Managed Endpoint Detection and Response

Paladin IT

The best way to manage today's security threats

Security used to be so simple. You installed anti-virus (AV) solutions, trained employees not to click on unknown links, and kept software and websites up to date.

AV solutions have done a great job of keeping small and medium-sized businesses (SMBs) safe for many years. However, the threat patterns are changing, and SMBs need a different type of protection to combat these increasingly sophisticated, severe attacks. Here's why: AV solutions rely on signatures to detect threats, but the latest threats don't use signatures and can slip through and enter your company's networks undetected.

Here are a few examples of some of the risks we're seeing in the marketplace now:

- Weaponized documents that may seem like harmless PDF attachments in your emails but execute attacks once they enter your network.
- Fileless threats that don't require downloads, but execute from memory, making them difficult to identify.
- Zero-day threats that find an unknown computer vulnerability and exploit it before software or hardware providers can issue updates.
- And of course, continued ransomware attacks, which can disable IT networks as cyber-attackers demand huge ransoms to restore data and services.

82% of SMBs say they have experienced a cyberattack that their AV systems didn't catch.

Source: Ponemon, 2018.

"The ransomware attack was the last straw. It took days to restore our systems. We've upgraded our security system with Managed Endpoint Detection and Response to keep our business safe from these types of threats moving forward."

Keep Your Business Safe from the Latest Threats

You want to keep your business, employees, and all your devices safe from cyberattacks. And we all know that mobile devices are often the weakest link of IT security, as workers use less caution on-the-go than they do in the office. Here's why Managed Endpoint Detection and Response (EDR) is the best choice now for your IT security and business continuity.

Managed Endpoint Detection and Response	Anti-Virus Solutions
Gain freedom from ransomware by rolling back devices to their pre-infection state.	Can't roll back to a pre-infection state, increasing your ransomware risks.
Use artificial intelligence (AI) to detect and prevent both current and emerging threats, with continual updates to the platform.	Use signatures to identify threats, meaning capabilities lag cyber-attackers' latest strategies.
Monitor processes before, during, and after execution, to prevent new threats from slipping in.	Fly blind during execution, creating an entry point for new threats from savvy attackers.
Monitor your systems in real-time.	Rely on daily or weekly scans, increasing your risks.
Keeps device performance fast with continual monitoring.	Can slow down your device performance with long scans.

Never worry about ransomware again with Managed EDR. Just click and restore your devices to their pre-infection state.

How Managed EDR Benefits You

- **Protect your business from ransomware attacks** – Gain peace of mind by using Managed EDR to roll back any and all devices to their pre-threat state. Simply click and restore infected machines to full productivity, no matter which strain of ransomware is holding them hostage. There's no need to pay expensive ransoms to cyber-attackers or hire high-priced consultants to rebuild network access. Managed EDR pays for itself by keeping you safe and secure.
- **Increase employee productivity** – Eliminate threats that outwit traditional AV solutions and maintain faster device performance, creating fewer distractions that eat into employee productivity.
- **Let the experts manage it for you** – Don't spend time trying to support and manage your own systems and security. Focus on running and growing your business, with ongoing support from your managed service provider.

Need more information?

Paladin IT
https://www.paladinit.co.uk/
info@paladinit.co.uk
020 3026 0834