Cybersecurity Infinite Endpoint Protection

WHY ENDPOINT PROTECTION?

The majority of cyberattacks originate on end user devices, or endpoints. Cybercriminals oftentimes prey upon endpoint devices at local governments and schools to gain access to sensitive information or to deploy malware, including ransomware.

Every endpoint is a potential gateway into your network, so it's essential to continuously monitor for malicious activity. But with hundreds, maybe thousands of devices, this can be a daunting task for many public sector organizations. With built-in Infinite Endpoint Protection, Managed Detection & Response makes it easy.

OUR METHODOLOGY

When monitoring endpoint activity, not everything new is malicious, but nearly everything malicious is new. This principle is an integral part of our threat hunting methodology.

Our process of focusing on new endpoint activity enables our cybersecurity security experts to accurately identify and confirm threats — and alert you within minutes, 24/7.

REMOTE DEVICES INCLUDED

Devices are just as susceptible — if not more — to a cyberattack when users are working remotely because your traditional network perimeter defense controls aren't able to see them. Managed Detection & Response closes this gap with Infinite Endpoint Protection.

All Windows devices are monitored continuously — even if they are not connected to your network.

MANAGED THREAT DETECTION FOR THE PUBLIC SECTOR

Continuous analysis of your network traffic is essential to quickly detect and contain threats. Managed Detection & Response is a subscription service offering around-the-clock monitoring of your entire network, including endpoints, for any behavior that poses a risk to your environment.

KEY FEATURES

- All Windows devices are monitored continuously 24/7, even if users are not connected to your network
- Endpoint protection is automatically enabled for users in the office, at home, or on the road
- Effective methodology combines artificial intelligence with human intelligence to quickly detect threats

KEY BENEFITS

- Expert security analysts confirm suspicious activity and alert you within minutes
- Notifications can help you stop an incident before it becomes a breach
- Insight reduces the risk that a remote employee will unknowingly infect your network

Want more information?

Contact us at **tylertech.com/cybersecurity** | **800.772.2260**

TO-CS-MDR-FO-17613-22249-BE-0222