The Digital Transformation Experts

The Essential Connected Workforce Guide

Learn how to empower collaboration across your organization for greater growth, agility, and accessibility.

microage.com
(800) - 544 - 8877

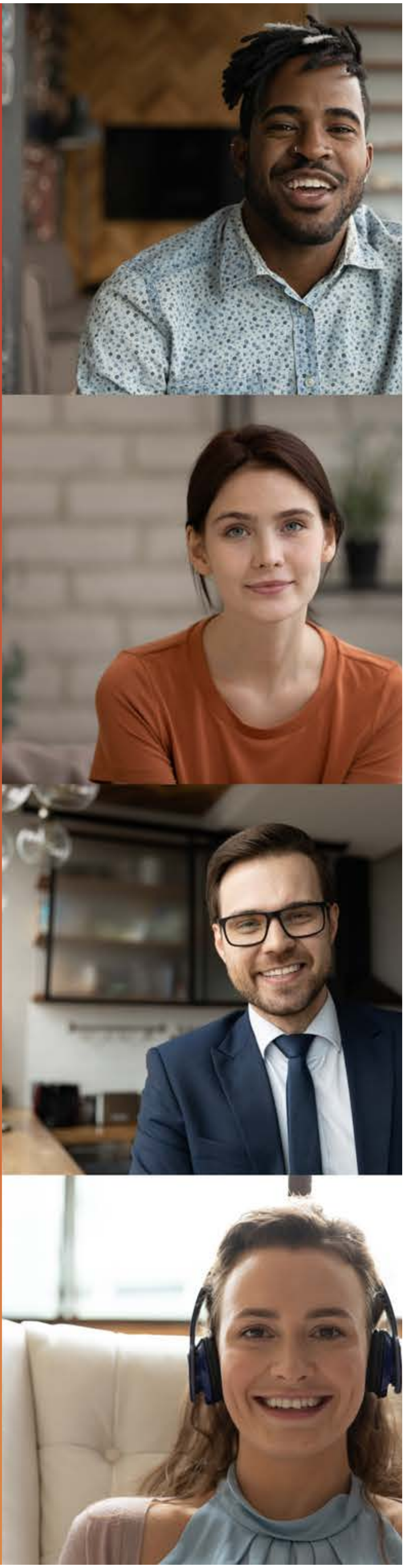


Table of CONTENTS

MicroAge®
The Digital Transformation Experts

Fuel smarter business outcomes and connect your workforce with MicroAge.

THECHANNELCO. CRN

MicroAge has been awarded:

- Top MSP 500 - Elite 150
- Top Tech Elite 250
- Top Solution Provider 500

2020 marked a dichotomy shift for business as usual as the enterprise went fully remote—and that isn't changing.

If we've learned anything in recent years, it's that remote work is the new normal. It saves on business maintenance and upkeep, travel expenses, and has challenged organizations and IT leaders everywhere to take a stronger approach to collaboration with an estimated 64% of employees able to work remotely, more than half working remotely full-time, and many expecting remote work to persist and increase in the coming years.

Over the last two years, the business block has catapulted to a remote workforce, and that isn't changing. Because more than 90% of professionals want to work fully remote or in a hybrid remote environment. Even without all the chaos of the last year, the workforce is changing. Millennials will make up more than 75% of the workforce in the next three years. With Baby Boomers retiring in droves and Zennials coming into the workforce, working styles are changing.

The shift to remote work has had some major advantages for employers. For instance, 77% of professionals reported higher productivity rates while working remotely. The WFH movement has also unleashed a broader talent landscape while making it easier for businesses to diversify the workforce without traditional geographic limitations. Until recently, applicants who live more than five miles away were given one third fewer callbacks according to the Harvard Business Review. That's right, just five miles.

Now with the proliferation of work from home, even more, localized, smaller organizations can tap into a national talent market for tough-to-find skills. While the gig economy powered by millennials and others who have left the full-time workforce to work for themselves is constantly in collaboration with professionals across the business enterprise.

The Connected Workforce Essentials guide explores how you can empower uninterrupted collaboration while securing a disparate, connected workforce.

Actively promoting a more connected workforce is essential to productivity and collaboration.

The connected workplace went from being a thought leadership topic about the future and the way we think about work to our daily reality, a.k.a. new normal. While some teams were already remote, for most of us, the transition to remote work was and maybe is still an adjustment.

Because whether you're balancing your work life with a new eLearning curriculum or strategically muting your dogs barking at the neighbors' dogs (barking) while responding to your manager, you're facing a new kind of challenge. We all are.

Two years into a remote workplace, we're finding a new work culture that's sometimes uncomfortably immersive. Amidst all the uncertainty and new norms, our workday and our home life has become impossible to separate. While 2020 came with its share of challenges, it's integrated our humanity in our day-to-day working habits and relationships in a way that's powerful and unshakeable. It's also been incredibly challenging for IT teams—everywhere.

With demands and expectations for IT teams changing while more teams are working remotely, there are still ways you can bring your team members and their counterparts closer together while empowering a better working experience. With these best practices, we put the focus on what is in your control, how you lead during the most dynamic and volatile times:

KEEP CYBERSECURITY AT THE CENTER OF YOUR WORK-FROM-HOME APPROACH

RECALIBRATE SECURITY OPERATIONS

KEEP EDUCATING YOUR WORKFORCE ON THE RISKS

SECURE SAAS APPLICATIONS

STEP ONE

Keep cybersecurity at the center of your work-from-home approach.

Cybersecurity attacks catapulted by 500% in 2020, and security experts don't see the threats or ransomware attacks slowing down in 2021 either. With Cybercriminals reigning in record profits via substantial ransoms this year they are likely only more emboldened and positioned to get more aggressive in their attacks. Unfortunately, in 2022 attacks are expected to wreak more havoc on businesses and IT teams globally. Cyber terrorist groups are only becoming more organized in targeting their campaigns and ransomware tools are accessible and easy to deploy.

In fact, according to DarkReading.com, many from the security community are anticipating a strong increase in ransomware attacks with the threat of data exposure. Meaning that regulatory and compliance risks will loom large for potential victim organizations. And organizations that are ready to pay to bring their systems back online risk being sanctioned by the U.S. government over—let's face it—legitimate concerns that ransom funds are fueling criminal entities on official U.S. sanction lists.

But there's good news, building a robust connected workforce security strategy can *dramatically* decrease the chances your organization will come under attack.

STEP TWO

Recalibrate security operations.

The mass exodus from office to new normal has obviously put tremendous pressure on already busy security operation centers (SOCs). Now with the connected workforce having a big moment, security operations are one of the largest pandemic challenges for any business.

Moving forward into 2022, (and beyond), security operations groups have a new mandate—defining, architecting, and implementing infrastructure that's built for hybrid environments and a large, connected workforce.

Not having everyone in the SOC (Security Operations Center) made a lot of teams quickly realize that their defenses weren't working at full capacity and that's a major problem for CIOs. For smaller businesses without an official SOC in place, finding the right managed services provider can be a game-changer to build a more robust, intelligent infrastructure to arm your organization against current and future Cyberattacks.

STEP THREE

Keep educating your workforce on the risks.

One thing hasn't changed since 2020. Security is still a common concern for any business taking its workforce remote. Case in point, in 2018, 86% of business leaders already had the same question about team members working remotely, *how can we protect their data and our business assets?*

Your employees are still your greatest asset and your largest vulnerability point when it comes to Cybersecurity threats (spear-phishing and ransomware attacks). And of course, that risk has only increased with teams going remote.

In addition to the basics—regular security and compliance trainings, simulated phishing campaigns, and keeping an active, company-wide dialogue buzzing around Cybersecurity threats and suspicious activity—there's some "new normal" ground to cover if you haven't already.

CHECKLIST

- First, run a manual virtual security training explaining the latest threats and countering them with basics like VPN, Single-Sign-On (SSO)... more on that later, and how to report suspicious emails or texts to your IT team. Because we know that Spam filters aren't stopping everything, and spear-phishing messages have a 5-6x higher open rate than most real emails. A heart-stopping 70% of employees fall for them, a number that's only increasing with more team members in isolation.

- Use a post-training Cyberattack simulation to measure your workforce and their progress. Cyberattacks and social engineering are powerful tools because too many employees aren't on guard or aware of the importance of data security—even more than usual when they're dealing with stressors outside of work. It's critical to educate your team members on how you are securing them and the business and on the role they play.

- Build or finetune your Cybersecurity policy for remote workers—guiding them through the why's and the important details and requirements before requiring them to review and sign. Every employee or outside contractor using your systems needs to be included. Guide your teams through the high-level details before sending the strategy out to all employees to review and sign.

- Keep reinforcing your security policy and its importance on a quarterly basis via email and on all-hands meetings. It's easy to get lost in tech talk on a Teams call, so, include why compliance is critical. Always, always, always hone in on ***the why*** for maximum compliance and engagement.

STEP FOUR

Secure SaaS applications.

Cybercriminals know that the enterprise and other businesses are moving workloads and data to the cloud in a mass exodus from the traditional data center. This started in recent years with more organizations looking to harness greater agility for a competitive edge and only increased in 2020 with businesses needing to quickly support a remote workforce for the health of their employees and their business operations.

So, it isn't a shocker that SaaS environments have become a big, red target for bad actors. Cybercriminals know that IT teams are even more burdened than business-as-usual with management of SaaS applications and their organization's cloud strategy and footprint, and they see that as a powerful vulnerability to exploit.

Tools for scanning APIs between applications to automate SaaS configuration while monitoring user access and activity and changes in the environment are becoming more important every day.

If your IT team is struggling to maintain the day-to-day with the recent onslaught of pandemic-triggered changes to operations, then you aren't alone.

68% **of IT Professionals have less time to invest in SaaS application management and security**

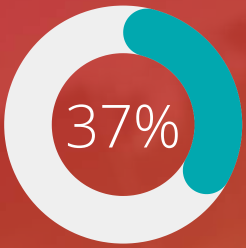
That's where having an extra layer of security expertise isn't just helpful, it's quickly becoming necessary. Partnering with a full solutions and services provider can reduce the pressure on your IT team while bolstering your business security so, you're prepared for whatever comes next.

SSO SOS

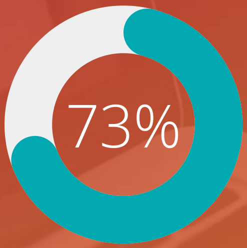
Not only does Single Sign-On (SSO) increase compliance, user satisfaction, and productivity, it instantly levels up your organization's cybersecurity. Why?

While SSO only uses one username and password for authenticity across all productivity apps, it makes it harder for hackers to compromise any of the accounts associated. Users have one username, one password, and an extra layer of security on all the applications they use daily. Compromised credentials are a key driver of breeches. Because the more usernames and passwords we have, the harder password management becomes. Users start simplifying passwords i.e., Password1, or, using the same credentials across multiple platforms—making them an easy target.

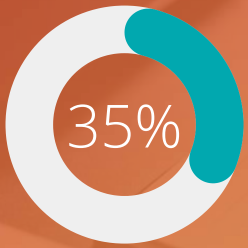
The remote workforce is rapidly expanding along with security risks. Single Sign-On (SSO) boosts security and user experience with one set of credentials across applications. Demand for SSO is reaching new levels—these stats explain why.



of organizations require unique passwords for more than 25 applications



of user accounts online use duplicate passwords



of organizations cross check credentials with common password lists

6 unique passwords are used to arm 4x as many accounts on average

500 number of hours the average company spends on password resets each year

2 in 5 people had a password stolen, an account hacked, or a notification that their account was compromised last year

Only 3 in 10 people still trust passwords

SSO SOS

Downtime from ransomware alone costs organizations $64,000 on average

Spear phishing messages connected to ransomware have an engagement rate 6x higher than actual emails

80%

of Data Breaches in 2018 started with a weak password

12%

Increase in Ransomware attacks costing organizations more than $8 Billion

29%

of all breaches are powered by stolen credentials

More than half of remote employees are using less secure personal devices

61% of Gen Y and 50% of workers over 30 find their personal devices more productive than ones at work

60% of the workforce uses a smartphone for work purposes

Create a company-wide security policy and make it accessible.

Knowledge is power. The reason spear phishing and cyberattacks are still so rampant is because too many employees just aren't on guard or aware of the importance of data security. It's mission-critical to educate your workforce on how you are actively maintaining your organization's security and what role they play.

Build a cybersecurity policy—explain why you're creating it and how they can help your organization stay secure. Walk your teams through the high-level details before sending it to all employees—new and existing—to sign.

What does this policy look like?

- **Start with a mission statement (why it was created)**
- **Specifics on security policies across the board—on and off organizational devices**
- **Reinforce why compliance is important and how you're supporting compliance with technologies, coaching and other resources**
- **Each employee should sign acknowledging they've read and agreed to the policy**

When in doubt, VPN.

Immediately prior to the mass-office exodus, Amazon started having employees test Virtual Private Network (VPN) weeks prior to prep for long-term remote work. That's because with VPN, employees can securely access shared files wherever they are. By putting the right controls and parameters in place, you can require VPN login for employees to gain access to any sensitive business data.

VPN is the keep-it-simple-stupid solution—enabling employees (after some quick education) to VPN in before signing onto any public Wi-Fi networks. VPN encrypts your remote workers' internet traffic while monitoring for any signs of alarm. No matter where remote workers are, your data is secure.

Arm your organization with the right security.

Remember that security policy we talked about?

It needs to require all employees to keep their firewalls, antivirus software and anti-malware current across devices. That means taking the time to restart and run updates.

The ability to wipe lost or stolen company laptops or other devices also comes in handy. Team members can shift to their personal laptop or phone in the meantime. These objectives should tie into your larger security strategy.

Define, plan, and implement your security strategy.

Having an IT security strategy is more important every day with an increase in remote work, and a move to the cloud. Ransomware attacks increased by 12% last year and cost organizations more than $8 billion.

And, according to Comparitech, downtime resulting from ransomware costs most organizations upwards of $64,000.

> Having the right security technology and processes is a mandate to staying in business in the digital age. Bringing in outside security subject matter experts promotes better anti-malware and ransomware software, comprehensive training, and a stronger security strategy overall.

Make *Work from Home* work for everyone.

The work from home movement has introduced a fresh mix of challenges for IT teams everywhere. From difficulties with collaboration tools and video conferencing to lagging internet connectivity on home networks, the new normal is anything but. That's why technology leaders need to act quickly to collaborate with organizational leadership on best practices for working from home instead of having each department on a separate set of collaboration technologies—both business continuity and productivity killers.

So whether you're assessing Microsoft Teams or other alternatives, having a unified communications platform is mission-critical to building a connected remote workplace with less room for pitfalls like siloes and communication gaps.

Many IT leaders are already purchasing additional licenses and upgrading their network for increased accessibility. CIOs can distribute 4G/5G modems or reimburse upgraded internet plans to upgrade ISP capacity at employee home offices.

The latest sea change in how and where we work pushed the needle on work culture everywhere. Technology leaders can help to empower cultural change by sharing best practices for keeping team members connected and working securely and by providing employee education on the latest collaboration tools and capabilities. Whether you're sharing why Single Sign On (SSO) matters and how to use it or reviewing the latest Microsoft Teams features to tap into, having regular updates keeps your workforce engaged and using the latest technologies for collaboration.

Technology leaders can help to empower cultural change by sharing best practices for keeping team members connected and working securely.

Get and stay aligned on goals.

Everyone’s day-to-day looks vastly different than it did a few years ago. It’s a lot of change and uncertainty to take on at once, and it can be easy to get overwhelmed or complacent and fall out of communication with your team and counterparts. Don’t.

Look to your team and executives for regular updates on their goals, progress, and achievements and how you can support them. In tandem, share the goalposts you’re tackling and how they will benefit the organization. Don’t assume everyone already knows what you’re doing or leave them floating in space.

Re-commit to unified communications.

Promote seamless communications across calls, video conferencing, and messenger with one unified communications platform. Your employees will be able to see if colleagues are available or tied up in another meeting. The right UCaaS strategy connects all the systems that power your organization to keep team members working together in real-time with technologies that integrate for powerful, productive, and fluid collaboration across your remote connected workplace.

Make collaboration a constant without any communication gaps. Having a unified communications platform is mission-critical to keeping interactions between employees seamless across calls, video conferencing, and messenger.

With a unified communications platform, employees can see if colleagues are available. Unified communications empower productivity by enabling uninterrupted collaboration. And the right UCaaS strategy connects all the systems that power your organization to keep them working together in real time.

Don’t get hung up with legacy phone systems.

Having the right phone systems keeps your team members connected with each other and with your clients. VoIP (Voice over Internet Protocol) solutions like Ring Central and cloud-based communications empower productivity wherever team members are. Added bonus? You can stop maintaining dated equipment and shift gears to a BYOD (bring your own device) strategy if it fits your long-term goals.

Foster new approaches to work.

If you're facing challenges ensuring the adoption of new tools and protocols, you aren't alone. With working behaviors in a constant state of flux, some professionals are still trying to navigate what can seem like an endless foray of tools without any experience using them effectively.

Because new behaviors take about a month to "fully bake," getting technologies leveraged in the right way is a journey. While it's important to provide clear guidance on downloading and using new tools, the new normal mandates an investment in training-for-adoption techniques.

This looks different for every organization—whether it's repeat trainings, certifications, or advanced seminars—find ways to ensure tools aren't just utilized but are helping people with better approaches to their work.

Role modeling is another way to move the needle with organizational behavior. For example, communicating through collaboration tools like Microsoft Teams with the new Together Mode to get everyone on the same page and screen.

Make turning cameras on mandatory during your weekly team meetings and empower your IT counterparts to get comfortable being in front of a camera to lead the way.

Support and empower your workforce.

Whenever possible, provide flexible working arrangements—whether that's flexible shifts, remote work, or preparing for absences. Recognize upfront which team members will be impacted by school closures and online learning to design backup support when it's needed for essential workers and to make sure they are technically equipped to do their job remotely whenever possible.

If you have employees who still need to come into the physical office, keep your working environment safe with rotating shifts and separate zones (areas) for essential IT workers. Work with human resources to create transparency when testing or quarantining may be needed to keep employees healthy.

Helping your people through these adjustments makes a positive impact on long-term employee loyalty and retention levels. So, make a point of reaching out to your team members just to see how they and their families are powering through all the recent changes and uncertainty. Being supportive and consistent can make a huge difference in providing some structure in their lives during these unpredictable times.

New Digital Workspace Era. Same Common UCaaS Questions.

Something that became abundantly clear as the remote workforce catapulted into action two years ago is that many organizations were lacking a robust UCaaS strategy. Unfortunately, because of the fast shift in dynamics, many IT teams jumped into reaction mode without the time to really develop a methodical UCaaS strategy.

In this section, we review some tried-but-true basics.

The Work from Home era has made UCaaS the best practice.

Unified Communications has always been paramount to an effective and collaborative business. Improvements in interactions and response times and bringing disparate team members together are key UCaaS business drivers. With more businesses expanding across locations—and continents—and including remote workers, the right video and soft phone options bring teams together for increased collaboration and quicker turnaround. Couple that with operational expenses versus capital expenses. It should be no surprise that Unified Communications as a service is quickly becoming the best practice.

Not every organization needs a Contact Center.

It depends on your business model and overall approach to customer service. Contact Center isn't for every company—it's more important for specific organizations looking to manage multiple customer communication channels—email, SMS, chat, voice, and social media—all in one place. Depending on your industry and organizational structure this may or may not be the right fit for your organization.

Are hard handsets going the way of the cubicle?

Not anytime soon. There is and will continue to be the need for handsets. Albeit the usage of handsets is steadily decreasing with the advent of the soft phone, handsets still have an active role in our modern working environment. With that being stated, soft phone and soft phone capabilities continue increasing and will be a viable solution moving forward. And with the remote workforce in full swing many professionals are opting to use their personal devices like AirPods for clearer communications with noise cancelling.

The right UCaaS strategy unifies remote workers while helping businesses amass a global presence—sooner.

Today’s business market is fast paced, constantly shifting and even virtual. Organizations must stay ahead of changes to keep pace with the methods clients select to do business. UCaaS delivers a consistent user experience wherever your employees reside. For employees to collaborate effectively, they need to use the same tools and a common interface for sharing information. When using different versions of an application, or even if a browser or operating system doesn’t support it, collaboration suffers. That defeats the purpose having widely dispersed teams working together making it more challenging to be productive and communicate across the board.

Simplify your collaboration approach with our team of experts.

Increasing operational expenses, high operational complexity, a growing remote workforce, and rising costs are making the telecommunications landscape increasingly more challenging for organizations of all sizes.

“My experience with MicroAge has been phenomenal! [They] do what no other vendor has in my experience: focus on understanding my business and how we maintain profitability. They do their best to offer solutions that meet our needs.”

-Chris Leonard, Cayuse Technologies
Information Technology Director

Tap into MicroAge’s deep knowledge and certifications and the power of our partnerships to architect a communications strategy centered around your business goals and unique connected workforce. Connect with our cloud experts today—call 800-544-8877 or visit MicroAge.com.

What's the MicroAge difference?

MicroAge combines a powerful mix of technology services backed by vendor-certified engineers and an acclaimed panel of experts to deliver the competitive edge technology leaders need to lead in a disruptive, digital environment.