



5 Vital Steps to Complete Network Security



There are two types of companies: those who have already been hacked and those who are going to be hacked.

What type of company are you?

Studies have shown data breaches are not only more common than ever, they're also more expensive – totaling an average \$194 per record that's compromised. Can you afford this?

For most companies, the cost of a data breach is far too much – recovering all lost or stolen records is just the beginning, you've also got to worry about paying in terms of loss of client trust, missed business opportunities, and reputational damage.

Fortunately, data breach is easily avoidable when the proper steps are taken.



Here are **4 vital steps to complete network security** – allowing you to avoid costly data breach and safeguard confidential information:

1. Configure all devices and systems properly:

A large majority of breaches are due to firewall misconfiguration or general flaws within the firewall. That's why it's vital to implement the right security measures, which means making sure devices are updated, patches are applied, and absolutely everything is properly configured.

2. Educate staff with ongoing security training:

Your employees are the biggest threat to your network security. That's why it's important to educate staff members with ongoing security training – making sure to keep them informed and reminded of proper security best practices, such as strong passwords, how to identify phishing emails, and what websites to avoid.

3. Keep all wireless access points encrypted:

More than 50% of all wireless networks aren't encrypted, which means they're left open to attackers looking to steal sensitive data and wreak havoc on companies. Make sure you've encrypted all wireless access points using WPA2 encryption – ensuring a highly complex key is used to avoid a dictionary attack.

4. Block inappropriate websites from being accessed:

Your employees likely browse the web once in a while – passing the time on social media platforms, online gaming websites, or video streaming websites. This often leads to malware infection as most of these inappropriate and time-wasting sites are malware ridden. Use web-content filtering software to set controls on what can be accessed via your network.



Veltec Networks is your trusted technology partner – we're here to help you achieve complete network security to prevent costly breaches. Call us at 855-5-VELTEC or send a message over to info@veltecnetworks.com.

855-5-VELTEC
(855) 583-5832

2051 Junction Avenue | Suite 218 | San Jose, CA 95131
www.veltecnetworks.com | info@veltecnetworks.com