C&T SOLUTIONS, INC

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 2023 "Cost of a Data Breach Report" by IBM and the Ponemon Institute states that:

"Organizations with fewer than 500 employees reported that the average impact of a data breach increased (2022 to 2023) from USD 2.92 million to USD 3.31 million or 13.4%."[1]

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 on time 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**

Nearly one-quarter of cyber attacks in 2023 involved ransomware.[1]

Keep Your Business Safe from the Latest Threats

Hybrid work is a growing trend that expands your efficiency 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 for your IT security and business continuity.

[1] *Source: Cost of a data breach 2023 | IBM – (accessed 2024-01-19)*

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 current and emerging threats, with continual updates to the platform.	Use signatures to identify threats, resulting in capabilities that lag behind the latest strategies of cyber-criminals.
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 Endpoint Detection and Response. Just click and restore your devices to their pre-infection state.

How Endpoint Detection and Response 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.
- **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 services provider.**

Need more information?

C&T Solutions, Inc.

Company URL

support@c-tsol.com

(601) 300-4251