Building a Secure Work-from-Home Strategy for Your Workforce

Using tech to maintain team collaboration, workforce productivity, and security

IE INTERNETWORK ENGINEERING

According to the New York times via eRepublic, **"200 million people in 21 states, 47 counties, and 14 cities are staying home."** You read that right. Nearly 2/3rds of the US population is staying home during this pandemic.

Furthermore, a Gartner, Inc. survey of 800 global HR executives on March 17, [2020] found that, "88% of organizations have encouraged or required employees to work from home, regardless of whether or not they showed coronavirus-related symptoms. Nearly all organizations (97%) have canceled work-related travel, more than an 80% increase since March 3."

According to Gartner, **"54% of HR leaders in our snap poll indicated that poor technology and/or infrastructure for remote working is the biggest barrier of effective remote working."**

Do your work-from-home technologies accommodate the increased demand for remote work?

Let's explore common WFH challenges due to the COVID-19 stay-at-home order and the technology solutions we can help you implement to overcome them. The end goal is to create a secure and productive work structure for your employees, ensuring your business services continue to run effectively.

CHALLENGES

Bandwidth Overload

Household Members WFH
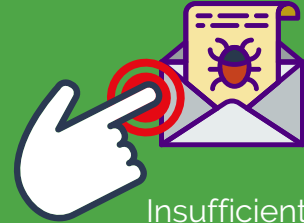
More Online Activity

Multiple Devices on 1 Router

Online Schooling

Cyberthreats

Emotet Malware & Other New Threats

Insufficient Security Awareness Training

COVID-19-Related Social Engineering

Outside Distractions

Children

Pets

Household Member Conference Calls

Maintaining Productivity

Only One Screen to Work From

Difficult Team Collaboration

Struggle Accessing Tools & Systems

SOLUTIONS

Reliable Connections

Cisco OfficeExtend

Extending Corporate wireless LANs to remote locations

Deploying APs for remote workers

Meraki AP SSID
(use Meraki MX as a VPN)

Cisco SD-WAN

Increased Security

Cloud-delivered firewall

Secure web gateway

Cloud access security broker (CASB)

DNS-layer security

Cisco Umbrella

Interactive threat inte

SD-WAN | ON/OFF NETWORK DEVICES
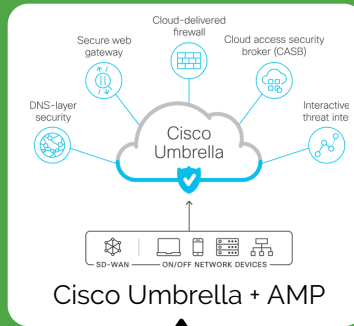
Cisco Umbrella + AMP

Endpoint Protection

Varonis Edge

Infoblox

BloxOne™ Threat Defense Cloud Service

Mitigate Distractions
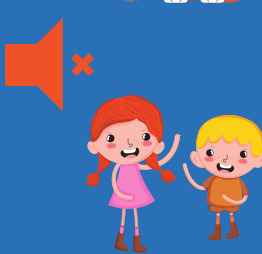
Noise-Canceling Headphones

Stay Connected & Productive

Link Multiple Screens with HDMI, DVI, or Display Splitter

Cisco AnyConnect Secure Mobility Client

Cisco Webex Teams and Meetings

iE

FREE TRIAL OFFERS

paloalto NETWORKS®

**NEW Cortex XSOAR Free Onboarding Package

Prisma Access QuickStart Service
(for new Prisma Access customers)

Prisma Access Additional Licensing
(for existing customers)

GlobalProtect
(for existing NGFW customers)

---

tenable

Elastic Asset Licensing
(for Tenable.io Customers)

Tenable.io Instance Made available
(for Tenable.Sc Customers)

Tenable.io Evaluation Instance Available for 30 days
(for Nessus Pro Customers)

Twice Weekly Virtual Office Hours w/ Principle Engineer
(For All Tenable Customers))

VARONIS

Varonis Edge License

Helps provide visibility and threat detection for VPN, DNS, and Web Proxies, Varonis Edge helps detect attacks like malware, APT intrusion, and exfiltration, and puts them in context with your core data stores.

Infoblox

BloxOne™ Threat Defense Cloud Service
90-day Access

Leverages the power of your core network services to provide a foundational layer of security for on-prem, cloud and cloud-hybrid networks, streamline and automate threat response, and unleash the full power of your existing security stack.

CISCO

Cisco AnyConnect Secure Mobility Client
90-day Corporate Trial

Cisco Webex
90-day Corporate Trial

Cisco Duo
90-day Corporate Trial

Cisco Umbrella + AMP
90-day Corporate Trial

LOOKING FORWARD

The likelihood of remote work becoming a more common practice in the future is high. Here are what a few industry leaders are predicting.

"Our best estimate is that 25-30% of the workforce will be working from home multiple days a week by the end of 2021," said Kate Lister, President of Global Workplace Analytics.

Gartner had a few more statistics on the topic,

- By 2030, the demand for remote work will increase by 30% due to Generation Z fully entering the workforce.

- 64% of today's professionals say they could work anywhere, and remote work policies are common (in place at 71% of organizations).

- Gartner CFO Survey reveals, "74% intend to shift some employees to remote work permanently."

The Boom in Mobile Use and IoT integrations for Business

- More than half (52%) of response in the Cisco 2020 CISO Benchmark Report said, "mobile devices are 'very' or 'extremely' challenging to defend". A Duo Security report found "45% of requests to access protected apps come from outside the business."

- "The use of IoT business platforms is growing year-on-year in almost all industries, with 61 percent of companies globally implemented IoT applications in 2019", said Kaspersky's Benefits and Challenges of IoT report.

- It further stated, "Even though the technology offers savings, new income streams and increased production efficiency, 28% of organizations experience cybersecurity incidents targeting connected devices."

- "The threat is booming by the day. There will be approximately 25 billion IoT connections by 2025," according to Gartner.

From a business perspective, the impact of COVID-19 showed us that remote work on a large scale is possible and sustainable if securely structured. The stats tell us that the demand for this type of work is not going away anytime soon. Knowing that, we must adapt to survive and thrive in this changing business environment. Part of this adaption will involve the evolution of cybersecurity to mitigate the risks associated with remote workforces.

If you need help securing your workforce and preparing for business after COVID-19, contact IE today at info@ineteng.com.

GET YOUR FREE TRIALS

IE