MANAGED ENDPOINT PROTECTION SERVICE

DELIVERING MAXIMUM CYBER SECURITY PROTECTION

Every day, businesses must deal with the changing demands of cyber security. The need to continually raise the bar across the three key pillars of people, process and technology in order to effectively protect against an everchanging threat landscape, is an infinite challenge - one that businesses can seldom tackle on their own.

At CSI, we offer a partnership that gives you a perpetual edge over cyber security threats. Our advisory, professional and managed security services are brought together by a methodology that puts the reduction of risk at the heart of everything we do and ensures successful delivery of the security outcomes that underpin your business.

CSI's Managed Endpoint Protection Service helps clients to deploy, manage, optimise and leverage the right endpoint protection technologies in order to deliver maximum protection against malware and mitigate the risk of end user and network-based threats.

CSI's Managed Endpoint Protection Service

Attackers gain access to corporate data through enterprise endpoints, and signature-based malware detection is no longer effective against today's malicious actors.

We understand that cost, complexity and not knowing what data to collect from an endpoint can prevent organisations trying to move from traditional network controls to endpoint controls.

This is why CSI is partnering with Blackberry Cylance to leverage AI and machine learning capabilities that provide automated endpoint protection to detect and prevent attacks before they can execute.

CylancePROTECT® is an AI-based Endpoint Protection Platform that blocks cyberattacks and provides controls for safeguarding against sophisticated threats - no human intervention, internet connections, signature files or sandboxes are required.

BlackBerry®

Cybersecurity

GROW   SAVE   INNOVATE   PROTECT

Managed Endpoint Protection - Service Levels

CSI's Managed Endpoint Protection Service can be tailored to suit your requirements with two levels of AI-based anti-malware service available:

1. **BASE** – Servers, VDI and WVD only - capped at a maximum of 100 endpoints

2. **PROTECT** – Servers and end-user devices

SERVICE LEVELS	BASE	PROTECT
Service Management		
Cylance console read-only access	✓	✓
Service Desk - 8x5 core business hours	✓	
Service Desk - 24x7 for P1 incidents		✓
Incident Management	✓	✓
Monthly cadence calls		✓
Service Delivery Manager	optional	optional
Notifications & Threat Management		
Notifications ingested into CSI SOC via API integration	✓	✓
CSI SOC triage all threats and complete remediation where applicable	✓	✓
Policies		
Single global standard configuration policy across all devices	✓	
Custom policies can be set up where appropriate		✓
File or Directory Exclusions		
Exclusions (file or directory) required during and after onboarding phase	✓	✓
Enhanced Capabilities		
Control use of USB mass storage devices		✓
Stop unauthorised scripts from running		✓
Restrict new applications from being added to user devices		✓
Prevent malicious use of memory		✓

Additional Cyber Resilience Services from CSI

- Managed Web Filtering
- Managed Detection and Response
- Managed Phishing Defence
- Endpoint Privilege Management
- Vulnerability Assessment
- Extended Detection and Response