DATASHIELD™ | an ADT company

Datashield Top 5 Remote Work Tips

1

Deploying a strong Enterprise Endpoint Detection and Response (EDR)

People will always be the primary target in attacks against organizations, usually from varying forms of social engineering such as phishing, malicious ads, and watering hole attacks. Ensuring that the devices that your employees connect to your network on are safe and secure should be a primary goal. Having a cloud-based Enterprise EDR will allow you to monitor your employee's computers, even when not connected to the company's network. This will provide great visibility and will help prevent any malware spreading from an infected employee's computer.

2

Utilize a VPN

Virtual Private Networks (VPN) provides protection not just for the user, but for the company as well. Having a VPN that uses strong encryption practices, verbose logging, and supports MFA will enhance your overall security posture and ease of access into your environment. Using a VPN will also allow you to apply various access control measures through your VPN policies.

One common question is when to use a split tunnel versus a full tunnel. Datashield recommends using a full tunnel, as this will route all traffic through the VPN and is generally more secure. However, this can cause an impact on speed. A split tunnel is used when there is a need to access local resources as well, but can be less secure if something isn't being routed over the VPN tunnel.

3

Multi-factor Authentication (MFA) Policies

Password re-use and overall weak passwords are primary targets for attackers. If your applications don't support MFA or if the user's password gets compromised without your knowledge, the attacker can access those services. While not unbeatable, having MFA on those user logins will impede most attackers and stop a user compromise.

4

Connect from trusted Networks

Educating your employees about the safety of where they are connecting from is crucial. Employees should only be connecting from trusted networks, such as a home or office network. Public Wifi's, such as Starbucks or open hotspots, should not be used to perform work duties. While a VPN can offset some of these risks, it is ill advised to use any untrusted networks.

5

Separation of Work and Personal Data

Your company's data is important. Having computers that are purchased and secured by the company will limit that data's exposure. Restricting work related tasks and applications to be done on company issued computers only is important. This will ensure that you can monitor those endpoints. It is also recommended to avoid having personal accounts or applications on work computers, as you can't control the security for personal applications.

Additional tips provided by CISA

https://www.cisa.gov/telework-reference-materials-non-federal-organizations