



Securing the Cloud with Deception Technology

Enhanced cloud security with the latest
version of **The Platform™**

Thank you for downloading this CounterCraft Datasheet. Carahsoft is the distributor for CounterCraft Zero Trust solutions available via NASA SEWP V, ITES-SW2, NCPA & OMNIA Partners Company, and other contract vehicles.

To learn how to take the next step toward acquiring CounterCraft's solutions, please check out the following resources and information:



For additional resources:
carah.io/countercraftresources



For upcoming events:
carah.io/countercraftevents



For additional CounterCraft solutions:
carah.io/countercraftresources



For additional Cloud solutions:
carah.io/countercraftsolutions



To set up a meeting:
countercraft@carahsoft.com
888.662.2724



To purchase, check out the contract
vehicles available for procurement:
carah.io/countercraftcontracts

Securing the Cloud with Deception Technology



Product Brief

Securing the Cloud with Deception Technology

Enhanced cloud security with the latest version of **The Platform**TM

By 2025, Gartner estimates that over 95% of new digital workloads will be deployed on cloud-native platforms. That is an incredible increase, considering this number was just 30% in 2021¹. This significant shift is happening as businesses recognize the numerous advantages of migrating their systems and applications to the cloud.

This new paradigm allows organizations to leverage the benefits of scalability, flexibility, cost-effectiveness and collaboration offered by cloud computing. However, this transition comes full of challenges. According to Michael Warrilow, research vice president at Gartner, "the shift to the cloud has only accelerated over the past two years due to COVID-19, as organizations responded to a new business and social dynamic."

\$4.2M

the average cost of private a cloud data breach

\$5M

the average cost of public a cloud data breach

45%

of breaches occurred in the cloud

15%

initial attack vectors related to cloud misconfigurations²

95%

increase in cloud exploitation incidents

The shift to the cloud: A cyber storm

Organizations must navigate several hurdles to successfully migrate their IT infrastructure to the cloud. This move to the cloud presents several security challenges:

- / Migration of existing infrastructure to the cloud
- / Cloud environment vulnerabilities
- / Breach vulnerability leads to on-prem breaches
- / Traditional security tools are limited in the cloud
- / Memory evasion thanks to fileless malware

Secure the cloud with deception

The PlatformTM is redefining sophisticated security with the world's most advanced **cloud-first deception platform** for protecting critical areas of enterprise risk — cloud workloads, endpoints, identity and data. CounterCraft is the sole deception vendor offering comprehensive cloud capabilities, allowing organizations to protect Linux and Windows server VMs running across AWS and Azure and Docker containers. As of today, around 55% of CounterCraft customers are using our cloud services.



¹<https://www.gartner.com/en/newsroom/press-releases/2021-11-10-gartner-says-cloud-will-be-the-centerpiece-of-new-digital-experiences>

²<https://www.ibm.com/downloads/cas/3R8N1DZJ>

CounterCraft is the sole deception vendor offering comprehensive cloud capabilities.

CounterCraft's cloud-first solution defends public and private cloud workloads and on-prem data centers by generating telemetry on zero-day breaches, memory injection, ransomware and APTs thanks to kernel access. It delivers adversary intelligence to the SOC team about their cloud workloads, facilitating rapid threat hunting, investigation, and response. Our DevOps-friendly solution delivers quick and scalable deployment, superior threat intelligence, reduced complexity and immediate time-to-value.

Deploy deception in the cloud in minutes

Yes, you heard right. Unlike other deception vendors, **The Platform** is able to deploy enterprise level deception VMs for multiple use cases in just 46 minutes. There's no need to navigate Amazon or Azure configuration settings — you can effortlessly design and deploy campaigns in the cloud or in a hybrid environment, without leaving **The Platform**'s interface. It only takes 4-5 clicks to install a cloud server/VM and instrumentation in AWS or Azure.

Furthermore, **The Platform** includes pre-made use case templates ready to be deployed for multiple verticals from finance, critical infrastructure, ICS/OT, retail, healthcare and manufacturing. CounterCraft has analyzed the most successful and utilized campaigns among customers, and has included them as one-click-easy-to-install for security teams. The latest version of **The Platform** reduces deception deployment cost and time drastically for both in cloud and on prem solutions. CounterCraft's cloud workload solution provides an efficient and reliable platform for organizations that want to deploy fast and secure their cloud workloads in AWS and Azure.

Cloud detection and response shouldn't be complex

CounterCraft's powerful and privileged agent collects attack telemetry unavailable elsewhere and provides the deepest knowledge of threat actors' initial attack vectors and post-breach activity available today. CounterCraft's lightweight agent provides unique insights into threat actor behavior and techniques occurring on organizations' cloud workload VMs and containers.

The average CounterCraft customer:

- / deploys 4-10 internal and external use cases
- / detects an average of 7 adversaries in 2 months.

Supported Distributions

AWS EC2

- / Any AWS region
- / Any Host type
- / Any AMI (Windows, Linux)
- / Features: Deployment, Monitoring and Snapshots

Microsoft Azure

- / Any Azure region
- / Any Host type
- / Any Image (Windows, Linux)
- / Features: Deployment, Monitoring and Snapshot

Cloud Services

- / AWS EC2
- / Microsoft Azure
- / AWS S3 Buckets
- / AWS SQS
- / AWS SNS
- / AWS SecurityHub
- / Microsoft Sentinel

Supported Linux Distributions

- / CentOS 7, 8, 9
- / Debian 10
- / Red Hat Enterprise Linux 7, 8, 9
- / Ubuntu 18.04, 20.04
- / Linux ARM

Windows Server Support

- / Windows 7, 8, 10
- / Windows Server 2012, 2016, 2019
- / Windows XP







How deception in the cloud helps our customers

22% of cloud-based attacks observed by our Threat Intel Team used defense evasion techniques that bypassed EDR/XDRs. Active defense is essential, and deception technology helps security teams implement it.

It looks a little something like this: CounterCraft's deception technology proactively deflects adversaries into decoy VMs.

Security teams receive an early alert as soon as adversaries interact with a decoy. CounterCraft customers are spared from the feared “boom moment” as they are able to deflect and engage adversaries. By incorporating adversary cloud/ SaaS forensics through deception, organizations add a valuable complement to their existing EDR/XDR/SIEM security tools.

The results: an average of \$4.6 million saved by early detection

Customer	Threat	NGAV/EDR/XDR detected?	CounterCraft Detected?	Estimated Risk Averted*
\$25B Financial Services	Insider Threat			\$5.97M
\$32B Retail company	External Threat			\$3.28M
\$10B Critical Infrastructure	External Threat			\$4.82M

*Cost of a Data Breach Report 2022

CounterCraft customers are implementing a proactive defense solution to defend their cloud workloads and prevent real world breaches through **The Platform**. Here are more key features and benefits for our cloud workload solution:

- / Cloud detection and response on AWS, Azure and data center
- / Auto-deploy agent to cloud instances in AWS and Azure
- / One multi-cloud management console for endpoint, server, workloads, and more
- / Preserves workload immutability
- / Protect any cloud anywhere. Any workload anytime
- / Countless deployment hours saved to the SOC team.
- / Single pane of glass console for endpoint, server and workloads management
- / Forensic data for rapid threat hunting, investigation and response

About Us

CounterCraft is a software company that goes beyond detection and response to provide proactive cybersecurity solutions and detect attacks faster for the world’s leading organizations. Their premier product, CounterCraft **The Platform™**, consistently stops red teams, spear phishing, ransomware attacks and insider threats. This distributed deception platform is a global leader in active defense, with tooling that provides real-time intelligence and the capability to manipulate adversary behavior. Their technology stops attackers in pre-breach recon phases, integrates contextualized threat intel with incident response workflows, and saves money and time by helping security teams prioritize their actions. CounterCraft **The Platform** is used successfully around the globe by Fortune 500 companies and government organizations, including the US Department of Defense.

Find out more. Request a demo at  countercraftsec.com