CYBERSLEUTH®
NEVER TRUST.ALWAYS VERIFY

Managed Endpoint Detection and Response

The best way to manage today's security threats

Security used to be so simple for the average business. You installed anti-virus (AV) solutions, trained employees not to click on unknown links, and kept software and websites up to date. For a few low-risk companies, that may still be the case, but the vast majority of small to midsize companies now need to fortify against new, advanced threats that can get around traditional AV.

With the rise of more advanced threat vectors and the use of Work-from-Home technologies businesses are facing greater threats to data and workflow and need a different type of protection to mitigate that risk.

The 2021 "Cost of a Data Breach Report" by IBM and the Ponemon Institute states that:

"The average total cost of a data breach was more than $1 million higher where remote working was a factor in causing the breach compared to breaches where remote working was not a factor."

Traditional AV isn't sufficient protection for your business because AV requires regular database updates of the current virus signatures to be effective. The protection afforded by AV software is only as good as the vendor's updates. New threats arise daily, and ensuring updates get pushed out in a timely fashion is a best-effort scenario. Often, threats are discovered only after the damage is done.

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.
- Ransomware attacks, which can disable IT networks and lock you out of your data/workflow.

Advanced Threats Continue to Rise
Global ransomware attacks increased by 151% from 2020-2021 and continue to rise. (304.7 million attacks worldwide in 2021)[1]

Keep Your Business Safe from the Latest Threats

Hybrid work is a growing trend that expands your effiency and improves your employees work/life balance, but it comes with cyber risks you need to manage.

You want to protect your organization against cyberattacks that put your employees, customers, and your business reputation at risk. 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.
Configure automated system remediation for fast threat incident response.	Manually gather information / investigate the health of the endpoint and remediate any misconfigurations or unwanted system changes.
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

- **Minimize costly downtime caused by threat incidents –** Protect against damage done by the latest threats with fast| AI-based threat detection, containment, and automated system remediation. Use Managed EDR to save time and protect your bottom line.
- **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?

CyberSleuth®

http://www.cybersleuthusa.com

cybersecurity@cybersleuthusa.com

(910) 685-7221

Source:

[1] Mid-Year Update: 2021 SonicWall Cyber Threat Report / 2021 Global Cyberattack Trends