CYBERSEER
THE VISION TO PROTECT

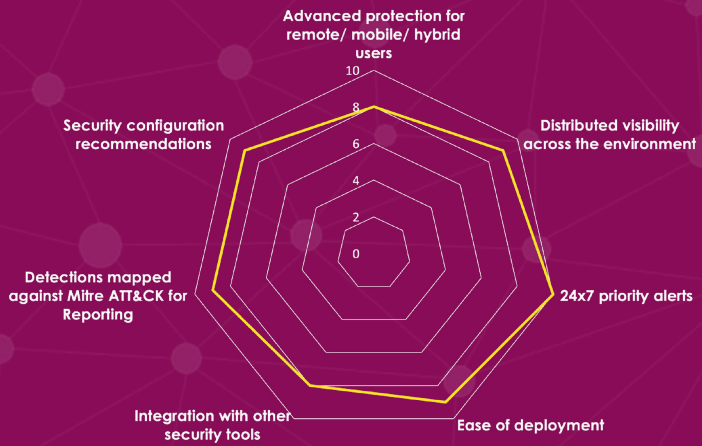
Microsoft Partner

Cyberseer SOC & Microsoft EDR

Solution brief

Discover how to get the most from Microsoft Defender for Endpoint when combined with a Managed Service from Cyberseer and get ahead of threats like ransomware, compromised insiders, accidental data loss and malicious insiders.

Defender for Endpoint Service at a glance:



Approximate read time: 6 min

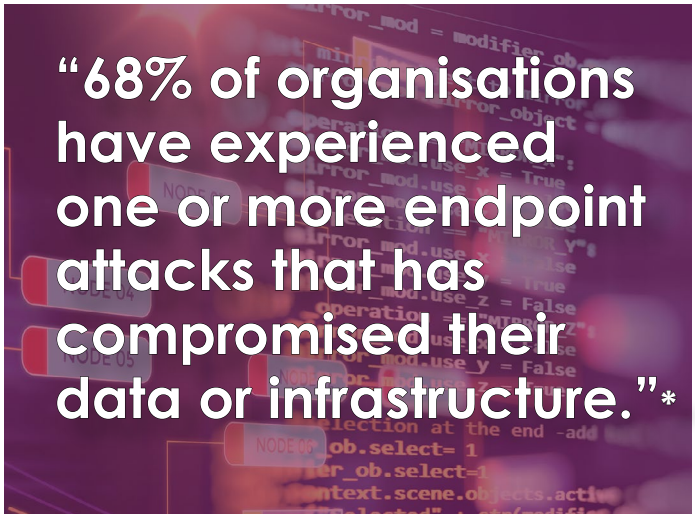
THE VISION TO PROTECT

Executive Summary & Key Benefits

- Cloud-powered vulnerability management, endpoint protection, endpoint detection and response and mobile threat defence.
- Utilise the full potential of Microsoft Defender for Endpoint.
- 24x7 threat detection & priority alerts.
- Actionable intelligence from Tier 3 Analysts.
- Reduced dwell time.
- Increased confidence in detections.
- Advanced threat hunting.
- Respond to issues using auto-remediation features.
- Unifed view of all discoverable endpoints and network devices.
- Attack surface reduction.

Cyberseer has integrated Microsoft Defender for Endpoint into its managed service offering to deliver managed detection and response across all endpoints and network devices. Cyberseer continually monitors your environment and our expert analysts triage and prioritise alerts, escalating threats that require your immediate attention.

The Challenge



The COVID-19 crisis of 2020 required organisations and their employees to adopt new working practices along with significant changes to their digital landscape. Whilst the increase in remote, mobile and hybrid working, alongside the adoption of Cloud based services, has delivered tremendous efficiency gains, it has also put user endpoint devices into sharp focus. Endpoints can now be considered the bastions of access to corporate data and services, that can remotely connect from anywhere. The security implications are obvious; poorly protected, trusted user endpoints connected to a corporate network are prized, easy targets for malicious actors.

Organisations must adopt the mindset that every endpoint can be the entry point for malicious activity. According to a study by the Ponemon Institute, "68% of organisations have experienced one or more endpoint attacks that successfully compromised data and/or their IT infrastructure. "*[1] Therefore, the risks posed by endpoints and their sensitive data is climbing and "the total average cost of a successful endpoint attack is $5million in lost productivity, system downtime, data theft, damage to the IT infrastructure, brand damage and fines."*[2]

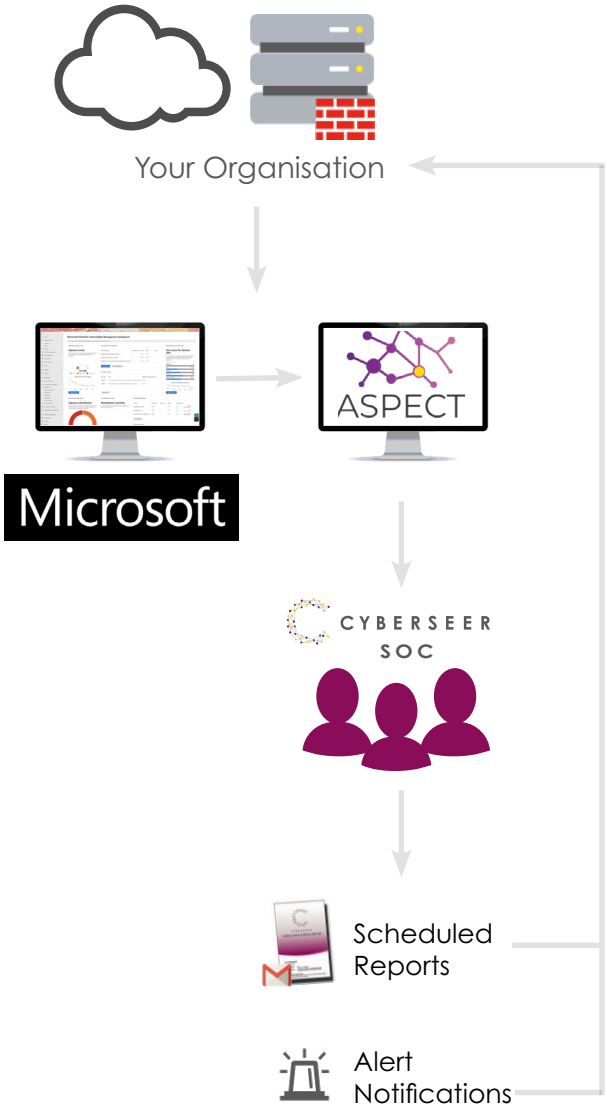
Cyber criminals actively target users and endpoints using phishing scams and social engineering to deliver malware that uses techniques that avoid detection by traditional anti-virus technologies. For example, Fileless malware combined with living-of-the-land (LOLbins) techniques are used. In this scenario, LOLbins - legitimate operating system tools, such as PowerShell, that are already installed on a system, are used to download and execute Fileless code that only runs in-memory. The upshot, there are no malicious files written to disk that can be detected on the target system.

The Solution

It is essential that organisations deploy advanced endpoint protection that provides visibility across the entire distributed estate. The technology must be capable of detecting suspicious behaviour and activity, as well as the full gamut of attacks in real time, offering both automated and manual response options to report and contain threats.

Deploying Cyberseer's Microsoft Defender for Endpoint Services equips organisations with comprehensive endpoint detection and response capabilities including:

- Cloud-powered behavioural next generation protection.
- Continual, risk-based vulnerability assessment
- Attack surface reduction
- Automated investigation and remediation capabilities
- Threat hunting



Cyberseer has integrated Microsoft Defender for Endpoint into ASPECT, the automation platform at the core of its MSS offering. ASPECT automates repetitive and time-consuming analyst tasks to enforce a 24/7 standardised workflow which eliminates human error whilst increasing the speed and effectiveness of our analysts, by escalating validated, enriched and fully anonymised priority threats that require attention. This combination of Defender and ASPECT means Cyberseer analysts are responding to priority issues ASAP which in turn reduces the time to respond minimising threat dwell time.

Cyberseer analysts work as an extension of your security team and build up a good knowledge of your environment and organisation. This style of working relationship is key as it provides further context for the analysts to understand the impact of a threat in your environment. Also, when you are contacted out-of-hours you will not need to bring the analyst up-to-speed on your environment which further reduces your overall response time.

All Cyberseer analysts are Tier 3 people who are trained to comprehensively threat hunt, triage, and investigate prioritised activity. An analyst will always perform an initial triage process to classify an incident, before alerting the customer using pre-defined communications channels and escalation contacts. The analyst will walk the customer through their current understanding of the incident and classification that has been assigned, and then support the customer with their response efforts and investigate the activity further.

Cyberseer provides all customers with three types of reports:

1. Priority incident reports detailing escalated priority threats
2. Weekly reports detailing all threat tickets raised during the week
3. Monthly trend reports detailing the number of incidents, threat classifications, breaches by attack phase, total threats and risk scores.

The Benefits

- Detection using behaviour and context, not rules to automatically identify unusual or anomalous behaviour.
- Identify compromised accounts, anomalies, accidental data loss, malicious insiders, and ransomware in real time across all environments.
- Threats accurately prioritised and qualified.
- Reduction in alert fatigue - only priority alerts are immediately escalated.
- Expert extension to SOC Staff, 24x7.
- Show value in weekly and monthly reports highlighting threats and areas of concern.
- Threat hunting.
- Indicators of compromise.

About Microsoft Defender for Endpoint

Microsoft Defender for Endpoint (MDE) combines anomaly-based detection, deterministic countermeasures, and automated response in a single modern interface to cover all tactics of MITRE ATT&CK framework. MDE empowers your enterprise to rapidly stop attacks, scale your security resources and evolve your defences by delivering best-in-class endpoint security across Windows, macOS, Linux, Android, iOS and network devices.

Microsoft Partner

About Cyberseer

Keeping your business safe is your number one priority. It's ours too. Fusing advanced detection technologies with deep forensic expertise, we help you join all the dots to rapidly distil threats. Our innovative solutions give you the confidence and proactive control you need – whatever comes your way.

We're here to help you keep your people and your reputation safe 24x7. It's what we do for companies around the world every day.

With Cyberseer, you're no longer on your own.

If you would like to know more about our Managed Security Service or the advanced technologies that we use, then please get in touch.

CYBERSEER

CONTACT US +44 (0)203 823 9030
info@cyberseer.net

Source: 1: https://expertinsights.com/insights/50-endpoint-security-stats-you-should-know/#:~:text=The%20Frequency%20Of%20Endpoint%20Attacks,-According%20to%20a&text=Further%20research%20by%20Ponemon%20found,involving%20compromised%20or%20stolen%20devices.
2: chrome-extension://efaidnbmnnnibpcajpcglclefindmkaj/https://www2.deloitte.com/content/dam/Deloitte/lu/Documents/risk/lu-endpoint-security-risks-rising.pdf