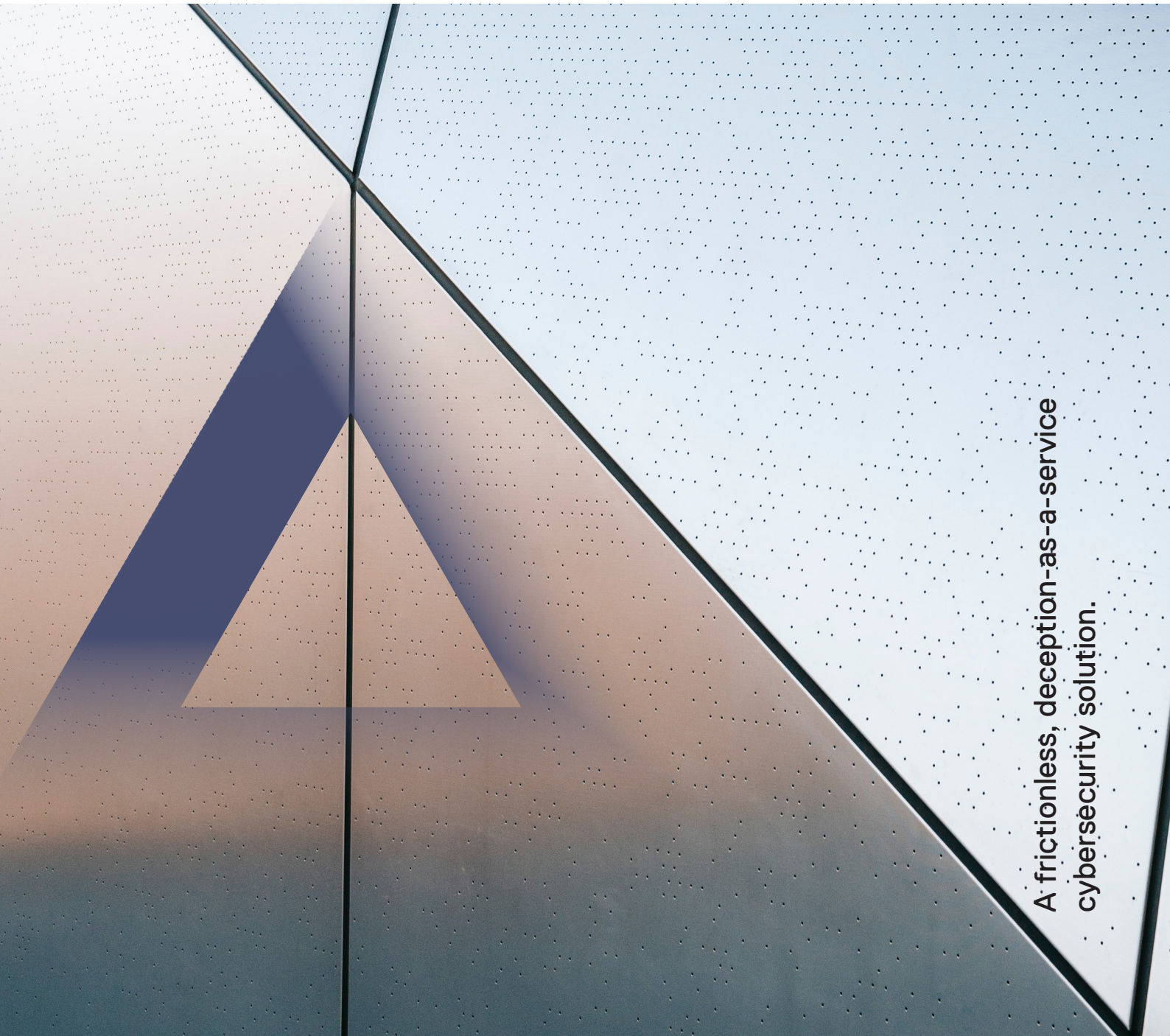
CounterCraft

Datasheet

CounterCraft The Edge™



The Edge™

Threat intelligence services that identify cyber threats before they attack your online IT assets, remote workers, and networks.

CounterCraft is redefining sophisticated security with the world's most advanced cloud-first deception services, created to protect critical areas of enterprise risk — cloud workloads, endpoints, identity and data. CounterCraft **The Edge**™ is a cloud-based managed service that is fast and easy to implement and delivers actionable threat intelligence tailored to your attack surface. Identify threats early—so you can adapt your defenses to stop them.

The Challenge

Until recently, VPNs were not considered to be a major cyberattack vector. Today, they are the primary access to enterprise applications and services, thanks in part to the increasingly remote workforce. As more enterprise services are accessed via teleworkers over VPNs, or are exposed as cloud-based services, the corporate attack surfaced has blossomed. More information and sensitive data is now communicated outside of known boundaries, using more personal devices, and across more different channels.

Cyber attackers have wasted no time in attempting to exploit under-secured VPNs, larger attack surfaces, and new vulnerabilities. Organizations might face the same threats and tactics, but the entire playing field has changed. Are your current security control sets effective against the new threats you face?

The Solution

CounterCraft **The Edge**™ is a fully managed service that provides early detection of external threats to your online IT assets, remote workers, and networks. The service is deployed and managed by CounterCraft, who creates threat intelligence campaigns using deception techniques, deploying attack vector discovery assets (breadcrumbs) to identify cyberthreats scouting your online IT assets from the outside. CounterCraft analyzes all surfaced threats and collects intelligence on the threat, the threat actor capabilities, and their intended target. Unlike generic threat intelligence feeds, CounterCraft alerts include information about attackers' Tactics, Techniques, and Procedures (TTPs) cross- referenced with the MITRE ATT&CK framework, as well as Indicators of Compromise (IOCs). You can easily feed this data into your incident response, SIEM, ticketing and other systems for taking action.

You choose the campaigns you want to deploy. Countercraft provides:


Dashboard


Infrastructure


Deployement


Support

The Edge services detect attacks in their initial stages, before they disrupt your organization.

Choose between different use cases that address your organization's most pressing, real-world vulnerabilities and deploy in a matter of days in the cloud:

Ransomware: Mitigate the threat of ransomware to your business by detecting the initial stages of targeted ransomware attacks.

VPN Attacks: Add a layer of assurance to your remote workers by deploying a vulnerable VPN service and associated breadcrumbs to detect threat actors searching for entry.

Spear Phishing: Mitigate the risk of spear phishing attacks penetrating your organization.

External Attack Surface: Provides early detection of attackers conducting technical reconnaissance of vulnerable external facing IT and cloud services associated with your on-line IT assets.

ICS/OT Network Protection: CounterCraft's approach does not require modifying existing SCADA/ICS networks. It provides early detection within your OT systems that goes hand in hand with operational continuity.

Active Directory Protection: Delivers actionable insight to reduce Active Directory and Azure AD attack surfaces by uncovering existing vulnerabilities and applying security best practices.

Supply Chain Attacks: An external-facing deception campaign is ideal for securing the supply chain, as it can serve the purpose of interception and deflection of the attacks as well be used to collect contextualized threat intelligence from the deception environment.

Insider Threats: Gives security teams the tools they need to enact a proactive, prevention-focused mitigation program to detect and identify threats, assess risk, and manage risk before an incident occurs.

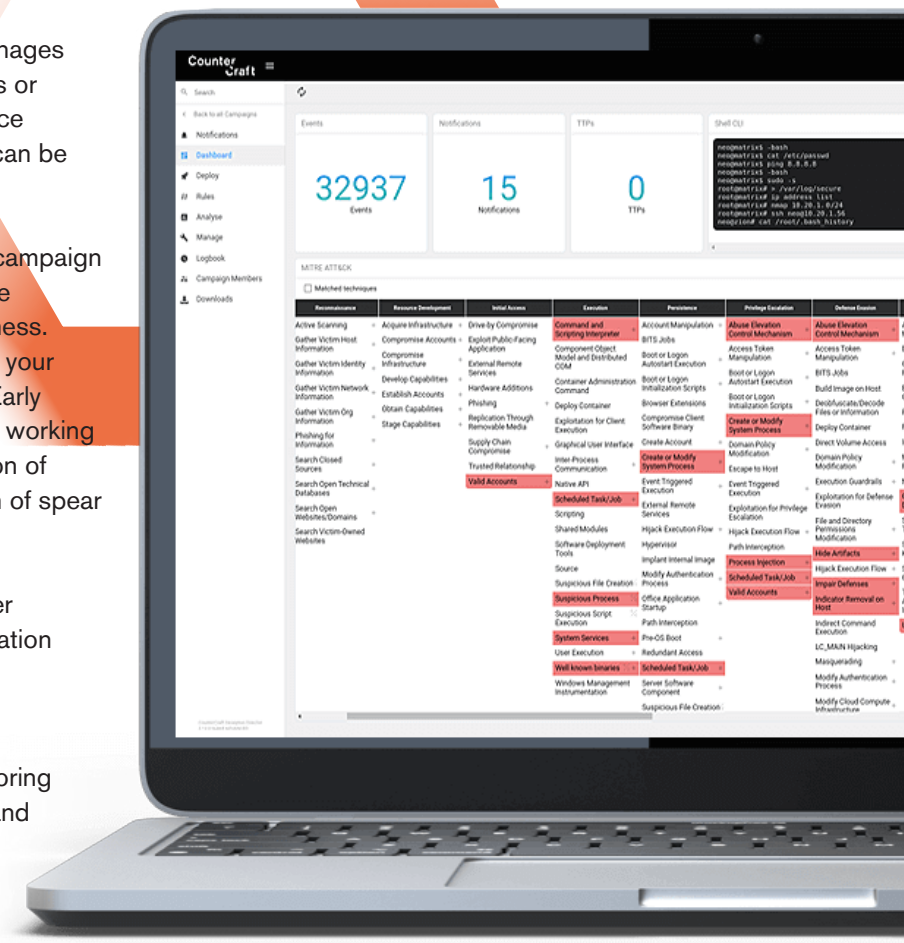
Features

1. **Plug and Play:** CounterCraft implements and manages the service. There is no need to dedicate resources or purchase, deploy, or configure infrastructure. Service terms are flexible with a monthly subscription that can be cancelled at any time.

2. **Tailored Campaigns:** CounterCraft deploys the campaign tailored to your specific organization, so you receive IOCs and TTP alerts targeted directly at your business. Intelligence events directly reflect threats attacking your online IT assets. Examples of campaigns include: Early detection of targeted ransomware attacks; remote working infrastructure assurance (VPN protection); detection of threat actor reconnaissance activities; investigation of spear phishing attacks.

3. **Rapid Deployment:** Begin a intelligence led cyber deception campaign and receive actionable information within hours.

4. **In-depth Actionable Data:** Our advanced monitoring dashboard enhances security, discovery, analysis and risk governance data while uncovering previously unidentified actors and cyber threats.



Business Benefits

/ No Additional Resources Needed

Our service requires no skilled staff or other internal resources from your team. As a turnkey service completely configured, managed, and delivered by CounterCraft **The Edge**™ automatically increases your team's productivity.

/ Proactively Protect Your Company

CounterCraft **The Edge**™ feeds can be connected with SIEM, TIP, SOAR, EDR, UEBA, and other tools for proactive defense. Use the data to block IP addresses, revoke credentials, harden firewalls, and take other measures to boost protections where needed. CounterCraft campaign data also can be integrated with orchestration solutions to automate response playbooks.

/ Improve Overall Security Effectiveness

CounterCraft provides high-impact intelligence, enriched by attackers' TTPs, IOCs, and threat actor characteristics. You receive contextualized profiles of external adversaries trying to compromise your remote working infrastructure or workers. You gain a time advantage, because decoys delay attackers as they try to identify vulnerabilities for exploitation.

/ Cover the New Attack Surface Cost-Effectively

For a simple monthly subscription, you can significantly improve reconnaissance and proactive defense of a much larger attack surface. At the same time, you gain enriched data that enhances capabilities of your existing systems.

/ Strengthen Your Strategy

Threat intelligence based on deception delivers actionable information for aligning corporate security strategy with available resources to build a stronger security posture. Information from CounterCraft **The Edge**™ provides threat intelligence breadth and depth for communicating the value of threat intelligence teams to key management and board members.

Start today

We have designed a low-friction journey for you to start enjoying the benefits of the service:

1 Choose a Campaign

CounterCraft **The Edge**™ offers campaigns suited to your organization's needs. These campaigns detect attackers of all types—from script kiddies to nation state threat actors—through deception assets created to identify different levels of penetration difficulty.

2 Contact our Sales Team

Access the full service description on our website and get in contact with us here.

3 Sign Up

Our team will help you expedite the sign up process to get off the ground quickly.

4 Enjoy the Service

The onboarding for **The Edge**™ is seamless and simple. Attend the onboarding tutorial, meet your account manager and deploy in just days.

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