IT 365

BEST PRACTICE GUIDE

Endpoint security…

Delivering cyber protection in depth

First the bad news: your IT security can't stop every virus or piece of malware from getting into your systems. Worse – there's a good chance that you've already got rogue software somewhere in your digital network.

Now the good news: when you adopt a layered approach to digital security, you make it very difficult for any of that nasty-ware to do any damage. Those security layers include endpoint security – a set of software tools that provide active threat protection.

Every day, endpoint security solutions repel massive numbers of malware attacks from a myriad of sources. Malware can be triggered by someone simply visiting a website, clicking a link in an email or connecting an infected USB stick into their computer. A comprehensive endpoint security solution detects and reacts to all these activities, and scans all incoming data for dangers.

The solution in more in detail...

HOW ENDPOINT SECURITY PROTECTS YOUR BUSINESS

To provide protection in depth, endpoint security starts by making your systems less vulnerable to attack. Every device and every network connected to the internet broadcasts signals that can reveal vulnerabilities to cybercriminals. A robust endpoint security solution minimises these signals, reducing the risk of your computers being targeted.

Another layer of endpoint security monitors the data arriving on your devices, whether it's someone browsing a website, downloading a PDF or opening a data file.

The challenge of all digital security systems is being able to detect new threats. Traditional anti-virus software has always been one step behind the cybercriminals, as it only works against known viruses.

Today's advanced endpoint solutions overcome this by using advanced techniques to detect suspicious activity and software, even when the specific threat is new and unknown.

Once a threat is detected, the security system takes appropriate measures to isolate rogue code, protect data and alert the administrator.

THE COMPONENTS OF AN ENDPOINT SECURITY SYSTEM

Anti-malware: Malicious code can enter your systems from many different sources, both inside and outside your business. Advanced anti-malware identifies and flags potential malware problems.

Anti-ransomware: Hugely popular with cybercriminals, ransomware has proved very difficult to prevent. However, the latest tools are now helping organisations block many of these attacks.

Anti-virus: Once inside your systems, a software virus replicates itself in order to infect other devices and data. Anti-virus solutions detect and contain the danger.

Content filtering: Digitally monitoring all the content being accessed by device users is an essential component of endpoint security.

The administrator: While endpoint security systems detect and repel most threats automatically, there's still a place for human analysis and intervention.

WE CAN HELP YOU IMPLEMENT ENDPOINT SECURITY

Because our clients need to be kept safe from the latest threats and risks, we stay up to date with the newest tools and best practices for digital security.

If you want to know how to further protect your business against cybersecurity risks, including the threat of cybercrime, give us a call on 0808 168 9135 or email enquiries@itsupport365.co.uk. We would be pleased to have a no-obligation conversation with you.

Alternatively, follow us as we share news updates and information on Twitter, Facebook and LinkedIn.

Your digital systems and data face many different risks, from flood, fire, hardware failure, accident or cybercrime. Whatever the threat, if you lose data, it could kill your business. Implementing robust endpoint security is an important part of your overall business continuity strategy.