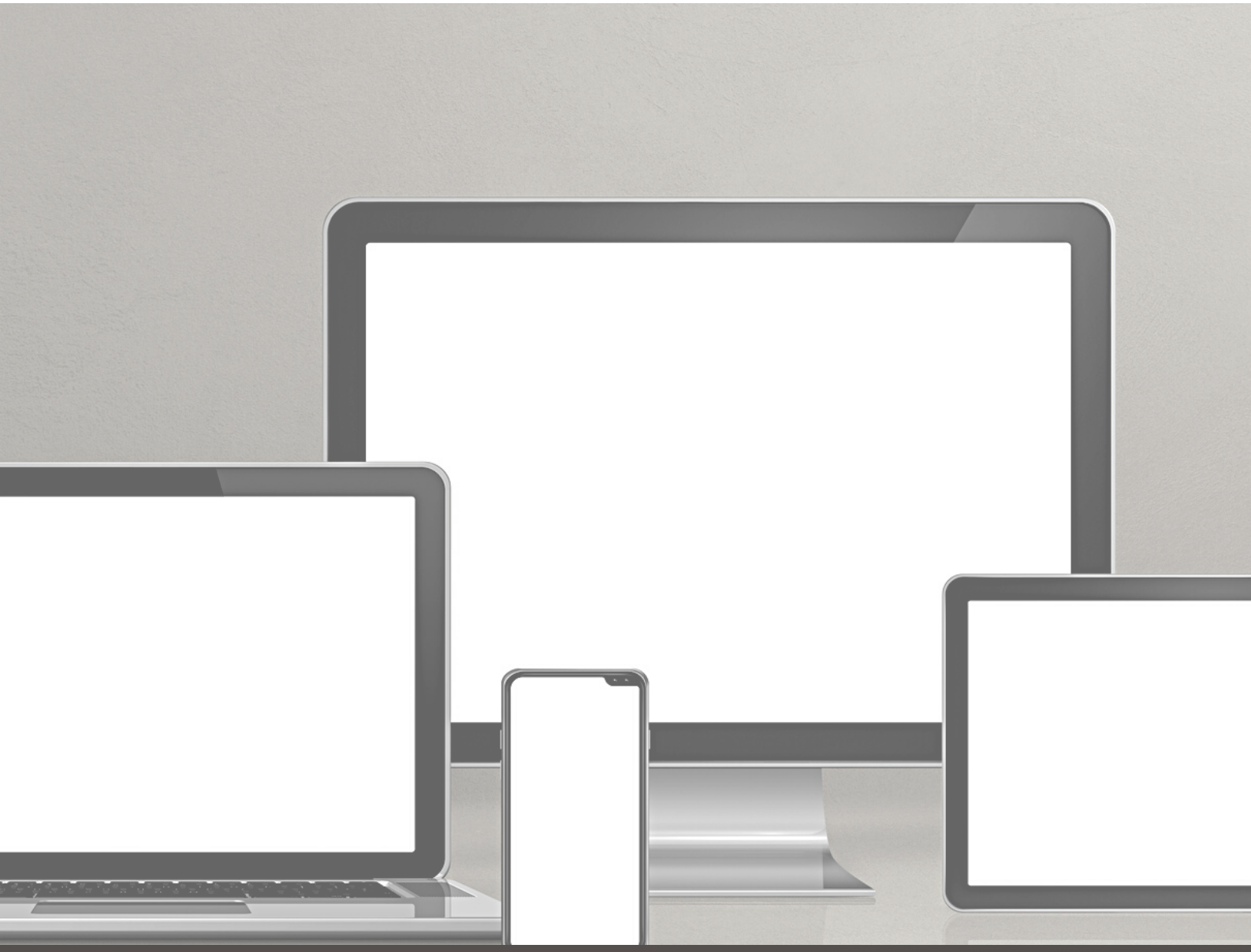
6 STEPS TO PROTECT YOUR ENDPOINTS



www.itguys.com
020 7241 2255
8 Woodberry Down, London N4 2TG.
info@itguys.com

Endpoints make up much of a company's network and IT infrastructure.

All of the computers, mobile devices, servers, and smart gadgets in your business that are connected to the company network as well as other IoT devices.

The number of endpoints a company has will vary by business size.

- Companies with less than 50 employees have about 22 endpoints.
- Small businesses with 50-100 employees have roughly 114.
- Enterprise organizations with 1,000+ employees average 1,920 endpoints.

Each of those devices is a chance for a hacker to penetrate a company's defences. They could plant malware or gain access to sensitive company data. An endpoint security strategy addresses endpoint risk and puts focused tactics in place.

> **64% OF ORGANIZATIONS HAVE EXPERIENCED ONE OR MORE COMPROMISING ENDPOINT ATTACKS.**

This guide will provide you with six straightforward solutions focusing on endpoint protection.

1. Address Password Vulnerabilities

Passwords are one of the biggest vulnerabilities when it comes to endpoints. The news reports large data breaches all the time related to leaked passwords. For example, there was the RockYou2021 breach. It exposed the largest number of passwords ever – 3.2 billion.

Poor password security and breaches make credential theft one of the biggest dangers to cybersecurity. Address password vulnerabilities in your endpoints by:

- Training employees on proper password creation and handling.
- Look for passwordless solutions, like biometrics.
- Install multi-factor authentication (MFA) on all accounts.

2. Stop Malware Infection Before OS Boot

USB drives (also known as flash drives) are a popular giveaway item at trade shows. But an innocent-looking USB can actually cause a breach. One trick that hackers use to gain access to a computer is to boot it from a USB device containing malicious code.

There are certain precautions you can take to prevent this from happening. One of these is ensuring you're using firmware protection that covers two areas. These include Trusted Platform Module (TPM) and Unified Extensible Firmware Interface (UEFI) Security.

TPM is resistant to physical tampering and tampering via malware. It looks at whether the boot process is occurring properly. It also monitors for the presence of anomalous behaviour. Additionally, seek devices and security solutions that allow you to disable USB boots.

3. Update All Endpoint Security Solutions

You should regularly update your endpoint security solutions. It's best to automate software updates if possible so they aren't left to chance.

Firmware updates are often forgotten about. One reason is that they don't usually pop up the same types of warnings as software updates. But they are just as important for ensuring your devices remain secure and protected.

It's best to have an IT professional managing all your endpoint updates. They'll make sure updates happen in a timely fashion. They will also ensure that devices and software update smoothly.

4. Use Modern Device & User Authentication

How are you authenticating users to access your network, business apps, and data? If you are using only a username and password, then your company is at high risk of a breach.

Use two modern methods for authentication:

- Contextual authentication
- Zero Trust approach Contextual authentication takes MFA a step further.

It looks at context-based cues for authentication and security policies. These include several things. Such as, what time of day someone is logging in, their geographic location, and the device they are using.

Zero Trust is an approach that continuously monitors your network. It ensures every entity in a network belongs there. Safelisting of devices is an example of this approach. You approve all devices for access to your network and block all others by default.

5. Apply Security Policies Throughout the Device Lifecycle

From the time a device is first purchased to the time it retires, you need to have security protocols in place. Tools like Microsoft AutoPilot and SEMM allow companies to automate. They deploy healthy security practices across each lifecycle phase. This ensures a company doesn't miss any critical steps.

Examples of device lifecycle security include when a device is first issued to a user. This is when you should remove unnecessary privileges. When a device moves from one user to another, it needs to be properly cleaned of old data. And reconfigured for the new user. When you retire a device, it should be properly scrubbed. This means deleting all information and disconnecting it from any accounts.

6. Prepare for Device Loss or Theft

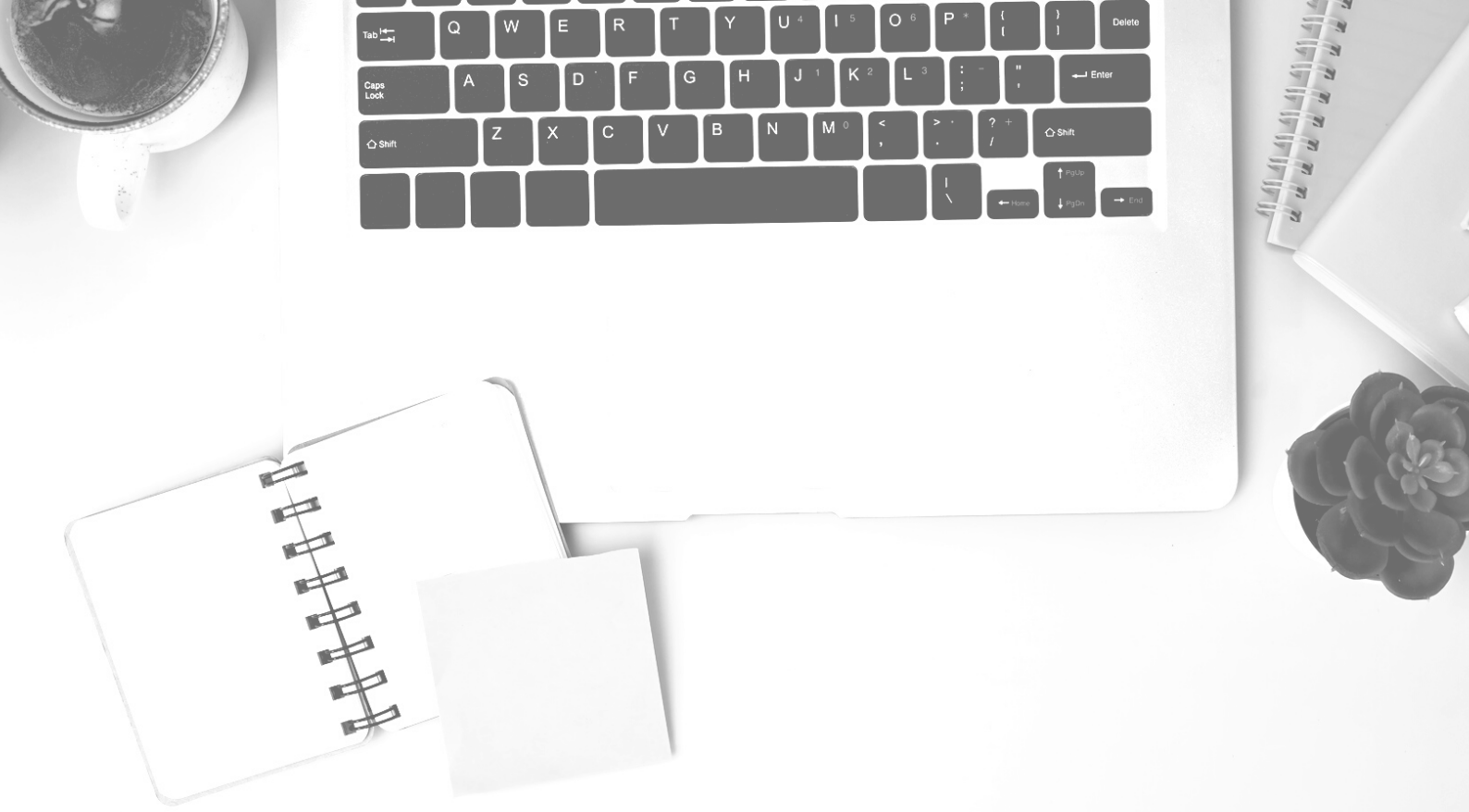
Unfortunately, mobile devices and laptops get lost or stolen. When that happens, you should have a sequence of events that can take place immediately.

This prevents the company from the risk of data and exposed business accounts. Prepare in advance for potential device loss through backup solutions. Also, you should use endpoint security that allows remote lock and wipe for devices.

REDUCE YOUR ENDPOINT RISK TODAY!

By implementing robust endpoint security step-by-step, we will ensure your organisation is secure. Contact us today for a free consultation.

Contact us today on 0207 241 2255



www.itguys.com

Follow us:

Contact us:

020 7241 2255

info@itguys.com