ThreatBook

TDP®

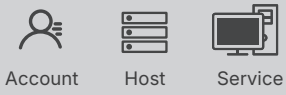
Threat Detection Platform

Threat Intelligence-Fused Network Detection and Response

Leveraging industry-leading threat intelligence and powerful AI, TDP provides the most effective network security capabilities, featuring high-fidelity detection of sophisticated attacks and automated response, to help enterprises address core challenges in frontline security operations.

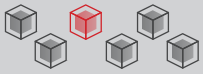
Before intrusion

Comprehensively sort out the attack surface to reduce security risks



During intrusion

Massive alert noise reduction, focusing on real threats



Post-intrusion

Efficient incident response minimizes the impact of intrusion

Have you encountered any of these issues while developing a network security system?

CSO A

Our group has far too many online businesses. We want to do attack surface management but do not know how to start. How did you manage it?

CSO B

We mainly focus on the assets identified by the situational awareness platform and then analyze them. However, there are many false identifications, and the attack surface display is not clear. It only works moderately well.

CSO A

Have you used network detection product? Many APT attacks are now difficult to detect with devices like IDS.

CSO B

Yes, but the effect isn't that good! Every day, there are so many alerts, and also many false positives, that the team didn't have the energy to determine whether it was a real threat or a false positive.

CSO A

I heard that the network detection product you bought is still usable. How did you deal with those detected problems?

CSO B

All these are processed manually, the device itself has no blocking ability, and it doesn't support linkage with third-party devices, actually we are under great...

Is the traditional way inefficient? TDP can help enterprises improve security operations

Capabilities

RISK PREVENTION

"You can't protect what you cannot see."

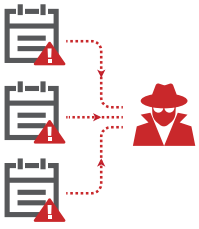
- **Comprehensive Visibility**
  Get real-time visibility into the network, including ports, services, applications, domains corresponding to the asset, and behavioral analytics on sensitive information and file uploading and downloading.
- **Attack Surface Reduction**
  Identify critical risks intelligently across newly launched applications, public entrances, login portals, cloud services and APIs, help optimize risk management policies.
- **Customizable Asset Risk Monitoring**
  Achieve flexible and centralized risk management based on various security scenarios and the specific needs of the SecOps teams.

ACCURATE DETECTION

"When 1% of real alerts are flooded with 99% false positives, it's meaningless to monitor alerts."

- **Zero-day Threats Detection**
  Accurately detect generic zero-day exploits as well as file-based zero-day vulnerabilities by leveraging high-performing machine learning and cloud sandbox.
- **Compromised Hosts Detection**
  Accurately identify compromised hosts by uniting rule based analytics with high-fidelity IOC intelligence.
- **Alert Noise Reduction**
  Reveal the most critical threats with powerful analytics of in-progress attacks that are enhanced with contexts to improves alert accuracy.

REAL-TIME ANALYSIS



"In the confrontation with the APT group, the enemy is secretive, but you are trying to see clues from the massive logs?"

- **Attack Path Analysis**
  Aggregate events in a timeline intelligently to clearly sort out hacker attack paths and activity trajectories, simplify correlation analysis.
- **Multidimensional Analysis**
  Conduct a comprehensive analysis of threats from the perspectives of attacker, defender, and alert, along with visual analysis of the security posture.
- **Attacker Profiling**
  Analyze and extract patterns of attack behavior automatically to build attacker profiles.

AUTOMATED RESPONSE

"The attacker's tools are increasingly automated, while the defender is still doing it... manually?"

- **TCP Reset Blocking**
  Realize high TCP reset blocking rate by using the TCP session mechanism to send reset packets to the attacking IP and internal host simultaneously.
- **Automated Investigation**
  Automate forensics to pinpoint malicious programs and active malware process through TDP Agent.
- **Firewall Blocking**
  Integrate seamlessly with firewall, configure the firewall blocking policy through TDP in real-time.

AI-Powered: Deep, Accurate, Lightning-Fast

TDP integrates over 200 AI models, including Generative AI (ThreatBook XGPT), to infuse AI capabilities across threat discovery and response, thereby reducing MTTA by up to 80%.

Anomaly Detection

Fusing AI-driven anomaly detection with real-time global threat intelligence delivers earlier and more precise identification of critical network anomalies.

Covert Attack Unveiling

Leveraging machine learning to uncover sophisticated attacks and covert channels, including DGA domains, DNS tunneling, and malicious file detection.

WebShell Analysis

Enhanced detection and analysis of persistent threats, such as Webshells, ensuring effective recognition even when adversaries shift their attack TTPs.

Alert Fatigue Minimizing

Intelligently correlating and aggregating massive volumes of raw alerts to automatically filter noise and reduce analyst fatigue.

More than 2,000 enterprises choose TDP for NDR

<0.03%	<3%	>81%	99%
FALSE POSITIVE RATE	UNDERREPORTING RATE	ZERO-DAY DETECTION RATE	TCP RESET BLOCKING RATE

Gartner

Magic Quadrant for Network Detection and Response (2025)

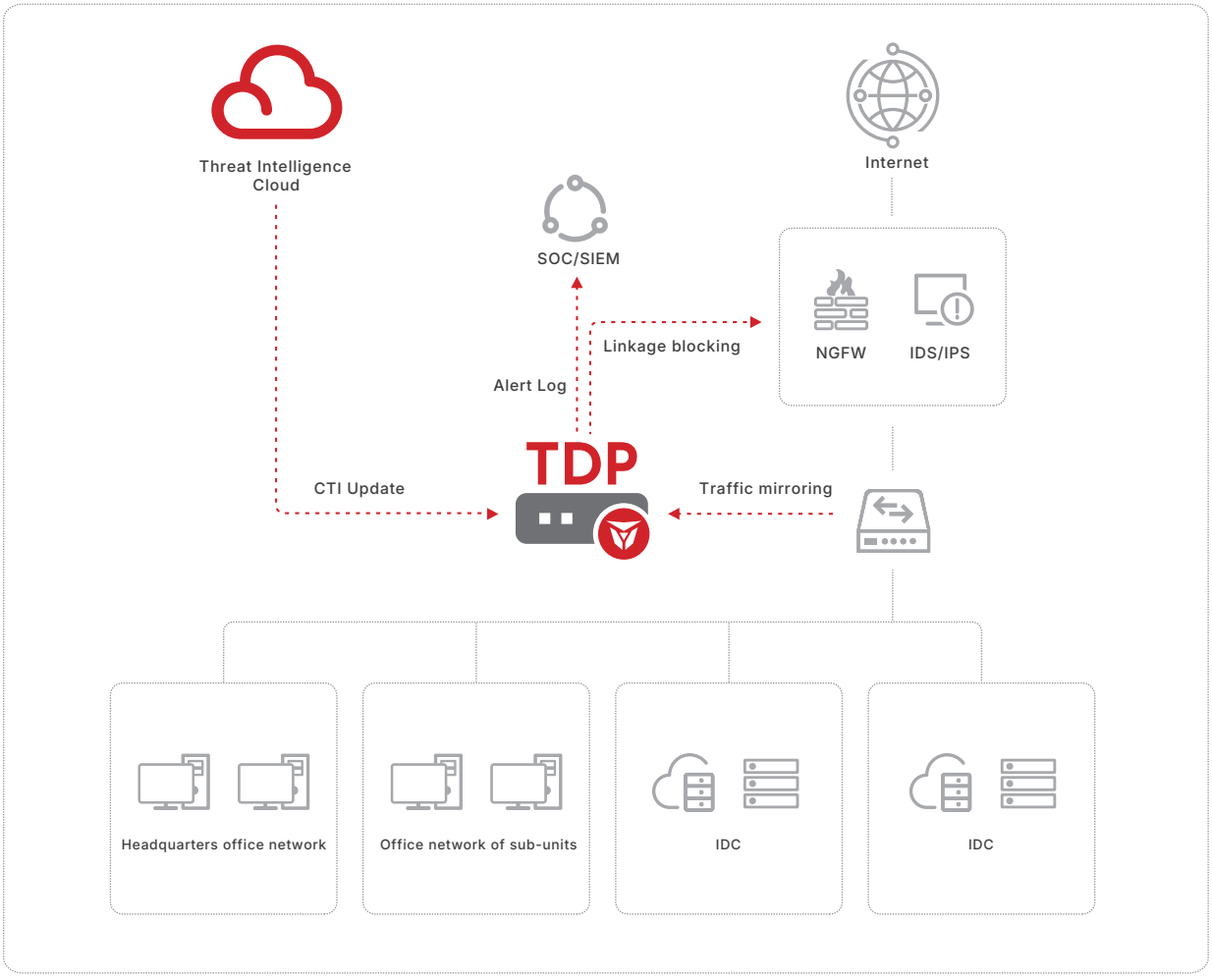
Gartner Peer Insights

Strong Performer in the Voice of the Customer for NDR (2023-2025)

FORRESTER

The Network Analysis and Visibility Solutions Landscape (2025)

TDP Deployment

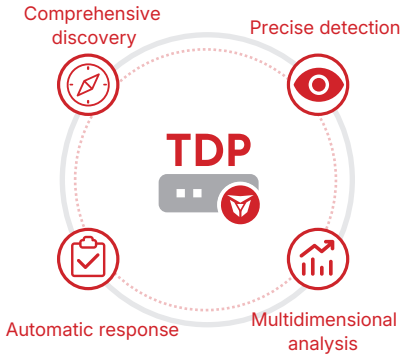


Use Cases

NETWORK-WIDE THREAT DETECTION

"The alerts of TDP are very accurate. It can automatically determine whether an attack is successful or failed, and it can also fully display the hacker's profile, which is convenient for us to carry out targeted protection. Since we implemented TDP, we no longer need to analyze tens of thousands of alerts one by one, saving us a lot of time and greatly improving our work efficiency."

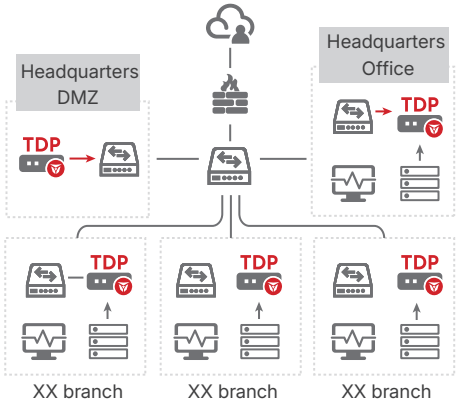
——CSO of a large internet company



UNIFIED MONITORING AND MANAGEMENT FOR MULTI-BRANCH THREATS

"We have deployed TDP in our headquarters' DMZ, office area, and all branch offices. For smaller branches, we have deployed the free HFish product. By cascading, we can unify the display of alerts from all regions on the headquarters platform, thereby realizing full network threat management at the headquarters. We no longer have to worry about the insufficient security protection capabilities of our subsidiaries."

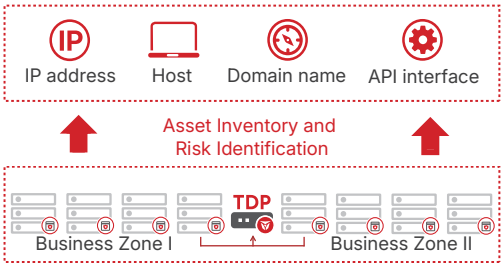
——CTO of a financial institution



ASSET RISK MONITORING

"Given the high volume of sensitive data traversing our production network and the inherent risks associated with heavy API usage, we needed a robust security solution. TDP has provided that, allowing us to comprehensively scan and assess our network assets. By identifying dozens of API risks and instances of sensitive data exposure, TDP has significantly enhanced our data security posture."

——CIO of an insurance group



FOCUS ON REAL THREATS

ABOUT THREATBOOK

ThreatBook is a leading provider of cyber threat detection and response that driven by TI and AI. We pioneered new approaches to deliver high-fidelity, efficient and actionable security intelligence and integrated the ability with full life cycle threat detection system and incident response capabilities to empower the protection on cloud, network and endpoints, help enterprises achieve high efficiency of responding to threats, reduce complexity and improve security operations.

No.1
Market Share of Threat Intelligence in GCR

The Largest
CTI Community in Asia, Over 300,000 Members

Representative Vendor
Listed in ***Gartner's Market Guide for Security Threat Intelligence Products and Services*** for 4 Consecutive Times

Representative Vendor
Recognized in the ***2025 Gartner Magic Quadrant for Network Detection and Response*** (NDR)

Trusted by Industrial Customers

Banking	Securities & Insurance	Energy	Internet & Telecom	Intelligent Manufacturing	Multi National Companies
BEA	GUOTAI JUNAN SECURITIES	SPIC	airbnb	BMW	BlackRock.
BANK OF COMMUNICATIONS	HAITONG	STATE GRID CORPORATION OF CHINA	bilibili	HONDA The Power of Dreams	CARLYLE
CHINA MERCHANTS BANK	HUATAI SECURITIES	CHN ENERGY	JD.COM	Li Auto	KPMG
ICBC	SSE	China Datang Corporation Ltd.	KUAISHOU	GREE	wilmar
China Construction Bank	SHENZHEN STOCK EXCHANGE	cnooc	ANT GROUP	BOE	HERBALIFE NUTRITION
CHINA EXIM BANK	PING AN	CHINA SOUTHERN POWER GRID	Tencent	oppo	lululemon
AGRICULTURAL BANK OF CHINA	CHINA LIFE	SINOPEC	ByteDance	SAIC	watsons
THE PEOPLE'S BANK OF CHINA	CICC	CNPC	CHINA TELECOM	vivo	ESTĒE LAUDER
BANK OF CHINA	CITIC SECURITIES	ChinaCoal	China Mobile	NIO	Envision digital
					CITIC Group

☆ Awards and Recognitions

Gartner

Magic Quadrant for Network Detection and Response
(2025)

Gartner Peer Insights

A Strong Performer in the Voice of the Customer for Network Detection and Response
(2023, 2024, 2025)

FORRESTER®

The Network Analysis and Visibility Solutions Landscape
(2025)

Gartner

Hype Cycle for Security Operations: CTI Tech Representative Vendor
(2024)

FROST & SULLIVAN

The Growth Index Leader of the Frost Radar™: Threat Intelligence Platforms
(2024)

Gartner

Market Guide for Threat Intelligence Products and Services
(2017, 2019, 2020, 2021)

FORRESTER®

The External Threat Intelligence Service Providers Landscape
(2023)

Gartner

Market Guide for Managed Detection and Response Services, China
(2022, 2024)

FROST & SULLIVAN

No.1 in growth index in the leader quadrant of China Threat Intelligence Market Report
(2022)

"Black Unicorn" Awards
(2021-2023)

RED HERRING TOP 100 WINNER 2019

Red Herring Top 100 Asia Winner
(2019)

CYBERSECURITY 500

Cybersecurity 500
(2017-2019)

The designated cybersecurity vendor of China International Import Expo (CIIE)
(2018-2024)

The designated cybersecurity vendor of UN Biodiversity Conference COP15
(2020)

BEIJING 2022

Awarded Outstanding Vendor in cybersecurity support of the Beijing Winter Olympics
(2022)

ThreatBook

www.threatbook.io
contactus@threatbook.io

SINGAPORE
12 Marina View #11-01,
Asia Square Tower 2,
Singapore
(018961)

HONG KONG
Units 309 & 311, Level 3,
IT Street, Cyberport 3,
100 Cyberport Road,
Pok Fu Lam, Hong Kong

BEIJING
10th Floor,
JD Technology Building,
No. 76 Zhichun Road,
Haidian District, Beijing

Follow Us on @ThreatBookLabs @Threatbook