN (SD-WAN), a subset of SDN, has application awareness built in, giving the organization the ability to prioritize applications or users on the network quickly and efficiently. And levels of sophistication increase dramatically when combined with deeper network visibility (which we discuss in depth below).

Network function virtualization (NFV) for rapid addition of scale and capability

VPNs deployed as NFV can scale much more easily and quickly (we're talking hours/days instead of weeks) via APIs, when compared to the need-to-deploy hardware. We know of many customers who had to dramatically increase VPN throughput to support their shift to working from home. For example, two European-based enterprises have started leveraging NFV to easily scale VPN connections across multiple network nodes to >1 Gbps per node to account for increased remote access traffic.

In another example, an India-based services company rapidly stood up a software-defined VPN to respond to users at home for the first time. While it's true that to date, adoption of NFV has been slow, organizations need to prepare for when the tide will turn. Gartner states that "39% of enterprises cited technology and vendor risk as the major blocker to wider adoption of NFV-based services. Leading Network Service Providers are striving to offer greater choice of hardware platforms and software functions while attempting to ensure quality and reduce complexity."[1]

API-driven orchestration

With APIs comes the ability to manage bandwidth and traffic routing across both public and private networks with better visibility. Visibility tools, which we will discuss below, will sense any infrastructure anomalies or issues—which could be caused by a spike in customer demand or a rapid shift to working from home—and feed predefined workflows that then invoke API calls to network elements (whether NFVs, traditional MultiProtocol Label Switching (MPLS) and internet networks or 5G). An organization is therefore able to scale up resources to accommodate these anomalies or issues without human intervention.

For example, a large U.S.-based global retailer scaled up network connectivity via API calls for action in an hour, compared with the several days required by a traditional order route. In another example, a European-based leasing company leveraged API-driven policy updates to change how it prioritized applications to support business-critical traffic during a period of network congestion.

Flexible access to cloud

The final aspect to consider when building a scalable network is cloud interconnection, and this means public and private networks into the hyperscale cloud and software as a service (SaaS) providers.

Applications and application elements will often continue to reside in different clouds but need to be quickly and easily accessed. Cloud and SaaS providers therefore need to be seen as an extension of the network, with cloud interconnection architectures able to quickly adjust both bandwidth and access, usage-based (platform) models and software-defined access in co-located data centers, and not rely on the need to install new physical connections.

In the case of a Latin American holding company, software-defined access to cloud hyperscalers rapidly enabled increased connectivity to Microsoft Azure for users working from home.

Cloud vendors typically refresh their hardware every two years, compared with four to seven years at most large enterprises, leading to a 20% performance improvement.

02 Cloud-ready applications

In this building block, again, the first must-do is creating an inventory of which applications you already have, and which are already mission-ready to be moved to the cloud. And this is an inventory check that should actually be repeated frequently. A BCG report states, "Cloud vendors typically refresh their hardware every two years, compared with every four to seven years at most large enterprises, leading to a 20% performance improvement. This improvement comes via the benefits of Moore's Law, as well as from faster data retrieval and improved operating systems and virtualization software." This is not so much of an issue for smaller organizations, who tend to have deployed more SaaS applications and so have an easier "transition to cloud" mission.

Once you know what you've got, it's about cloud-enabling those mission-ready applications (and moving the workflows) and then building a security-first, cloud-first strategy for future application enablement. Again, as BCG finds, "Large enterprises that move to the cloud effectively can improve delivery of IT services by 25% to 50%."[2]

2 https://www.bcg.com/publications/2019/enterprise-applications-cloud-ready-prime-time.aspx

You then need to define your collaboration strategy and choose which platform you want to use for internal communication – as well as potentially communicating with partners, vendors and customers too – again with an eye on which policies and procedures will need to be in place to address any industry-specific compliance requirements. Working out what type of collaboration you want will enable you to choose a unified communications solution that will work for your specific needs. Some organizations will need more video than others; for others, a chat function is key.

Software-based perimeter protection solutions are one key solution for consideration when enabling cloud applications. These can protect evolving infrastructure and the application threat surface. These solutions are beginning to gain traction (refer to figure below).

It's then all about monitoring those assets across cloud networks and cloud compute, especially with hybrid deployments. This might require controlling user and developer access to cloud apps, as well as monitoring any changes and updates. You then need to ensure that you can continually assess cloud security in line with industry best practice – for example the ability to monitor cloud security through log integration, penetration testing and vulnerability management. Finally, you also need to consider cloud access (including private network access to major cloud assets) and backup and capabilities to offer simple visibility and control across multiple cloud nodes.

When it comes to strong and secure mobile connectivity, the quality of the physical connection cannot be overlooked, so organizations should consider multiple options to get the right performance.

Software-defined perimeter solutions (SDP)*

***Zero-trust network access (ZTNA) is also known as an SDP.**

Source: *Guide for Zero Trust Network Access*, Gartner, April 29, 2019.

2022
Eighty percent of new digital business applications opened up to ecosystem partners will be accessed through ZTNA.

2023
Sixty percent of enterprises will phase out most of their remote access VPNs in favor of ZTNA.

03 Strong and secure mobile connectivity

The must-dos of this third building block are all about delivering reliable and secure connectivity. The quality of the physical connection cannot be overlooked here, so organizations should consider multiple options to get the right performance. As an example, a Verizon customer (global financial services company) recently deployed LTE hotspots to augment areas where consumer broadband connections didn't perform as expected.

VPNs are the next key item and a foundational piece of this, which can then be augmented with private wireless gateway services. But security must not be an afterthought and, rather, has to be built in as standard. And this is not just about anti-virus protection but rather zero-day protection, leveraging, if possible, AI technologies and threat intelligence to predict potential data breaches.

As an example, a U.S.-based investment and insurance Fortune 500 company has deployed an integrated threat prevention solution that combines the power of AI to block malware infections with high effectiveness and little system impact, helping prevent zero-day attacks. The solution works where most attacks occur (at the endpoint) for better efficacy, fast resolution and less disruption.

It goes without saying that any wired and wireless connectivity devices need to be able to be deployed rapidly but also with control, and you also need to be able to monitor the deployment of any unauthorized mobile applications. For example, a U.S.-based global investment firm recently deployed 7,000+ endpoints to remote workers to manage proper traffic prioritization as well as sufficient visibility tools to address regulatory compliance requirements. And finally, you need to carefully manage internet access and policies across public websites through regional internet breakout services.

Dynamic and adaptable remote access, mobile device management and endpoint security are just some of the solutions that you should be considering to make strong and secure mobile connectivity a reality. These need to be augmented with Domain Name System (DNS) protection services for network-based blocking of malware, Internet gateway and breakout solutions for policy control and overall performance improvement, and DDoS protection to enable your growing remote workforce to continue to securely reach corporate assets.

You also need to remember that people are often an organization's weakest link, so ensure that you continue to train your employees on simple steps to take to counter phishing, malware or other social engineering scams, and track the latest and greatest with threat and intelligence feeds that work directly with email filtering.

The Verizon Data Breach Investigations Report (DBIR) is always a great source of information on security and threat trends. And remember, the best way to keep your network secure is to do the basics well, so make sure you keep up to speed with patch and update programs.

Remember that people are often an organization's weakest link, so ensure that you continue to train your employees on simple steps to take to counter phishing, malware or other social engineering scams.

04 End-to-end monitoring of performance

The first must-do for this fourth block is the discovery process that we've already described above. This is important if you are to be able to properly understand your network data flows. The second is to define how your network is working with respect to visibility, insight and execution. We refer to BCG's interview with industry experts to cover the nine prevalent core use cases across these three areas (refer to figure on next page).

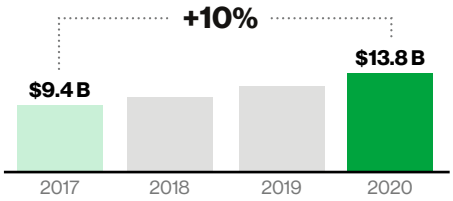
Adoption will follow the IT operations value chain.

	Core use case	Currently using AIOps (%)	Currently using AIOps (%)
Visibility	Anomaly detection	11	42
Insight	Noise reduction	9	42
	Triaging and alert correlation	10	10
	Service impact analysis	5	35
	Root-cause analysis	6	33
	Forecasting	9	38
	Incident prediction	9	38
Execution	Remediation recommendation	7	32
	Automated issue remediation	3	21

AIOps: AI operations

Source: Interviews with 25+ industry experts; CIO survey (N=112); BCG analysis, August 2019.

BCG analysis: three year compound annual growth rate



The market for core AIOps is projected to grow from $9.4 billion in 2017 to $13.8 billion in 2021, a compound annual growth rate of 10%.

AIOps orchestrators—platforms built to orchestrate insight and actions on the basis of log data from various monitoring solutions—are expected to grow by 26% over the same period.

Source: BCG analysis, August 2019.

The overall objective is to curate an accurate data set so you can understand how you might re-instrument different parts of the network, incorporating predictive analysis to help predict and prevent anomalies or outages, and automating actions, whether for users, transactions or applications.

With the shift in traditional corporate data flows away from the office setting and into remote scenarios, CIOs must be able to glean data directly from the network itself in order to quickly identify and address anomalous behavior. For example, Verizon saw a massive increase (greater than 200%) in UDP (user datagram protocol) versus more normal TCP (transmission control protocol) traffic for one large enterprise. Upon further inspection at the port level, the traffic shift was almost exclusively remote workers using VPNs.

In this case, it was an expected shift, but a heightened level of visibility is needed to validate the expectation.

And the holy grail is to leverage AI technologies across IT operations (AIOps solutions) to turn big data into meaningful insights that makes network management and orchestration simple and effective. AIOps solutions is a growing market according to BCG research.

The holy grail of performance monitoring is to leverage AI technologies across IT operations (AIOps solutions) to turn big data into meaningful insights that make network management and orchestration simple and effective.

Monitoring is important for the IT side of the organization; for the business side, it is all about staff morale and productivity, and for this you need visibility. Ultimately, the human experience of working with critical business applications is the most important element. The goal is to be able to understand what is causing productivity loss and take action, even when you don't own the internet/network your applications are being delivered across and have limited ability to instrument the "as a Service" platforms from which your applications are being delivered. Your digital supply chain is a mixture of public, private, personal, corporate and other assets, and it's vital to understand how the user experience (both internal and external) is being delivered, end to end.

BCG has worked with the U.S. National Institute of Standards and Technology (NIST) to develop both Key Practices for Digital Supply Chains and an open source Supply Chain Interdependency software tool that can help you manage the digital supply chain.

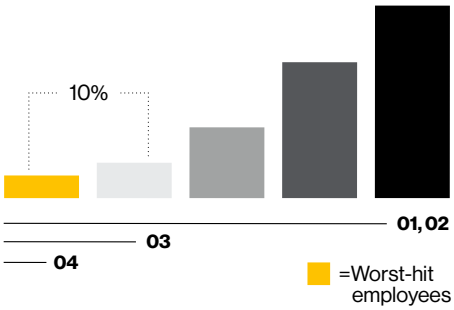
Visibility profiles are packaged to represent best-practice measurements, thresholds, timing and alerts to notify when a service is up, down or degraded and the associated impact. Analyzing your business' digital ecosystem within the context of experience/digital scoring (similar to telephony quality Mean Opinion Score [MOS] scoring) and business outcome delivery complemented with the lens of human experience provides better correlation and context to drive faster average repair time and automation through AIOps.

Additionally, some of the solutions that could be considered include synthetic transaction, role-based end-user experience or business process monitoring—and of course, intelligent workflow automation.

One example on visibility is a tool that Verizon has started to deploy internally and that is also available for external consumption. Verizon technology partner Actual Experience offers a tool that synthetically measures your global digital ecosystem, then uses advanced "human experience" algorithms and correlation techniques to rapidly determine whether the cause of lost productivity is home Wi-Fi, the local ISP, corporate infrastructure or a cloud service provider. The graphic above shows some of the actionable information gleaned from this type of instrumentation for a select division of the Verizon Business Group. As organizations conduct and scale up similar visibility tests, the availability and transparency of the productivity metric will then guide the set of focus areas within the supply chain to drive best use of resources. Again, the answer set may differ by divisions and/or applications, but that is the beauty of data granularity, where slicing and dicing de-averages the answer to drive specificity.

Selected example: One division within Verizon Business Group and around 40 locations

Key insights



01
4 min
Time lost per day per avg. employee

02
No loss
Time lost per day 30% of all employees

03
>15 min
Time lost per day 10% of all employees

04
31 min
Time lost per day Worst-hit employees

Root causes

Wi-Fi **19%**

ISP **70%**

VPN **79%**

Cloud **11%**

05 Zero-trust security

The U.S. National Institute of Standards and Technology (NIST) states that "Zero trust [security focuses] on protecting resources, not network segments, as the network location is no longer seen as the prime component to the security posture of the resource." The first must-do in this building block is to identify those business-critical applications and data feeds that are your organization's most critical assets ("crown jewels")—without which you could not operate. These could be virtual or data assets or physical assets such as manufacturing or energy production and transmission equipment.

Verizon has visibility into COVID-19-related security impact through its vast, global voice and data networks. These range from social engineering scams in the voice network to changing communications trends and associated threats and vulnerabilities resulting from the rapid and massive transition from working in an office setting to the home. BCG research has shown that nation state actors are targeting family members of corporate executives, knowing that the unwitting and untrained family member and corporate executive are on the same insecure home network. After compromising the family member's computer, the nation state adversary attempts to pivot into the executive's laptop and infiltrate the corporate systems.

The purpose of social engineering scams is usually financial gain (to obtain credit card or bank account information) or to collect valuable identity credentials to commit fraud or compromise the security of critical corporate systems. Using our own intelligence collection tools throughout our network, Verizon captures hundreds to thousands of spam and bot calls per day and then identifies and logs them. This work has identified plots whereby hackers are offering free COVID-19 testing kits, stimulus funds assistance or other related services. Verizon works with federal agencies and partners to identify the sources of these scams to mitigate and eliminate them as they emerge and change.

Similar attacks could breach corporate security perimeters that now extend into the home, and this threat vector is actually growing as hackers move their focus toward smart devices, which are usually viewed by users as trusted. In the future, CIOs and CISOs must incorporate an evolved protection strategy with appropriate tooling or partnerships to accountfor and mitigate such attacks.

So, firstly, you should look to build ultra-, cross- or micro-segmented networks using the very latest firewall technology, allowing access to applications rather than just to networks themselves. These should follow the NIST 800-207 zero-trust strategy, i.e., servers should be isolated and end-to-end encryption and multi-factor authentication be deployed to defeat credential theft. And you need to ensure that you are looking at applications and data in both corporate data centers and the cloud.

You then need to consider upgrading the security of application and authentication data flows by separating the path of data from the path of its control, and think about enabling privileged access to applications as well. Jump hosts can support this by establishing a separate security zone to access and manage devices. And then you must also consider the true sharing and application access requirements of partners and develop models to enforce the chain of trust across assets such as supply chain, IoT devices and transactions of record. And then, perhaps most importantly, you need to build a comprehensive breach response program, implementing dynamic and up-to-date threat detection and analysis capabilities. BCG has worked closely with Massachusetts Institute of Technology (MIT) and the World Economic Forum to develop unique tabletop exercises that are able to find and fix weaknesses in breach response and business continuity programs.

Perhaps key to zero-trust security is the deployment of software-defined perimeter (SDP) protection solutions. These effectively put a “virtual wall” around your applications and devices to help better protect against potential threats. They also improve the user experience by enabling a shorter path to application, whether SaaS applications or corporate applications in hosted cloud environments, and offer both internet breakout and direct cloud access. Secure infrastructure as a service (IaaS) enclaves should also be considered, especially when you consider IaaS’ rapid growth.

We have seen multiple organizations across different industries deploying SDP solutions. Here are just three examples:

Example 1

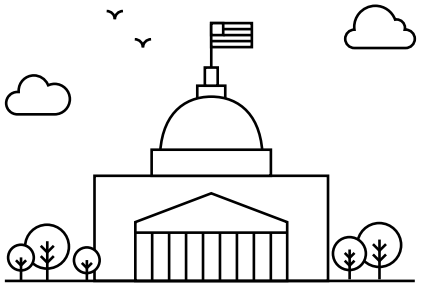
Secure access to multiple clouds for an American financial institution

Context and challenges

- Wanted the agility of cloud but prohibited by federal banking laws
- First considered move to Amazon Web Services™ but was offered access to free Microsoft Azure servers
- Challenge was to identify a solution that allows for secure access to multiple clouds

Solutions

- Test, production and shared services were set up in both clouds with access isolated by the SDP
- Helped address the security requirements of the Federal Financial Institutions Examination Council (FFIEC), and gateways in both AWS and Azure provided fast access to both clouds simultaneously



Example 2

Privileged access setup for a global medical equipment provider

Context and challenges

- Wanted a DevOps environment to enable its developers to have some server admin capabilities
- Existing policy was to have no Secure Shell (SSH) access from the user side of the network
- Additional complexity with developers located all around the world

Solutions

- SDP solution enabled developers to access the servers on all necessary ports while denying access to all unauthorized users and all unauthorized devices
- Able to maintain policy of locked-down access to SSH while also providing server access to developers

Example 3

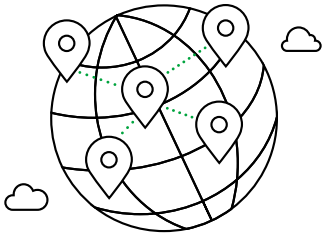
Access control for global manufacturer of telecommunications equipment

Context and challenges

- Product development process involved hundreds of globally distributed software engineers, different employee types (full-time, contractors) and disparate working models (onsite, remote, working from home)
- Required a solution that secures the software repository from adversaries yet provides global access for authorized engineers

Solutions

- SDP solution with holistic multifactor authenication (MFA), server isolation and the capability to defeat man-in-the-middle attacks was eventually adopted



Complementary solutions to zero-trust security include the deployment of network detection and response solutions for advanced inspection services, and managed detection and response solutions to help reduce the time between breach and resolution. And don't forget to test the solutions in tabletop exercises to determine response readiness.

06 A resilient end-user support model

A resilient end-user support model might not be something many organizations consider as a technical building block, but it's vitally important when it comes to the transformation agenda. No longer will users necessarily have tech support onsite or similar organizational services. The must-dos here include validating that employees, partners and customers have access to the right technologies in an appropriate way across a business. New technology rollout strategies must be created to reduce adoption friction. And then making sure that you have effective communication in place to support your end users, whether for new technology rollouts or simply with day-to-day business processes. For example, Verizon moved 700 employees from stores to inside sales and customer service representatives. Thus having protocols, trainings and tools available was critical, and such should be baked into part of the overall enterprise planning.

Best practice here includes specialist on-demand chat capabilities, how-to white papers and videos, regular communication updates, and digital customer self-service (to focus support team time on the most important issues and empowering users to solve more minor issues themselves). And ongoing communication also needs to be considered, whether via a web page, video collaboration, audio calls, streamed guide sessions or even a good old-fashioned newsletter. Most important, though, is to build a flexible support system that can adapt as user needs change.

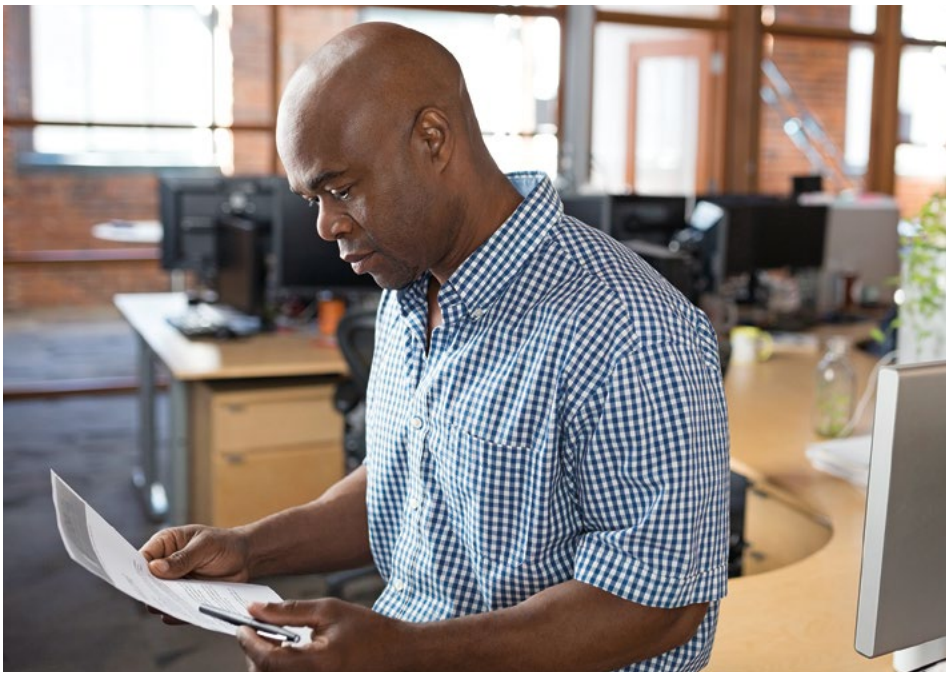
Lastly, organizations must consider the critical technology in their digital supply chain and build business continuity plans around them. If an entire business model is based on leveraging tablets and all manufacturing is shut down due to a natural disaster, pandemic, etc., what happens to the business? Tabletop exercises, war gaming scenarios and identifying gaps are critical activities every organization should undertake.

Tabletop exercises, war gaming scenarios and identifying gaps are critical activities every organization should undertake.

The time to act is now.

So, we have now outlined both the technology transformation agenda and the in-depth checklists that organizations should follow when it comes to deploying the technical building blocks that will enable remote working as business as usual. It's a lot of information, but it offers a thorough articulation of steps that organizations should take today to secure their business tomorrow.

Most important is to move sequentially. You need to understand the agenda for your organization, then run through the checklist to assess if you have most elements in place to begin—or continue—your transformation. One thing is sure: By working through the steps we've outlined here, you will be able to understand if your organization is truly ready to embrace the fourth wave of remote working in the world of "business as unusual."



In our next paper, we will look at the specific work trends underpinning the future workplace and implications on the people building blocks (as mentioned in our tech transformation agenda above) and the leadership mindsets required to emerge as remote leaders in a post-COVID-19 world, another issue that we also teed up in the first article.

Authors

Sampath Sowmyanarayan, President, Global Enterprise, Verizon Business

Jay Venkat, Managing Director and Senior Partner, Lead of North America Technology Advantage Practice Area, Boston Consulting Group

Michael Coden CISSP, Managing Director, Global Leader of Cybersecurity Practice, Boston Consulting Group Platinion

Val Elbert, Managing Director and Partner, Boston Consulting Group