CYBERSEER
THE VISION TO PROTECT

DARKTRACE Microsoft

Cyberseer SOC & Darktrace NDR & Microsoft EDR

Solution brief

Discover how to get the most from Darktrace Network Detection and Response (NDR) when combined with Microsoft Defender for Endpoint (EDR) with Cyberseer's SOC to overcome resource issues and obtain comprehensive visibility and bolster advanced threat detection and response capabilities.

Approximate read time: 6 min

THE VISION TO PROTECT

Executive Summary & Key Benefits

- Cloud-powered vulnerability management, endpoint protection, detection and response.
- Utilise the full potential of Microsoft Defender for Endpoint.
- Darktraces’ strategic partnership with Microsoft enhances ease of integration.
- 24x7 threat detection & priority alerts.
- Reduced dwell time and increased confidence in detections.
- Advanced threat hunting and automated response capabilities.
- Unified view of all discoverable endpoints and network devices.
- Combined endpoint and network alerts for further context.
- Attack surface reduction.
- Combined Management Information.

Cyberseer has integrated Microsoft Defender for Endpoint (EDR) into its managed service offering for Darktrace (NDR), providing managed detection and response across all endpoints and network devices. Cyberseer has partnered with Darktrace and Microsoft Defender to deliver AI across all environments, whether Datacentre, Cloud or Saas. With comprehensive visibility, Cyberseer continually monitors your environment, triaging and prioritising alerts, and escalating critical threats that require your immediate attention.

The Challenge

Today’s businesses face complex challenges in securing the digital landscape, driven by digital transformation initiatives, remote work, cloud adoption and diverse infrastructures. As the threat landscape grows, security teams struggle to keep up while facing business pressures to rationalise spending.

Visibility: A Crucial Imperative

Achieving comprehensive visibility is crucial to effectively detect and respond to potential threats.

The Endpoint Challenge

The focus on user endpoint devices has intensified given their role as access points to corporate data and services from anywhere. The security implications are obvious; poorly protected and trusted user endpoints connected to a corporate network become prime targets for malicious actors. A study by the Ponemon Institute indicates that “68% of organisations have experienced one or more endpoint attacks that successfully compromised data and/or their IT infrastructure. Therefore, the risks posed by endpoints and their sensitive data are climbing” [*1] and “the total average cost of a successful endpoint attack is $5 million in lost productivity, system downtime, data theft, damage to the IT infrastructure, brand damage and fines.”[*2]

“68% of organisations have experienced one or more endpoint attacks that have compromised their data or infrastructure.” *

Cybercriminals employ sophisticated techniques such as file-less malware combined with living-of-the-land (LOLbins) techniques, which evade detection by traditional antivirus technologies. These techniques leverage legitimate operating system tools like PowerShell to execute file-less code that solely runs in memory, leaving no malicious traces written to disk that can be detected on the target system.

Protecting endpoints from a wide range of potential attacks requires a multi-layered approach that combines advanced technology, user education, and vigilant monitoring. With the evolving threat landscape, organisations must adapt their endpoint security strategies to effectively safeguard their digital assets and sensitive data.

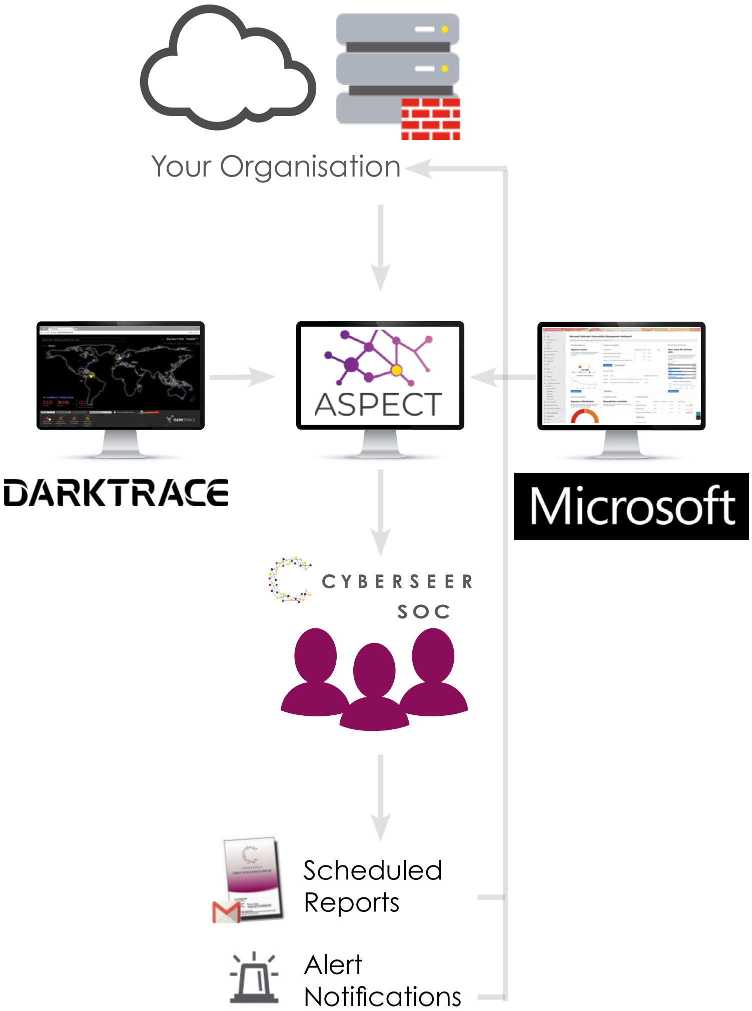
The Integration Challenge

Security teams struggle to gain a holistic view of the environment due to the use of multiple security solutions. The lack of integration between these best-in-class security tools makes it cumbersome for teams to correlate information for investigation and triage.

The Solution: Cyberseer SOC, Darktrace NDR & Microsoft EDR

Cyberseer's integration of Microsoft Defender EDR with Darktrace NDR through Cyberseer's ASPECT platform provides a comprehensive and powerful solution for managed detection and response. By combining the strengths of Daktrace AI-driven network monitoring and Microsoft Defender's endpoint protection, Cyberseer streamlines the process of alert enrichment, prioritisation, and escalation. Therefore reducing response times and minimising threat dwell time, enabling a quick and effective response to critical threats.

ASPECT from Cyberseer – is at the core of the Cyberseer SOC. It is a proprietary, 24x7, distributed platform that integrates with Daktrace (NDR) and Microsoft Defender (EDR) via API to pull alerts for enrichment, prioritisation, and escalation to our Forensic Analysts. The automation of these repetitive and time-consuming processes, along with the enrichment of alerts with internal and external contextual threat data, enables us to do more with less by efficiently and effectively identifying and routing priority threats to Analysts. This combination of Darktrace, Defender and ASPECT means Cyberseer Analysts are responding to priority issues A.S.A.P.



All Cyberseer Analysts are Tier 3 people who are trained to comprehensively threat hunt, triage, and investigate prioritised activity; and become an extension of your security team, building a deep understanding 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.

Cyberseer Analysts perform an initial triage process to classify an incident, before alerting the customer using pre-defined communication 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.

Benefits

- **Improved Visibility.**
  The combination of endpoint and network detection creates a holistic view of the environment, aiding in the identification of adversary tactics and techniques.

- **24/7 Priority Threat Detection.**
  Cyberseer's SOC offers around-the-clock threat detection, alleviating resource constraints and providing immediate attention to critical threats.

- **Reduced Time-to-Detection.**
  Rapid identification and prioritisation of threats lead to early intervention, minimising threat dwell time and mitigating business risks.

- **Enhanced Productivity**
  The Cyberseer SOC reduces alert fatigue whilst providing an effective threat detection process which boosts the productivity of customer security teams.

- **Accelerated Threat Hunting**
  Cyberseer's Tier 3 Analysts uncover subtle and sophisticated signals in both endpoint and network data sets, proactively identifying threats.

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 the entire 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

About Darktrace

Darktrace is a pioneer in AI driven cyber defence, utilising its Enterprise Immune System to detect diverse cyber threats at their early stages – including insider attacks, latent vulnerabilities, cloud-based threats, and even state-sponsored espionage. Darktrace founders also include cyber security experts from government intelligence backgrounds united in their mission to fundamentally transform organisations' ability to safeguard critical assets.

DARKTRACE

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-securityrisks-rising.pdf

axi | ADDISON LEE | MARKERSTUDY LIMITED | TRADEX INSURANCE SERVICES | ganado advocates | MIZUHO | Knight Frank