Secure Remote Worker Environment

Build a secure desktop environment for remote workers to access key line of business applications and data.

1. Users connect to their desktop using the Amazon WorkSpaces application by supplying a username, password, and MFA code.


3. MFA code is authenticated against MFA service’s RADIUS server. For example, OneLogin.

4. Users are connected to their desktop through Amazon WorkSpaces.

5. Users access core systems and files hosted on Amazon EC2 and Amazon FSx.

6. Group policy is implemented in Active Directory to prevent unwanted activities, such as printing to local printers from Amazon WorkSpaces.

7. Domain Controller DNS forwards to Amazon Route 53 VPC DNS resolver with applied Route 53 Resolver DNS Firewall rules.

8. Outbound internet traffic is filtered first by AWS Network Firewall, then sent through a NAT gateway and internet gateway to the public internet.

9. Firewall rules are set up to block outbound traffic to unwanted sites (such as file-sharing platforms) to prevent data leaks.