avanade

Elastic Digital Workplace for the Microsoft Platform

Remote working and the first step to Workplace Experience transformation in exceptional times

COVID-19 is a global crisis, evolving at unprecedented speed and scale. It's creating a universal imperative for governments and organisations to take immediate action to protect their people. The virus continues to spread rapidly, with scores of countries impacted and thousands of new cases reported daily.

avanade

No industry is immune. All are grappling with the immediate impacts of COVID-19 in varying degrees of severity and complexity. Travel and tourism companies are experiencing a significant hit to their business. Retail and consumer goods organisations are dealing with stock shortages due to production delays, disrupted manufacturing and broken supply chains. Industry and technology conferences, along with large group gatherings, are being postponed or cancelled entirely. To protect their people, organisations are implementing travel bans, restricting who they let into their offices, and re-examining how their workplaces operate, and how their people work.

Experts don't know how long it will take to contain the virus. Leaders must prepare for the short term while also developing new capabilities and ways of working that will seamlessly enable longer-term changes to how they operate.

The time to act is now.

This document outlines the practical steps you should take, whether you're getting started or already using the Microsoft 365 platform.

avanade

Protect your people and your productivity

In this climate of crisis, your decisions not only determine how you operate in the near term, but also significantly impact how you'll operate in the future. Smart leaders will seize this opportunity to take swift action to navigate the crisis to avoid business disruption and potential revenue loss, forge new levels of trust with their workforce, and position their businesses for greater resiliency and productivity in the future.

An important first step is to begin planning to enable a remote workplace at scale. Develop and provide clear guidelines to your people about self-quarantine and/or travel restrictions. Prepare for a larger than normal percentage of employees to be on sick leave. Each company, industry and region will have different needs and requirements for a workplace with people management, customer service, data management and business continuity. But there are three major foundations that all organisations should consider.

1. Protect and empower your people:

Modernise your workplace technologies to enable scalable and sustainable remote working. Evolve ways of working and employee experiences to fit the new context. Empower your people through skills development, delegated authority and a focus on their well-being.

2. Serve your customers' core needs:

Adapt to changing global and local conditions by serving your customers' core needs, including being transparent in your operations and compassionate in your engagements – all of which will create deeper, more trusted relationships.

3. Establish business continuity:

Ensure supplier relationships and business-to-business processes are effectively supported. Develop new business processes to adapt to new ways of collaboration and decision-making. Use automation and AI to create capacity and augment your valuable human workforce.

avanade

Start today: The Elastic Digital Workplace for the Microsoft Platform

Our Elastic Digital Workplace solution is the first stage of a comprehensive Workplace Experience transformation, creating a highly extensible environment that allows you to quickly scale and dynamically adapt to changing business needs based on global and local conditions.

The first step is a quick Elastic Digital Workplace assessment. This allows your organisation to quickly evaluate your capabilities across multiple dimensions and prioritise where to focus.

While many organisations have some form of remote working environment, most have never conducted a full remote worker business continuity test, much less developed the culture, technology, experiences, communication and policies that will have to work together nearly simultaneously in today's global context.

To get started, consider the following six questions:

1. How prepared is your organisation to equip your employees to work effectively from remote locations?
2. Do you have a team dedicated to helping your employees work remotely?
3. Do you provide clear guidance to your remote workers on home office/network setup and troubleshooting?
4. Do you have a clear mobile device and application strategy that provides your employees with guidelines on using personal (and company-owned) devices?
5. Do you have collaboration solutions that seamlessly and securely connect with your customers and strategic partners?
6. Do your solutions for employee "moments that matter" (e.g., on-boarding, device failure, real-time expert guidance) work in a remote scenario?

avanade

The Elastic Digital Workplace for Microsoft roadmap outlines six dimensions that have proved effective in quickly transitioning to a remote workplace environment:

- **Culture and adoption**
- **Elastic collaboration**
- **Virtual work environment**
- **Seamless networking**
- **Distributed continuity**
- **Accelerated security**

avanade

Enhance workplace practices

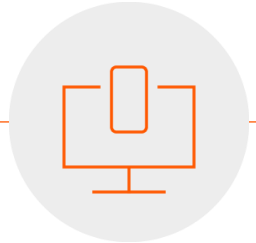
Culture and adoption

Adapt leadership practices and behavioural norms for the current context while protecting the culture and engagement of your distributed workforce.

Elastic collaboration

Rapidly deploy or extend Teams, SharePoint and OneDrive to enable collaboration and remote working at scale.

Use workplace analytics to help understand adoption and use this as an opportunity to improve employee experience, leading to improved customer and partner experiences.



Virtual work environment

Evaluate your network, accelerate device deployment and leverage virtual environments such as Microsoft Virtual Desktop to support increased mobile demand.

Seamless networking

Enable reliable and secure remote network connectivity and a modern access mechanism to your employees, supply chain and your customers.

Integrate detection, protection and response capabilities to monitor, remotely support and keep your remote workers protected.

Distributed continuity

Enhance business continuity plans to include a reduction in workforce, travel restrictions and large-scale remote working environments. Use Power Apps to rapidly fill urgent needs.

Accelerated security

Large-scale remote working brings about additional security risk as employees and partners stretch the boundaries of where they work and how they access your corporate information.

The threat landscape has evolved as rapidly as the adoption of remote working, and enhanced security controls and measures are needed to protect your people and your business.

Culture and adoption

Avanade has become accustomed to a highly distributed and cloud-based way of working, which we have evolved over the years. We rely on Microsoft 365 to create, connect and collaborate. We have a staff of highly trained digital workplace adoption professionals who teach people how to work effectively in remote environments.

Our people are accustomed to collaborating remotely on a continual basis with their co-workers worldwide. However, each organisation will have its own nuances. At a more virtual company, your best gig economy workers might be worried about continuity of work and a paycheck during the crisis. In a company with workers mainly in physical locations, there may be concerns as basic as hand sanitizer and avoiding in-person meetings.

They need to feel safe while working, the most basic of human needs. Once these risks are addressed and realised, only then can they begin to work on technology training and adoption.

Over the first week, implement the following:

- Support leaders in modelling virtual behaviour: Take special care to direct leaders to exemplify remote-working behaviours. Coach them to schedule Teams meetings with video and to move away from working on local versions of data and documents to cloud-based applications and storage. Pay attention to the small things like coaching on video meeting etiquette and guidance on home network bandwidth.
- Recognise working from home is not the same as remote working: Employees working from home are likely taking on additional responsibilities and may have increased distraction. Keep the well-being of employees front-and-centre, and consider things like flexible work hours, shared roles and postponing non-essential work.
- Keep engagement high: Use Teams video to replace the drop-ins and informal conversations essential to business continuity. Embrace the fun by encouraging project teams to run virtual team-building events and competitions. Incorporate photos of kids, pets or other personal interests into virtual meetings and town halls.

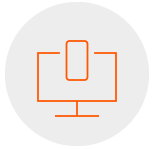
Elastic collaboration

The new reality is that employees need to get work done with zero face-to-face interaction. They need tools that allow them to make decisions and produce documents, presentations and spreadsheets efficiently. Building their workday around a platform that allows multi-modal communications and simultaneous document creation on any device is the way towards a new normal of broad-spectrum collaboration.

Microsoft Teams enables multi-user texting, voice calling and video conferencing on the desktop, in the browser, and on tablets and smartphones. When people can hear and see each other while they take notes or produce results, they are more engaged, less distracted and better equipped to accomplish their tasks.

Actions to take immediately include:

- **Adopt and measure collaboration:** Starting today, expand the existing footprint of collaboration and communication capabilities to provide large-scale employee coverage. Restructure SharePoint to help people work on documents and share know-how from home. Consider a digital hub to take away some of the friction of day-to-day tasks.
- **Determine your collaboration strategy:** Review standard governance and policy guidelines for safe and compliant collaboration with Teams and modify them for the needs and culture of your organisation. Determine your roll-out strategy and how these new users will be trained and supported as they shift into a new way of working. Provide guidance on the best headsets and cameras that will support a quality remote working experience.
- **Enable rapid adoption of the new platform:** Train and support the leaders in the organisation who will model behaviour for their direct reports and the pyramids below them. Help them understand the etiquette and rules of the new paradigm and show them how to encourage and reassure their teams that they can get their work done with speed and quality by using their tools well. Identify champions at all levels who can help their peers to feel comfortable and productive.
- **Cross-business enablement:** Identify key business-to-business contacts and relationships across your ecosystem. In the next 24 to 48 hours, assess current virtual meeting capabilities (web conferencing, video services) and deploy a pilot of video and messaging bridging services for seamless interaction with partners, suppliers and customers. Create integrated communications and training materials to enable business users to adopt the shift in work style. Use data and analytics to identify opportunities to increase adoption and improve employee experiences.



Virtual work environment

Virtual work environments provide employees with the key resources they need to be productive, such as a secure laptop, and provide seamless access to corporate applications and data.

Key aspects that should be addressed within the first two weeks are:

- **Coordinate virtual work environment:** Start by educating workers with security initiatives and open communication with operational teams. This means making sure that access policies, permissions and audit logs are in place to enable the use of a virtual work environment. You can manage user identity, network security and device security together.
- **Explore virtual desktops:** Within the first week, explore and implement Microsoft Virtual Desktop solutions, which offer virtualized workspaces that can extend across boundaries while allowing secure access to remote applications and data for employees who don't have access to secure mobile devices. Your ability to enable these rapidly will depend on whether your corporate applications are located primarily on your internal corporate network or are cloud-based.
- **Enable large-scale virtual sessions:** Enable interactive broadcast and web conferencing for one-to-many events with Teams Live Events to support the shift from physical to virtual workshops and conferences. Identify and train high-touch session facilitators to support the best possible user experience. Consider your needs for production assistance. For more interactive engagement with groups under 250 participants, use regular Teams meetings.
- **Augment remote working experience:** Establish dedicated service management teams enabled with remote user-specific standard operating procedures/ FAQs to effectively support the workforce in a high-touch environment using offerings from Azure Marketplace. Establish specific service level agreements and policies to manage incidents and service requests.
- **Device enablement and mobility acceleration:** Prioritise enabling workers who have critical roles in driving the business by ensuring they have the tools and access they need. Reclaim devices from users with more than one device and use contractor devices or explore creative sourcing options such as Device as a Service from providers such as Dell, HP and Lenovo. Are you starting by enabling users with corporate-approved, secured and managed devices only, browser access or allowing a "bring your own device" policy? Balancing the need to quickly enable virtual work environments can be further orchestrated with management solutions such as BitLocker or Intune. Additionally, how user identity is managed and controlled (modern authentication and multi-factor authentication enabled for specific device access) will govern experience and training needs.

Seamless networking

When many of your employees are working remotely, they may encounter network issues such as bandwidth challenges with other family members at home, slow corporate VPNs and blackouts due to worldwide volumes. Seamless connectivity is key to ensuring the work-from-home experience is equal to or better than the office experience. Users need to be properly educated on security while working at home; this becomes harder to control when a worker is outside the corporate network. Reliable connectivity to corporate networks, cloud assets and strategic partners is key to working productively from home. Over the last few weeks, video and audio conferencing have jumped by 80% – this strains a user's ability to access resources from home. Make sure that your team is ready for and understands these issues are to be expected and acceptable.

Over the first week, implement and explore the following:

- Explore modern remote access mechanisms: Rapidly complement your traditional VPN technology with new cloud remote access solutions such as Microsoft Azure Application Proxy, Microsoft Always On VPN, Zscaler and other providers.

  These new approaches will improve remote worker experience, performance and security while mitigating the risks of capacity issues and single points of failure.

  With VPN solutions, enable split tunnelling where possible so users can get the fastest access to cloud services. If internet browsing threat protection and control are concerns, explore cloud-based internet proxy services that are able to perform high-compute tasks such as SSL inspection at cloud scale.

- Remote and home networking: Provide clear and prescriptive guidance to employees about broadband connectivity options and packages in their home locations. Consider subsidising higher bandwidth and quality of service solutions. As most network issues start at home, provide guidance to employees on the best Wi-Fi home network solutions and configurations. Ensure users at home are following corporate guidance to secure their network. If using commercial routers, work-from-home employees need to change the default password on the router to a strong password to ensure corporate data safety.

- Mobile connectivity: Many users may have to rely on mobile networks for connectivity and the use of mobile apps to connect to the corporate network. Mobile users face challenges such as cellular network coverage, mobile access, security and computer tethering. Educate users that mobile tethering can cause additional data charges if they exceed their plan limits. To allow users to access the corporate network, two-factor authentication such as Microsoft Multi-Factor Authentication should be used to secure identities. To protect corporate information, Microsoft Mobile Application Management service can be used to protect corporate and/or employee-owned devices.

- Internal network: If possible, use the corporate backup ISP connections to route internal communication traffic such as cloud backups directory synchronisation, file storage and such. Try implementing traffic shaping on the edge for unified communication traffic if using central egress and ingress. Remove non-essential devices from the internal network to reduce as much overhead as possible.

- Partner connectivity: Establish a SWAT team to quickly provide, or to expand, business-to-business connectivity solutions to strategic partners, including identity provisioning considerations.

Distributed continuity

Distilled to one essential message, your workforce is looking to trust you. And they will trust you if they believe leadership cares for them and humanity as a whole. But beyond caring, leaders must show they have a plan. You don't have to know everything, but you do need to be transparent about what's driving decisions. A leadership team that looks ahead proactively, and responds rather than reacts, goes a long way toward helping a workforce in volatile times. This requires assessing and monitoring a quickly evolving environment, making timely business decisions and communicating clearly and prescriptively to your people on how to navigate the situation.

Ongoing actions include:

- **Enable a more distributed virtual way of working:** Use Teams to enable virtual connections among employees, suppliers and customers. For example, we're working with healthcare providers to enable virtual video consultations around patient cases, which cuts down the need for face-to-face meetings and reduces the risk of spreading disease. This can be especially effective if key resources are subject to quarantine or sheltering in place.
- **Employee contingency planning:** Keep a check on employee health by having regular employee touchpoints. At the same time prepare contingency plans to cover for absence due to sick leave for critical employees. To avoid a single point of failure, encourage employees to share and record daily updates and progress on critical deliverables in Teams or OneNote and keep track of tasks though Planners.
- **Leverage Power Platform:** Use Power Platform for rapid app development and continually provision information for the most urgent needs.

Accelerated security

At an unprecedented rate, businesses are forced to rethink a work-from-home security strategy due to recent events. This brings about additional security challenges in the form of risk as we see new populations of employees stretching the boundaries of where they're performing their work tasks and how they're accessing potentially sensitive information. In many cases the processes and technology that empower businesses to enable employees to work from home were not designed to meet the needs of today's threat landscape, and the security training is not focussed on the unprecedented increase in targeted social engineering attacks.

Some key risks you need to be aware of and focus on are:

- **Social engineering:** This is one of the greatest risks your employees, contractors, third parties and partners will face during this time. With the increase in malicious activity linked to the COVID-19 pandemic, your remote workers need to be aware that these social engineering attacks won't just be phishing email, but could also be calls, texts and fake news online, all with the general aim of stealing credentials or corporate information. Implement additional cyber awareness training to help your people to be extra vigilant.
- **Business continuity:** Malicious threat actors may target VPN ingress points with a distributed denial-of-service (DDoS) attack. Microsoft's Application Proxy and Always On VPN service comes with DDoS mitigation from Microsoft built-in and can be rapidly enabled to mitigate.
- **Sensitive information workers:** Sensitive use cases such as financial or governmental workers may not be able to safely and securely access systems to perform their jobs. A combination of technology solutions can provide the layers of security and segregation if required to enable them to work from home
- **Information protection:** Bring your own device (BYOD) users may not have sufficient security controls on their devices to protect information from attacks. Intune MAM without enrolment can be used to protect your corporate information on BYOD devices.
- **Endpoint protection:** VPNs could become compromised by users who have fallen victim to a targeted social engineering attack. Deploying Microsoft's Defender ATP can quickly protect your remote workers from advanced threats and zero-day attacks.
- **Weak passwords:** These represent a consistent risk to all organisations, especially those that do not deploy a multi-factor authentication solution. With the shift to remote working, if your inbound access mechanisms such as VPNs and web services are only protected with a username and password, then there is increased exposure during this time when the entire workforce is using those mechanisms. Microsoft's Azure AD Password Protection can be used to prevent well-known passwords and prevent weak passwords from being used.
- **Policies and behaviours:** Review and assign policies to ensure and enforce secure behaviours. In parallel, provide employees with clear, prescriptive guidance to help them adopt the behaviours required to remain secure in remote working scenarios.
- **Detection and response:** Security detection and response mechanisms need to evolve to meet the new remote workforce's needs across devices and new access mechanisms. Microsoft's Azure Sentinel can be quickly enabled to provide security monitoring and leverages AI and machine learning to piece together threats across the remote workforce.

How do I get started?

Every deferred decision has real consequences for people, business and society. Time is of the essence.

Here's a quick summary of how you can rapidly create a highly effective Elastic Digital Workplace:

01

The top priority is to immediately help employees adapt to remote working and optimise the experience to maximise productivity, including how to effectively run large and small virtual meetings.

02

Immediately deploy or scale the use of collaboration tools, such as Microsoft Teams, and provide targeted prescriptive guidance for effective productivity for the remotely connected workforce.

03

Organise an Elastic Digital Workplace task force today with representation from the business, Legal, HR, IT, Marketing and Communications, and Security.

04

Equip traditional desktop workers with mobile solutions and implement virtual desktop solutions from the Microsoft ecosystem to provide secure remote access to applications and data.

05

Use the experience available through Avanade and take advantage of limited free-use solutions from our ecosystem of strategic partners and providers to rapidly scale your capabilities to meet the new demand.

avanade

Further information

- COVID-19 – we're here to help
- Microsoft Teams Rapid Deployment Resource Centre
- Workplace Experience

North America
Seattle
Phone +1 206 239 5600
America@avanade.com

South America
Sao Paulo
AvanadeBrasil@avanade.com

Asia-Pacific
Australia
Phone +61 2 9005 5900
AsiaPac@avanade.com

Europe
London
Phone +44 0 20 7025 1000
Europe@avanade.com

About Avanade
Avanade is the leading provider of innovative digital and cloud services, business solutions and design-led experiences on the Microsoft ecosystem. Our professionals bring bold, fresh thinking combined with technology, business and industry expertise to help make a human impact on our clients, their customers and their employees. We are the power behind the Accenture Microsoft Business Group, helping companies to engage customers, empower employees, optimize operations and transform products, leveraging the Microsoft platform. Avanade has 38,000 professionals in 25 countries, bringing clients our best thinking through a collaborative culture that honors diversity and reflects the communities in which we operate. Majority owned by Accenture, Avanade was founded in 2000 by Accenture LLP and Microsoft Corporation. Learn more at www.avanade.com

avanade