UGUARD® NETWORKS

DefenseTrust
New Generation Threat Management

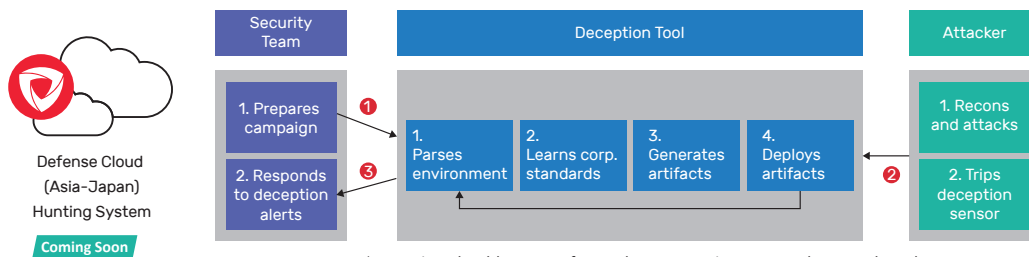## Defense Trust New Generation Threat Management (NGTM)

UGUARD's Defense Trust uses the most comprehensive IP and Domain threat database to effectively neutralize over 80% of known malicious websites. These include phishing sites, malware downloads, botnets, C&C connections, etc. Deployed in inline mode, Defense Trust ensures rapid threat analysis, minimal network latency, and precise inspection. UGUARD's threat intelligence database that offers the industry's fastest update rate and together with UGUARD's proprietary Threat Analysis engine provides near-zero false positives.
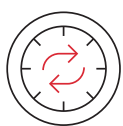
New-Generation Defense Cloud

The honeypot mechanism is for users to actively detect any potential threats or attacks from hackers through decoy setup.

The deception technology mechanism focuses on proactively empowering users in establishing chaos network environment for misleading potential attackers' perception and decision-making process and letting Defense Cloud threat intelligence hunting system easily identify unknown attacks.

Defense Cloud
(Asia-Japan)
Hunting System

Coming Soon

Security Team	Deception Tool	Attacker
1. Prepares campaign	1. Parses environment / 2. Learns corp. standards / 3. Generates artifacts / 4. Deploys artifacts	1. Recons and attacks
2. Responds to deception alerts		2. Trips deception sensor

Source: Gartner, Inc/Deception Should Be Part of Your Threat Detection Strategy by Pete Shoard

Precise Blocking & Rapid Global Intelligence Updates

Close to real-time updates on global threat intelligence to help enterprises defend against known zero-day attacks.

Integrated with the latest global intelligence sources to provide the most comprehensive threat database of IPs and domains.
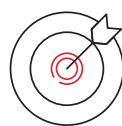
Blocking malicious IPs with near-zero false positives, eliminating unnecessary alerts, and enhancing cybersecurity operational efficiency.

Newly Developed With High-Speed Processing Performance

Newly developed with DPDK (Data Plane Development Kit) to enhance bidirectional forwarding performance and achieve high-performance packet processing.

DPDK
DATA PLANE DEVELOPMENT KIT

Built on a new database and data structure to enable faster query performance.
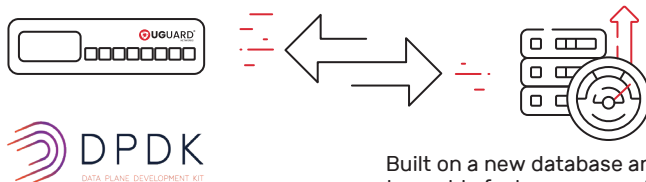
Enhanced Security Framework and Optimized NGFW Performance

Defense Trust can significantly reduce the NGFW security workload, freeing up computing power for more complex security event analysis.

- Malicious Website IP
- Phishing Website IP
- Malware IP
- Malicious relay connection IP
- Web attack IP
- Botnet IP

Analyze Suspicious Network Traffic

Features

IP Whitelisting Mechanism (1 hour)

Latest Global Threat Intelligence

X-Forwarded-For (XFF)

Hunting System (15 Types of Threat Intelligence)

AI Intelligence Report

Real-time Comparison/ Update of Global Blacklist

Contact UGUARD

www.uguardnetworks.com