

# HOW TO BOOST YOUR NETWORK'S IMMUNE SYSTEM

A malware attack is nasty business; this infectious software can latch to legitimate code and spread throughout your whole system. It can lurk in useful applications or replicate itself across the Internet.

But there are several measures you can take to mitigate these attacks and boost your network's defenses.

Click [here](#) to connect to our vendor line card and discover some of the most sophisticated security solutions available to help you and your customers mount a healthy defense against malicious software attacks.



## BE CONSISTENT

Keep your systems and antivirus databases up to date. A lapse in these critical defenses leaves you vulnerable.

## KNOW THE SIGNS.

Train yourself and others how to spot potential attacks. Understanding the tactics and entrance points of cybercriminals enables you to better recognize and avoid threats.

## CHOOSE WISELY.

Configure your firewall to whitelist only the specific ports and hosts you need.

## MAKE IT DIFFICULT.

Keep your passwords strong. Use at least 15 characters or a phrase, such as “Maryhadalittlelamb”, “Youwillfindmeatthebeach”, “Livelongandprosper”, etc. A longer password makes you a less attractive target to a bad actor.

## LAYER UP.

Add multi-factor authentication for users and employees. The more access layers you have in place the better.

## YOU DON'T NEED IT.

Use a least-privilege model in your IT environment. Limit access rights for users to the bare minimum permissions they need to perform their work.

## BACK IT UP.

Make regular backups of data to multiple trustworthy sources and off-site.

## STAY ALERT.

Continuously audit your IT systems for suspicious activity. Apply patches and run vulnerability scans regularly to catch risks.