6 STEPS TO HELP SECURE YOUR NETWORK

1. Closely monitor your traffic.

Monitor the traffic coming in and going out of your firewall and read the reports carefully. Don't rely on alerts to flag dangerous activity. Make sure someone on your team understands the data and is prepared to take the necessary action.

2. Stay up to date on new threats.

Keep an eye on new threats as they're discovered and posted online. For example, you can have the U.S. Computer Emergency Readiness Team (US-CERT, a division of Homeland Security) email alerts to you about recently confirmed software vulnerabilities and exploits.

3. Regularly update your frontline defense.

To prevent threats from getting in, your business must deploy a strong frontline defense at the edge of the network. Make sure your firewall and anti-virus software is secure by enabling regular updates.

4. Train your employees on security protocols.

Train employees on an ongoing basis so they understand any changes to your acceptable use policy. Also, encourage a "neighborhood watch" approach to security. If an employee notices anything suspicious, such as not being able to log into an email account right away, he or she should notify the appropriate person immediately.

5. Protect against data loss.

Install an offline data protection solution. This type of device can protect your business from data loss if your network's security is breached.

6. Partner with a Managed Services Provider.

Working with a Managed IT Services Provider (MSP) is an effective step toward protecting your business from threats. Many MSPs offer a range of proactive support that includes 24/7 monitoring, data encryption and backup, real-time threat prevention and elimination, network and firewall protection, security awareness training and more.

NEXT STEPS

Are you ready to build a cybersecurity plan for your business?

cspire.com/cisco

cisco Partner
Gold Certified

c spire business