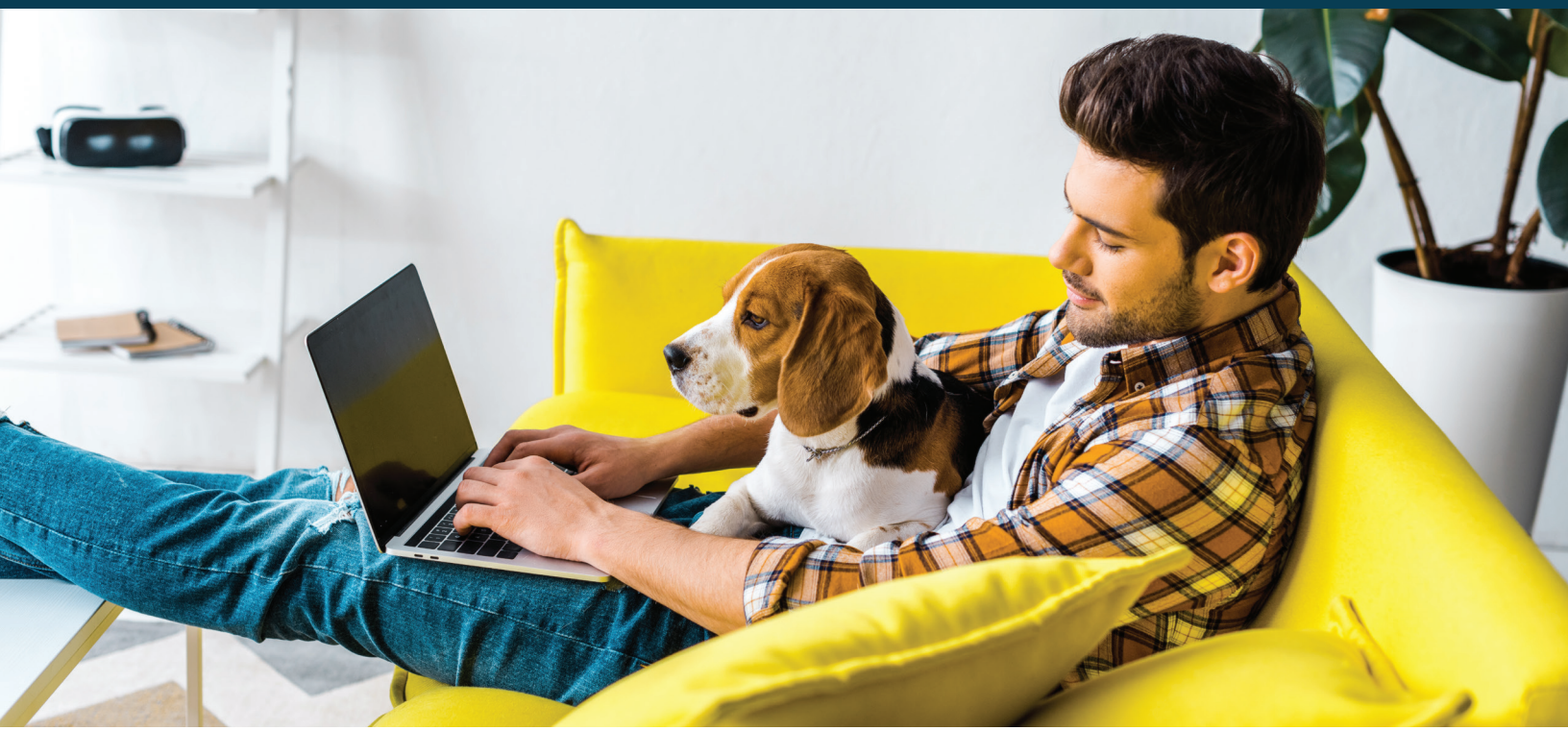
Use Case: Amazon WorkSpaces For Business Continuity



CHALLENGE:

During COVID-19, many organizations had to declare work-from-home overnight to protect employees and prevent the spread of the deadly virus. Business owners and organizations who are fortunate enough to enable a remote workforce and continue operations now face the need to adapt to the changing business environment in order to minimize disruption. Remote working can always be a challenge for team members, system infrastructure, and the IT security team.

During time-sensitive emergencies, e.g. COVID-19, the primary pain points that need to be addressed are scalability and security. The infrastructure team needs to confirm whether the current network and infrastructure has the capability to handle the volume of all employees working remotely. Without compromising on performance, access, and security, virtual teams need to have access to tools, documents, and technology in order to minimize work disruptions and maintain productivity. While many teams prepare for a change in the work environment, it has never been done at this scale and under such critical circumstances. With little time to prepare, it is unlikely many infrastructure teams had enough time, resources, and manpower to enable the facility, let alone procure new remote devices.

SOLUTION:

Amazon WorkSpace is an optimum solution to address this challenge. A fully managed, Desktop-as-a-Service (DaaS) solution, WorkSpace provides users with Windows or Linux desktops in minutes and can provide thousands of desktops to workers across the globe. Amazon WorkDoc is a secure content creation, storage, and collaboration service. Users can easily create, edit, and share the documents they need to get their job done with WorkDoc. Both services can run almost anywhere and on almost any device, including on a home PC, laptop, and tablet. Together, WorkSpaces and WorkDocs provide teams with the ability to securely and collaborate with colleagues from anywhere. WorkSpace & WorkDoc now offers 50 users at no charge, making it a cost-efficient option. Both offers are for new customers that have not previously used these services and are available through June 30, 2020.

idexcel

SECURITY WITH AMAZON WORKSPACE

Amazon WorkSpaces conforms to the AWS shared responsibility model, which includes regulations and guidelines for data protection, ensuring optimized security protocols are in place. AWS is responsible for protecting the global infrastructure that runs all the AWS services. With maintained control over data hosted on this infrastructure, including the security configuration controls for handling customer content and personal data, WorkSpace is a highly secure and reliable solution for enabling a remote workforce. AWS customers and APN partners, acting either as data controllers or data processors, are responsible for any personal data that they put in the AWS Cloud. Refer to Table 1.a below for Data Security implementation options.

Data Security Implementation Options	Infrastructure Security Implementation Options:
• Use Multi-Factor Authentication (MFA) with each account. • Use TLS to communicate with AWS resources. • Set up API and user activity logging with AWS CloudTrail. • Use AWS encryption solutions, along with all default security controls within AWS services. • Use advanced managed security services such as Amazon Macie, which assists in discovering and securing personal data that is stored in Amazon S3.	• Network isolation by provisioning VPC • Isolation on Physical hosts using hypervisor • Authorization of corporate users managed through Active Directory • Provision VPC Interface endpoint • Implement proper IAM Roles & Policies • Use advanced managed security servicessuch as Amazon Macie

Table 1.a

Table 1.b

As a managed service, Amazon WorkSpace is protected by the AWS global network security. You use AWS published API calls to access Amazon WorkSpaces through the network. Clients must support Transport Layer Security (TLS) 1.0 or later. AWS recommends TLS 1.2 or later. Refer to Table 1.b above for Infrastructure Security implementation options.

WHY IDEXCEL

Increased Workforce Accessibility: Idexcel can setup a secured WorkSpace environment to allow resource accessibility for remote users.

Holistic Strategy: Amazon WorkSpace simplifies your desktop delivery with reduced overhead by eliminating many administrative tasks associated with managing your desktop lifecycle including provisioning, deploying, maintaining, and recycling desktops.

Secure System Infrastructure: Our security team will also provision the entire security parameter for the WorkSpace.

Flexible Scalability: We also manage the WorkSpace environment and create a strategic solution for scaling up/down to accommodate changes in demand needs.

Cost-Conscious Solution: Reduce expenditures by eliminating the need to over-buy desktop and laptop resources

Uniquely Tailored Approach: Providing on-demand access to cloud desktops that include a range of compute, memory, and storage resources to meet your users' performance needs.