

HCL



**The home is still the
office and new services
in times of crisis**



Ensuring Worker Safety and Business Continuity with HCL's Secure, Software-Defined Remote Access Offerings



Impact on Long Term Operations and Business Goals



New Services for Times of Crisis



Securing Your Remote Workforce with Software-Defined Remote Access

In a matter of a few short weeks, the COVID-19 pandemic has had a revolutionary impact on people's lives. As lockdowns and quarantines have been declared in nearly every country, the nature of work has also changed. Today, more than any time in history, there are more people working from home than ever before. Of course, this has only been possible due to the developments in modern technology. But one thing has become abundantly clear - migrating the workforce to an entirely digital and remote work model comes with its fair share of challenges.

So even as responsible organizations take the necessary steps to protect their workers and employees from the pandemic, they are taking on new risks in the digital realm. This is in the form of increasing cyber threats targeting large organizations and business entities. There is no doubt - the COVID-19 pandemic has led to an increase in cyberattacks that use malware and phishing techniques to take advantage of people's fears, and prey on an organization's weakened processes and infrastructure.

But this is only the tip of the iceberg. The pandemic has also led to a host of other organizational challenges in efficiency and productivity which make the optimal prioritization of solutions harder. In this document, we will assess the various challenges facing organizations under the new paradigm and how HCL Cyber Security & GRC services can help address these challenges. HCL is already helping organizations deploy new software solution for a resilient work-from-home model that ensures security and productivity in these uncertain times.



Impact on Long Term Operations and Business Goals

As the pandemic continues, both customers and organizations are under tremendous pressure. The need to ensure efficient operations is a major challenge as the workforce, applications, and communications switch to a working from home model. The need for a resilient business continuity plan (BCP) has never been higher. But in most cases, traditional BCP can only go so far, and as global lockdowns extend, the stress is ever increasing.

In the face of this impending threat, corporates know that they need to revitalize and reimagine their BCP in order to avoid or endure the broader economic crisis as much as possible. This begins with an increased focus on optimizing operations, reducing expenses, and ensuring customer experiences. But this is only possible if the corporate workforce can securely deliver results while working from home. Consequently, the need to maximize productivity and security while working from home go hand in hand and have become a critical business goal.

The risks associated with working from home pose a major obstacle in this regard for organizations in every sector. Recently, the American space agency NASA reported that they experienced a major rise in cyber-attacks, a majority of which was coronavirus related attempts at email phishing and malware injections. This trend is further exacerbated since the distribution of a remote access workforce significantly magnifies the cyber-attack surface. The burden falls on corporate IT teams to ensure enterprise level security across high volumes of decentralized systems. Not an easy task to accomplish.

Corporate IT teams lack the necessary capability to control a home-based IT environment as well as they can in an enterprise setting. As the number of exposure end-points increase, their ability to secure data, equipment, and communication networks is further stretched thin. This isn't just a possibility but a fact. In mid-March, we learnt that criminals had targeted consumer-grade routers from D-Link and Linksys to compromise home network security. As a result,

users attempting to access such as Amazon AWS, Bit.ly, and Google were redirected to malicious spoofed domains. And these are only the cyber threats that have been discovered so far. Being vigilant in the face of such cyber threat is the highest priority when attempting to design a resilient BCP. It's important to note that the risk isn't simply on the user or the organization, but also their customers and the overall business reputation. In general, there are three critical challenges faced by any enterprise:



Limited Infrastructure

- ▶ Existing systems lack scalability and encounter capacity issues
- ▶ Data center face connectivity problems restricting productivity
- ▶ Traditional VPN infrastructure is vulnerable to digital threats
- ▶ Network traffic is opaque with zero-visibility leading to high risks



User Activity/Productivity

- ▶ Monitoring user activity and ensuring productivity is restricted
- ▶ Protecting the end users from falling prey to phishing attacks is impossible
- ▶ Critical user credentials shared between co-workers risks a malicious attack



Secure and Seamless Application Access

- ▶ Securing enterprise application and access for remote users is lacking
- ▶ Undertaking a granular control of traffic to internal applications across networks, including SaaS applications is limited
- ▶ Monitoring third-party access to enterprise environment is also restricted



New Services for Times of Crisis

At HCL's Cyber Security & GRC Services, our goal is to empower our customers so they are prepared for extreme situations, ensuring uninterrupted operations and continued business continuity. We work closely and continuously with our customers to assess their individual challenges and offer a personalized solution to address their most pressing problems.

This involves a comprehensive review and assessment of their existing challenges and close collaboration to mitigate the same. HCL's solutions are focussed on meeting the top three priorities for any organization facing challenges:



Ensuring rapid enterprise transformation at reasonable costs

With HCL's expertise as a managed security service, customers can easily acquire the right security strategy that is designed to solve their immediate challenges while also being sensitive to cost and budgetary requirements caused by these trying times.



Offering users peace of mind with best-in-class security measures

HCL's solutions enable seamless and secure end-user access to enterprise applications across the cloud while offer the same user experience as they did while working from office. This not only helps maintain their productivity but also keep them motivated and engaged against any disruptions.



Supporting the safety and health of users everywhere

HCL's approach adheres to every safety guideline to offer privileged users uninterrupted and easy accessible service. We securely collaborate with enterprise teams to ensure that users do not need to rely on alternate solutions or "shadow IT" in case of any service disruption.

With these priorities in mind, business leaders can begin to take the steps necessary to ensure the longevity and stability of their organizations. Here are the four immediate steps they need to take:

Ensure existing security laws to be effective

Enterprises should ensure that the end-users are abiding by the security laws laid down at the enterprise level. They also need to check that the pertinent security controls implemented on end-user devices are up-to-date for maximum efficacy. In turn, users should follow the security guidelines diligently and inform their IT team if they experience any malicious activity on the network security controls.



Assess their existing IT infrastructure and system

Enterprises should undertake a thorough and honest evaluation of their existing infrastructure systems and capabilities. Using this assessment, they should proceed to gauge the essential technologies required for them to extend and improve their work-from-home policy.



Define a target state for both the short and long term

Business leaders need to carefully evaluate their technology roadmap, adopting the right strategy which ensures that security policies are aligned to business goals. This is all the more necessary keeping in mind the volatility of near future scenarios. Organizations should also evaluate such solutions that can support them in the immediate situation as well as be capable of long-term scalability and stability.



Correctly execute extended enterprise security measures

Despite any strategic and technological advice or solution that an organization adopts, it is incomplete without the correct planning and execution. Software based, cloud-led strategies are critical in enabling enterprises to establish the right security solutions without wasting much time in design and implementation.

The realities of the new era have positioned organizations in a battle on two fronts – operational efficiency and risk management. In fact, the challenges of today demand that organizations be more agile, flexible, efficient, and cost-sensitive than ever before. This kind of radical and difficult transformation requires solutions that are not only innovative but also built on experience and best practices so they can scale over time. The period during and after the COVID-19 pandemic is fraught with such challenges. Enterprises have no choice but to adopt security policies that help them achieve all these goals, and this requires finding the right technology partner.



Securing Your Remote Workforce with Software-Defined Remote Access

Most enterprise solution advocate the adoption of virtual private network (VPNs) to provide secure, encrypted channels for data and communications. As millions in the workforce shift to remote access work models, VPNs have become a standard add-on in the home office. The assumption in nearly every case is that this will establish a secure IP transport channel that encrypts and protects valuable enterprise data. There is a predominance of trust in this solution which can all too easily be misplaced.

Enterprises can secure their remote IT environments with software-defined remote access, there is no need for such an assumption. They can accelerate their strategic security programs to deploy a zero-trust strategy with privileged access management. This will not only ensure that only authorized users are given access to specific resources in a secure manner but also that this access can be provisioned across critical application, data, and network resources. By using a software-defined remote access system, IT teams can not only optimize network traffic but secure their user data and brand reputation.

This approach offers enterprises a host of benefits, such as:



Secure Access to All Applications for Remote Users

- ▶ Direct the users connecting from home to internal apps on cloud and SaaS apps through cloud-based web access services
- ▶ Provision secure connections to applications without any need to define policy by IP Address or ACL
- ▶ Provide micro-segmented access from user to application in order to protect internal applications by making them invisible and unexposed to the internet



Protecting Users from Phishing Attacks

- ▶ Provision a cloud-based solution that will be able to integrate better with O365 and G-suite
- ▶ Establish AI based identification of phishing mails, phishing incident response, federation, and alerts to end-users
- ▶ Integrate automated and one-click remediation for administrators
- ▶ Assure advanced protection for business emails against malicious attacks



Extending Privileged Access from Office to Home

- ▶ Integrate existing Privileged Access Management solution with a Virtual Desktop Infrastructure (VDI) environment to provision access to critical environment remotely
- ▶ Enforce least privilege by elevating rights to applications and commands instead of end-users
- ▶ Delegate privileges by deploying fine-grained policy controls
- ▶ Simplify single sign-on feature across various platforms like Windows, Mac, and Linux

HCL has already deployed these solutions to great effect for a number of organizations in a variety of industries and locations, such as:

- ▶ One of the worlds' largest automotive manufacturers of luxury vehicles
- ▶ An end-to-end, fully integrated biopharmaceutical solutions company
- ▶ A leading American multinational manufacturer of household cleaning products
- ▶ A global leader in healthcare safety and medical technology enterprise
- ▶ A global company engaged with dairy nutrition and export

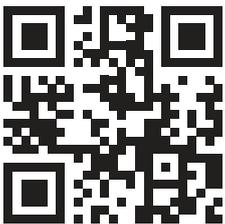
Contact an HCL Ideaprenuer today to learn more about how HCL's portfolio of innovations can help transform and revitalize your organization amidst the challenges of the COVID-19 pandemic.



HCL Technologies (HCL) empowers global enterprises with technology for the next decade today. HCL's Mode 1-2-3 strategy, through its deep-domain industry expertise, customer-centricity and entrepreneurial culture of ideapreneurship™ enables businesses to transform into next-gen enterprises.

HCL offers its services and products through three lines of business - IT and Business Services (ITBS), Engineering and R&D Services (ERS), and Products & Platforms (P&P). ITBS enables global enterprises to transform their businesses through offerings in areas of Applications, Infrastructure, Digital Process Operations, and next generation digital transformation solutions. ERS offers engineering services and solutions in all aspects of product development and platform engineering while under P&P. HCL provides modernized software products to global clients for their technology and industry specific requirements. Through its cutting-edge co-innovation labs, global delivery capabilities, and broad global network, HCL delivers holistic services in various industry verticals, categorized under Financial Services, Manufacturing, Technology & Services, Telecom & Media, Retail & CPG, Life Sciences, and Healthcare and Public Services.

As a leading global technology company, HCL takes pride in its diversity, social responsibility, sustainability, and education initiatives. As of 12 months ending on March 31, 2020, HCL has a consolidated revenue of US\$ 9.94 billion and its 150,000+ ideapreneurs operate out of 46 countries. For more information, visit www.hcltech.com



www.hcltech.com