CALTEC SOLUTIONS

MANAGED ENDPOINT DETECTION AND RESPONSE (EDR)

Confronting today's cyber threats

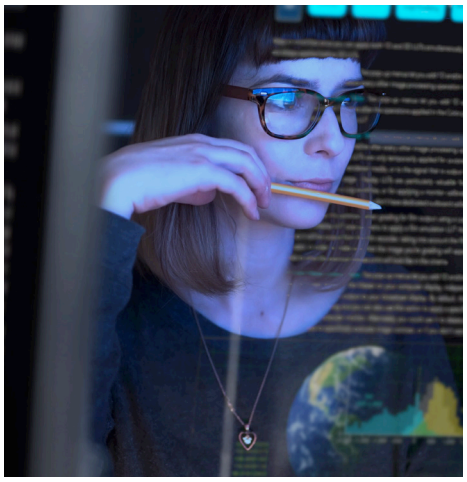
with cutting-edge technologies and tactics

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 up to date. That day is gone. Small to midsize companies now need to fortify against new, advanced, real-time threats that can get around traditional antivirus solutions.

You need a cybersecurity tool that can keep up with how your employees work and the vulnerabilities they may inadvertently open in the process. Gartner has predicted that "by 2025, lack of talent or human failure will be responsible for over half of significant cyber incidents."[1]

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.



Here's why Managed Endpoint Detection and Response (EDR) is the best choice now for your IT security and business continuity.

- Gain freedom from ransomware by rolling back devices to their pre-infection state.
- Use artificial intelligence (AI) to detect and prevent both current and emerging threats, with continual updates to the platform.
- Configure automated system remediation for fast threat incident response.
- Monitor processes before, during, and after execution, to prevent new threats from entering.
- Monitor your systems in real-time.
- Keep optimal device performance utilizing continuous threat monitoring.

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.

How Endpoint Detection and Response benefits you.

- Minimize costly downtime caused by threat incidents
- Help increase employee productivity
- Maintain device performance, lowering the distractions that eat into employee productivity.
- Rely on IT security professionals to manage your cyber-security protocols
- Mitigate the negative impact of ransomware attacks

What's wrong with my current reliance on antivirus alone?

- You can't roll back to a pre-infection state, increasing your ransomware risks.
- You are usings signatures to identify threats resulting in a capabilities lag behind cyber-attackers' latest strategies.
- You must manually gather information / investigate the health of the endpoint and remediate any misconfigurations or unwanted system changes.
- You aren't doing real-time monitoring. Daily or weekly scans increase your risks.
- Your antivirus can slow down your device performance with long scans.

Need more information?

Caltec Solutions

http://www.caltecsolutions.com

info@caltecsolutions.com

604-761-4342