CYCRAFT

DATA SHEET

CYCRAFT MDR

MANAGED DETECTION AND RESPONSE MADE

F / A / S / T Fast / Accurate / Simple / Thorough

WHAT IS CYCRAFT EDR?

CyCraft Managed Detection and Response is uniquely designed to automatically detect malicious behavior and continuously monitor and manage the cyber situation of even large-scale enterprises with hundreds of thousands of endpoints; covered by Gartner and trusted as a leading solution in Asia, CyCraft MDR stops threats for all manner of orgs.

CYBER DEFENSE MATRIX

	Identify	Protect	Detect	Respond	Recover
Devices		Malware Protection Module Enabled	🟥	🟥	
Applications			🟥	🟥	
Networks			🟥	🟥	
Data					
Users			🟥	🟥	

CRITICAL DELIVERABLES

- Multi-group management console with the ability to carry out remediation and adjust CPU/memory load
- Rapid post-investigation reports replete with
  - Full storylines of any & all malicious activity
  - True, system-wide root cause analysis
  - Malicious domain, IP, URL analysis
  - Malware analysis
  - Proactive CyberTotal threat hunting
  - Graphs of all affect nodes and executions
  - A step-by-step plan for eradication
- Eradication confirmation
- Up-to-date Global Cyber Threat Intelligence integration
- Optional Managed Detection and Response analyst support

> “CyCraft's service provides customers with continuous 24/7 monitoring for severe cyber threats. Automatic behavior investigations and root cause analysis have dramatically increased their high-quality services. They have fewer false positives than other cybersecurity solutions and can validate the accuracy of alerts from other cybersecurity products.”
>
> Dayu Kao Prof./Dr.
> Bank SinoPac,
> Deputy Head of InfoSec Division

> “CyCraft's weekly Endpoint Forensic Report not only gives us the whole picture of all endpoints, but the details make internal investigations more efficient. It also helps us review IT policy and improve our IT procedure.”
>
> Associate Executive VP,
> Security and Risk Management,
> Banking, 30B+

READY FOR A DEMO?

Visit **CyCraft.com**

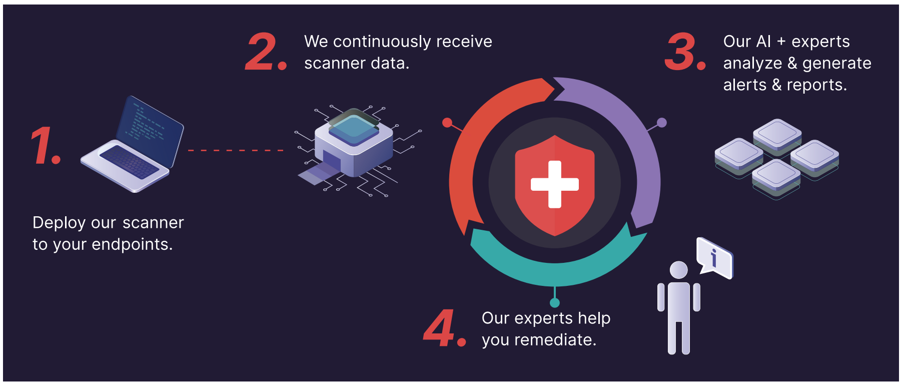
About CyCraft

CyCraft provides organizations worldwide with the innovative AI-driven technology necessary to stop cyber threats in the 2020s. CyCraft technology is uniquely designed to detect the latest trends in malicious behavior, automate investigations, and auto-triage alerts, allowing CyCraft customers to detect, track, contain, and eradicate threats in near real-time.

engage@cycraft.com

HOW DOES IT WORK?

With proprietary breakthroughs in forensic AI, CyCraft EDR performs the heavy lifting and automates monitoring, triage, investigation, and response planning of all threats to your organization, providing SOC teams with an efficient, data-driven workflow without guesswork. CyCraft EDR endpoint scanners collect forensic metadata and send it to CyCraft AI for rapid analysis to generate reports for your team to take action on, which can be done through Xensor. With the MDR upgrade, you can work with a human analyst to understand and remediate threats.


1. Deploy our scanner to your endpoints.
2. We continuously receive scanner data.
3. Our AI + experts analyze & generate alerts & reports.
4. Our experts help you remediate.

EASE OF USE

- **Deploys quickly** with standard deployment tools and has minimal and adjustable impact on CPU, memory, and network across Windows, Linux, and MacOS, including legacy versions
- **Hands-free:** Skip to the end of the investigative workflow with incident reports, dodging alerting, triage, validation and investigation
- **Replace your legacy AV** with CyCraft EDR's optional malware protection module

WHAT SETS CYCRAFT APART?

Unlike other EDR solutions, CyCraft has automated the detection, investigation, and forensic processes and can integrate them directly into SecOps. Now you can enjoy automated detection and response from a solution that is MITRE-validated and battle-tested against the most pernicious APTs on the planet with minimal human investment from your SOC team and maximum results.

CYCRAFT MEETS GDPR & JAPAN PRIVACY LAWS

- We collect far less data than Windows
- We don't collect payment data, presentation files, messaging/email contents, or anything that would violate GDPR/Privacy laws
- In fact, we aid in GDPR/Privacy law compliance:
  - We stop attackers from stealing your data
  - We enable quicker reporting to meet compliance

WHY IT MATTERS

URGENT PAIN RESOLVED

- **Speed to Truth**
  Receive automated investigations in geographically dispersed, large, hybrid environments across all endpoints in minutes, not days
- **Reduce SecOps Overhead**
  Get accurate post-investigation reports that avoid adding more false positives, avoid more alerts, and avoid more alert fatigue by giving you the final results you are looking for: what is malicious, where it is, and what to do about it
- **Lightweight & Hands-Free**
  Preserve operational performance during deployment and operation and say goodbye to querying and manual endpoint investigations, speeding your time to secure and freeing your teams to engage in other security tasks

BENEFITS TO CUSTOMERS + PARTNERS

- **Free Up Resource-Limited Teams** to tackle other security issues by leveraging CyCraft EDR's breakthrough SecOps automation and reduced workflow lag on incident investigations with fast, comprehensive, and precise automated whole-site endpoint reporting
- **Drastically Increase Security** and reduce response times and alert fatigue with accurate alert triage automation and automated forensic investigations 24/7
- **Know Clearly** how to handle every cyber incident and stop them early on before they metastasize into reportable breaches
- **Manage Endpoints** in groups regionally for large organizations through a simple and intuitive management console
- **MDR Upgrade:** Responsive and reactive human analyst support to immediately relieve any friction in the detections and response process