Waystar's secure network

Remote work strategy and testing

We are in excellent shape to operate our business with a distributed workforce. We have spent the last 5 years building to a remote work force strategy and have moved every major component of our infrastructure to highly scalable cloud offerings. This includes our email, collaboration, phone, financial, marketing, CRM and HR systems. We equip every employee with a laptop preconfigured with all major tools, like VPN connectivity and soft phone installation.

Most of our departments allowed employees to work from home one day per week to constantly test our configurations and readiness. As we moved into a temporary distributed work force, the issues we are having are mostly mundane, and revolve around things like password rotation for corporate credentials that now take place remotely rather than when on site. For this example, our technical services team has updated our FAQ documentation around the process to help our team members when password rotations occur.

Device and data security

Similar to our general remote strategy above, we have spent the past two years deploying state-of-the-art security tools that protect our endpoints, regardless of where the endpoint is. From advanced threat detection to patch management to content filtering, every endpoint can operate as securely in a remote setting as it can in the office. The team is continually monitoring our security dashboards to ensure our systems are operating in our approved secure configuration. Of course, device security is just one part of the equation. We also are routinely communicating our corporate best practices for handling sensitive data when out of the office.

Technical capability

From a technical standpoint, we can operate remotely as long as necessary. While we expect we will need to tweak our systems here or for maximum efficiency, the teams are very comfortable with the technology supporting the distributed workforce.