HIRING A YOLKER

Your Security Plan

ENABLING A SECURE REMOTE TEAM TO THRIVE

1 The Right People

Background checks on all developers before we onboard. This includes:
Police checks.
Credit checks.
Reference checks.

2 The Right Process

All parties should be clear on their duty and obligation to protect data and privacy at all times. Before starting any engagement we ensure:

- NDA's are signed by Double Yolk.
- A Code of conduct is signed by all developers with employment contingent on strict adherence.
- Training is provided to all developers on threat identification and mitigation.

3 The Right Equipment

All laptops:

- Are encrypted using Bitlocker 256-bit.
- Are configured to auto-update any firewall / Antivirus upgrades.
- Are configured with 'remote-wipe systems should they be stolen or compromised.
- Are owned and administrated by Double Yolk with enterprise scale device management.
- Have endpoint detection installed to detect any suspicious behaviour.
- Have no cold storage so data cannot be removed from the laptop via hard drive or USB.

4 The Right Access

We work with you to understand your tech environment and data sensitivity to build an access plan that will work well for your remote team.

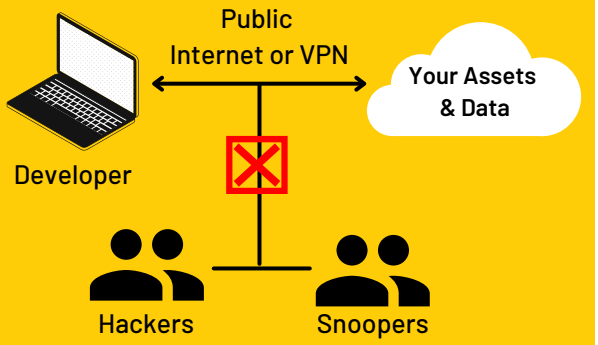
OPTIONS FOR ENSURING A SECURE REMOTE TEAM ENVIRONMENT

1 Set-up Two-factor Authentication on your repositories and systems

2FA helps prevent against the risk of password compromise. It's easy to set-up and is supported by most development tools and services.

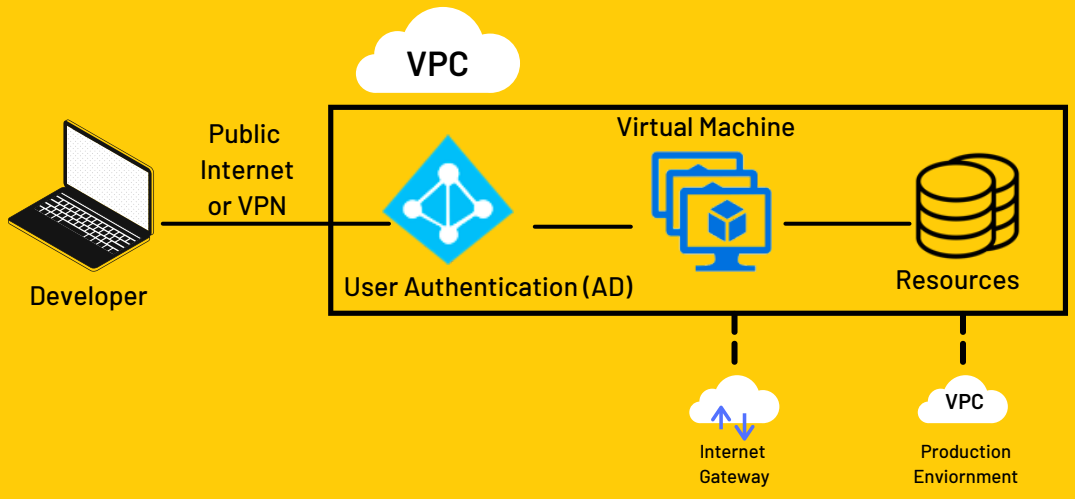
2 Use a VPN for your remote developer to connect to your cloud environment or on-premise servers

A VPN encrypts all of the data that comes from the developer's computer and device, which will render your data useless for hackers.



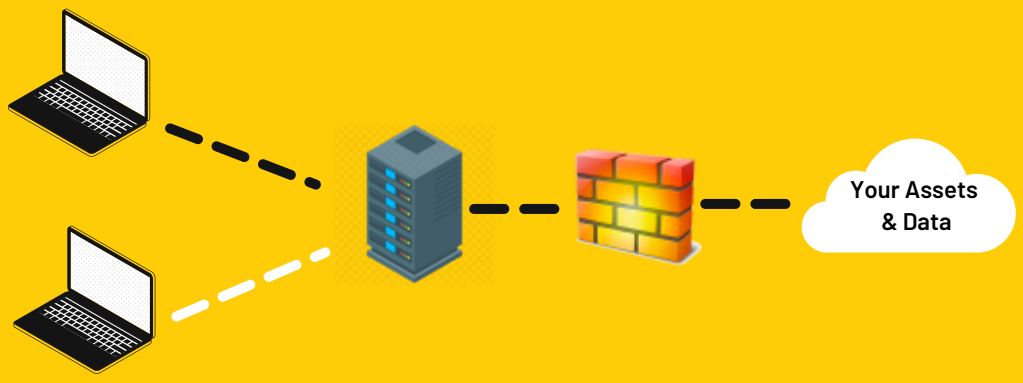
3 Have your offshore developer operate from a Virtual Machine

By leveraging a Virtual Machine you can keep a tight control on exactly what services the developer needs to access with strong security containing them. By standardizing the configuration of your virtual computers, you remove limitations of hardware or software the developers may face on their laptops.



4 Leverage a Bastion Host as the gatekeeper to your Virtual Private Cloud

A Bastion host is a server configured for the purpose of preventing unwanted attacks while permitting access to trusted traffic. It acts as the single point of entry into your protected environment.



5 Whitelist our DY Office static IP address

You can have your developers connect through our proxy server which is protected by a proxy firewall. Our server is routinely tested for vulnerabilities and pen-tested by a 3rd party every 12 months.