optec

Advanced Endpoint Detection and Response

Boost your Endpoint Security and Protect Against Fast-Moving Threats

As more and more people work remotely, the devices we use to connect to corporate networks, and to one another, have become a prime attack vector for nefarious actors. Whether your employees dial in from a mobile device at home or are using a laptop at the office, it can take just minutes, or sometimes even seconds, for sophisticated attacks to compromise these endpoints and, in turn, your organisation.

Since January 1, 2016, more than 4,000 ransomware attacks have occured daily on average

It's never been more important to implement an advanced endpoint detection and response (EDR) solution—one that provides real-time pre- and post-infection protection to stop attacks and reduce potential damage. However, first generation EDR solutions just can't keep up with the evolving threat. Many solutions require manual triage and generate a lot of noise. Antivirus protection alone is not sufficient for endpoints, either, as attackers may even attempt to download an antivirus uninstaller on a compromised system!

Enter **Optec's FortiEDR solution from Fortinet**, a global leader in cybersecurity solutions. FortiEDR is your critical weapon against endpoint intrusions, allowing you to:

- Proactively reduce your attack surface
- Prevent malware infections
- Detect and defuse potential threats in real-time

Optec's FortiEDR solution not only stops breaches and costly ransomware attacks, but it does so automatically and efficiently. You'll streamline your security operations, protect your people, and keep your critical production equipment online and working.

How it Works

FortiEDR is the only endpoint protection-plus-response solution that provides both pre-infection protection and post-infection response. Before this, solutions were mostly limited to pre-infection protection and post-infection detection. FortiEDR achieves all this with a lightweight footprint, allowing your business to:

- **Understand what's happening** at a granular, yet practical level. FortiEDR tracks system behaviour in detail so you can identify the specific activity that poses a risk, such as file encryption or outbound communication.
- **Take precise action** to stop risky activities, without impeding normal device operation to keep your system operational and online.
- **Respond immediately and appropriately** with predefined, customisable, and automated playbooks based on the risk tolerance of specific endpoints. Automated incident response and remediation might include terminating malicious processes, notifying users, or opening tickets.

How FortiEDR Post-Infection Protection Works

FortiEDR proactively identifies vulnerabilities and can shield them from exploit.

The FortiEDR agent on the endpoint blocks most file-based malware pre-execution to prevent infection.

When infection occurs, FortiEDR detects and defuses the threat in real time to contain damage.

Once the threat is contained, FortiEDR orchestrates incident response based on playbooks and cloud-based intelligence.

FortiEDR retains memory, snapshots, and provides guidance for forensic investigations.

Advanced, Automated Endpoint Protection, Detection and Response

Faced with fast-moving cybersecurity threats like ransomware, today's organisations need real-time protection to stop the attack and automated actions to prevent the attack from spreading and clean up any damage. With FortiEDR and managed services from Optec, you can rest assured that if something happens to your network, our experts can move quickly to address it.

Key capabilities of FortiEDR include discovery and risk mitigation, next-generation antivirus (NGAV), behaviour-based detection, real-time blocking, automated incident response, forensic investigation, threat hunting, and virtual patching capabilities. FortiEDR leverages the the Fortinet Security Fabric architecture and integrates with Security Fabric components such as FortiGate, FortiNAC, FortiSandbox, and FortiSEM.

Top Benefits

- **Stop ransomware and advanced threats** including file-less and in-memory attacks
- **Improve endpoint hygiene** by discovering potential vulnerabilities and automatically patching
- **Non-disruptive** to user's daily activity

Get Started Today with Next-Generation EDR and Optec Services

The first step is to properly configure and implement an advanced, real-time EDR solution, and Optec is here to help. Our expert Fortinet engineers are ready to help your organisation assess its existing security posture and create a customised security implementation plan to ensure successful and proactive architecture and planning.

This includes deployment and installation, configuration, playbook setup, customisation, and tailored training with your team. Our Fortinet experts can also provide 24/7 threat monitoring, alert triage, and remote remediation services.

Want to learn more? Get in touch with us on 01280 878597 or email us at sales@optec.co.uk.