CYCRAFT

DATA SHEET

THREATWALL

Next-Generation Threat Intelligence Gateway

WHAT IS THREATWALL?

The CyCraft ThreatWall Threat Intelligence Gateway (TIG) unifies automated detection and response with the latest in global threat intelligence surveillance in one multi-purpose box that stands guard 24/7/365.

ThreatWall blocks both potential inbound threats from entering and compromising your environment as well as outbound traffic towards any unauthorized or malicious C2 server.

CYBER DEFENSE MATRIX

	Identify	Protect	Detect	Respond	Recover
Devices					
Applications					
Networks		🟥	🟥	🟥	
Data					
Users					

	ThreatWall G8	ThreatWall T20
High availability (HA)	Architecture	
Network Interface	1G RJ45*8	10/1G SFP+*20
Management Interface	IG RJ45	
Hardware Bypass	RJ45 port pair *1	External
System Operation	HTTPS, SNMP v2/v3, GRISM XML script	
Data Format	Ethernet/PCAP	External
Advanced Processing	4Gbps	90Gbps
Forwarding and Replication	8Gbps	200GBps
IoC (IP/ Domain/ URL) Capacity	Max 1M	Max 10M
Power Supply Unit	AC 110V-220V	Dual AC 110V-220V

CYCRAFT ADVANTAGE

CyCraft customers choose us for our strong customer focus, ability to create internal/operational efficiencies, enhance and enrich decision making, improve compliance issues, tackle risk management, expert service and support, as well as our platform's functionality and overall performance.

As your organization grows and expands, your security team can lean on CyCraft to not only adapt and scale with you but ensure that you are ready to tackle the active and emerging cyber threats of today and tomorrow.

> *CyCraft's customer support provided excellent communication, reports, and response times, leaving us feeling confident and at ease with our security situation.*

Telecommunications,
Security Analyst

READY FOR A DEMO?

Visit **CyCraft.com**

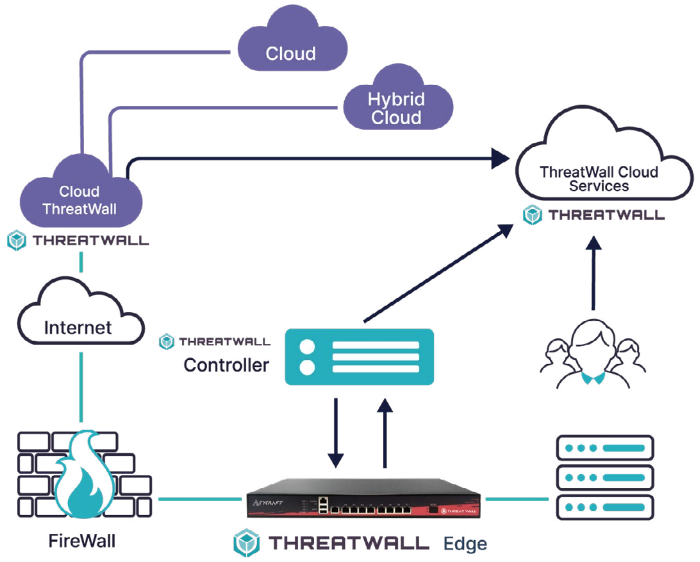
About CyCraft

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?

ThreatWall continuously scans north/south traffic for known malware, malicious IPs, and C2 servers. By integrating with our global threat intelligence surveillance platform CyberTotal, ThreatWall uniquely provides effective and efficient detection and blocking for your entire digital environment. In addition, ThreatWall can display all blocking records in real-time, provide automated reputation ratings for IPs, and supply analysts with enriched contextual threat intelligence for indicators of compromise (IoCs).



EASE OF USE

- Flexible and fast deployment: ThreatWall deploys in minutes dues to its plug and play architecture and offers both inline-block and mirror mode.
- No intervention needed: Threat wall automatically blocks both inbound traffic from malicious IPs and outbound traffic to malicious C2 servers.
- Hands-free: ThreatWall automatically updates and reports.
- Light weight: Unlike other threat intelligence gateways, ThreatWall does not slow down your traffic or hinder day-to-day business operations.

WHAT SETS CYCRAFT APART?

By leveraging CyCraft's industry-leading CyberTotal threat intelligence hourly, in addition to NODs and RPZ, ThreatWall will detect and block with the highest efficacy rate on the market without slowing your north-south traffic. CyCraft offers the highest level of protection with the lowest impact on performance.

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

- **Accurately block** the vast majority of malicious and highly suspicious traffic vastly enhancing the security of your organization, without slowing your network
- **Strict Security. Intuitive Interface.** Allowlist domains and IPs essential to business operations with ease
- **Reduce your internal SecOps workload** by blocking the majority of attacks, further securing your org by greatly reducing the ensuing triage, validation, and investigations from internal incidents that won't happen due to ThreatWall's blocking

BENEFITS TO CUSTOMERS + PARTNERS

- **Flexible architecture** for inline-block and mirror mode on the front line of defense, greatly reducing the processing burden on back-end security solutions.
- **Covers the basics:** Deployed in minutes. Clear intuitive UI. Sustains efficient inline processing speed regardless of environment size. No need for SSL decryption keys to respond to related cyber threats.
- **Real-time:** Analyzes and dynamically updates blocking policies in real-time to more accurately detect and block new suspicious connections, reducing the risk of zero-day attacks.
- **Compatibility:** Compatible with DNS RPZ, effectively preventing malicious DNS queries.
- **Compliance:** Built-in compliance reports adhering to standards issued by ISACs and other institutions.