WHEN YOUR WORKFORCE IS REMOTE

5 FUNDAMENTAL SECURITY ACTIONS

Remote work forces are keeping many organizations going. But configuration changes to accommodate remote work can expose your critical data.

Here are five fundamental cybersecurity actions you can take to avoid these exposures and how RedSeal will help you:

1. **Know the impact of network changes before you make them.**
   RedSeal alerts you to issues as you open ports and protocols to allow remote worker access. You'll see what internal host(s) may be exposed, and if any network segmentation policy you've implemented would be impacted—before you make a change.

2. **Verify that all endpoints (including remote laptops) have up-to-date protections.**
   RedSeal inputs information from all available endpoint solutions and rationalizes it so you can verify you have full coverage of your endpoints, including remote laptops. You'll know if up-to-date security software is installed on all remote endpoints, reducing remote employees' vulnerability to attacks.

3. **Discover unscanned subnets—vulnerabilities may be newly exposed.**
   RedSeal helps ensure that you've scanned all your systems to identify vulnerabilities that might be exposed due to the additional access allowed by new VPN connections.

4. **When you identify an incident, quickly view containment options.**
   When you detect an indicator of compromise (IOC), RedSeal can determine which device is showing the IOC, where it is logically and physically, and which VPN connection or switch port it's connected to.

5. **Continuously monitor your compliance with network segmentation policies.**
   RedSeal continuously monitors your network segmentation policies so you'll know they're in place and your remote workers have the right level of access.

REDSEAL

1600 Technology Drive, 4th Floor, San Jose, CA 95110

+1 408 641 2200 | 888 845 8169 | redseal.net | info@redseal.net

May 2020

WHEN YOUR WORKFORCE IS REMOTE

These issues won't go away once we're past the current crisis. Knowing what's on your network, how it's connected, and the associated risk remains fundamental as our networks continue to change.

- Some employees will continue to work remotely
- Cloud transitions can create unintended risks
- Valuable data and unpatchable devices will always need protection
- You'll need to comply with internal and industry segmentation policies
- Understanding network inventory is becoming more challenging. Cloud instances and/or shadow IT are easy to set up.
- There will always be too many issues to patch quickly. The best answer is to prioritize patching based on actual risk to your network

Our RedSeal Professional Service Engineers and Consulting Engineers are experienced with remote working and available to help walk you through any of the above steps. Let us know how we can help.

REDSEAL

1600 Technology Drive, 4th Floor, San Jose, CA 95110

+1 408 641 2200 | 888 845 8169 | redseal.net | info@redseal.net

May 2020