Secure Remote Workforce

Securing the Remote Workforce: Cisco Secure Remote Worker was launched to provide customers and prospects a one-stop-shop to learn how Cisco can continually secure their remote workforce now and in the future with a simple, scalable, integrated security solution that delivers the strength and breadth of the Cisco platform to protect their workforce everywhere. This includes (but not limited to) *Umbrella*, *Duo*, *AnyConnect, Meraki MX* and *Secure Endpoint* products.

Remote working security considerations:

- Increased percentage of remote workforce no longer protected at the perimeter
  - 81% of breaches involve compromised credentials
  - 52% of respondents stated mobile devices are challenging to defend
  - 27% of organizations are currently using multi-factor authentication (MFA)

Benefits for Employers and Employees:

- **Lower Overhead Costs**: *Employers save $11k/year per employee on average*
- **Lower Employee Costs:** *Workers save $4k/year on commuting, parking and food*
- **Business Continuity:** *Workers maintain productivity, saving employers $400/day*
- **Higher Productivity and Efficiency:** *Workers save 30 days/year in commute time*

Work From Home Models:

HW **Hardware User**: Executives and client-facing employees, requiring hardware devices
SW **Software User:** Field employees benefitting from an all software solution
CL **Cloud User:** Employees using only cloud-based applications and mobile devices
IT **IT Operations:** Employees in charge of rapid deployment and support

Questions to ask your Customer:

- How does your long-term business continuity plan to evolve?
- Would it be easier if all your security products **worked together**?
- Can you **verify** user identity when your teams are remote? *(Duo)*
- How do you enable secure access to company applications? *(Duo)*
- Do you currently have **Multi-factor Authentication** in place? *(Duo)*
- How are you defending against Phishing and Ransomware attacks? *(Umbrella, AMP)*
- What are you doing to protect users who are "off the network"? *(Umbrella, AMP)*
- How can your users get **access** to company apps and sensitive files? *(VPN, Meraki)*
- Do you have visibility into **user behavior** and potentially malicious sites they might be accessing? *(Umbrella)*
- Do you require hardware-based VPN for users to connect to Corporate? *(Meraki)*
- Do you have VPN & bandwidth capacity for every employee?

Product Use Cases:

AnyConnect: SW
Enable secure access to your network for any user, from any device, at any time, in any location. Gain visibility and control over who's accessing the network and on what devices. Perform continuous endpoint posture checks.

AMP for Endpoints: HW SW CL
Cloud managed endpoint protection that provides the last line of defense, enabling protection, detection and response on the endpoint against known and unknown threats detecting malware as well as remediating advanced threats. *(Win, Mac, Linux, Android & iOS)*

Duo (MFA): HW SW CL
Proactively reduce the risk of a data breach. Verify users' identities before granting access, gain visibility and posture into every device, and enforce adaptive policies to secure access to every application.

Meraki MX: HW
Cisco Meraki MX Security Appliances are Cloud managed Unified Threat Management (UTM) products that offer multiple security features in a simple-to-deploy, consolidated form factor. Cisco Meraki MX firewalls make intelligent site-to-site VPN easy with Auto VPN. Advanced security services including next generation firewall, intrusion prevention, content filtering, anti-malware, geo-based firewalling and advanced malware protection.

Umbrella: HW SW CL
Hold the first line of defense against threats on the internet wherever users go. Protect remote workers against malware that uses DNS. Detect compromised endpoints through persistent DNS monitoring. Block threats before they compromise you on and off the corporate network.

- **Additional Information:** https://salesconnect.cisco.com/#/program/PAGE-16410
- **Business Resiliency:** click here
- **Security Enterprise Agreements (EA):** click here