SECURE REMOTE ACCESS (WORK FROM HOME) SOLUTION

Security & Productivity. Connected

The COVID-19 pandemic has forced Organizations to quickly enable their employees to work remotely for an extensive period of time. Having people work remotely changes many things. This sudden spike in Work From Home scenario has exposed enterprises to serious security risks that security teams across the world are grappling with.

How do we address this?

Tech Mahindra's **Secure Remote Access (Work from Home) Solution** is a fast & remotely deployable, cost-effective, scalable & trustworthy VPN solution with CISCO Tech/DoD approved available options. Unique cloaking capability against attacks.
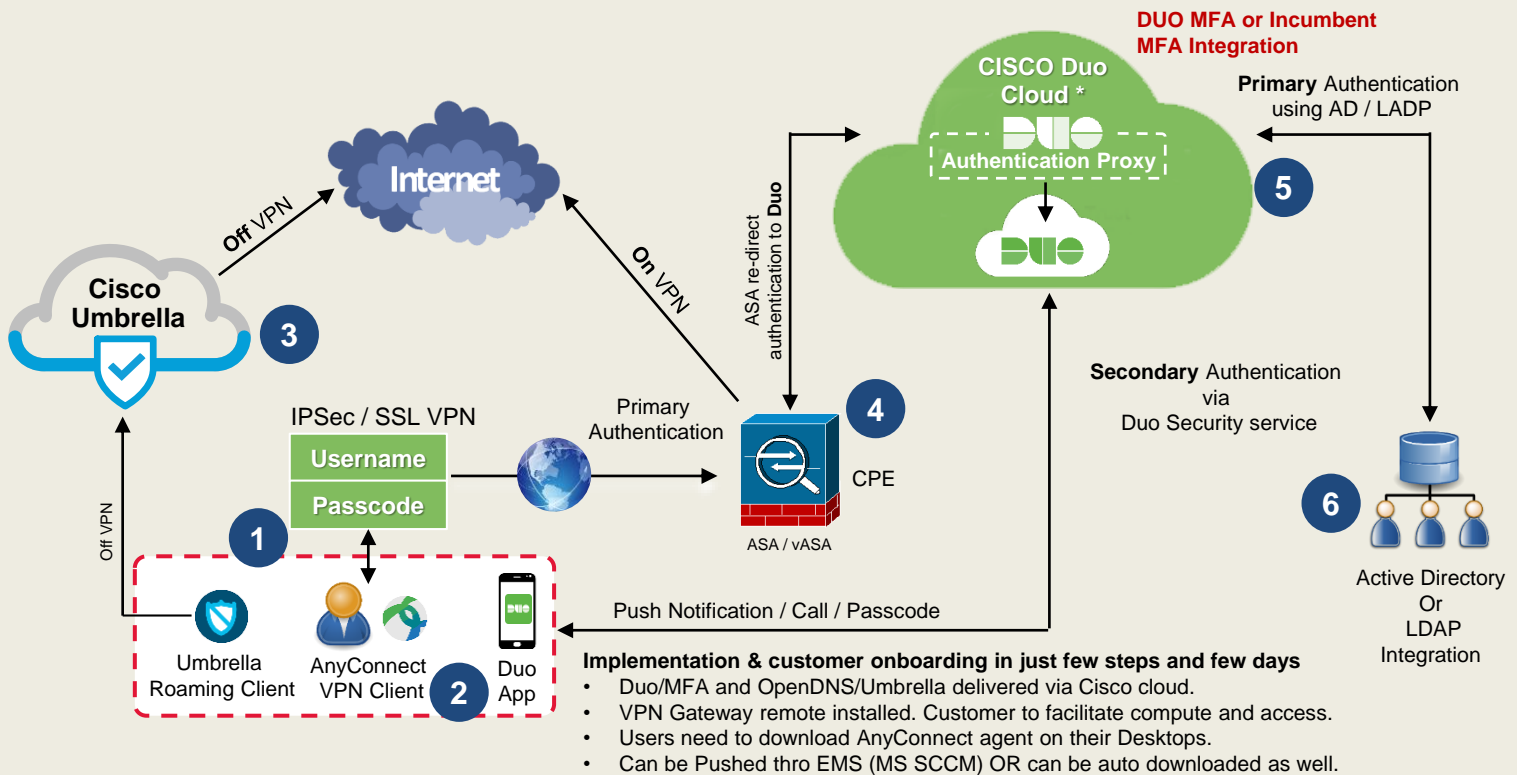
The most common risks for companies when it comes to remote workers are the following:

- Inability to ensure the physical security of a home office, coffee shop, or public workspace.

- Unable to control or ensure the security of the network that employees are using.

- Lack of training or understanding of best practices when it comes to information security for workers both at the office or at home.

- Lack of undertstanding of their role and responsibilities when it comes to working remotely securely.

- Well established procedures are being rewritten, best practices quickly rethought, and policies stretched to breaking point.

- New technology and working practices need new security measures which is managed over time. Covid-19 has not afforded us that luxury.

- Email Scams

- Attacks on remote-working infrastructure

**Connected World.
Connected Experiences.**

This Solution

- Enhances WaaS to address US-Cert specs
- A door-opener with a quick and easy sale
- Simple and focused solution which addresses foll. Issues during COVID
- Secure Network Channel (AnyConnect VPN)
- Secure Gateway (OpenDNS Umbrella)
- Multi-factor Authentication (DUO)
- End Point Protection (AMP)
- Cloaking Host Identity (Transport Access Control)

Tech Mahindra's Cisco Secure Remote Access Solution…

DUO MFA or Incumbent MFA Integration

CISCO Duo Cloud *
Authentication Proxy

Primary Authentication using AD / LADP

5

Internet

Off VPN

On VPN

ASA re-direct authentication to **Duo**

Cisco Umbrella

3

Off VPN

IPSec / SSL VPN
Username
Passcode

Primary Authentication

1

4

CPE

ASA / vASA

Secondary Authentication via Duo Security service

6

Active Directory Or LDAP Integration

Umbrella Roaming Client

AnyConnect VPN Client

2

Duo App

Push Notification / Call / Passcode

Implementation & customer onboarding in just few steps and few days
- Duo/MFA and OpenDNS/Umbrella delivered via Cisco cloud.
- VPN Gateway remote installed. Customer to facilitate compute and access.
- Users need to download AnyConnect agent on their Desktops.
- Can be Pushed thro EMS (MS SCCM) OR can be auto downloaded as well.

Solution has multiple options

Secure Remote Access Solution – I

Multi-Factor Authentication & Authorization for Remote Workers exclusive access	Integrate Secure Remote Access within existing AD/LDAP Infra	Overcome Operational Risk arising out of inadequate control and monitoring of remote user environment
User Awareness and Standard Operating Controls Integration	Can be integrated with existing MFA platforms such as Bio-Metric Access Controls	Continuous Auditing & Monitoring of end user activities to ensure information protection
Integrate the VPN, DNS and MFA logs with SOC / SIEM for threat analytics & cyber defense	Rapid deployment – 7-10 days	US-Cert compliant solution In compliance with regulatory standards

**Connected World.
Connected Experiences.**

Secure Remote Access Solution (Cloaking against attacks)

🔒 Cloaking of Asset to protect against Remote Recon Scans	🖥 Business continuity through remote workforce	⚠ Reduce operational, transactional & reputational risk
👁 Policy based access control at the network layer	👆 No network engineering & re-engineering	🏛 Approved by Dept. of Defense, USA
🖥 Rapid deployment – 7-10 days		

Business Benefits of Secure Remote Access Solution

- Cloud-based & Light-weight solution
- Push deployable within 4-7 days
- Scalable and flexible to handle surge in user volume
- Leverages existing setup
- Trusted partner – Cisco
- Compliant with US-CERT released advisories
- Cost effective & budget friendly solution
- Remotely deployable and functional with 7-10 days
- **A Very Unique but add-on optional feature that can be delivered through TechM Remote Secure Access Work From Home platform**
- **De-Identify Device across TCP environment from hackers using TAC (Transport Access Control)**
- TAC enables **"First Packet Authentication™" (FPA)**, to change network's DNA to seamlessly include identity and trust throughout network.

https://www/us-cert.gov/ncas/alerts

Why should you engage with us?

With 18+ years of experience in Cyber Security Services, 1200+ dedicated security professionals and 170+ large Enterprise clients, Tech Mahindra is in a strong position to help organizations in Security Consulting, Data Security/ GDPR services, Identity & Access Management, Cloud Security, IoT /OT Security, Advance threat management, Application Security.

Tech Mahindra has pioneered in some of the innovation in Cyber Security domain like Deep Dark Web Services, Threat Hunting, Zero Day Attack Mitigation and AI - Micro Segmentation

Tech Mahindra is a Cisco Partner & the recommended Remote Secure Worker Platform is US-Dept of Defence specifications compliant architecture

Tech Mahindra has been awarded as the most Innovative Cyber security Company in the Cyber Security Excellence awards, 2019

Tech Mahindra is recognised as leaders by leading analysts like Forrester and Avasant.

Connected World.
Connected Experiences.