Keeping Your Data Secure in the Era of "Work from Home"

With the COVID-19 pandemic growing, these are unprecedented times. With almost all non-critical workforce working from home, the mandate has changed and the need to be cognizant of the problems in a *borderless data access* is paramount.

Is your organization prepared for such a large-scale transformation? As the boundaries have dissolved, the attack surface has grown, and IT departments are challenged with how to secure company data. End-user infrastructure/access points are unchecked and completely susceptible to a variety of known attacks in this newly distributed infrastructure. Here's a non-comprehensive list:

· **WiFi:** Man in the middle, vulnerable security protocol (e.g., WEP), rogue access points, evil twin, war driving, packet sniffing.

· **Enterprise VPN/Modem:** Low performance, and as a result, download data to consume.

· **Web:** Personal access combined with business, phishing, malware.

· **Data stores:** Use of local and removable drives and personal public cloud accounts.

Your workforce is remote; how about your data?

DAtAnchor is a simple and affordable universal transparent encryption solution. It ensures the sensitive data is unable to leave the business without consent, no matter where it is consumed. DAtAnchor encrypts and restricts access to that data based on dynamic boundaries, independently of how the workforce is deployed. Boundaries can be physical, such as requiring a user to be within a specific location physically and/or virtually, such as being a part of an active directory group within the organization. The encryption runs in the background unbeknownst to your employees. Data access is fully monitored, logged, and can be revoked instantaneously. Existing data files are relegated unreadable, based on governance rules. The DAtAnchor platform can be deployed in a matter of hours and guarantees the following:

· No change in existing workflow

· No plugins needed with applications

· Collaborate safely in the cloud/network shares

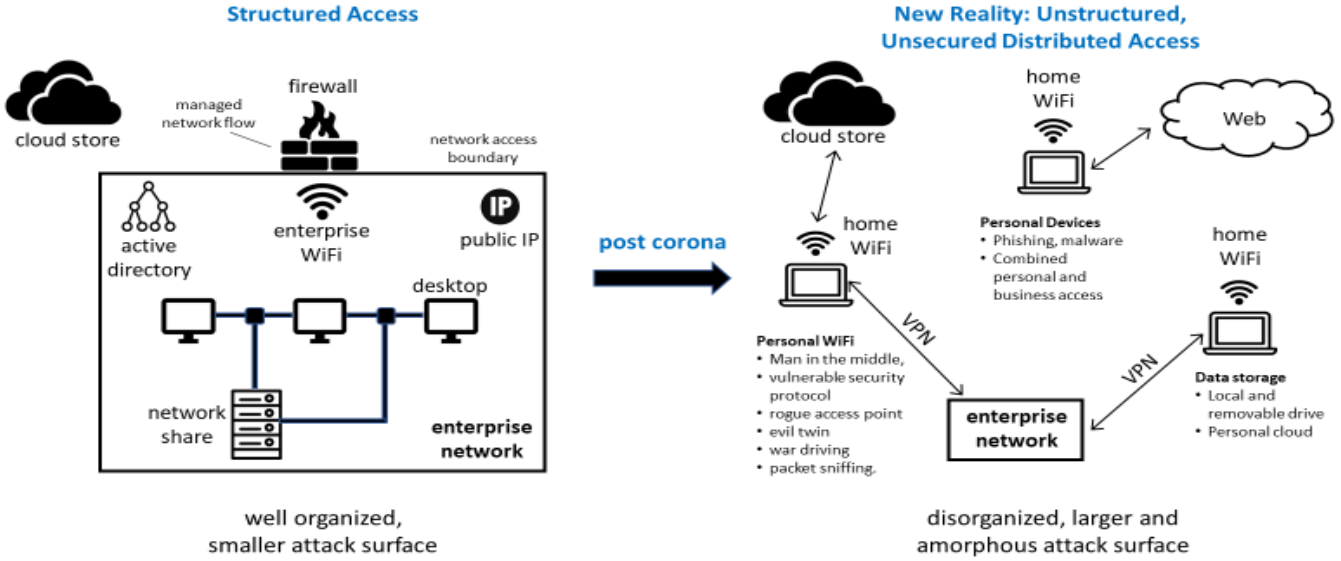
· Comply with CCPA, HIPAA, NIST, etc.

· Real-time logs of all access to data.

Call to Action: *Fill out the questionnaire* at this link to assess your preparedness for remote workforce.

Ask your MSP about DAtAnchor's comprehensive solution that requires no training for the employees thanks to its simple, low-maintenance design. Encryption can save your organization from a costly attack – whether that be internal or external – during an especially vulnerable time for organizations shifting to a remote workforce. With DAtAnchor, you gain full control of your data, integrated within your current platform in a matter of hours.

Drex DeFord, Former CIO for Scripps Health & Seattle Children's Hospital: "*A key challenge for IT and security teams is providing and protecting devices for employees to take home. Security pros who rush to get devices set up and deployed may lay land mines [they] may step on later. It's often simple misconfigurations that accidentally leave data exposed on the Internet…*"



datanchor.io

8000 Walton Pkwy #200,
New Albany, OH 43054

Contact: Eric Flecher
Head of Product
eric@datanchor.io