CYCRAFT

SECURE FROM HOME

FOR FREE

We understand your business needs to keep going despite **Covid-19,** and we are here to **help**. As more remote endpoints are added to your organization, some of them newly purchased and others personal computers, you need to find a way to secure your organization when uncontrolled endpoints VPN directly into your internal network. Personal computers are often less secure than office computers and could have anything on them, including unknown threats, whether they be Mac, Windows, or Linux. Additionally, firewalls and other preventive security won't be able to stop those threats as VPNs are designed to bypass that type of security—opening up an alluring attack route: unsecured endpoints with direct access to the internal network.

SECURE FROM HOME

Your organization may be more at risk than ever before as relying on AV and native OS solutions can only go so far—they can't find the global root cause, detect lateral movement, find hidden devices, show you your organization-wide cybersecurity situation, or respond in time to save you. We can do all of those things and more: with CyCraft's lightweight Secure From Home solution combining NGAV (for prevention) + MDR (managed detection and response) all in one lightweight agent, you can rest assured that your work from home employees, and your whole organization will be secure from even the most advanced threats on the planet, 24/7.

Whether it is work from the office or work from home, we've got you covered. Stay cyber healthy and maintain business continuity in these challenging times with CyCraft.

CASE STUDY:
A TALE OF TWO FIRMS FACING OPERATION SKELETON

"It was the best of times, it was the worst of times, it was the age of wisdom, it was the age of foolishness…." Firms A & B are both world-leading hi-tech firms. Firm A is our client; Firm B wasn't, but soon became one. Both firms faced a sophisticated never-before-seen attack from one of the world's most notorious threat actors.

The attack was Operation Skeleton, a new type of fileless attack that abused the memory of Windows Domain Controllers to create a skeleton key which allowed them to log in with admin privileges to any system on the network. A true security nightmare. But luckily for Firm A, our MDR is sophisticated enough to detect this type of attack and prevent a breach from occurring. For Firm B, once they saw they had a problem, they called us in for incident response. We were able to show them exactly what the hackers did—every step and every exfiltration. If only they had deployed our solution earlier, they would have been spared IP theft.

We discover never before seen, highly sophisticated APT attacks and block them every day. Our AI produced a full report on every facet of the attack in minutes, for each client.

Unfortunately VPNing in only increases the likelihood of this kind of attack. You can prevent attacks like this on your organization by taking advantage of this Secure From Home program to secure your firm from work from home threats… for free.

SECURE FROM HOME … FOR FREE

We know the combination of Covid-19 and the sudden transition to WFH has been tough for everyone. That's why we are offering free MDR for our current clients' WFH endpoints from March 26th until June 30th. That means you have unlimited remote licenses for your organization until then. Contact us using your work email to get started right now: contact@cycraft.com

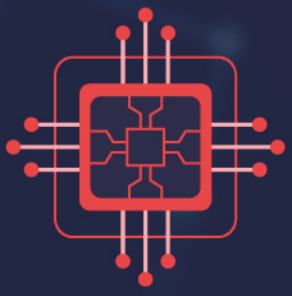
WITH OUR ALL-IN-ONE AGENT + CLOUD PLATFORM, YOUR ORGANIZATION WILL GET:

- NGAV: Real time blocking of known & suspicious threats
- MDR: Detection of the most advanced threats on the planet, with full forensic analysis and response, measured in minutes
  - Threat intelligence
  - UEBA analysis
  - Remediation playbooks
- Reporting & Visibility
  - System Forensics (caches, logins, scheduled jobs, auth/event logs and more)
  - Process, memory, & file inspection
  - MITRE ATT&CK mapping
  - Hidden device reporting
  - Full storylines of any & all hacker activity
  - True root cause analysis
  - Malicious domain, IP, URL analysis
  - Suspicious user accounts analysis
  - Malware analysis
  - Graphs of all affected nodes & executions
  - A plan for eradication & eradication confirmation

And when individual endpoints are not connected to your org's network you will still experience NGAV and single-endpoint MDR, so stop wasting your time panicking about remote endpoint security, querying your SIEM or EDR for C2 and AV logs for all the new endpoints coming in. Stop wasting time on prioritization and investigations. Start getting secure fast.

HOW IT WORKS

Install our Secure From Home scanner



We continuously receive the scanner data

Our AI & experts analyse the data to generate alerts & reports

Our experts help you eradicate hackers

HOW CAN WE DO THIS

We make use of the latest advances in AI such as GANs, DeepRL, & UEBA to analyze forensic evidence from multiple layers including artifact, endpoint, users, network, & threat intelligence, to prevent malware, breaches, data loss, and incidents and every other thing hackers do.

Supported Systems:

Windows: 7/8/10, Server 2008 - 2019
Mac: macOS 10.10 - 10.15
Linux: Ubuntu 9.10 - 18.04, Debian 7.0 - 9.0, RHEL 6.0 - 8.1, CentOS 6.0 - 8.0

FOLLOW & LEARN

cycraft.com
twitter.com/cycraft_corp
medium.com/@cycraft_corp
linkedin.com/company/cycraft/

INDUSTRY RECOGNITION

MITRE ATT&CK™

- Joined MITRE ATT&CK round two against APT29

CYBER SECURITY EXCELLENCE AWARDS ★ WINNER ★ 2020

- Winner of over 20 Cybersecurity excellence awards including: MDR, Forensics, Incident Response, and Artificial intelligence Gold awards as well as a best cybersecurity company Gold award

FIRST

- Member of FIRST—The premier Incident Response organization

ABOUT CYCRAFT

CyCraft secures government agencies, Fortune Global 500 firms, top banks and financial institutions in Asia, critical infrastructure, airlines, telecommunications, hi-tech firms, and SMEs in several APAC countries, including Taiwan, Singapore, Japan, Vietnam, and Thailand. We power SOCs with our proprietary and award-winning AI-driven MDR (managed detection and response), SOC (security operations center) operations software, TI (threat intelligence), Health Check, automated forensics, IR (incident response), and Secure From Home services.