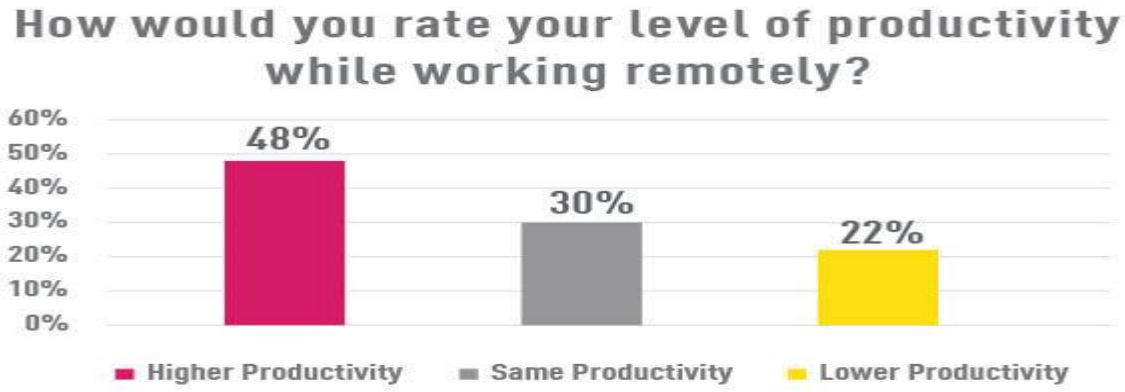
CYBERSECURITY BEST PRACTICES TO STAY SAFE IN A NEW NORMAL

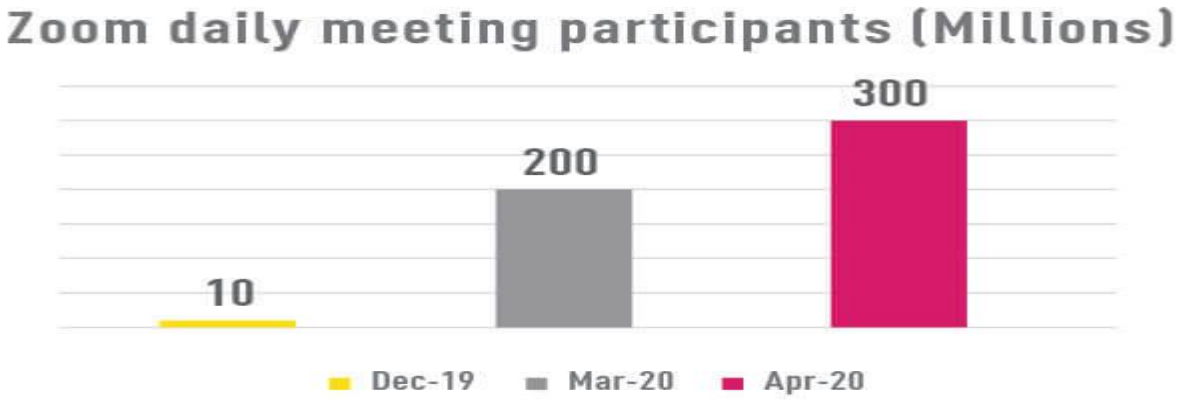
The world has changed

It's only 20 weeks since the first lockdown measures were implemented in Wuhan, in January 2020, but since then the emergence of the Covid-19 pandemic has reshaped our entire working culture. The changes were global, rapid and widespread, compressing several years' worth of IT changes into just a few weeks:



1. Remote working is the 'new normal' – as Governments worldwide mandated lockdowns, organizations transitioned to a majority of employees working from home and accessing corporate resources through secure access (e.g. VPN) . Most Organization all over the world shifted to work from home, for the first time in our history. In a recent Gartner CFO survey, 74% of companies said they intend to shift employees to work from home permanently.

So, this 'new normal' will simply become normal for many organizations and employees



2. Use of collaboration tools is 'zooming' up – as face -to-face meetings were not possible, organizations switched to using collaboration tools such as Zoom, Teams and Slack more than ever before.

3. Accelerating digital transformation and the move to cloud – A recent survey by Fortune magazine showed that 75% of Fortune 500 CEOs said the pandemic forced their companies to accelerate their technological transformation, with cloud resources at the top. To put it another way, if you move too fast, there's a greater of risk of breaking things. Having a weakened security stance is not a 'new normal' behavior organizations can afford to keep – so they need to fix what's broken, and fast.

Rapid changes mean security can't keep up

In its insight report on COVID-19 the world economic forum found that out of 350 of the world's top risk professionals, 50% are worried by cyber-attacks and data fraud resulting from a sustained shift in working patterns.

BEST PRACTICES TO STAY SAFE IN A CYBER PANDEMIC

REAL-TIME PREVENTION

As we've learned, vaccination is far better than treatment. The same applies to your cyber security. Real time prevention places your organization in a better position to defend against the next cyber pandemic.

SECURE YOUR EVERYTHING

Every part in the chain matters. Your new normal requires that you revisit and check the security level and relevance of your network's infrastructures, processes, compliance of connected mobile, endpoint devices, and IoT.

The increased use of the cloud means an increased level of security, especially in technologies that secure workloads, containers, and serverless applications on multi- and hybrid-cloud environments.

CONSOLIDATION AND VISIBILITY

Dramatic changes in your company's infrastructure presents a unique opportunity to assess your security investments. Are you really getting what you need and are your point solution protecting the right things? Are there areas you've overlooked?

The highest level of visibility, reached through consolidation, will guarantee you the security effectiveness needed to prevent sophisticated cyber attack. Unified

management and risk visibility fill out your security architecture. This can be achieved by reducing your point product solutions and vendors, and your overall costs.

Your New Cyber Security Normal

With a cyber pandemic, your cyber security demands that you understand the cyber risks with your changed computing environment. The matrix below provides a starting point as you re-assess your cyber security strategies.

Change	Effect	Risk	Top Process & Technology
Working from home	Personal mobile and computers provided access to corporate networks	Data breach (e.g. key logger, screen logger on pc/mobile)	1. Implementation of endpoint security and hygiene with compliance check (latest patches, AV…) 2. User training awareness (e.g. phishing simulation) 3. Mobile threat defense on mobile
Rapid move to cloud »	Speed of deployment on the expense of security	Basic security controls can lead to data loss and manipulation	1. Invest in Cloud Security posture management 2. Deploy workload security for containers and serverless apps. 3. Real time prevention of threats with IaaS security
Critical infrastructure »	Allowing critical infrastructure remote access	Critical infrastructure breach	1. IoT security for IoT devices 2. bolster network security posture with red team … 3. OT security with Scada enforcement
Increased network capacity	More throughput is needed to address data in motion	Lack of service	1. Invest in network security that scales according to needs 2. All protections must be enabled while keeping business continuity 3. Scalable secure remote access

References:

- https://www.checkpoint.com/cybersecurity-protect-from-cyber-pandemic/
- https://blog.checkpoint.com/2020/06/09/securing-the-new-normal-protecting-the-post-covid-19-world/
- https://www.globenewswire.com/news-release/2020/06/09/2045445/0/en/Securing-the-new-normal-survey-shows-organizations-security-priorities-as-they-emerge-from-Covid-19-lockdown.html