SIX STEPS TO A VIBRANT REMOTE WORKFORCE

Operating a remote workforce is no longer just a remote possibility. A work-from-home war is being quietly waged across many organizations throughout the country, as workers who were forced to quickly establish home office environments now wish to remain in their home rather than return to commuting to an office. This tipping point has deep and wide ramifications for organizations attempting to return to pre-COVID-19 productivity levels.

The next normal will be led by organizations that embrace a vibrant remote workforce culture and establish a productive, hybrid workplace. Organizations will begin to leverage their remote workforce capabilities as an integral component to recruiting top talent, similar to how Silicon Valley start-ups promote their expansive food and beverage benefits.

When employees were first sent to work from home, organizations scrambled to provide work-from-home software, devices, and infrastructure and accomplished the herculean task of supporting a mass remote workforce in six to nine days when it would normally take six to nine months. As we transition to a new normal, it's now important to reevaluate the initial infrastructure laid to support remote workers against a lasting, best-practice architecture.

June 2020

ConvergeOne

REMOTE WORKFORCE PILLARS

1. Secure Workspace

Millions of computing devices – ranging from laptops, Chromebooks, tablets, and more – were purchased to support work from home environments. Due to supply constraints, many workers leveraged devices they already had at home or purchased and expensed a new device from a local retailer. However, with millions of workers now connecting their home to headquarters via fresh-out-of-the-box devices, security risk becomes an exponential concern. Couple the increased risk with the well-cited increase in targeted attacks and a perfect storm begins to brew, challenging organizations to defend against a much broader attack surface.

Organizations seeking to secure their remote workforce can focus on a few key elements to assist in their journey. It's important to remember that the traditional tools of past, such as a traditional firewall and anti-virus, are no longer effective means of stopping modern-day malware. Advancements in "next-generation" platforms have come a long way to match wits against leading threats. A next-generation endpoint solution, paired with a secure method for remote access to corporate resources, is a strong starting point to securing the user experience. Multi-Factor Authentication (MFA) is another integral component to the remote workforce security fabric. Credential compromise, especially across cloud applications, is a very real issue, and without a secondary method of authentication, attackers can often gain relatively simple access to corporate assets by applying stolen credentials.

Of course, the list does not stop here – Robust email filtering, patching, cyber awareness training, and more are important elements to a secure remote workforce strategy.

2. Resilient Connectivity

Reliably connecting home to headquarters is a challenge that should not be underestimated. Internet service providers continue to face a rising demand to support streaming video traffic, whether it be a corporate video meeting, a remote learning classroom, or the latest blockbuster. Localized outages impacting a primary hub can result in a global workforce twiddling thumbs waiting to be reconnected. These outages apply beyond just internet service, as an organization's core IT infrastructure was often never designed to support a fully remote workforce. Firewalls are overloaded by VPN usage, core routers become saturated, and connectivity to clouds reach capacity.

Software-defined WAN (SD-WAN) has taken off in recent years—and for good reason. A benefit of a remote workforce includes limited need for expensive MPLS circuits, which can be converted to multiple, high-throughput internet circuits. A strong SD-WAN solution will also enable the infrastructure to make automated decisions for traffic routing to best utilize and preserve the available capacity. For organizations that require an immediate infrastructure upgrade or desire elasticity, hosting remote access infrastructure virtually in a public cloud will enable organizations to increase (and decrease) capacity on-demand.

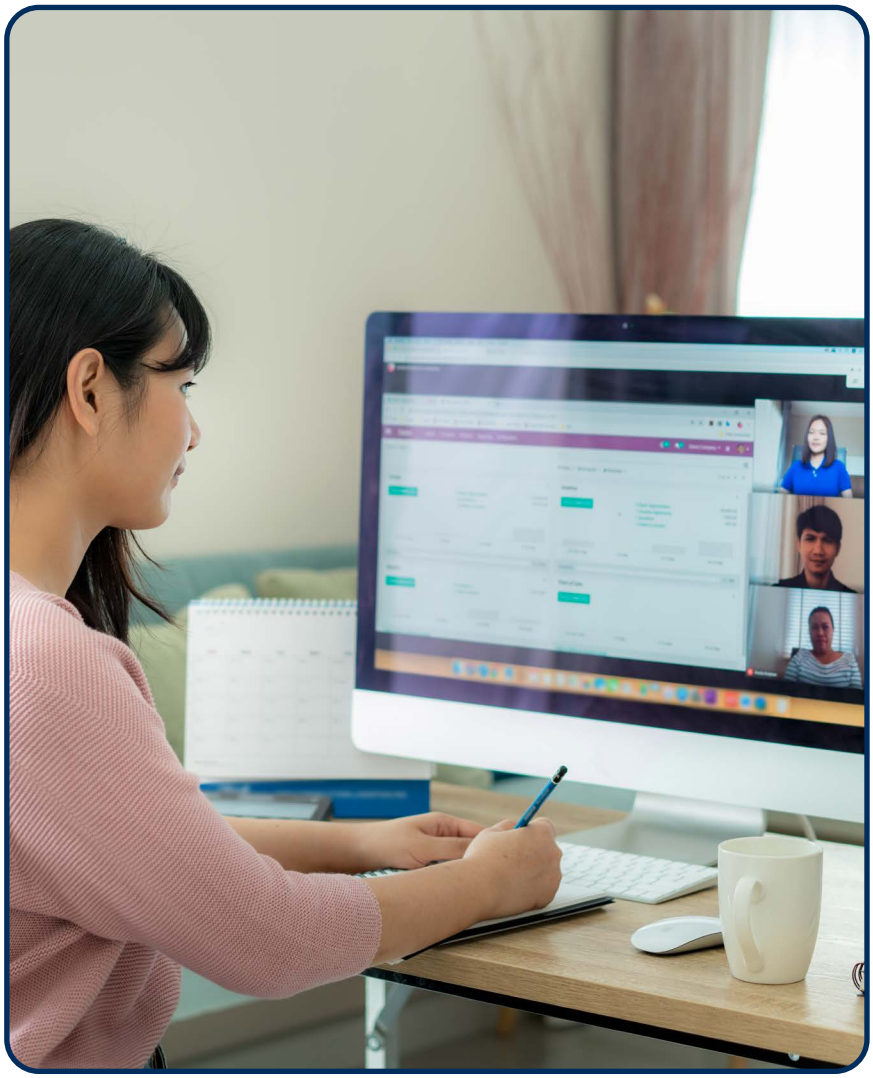
3. Data Protection

We've entered a time where data has both never been more valuable nor under greater attack. The data economy is rivaled only by the extortion economy, with cybersecurity in the center of a global battle. Organizations are finding it crucial to uphold the ability to not only protect their data, but also recover it. The recent evolution of ransomware has resulted in attackers encrypting as a last act—rather than the first—with data backups being targeted for deletion or encryption prior to launching the broader ransomware attack. As such, we saw the average ransomware payment skyrocket to over $84,000 toward the end of 2019.

A robust remote workforce data protection program incorporates a few key elements. First, remote workspace (user) and workload (server) data needs to be consistently and automatically backed up to a secure, central repository following a set, structured schedule. It's important to remember that these backups are a lynchpin to payment for many attackers, which is why we're seeing an industry shift toward the notion of cyber recovery vs. disaster recovery. It's far more likely an organization will suffer from a ransomware attack than a data center burning down. Cyber recovery introduces the concept of immutability and focuses on rapid recovery from a sophisticated cyber-attack.

4. Video Collaboration

Substituting the office workplace with an at-home workspace is no easy feat. However, organizations can maximize the benefits of interpersonal communication virtually with a rich, seamless video experience. One of the most interesting dichotomies of the pandemic was the emergence of the virtual happy hour. As texting and social media have seemingly replaced phone calls and gatherings over the last decade, especially for younger people, it would be fair to think that workers would adapt well to a reduction in human contact. However, the opposite quickly emerged, as virtual happy hours and "quarantinis" became all the rage, showcasing an intrinsic craving for camaraderie.



Implementing a unified visual and video collaboration solution with a top-down culture of camera-on is a great way to maximize workforce productivity—and sanity. If you've been reading along so far, it's no surprise that security should be a top-of-mind requirement when standardizing on a collaboration solution.

ConvergeOne

5. Distributed Communications

Communication patterns that have been established over the last decade are difficult to break, and when broken, miscommunication is a common occurrence. A prime example is a corporate telephony system that scales to office use, but is unavailable in a work-from-home setting. Furthermore, when that corporate telephony system lacks modern features—such as voicemail to the inbox or simultaneous dialing of a desk phone and cell phone—miscues are bound to happen between employees trying to reach each other. Fortunately, there are many avenues to extend telephony capabilities into a distributed remote workforce, whether it's a mobile app, computer application, desk phone, or home video unit.

6. Operational Management

One of the major identified risks that came out of the early days of COVID-19 was the potential for critical loss of talent and knowledge. Gartner estimated up to 40% absenteeism in the workforce due to the coronavirus, whether related to personal health or an overall reduced ability to work. Organizations that have fully encapsulated their IT operations to an internal team in an on-premises-only setting are at greater risk of disruption compared to organizations with a distributed support structure across a hybrid infrastructure. Building an operational IT structure that leverages trusted partners whose in-crisis capabilities have been vetted along with cloud technologies is an important element to sustaining operations, both during a crisis and in a lasting remote-workforce environment.

About the Author

TIM FEMISTER
VP, Digital Infrastructure

Tim Femister is the Vice President of Digital Infrastructure for ConvergeOne. An experienced industry thought leader, technologist, and advisor, Tim is fiercely passionate about helping customers reach their desired cybersecurity, data center, and enterprise networking postures. He does so by sitting at the intersection of People, Process, and Technology, consulting with customers to develop overarching strategies and roadmaps for operational improvement, programmatic development, and implementation.

SECURE REMOTE FOUNDATIONS ENGAGEMENT

Holistically assess the current state of your remote workforce against six proven pillars in a sixty-minute structured workshop. A complimentary, comprehensive engagement report is provided to you upon completion. Get started today.

Register for a workshop:
convergeone.com/remote-workforce-workshop

REV: 5.20-6-pillars-r3|042018