ThreatBook

LEADING PROVIDER OF

THREAT INTELLIGENCE DETECTION AND RESPONSE

September 2024

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.

ThreatBook has been named one of the Cybersecurity 500, and consistently been featured in industry-leading reports such as Gartner's Market Guide for Threat Intelligence Products and Services and Forrester's The External Threat Intelligence Service Providers Landscape. Our inclusion as a Sample Vendor in Gartner's Hype Cycle for Security Operations report in 2024 further solidifies our position as a market leader. Moreover, our leadership position in the Frost & Sullivan's Frost Radar™ report for Threat Intelligence Platforms and consistent "Strong Performer" recognition in Gartner Peer Insights "Voice of the Customer" for Network Detection and Response underscore our commitment to providing exceptional cybersecurity solutions.

No.1

Market Share of Threat Intelligence in GCR

The Largest

CTI Community in Asia, Over 250,000 Members

Representative Vendor

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

A Strong Performer

Gartner Peer Insights "Voice of the Customer" for Network Detection and Response Ranks in Top 5

OUR MISSION

Secure the digital world

Fight against cyber threats
Empower digital transformation

OUR VISION

Become a world-class cybersecurity leader

Focus on technology development
Build and expand security capabilities

ELEVATE YOUR SECURITY OPERATIONS WITH TI AND AI

ANALYST RECOGNITION

The Only Chinese Vendor Listed in the Report of Hype Cycle for Security Operations (2024)

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

Two-time Selection as A Strong Performer in the Voice of the Customer for Network Detection and Response (2023, 2024)

Two-time Selection in the Market Guide for Managed Detection and Response Services, China (2022, 2024)

The External Threat Intelligence Service Providers Landscape (2023)

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

INDUSTRY RECOGNITION

"Hot Company, Network Detection and Response", "Most Innovative Threat Intelligence" (2024)

The 1st Amazon GuardDuty CTI provider in China (2023)

Cutting Edge in Endpoint Security(2023) Infosec Awards as "Best Solution in Cybersecurity-as-a-Service (CaaS)", "Cutting Edge in SaaS/Cloud Security", "Publisher's Choice in Threat Intelligence" (2022)

The only Chinese vendor as finalist of "Black Unicorn" Awards (2021-2023)

Red Herring Top 100 Asia Winner (2019)

Cybersecurity 500 (2017-2019)

SERVICES & SUPPORT RECOGNITION

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

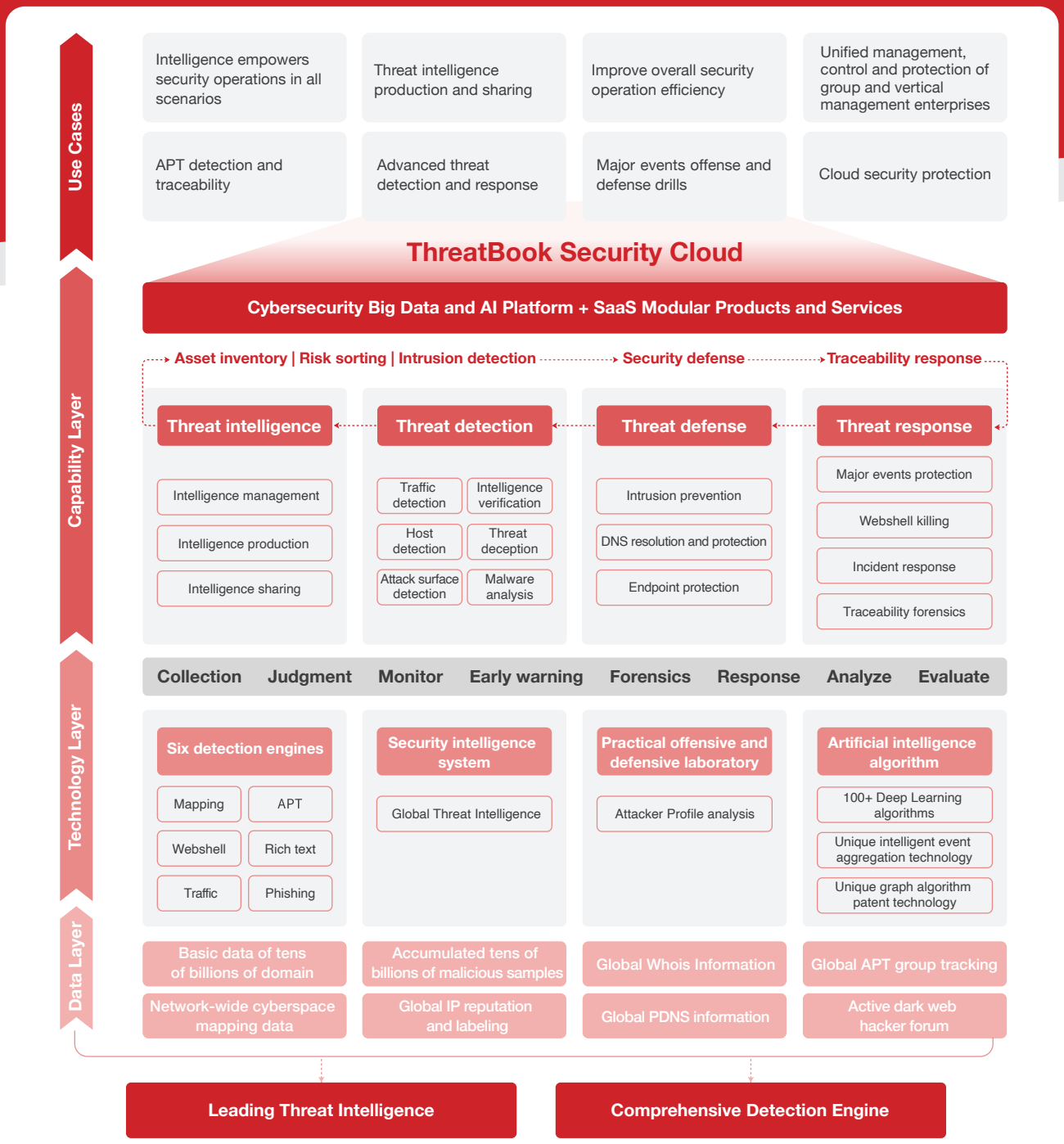
The designated cybersecurity vendor of UN Biodiversity Conference COP15 (2020)

The designated cybersecurity vendor of China International Import Expo (CIIE) (2018-2023)

The designated cyber security vendor of The Summer Davos World Economic Forum (2017-2019)

CYBERSECURITY CAPABILITIES OVERVIEW

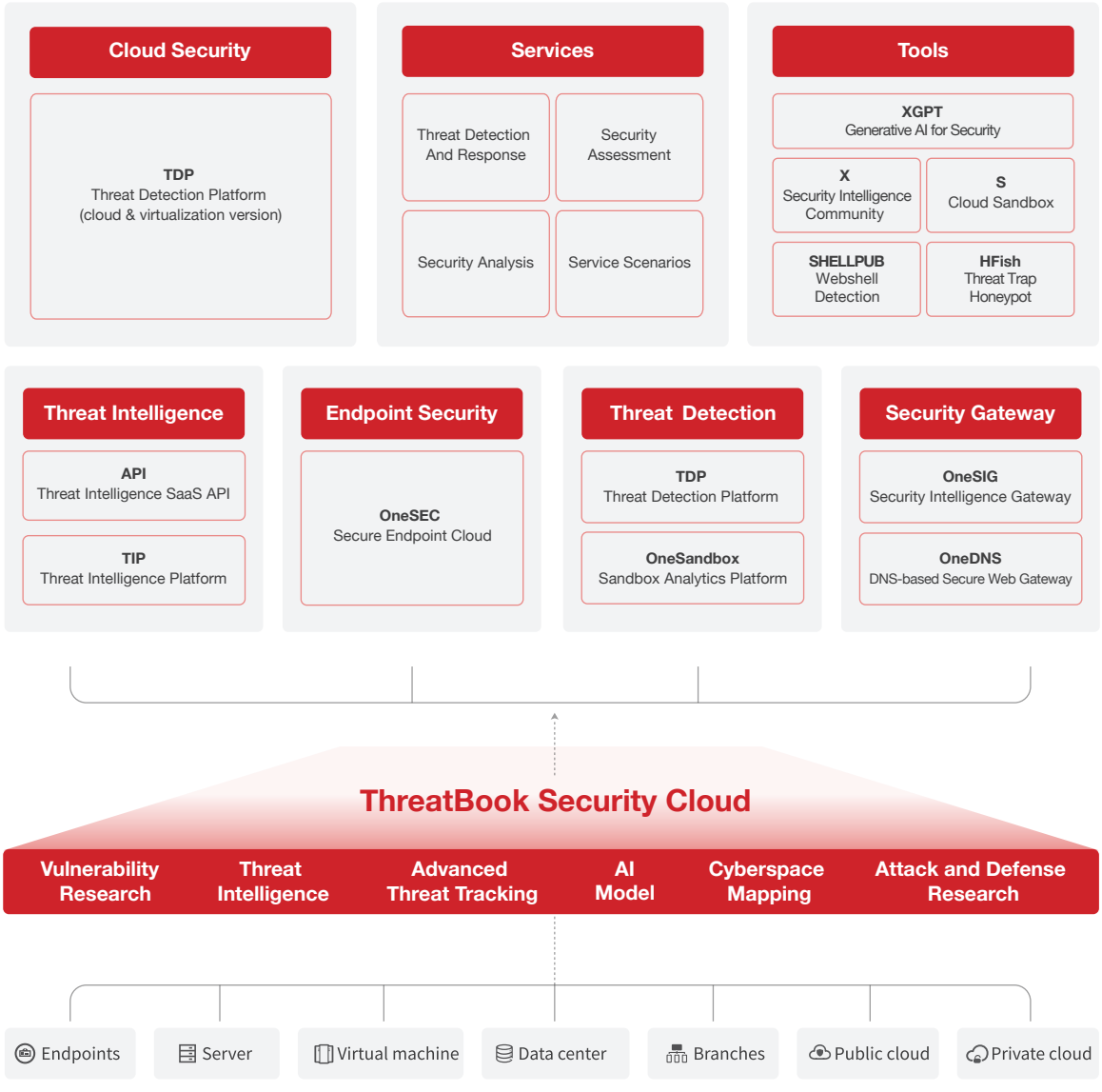
Help resolve attack-defense challenges and secure digital development



COMPREHENSIVE PRODUCTS & SERVICES

"Cloud+Traffic+Endpoint" All-round Threat Discovery and Response

Creat the next generation of network security



TRUSTED BY THOUSANDS OF 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	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

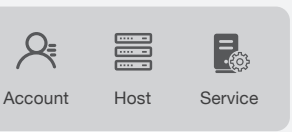
THREAT DETECTION PLATFORM-TDP®

The Best CTI-based Network Detection and Response

Leverage the industry-leading threat intelligence, TDP provides the most effective network security capabilities with high-fidelity detection on sophisticated attacks and automated response, help enterprises address the core challenges in frontline security operations.

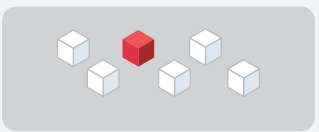
Before intrusion

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

Capabilities

RISK PREVENTION

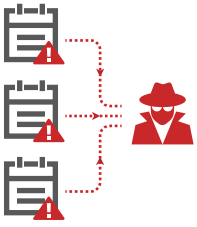
"You can't protect what you cannot see."

- **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.

More than 1,500 enterprises choose TDP for NDR

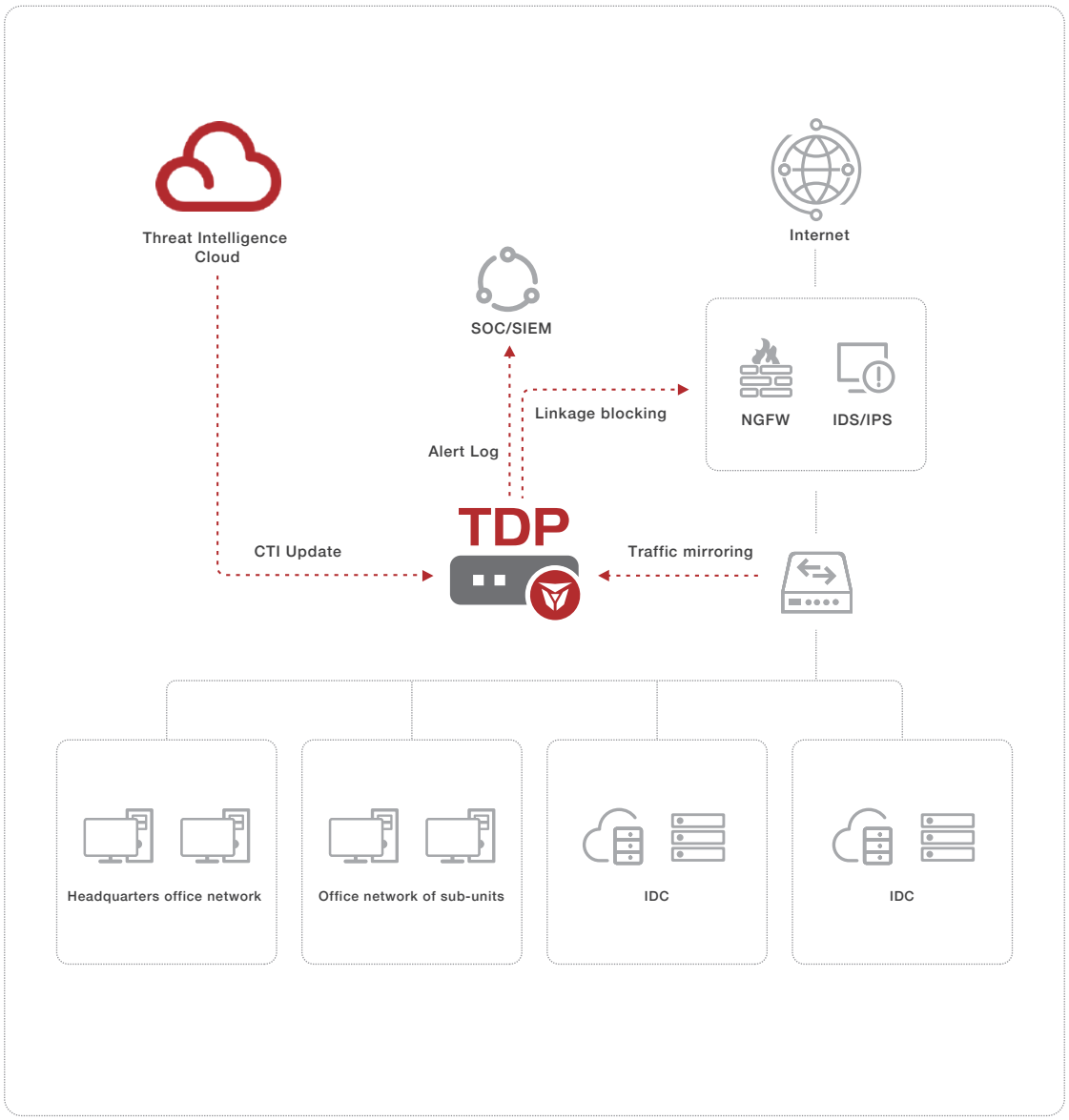
<0.003%	<3%	>81%	99%
FALSE POSITIVE RATE	UNDERREPORTING RATE	ZERO-DAY DETECTION RATE	TCP RESET BLOCKING RATE

Gartner Peer Insights

A Strong Performer in Gartner Peer Insights™

FOCUS ON REAL THREATS

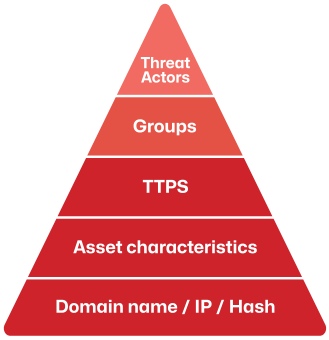
TDP Deployment



CYBER THREAT INTELLIGENCE

ThreatBook provides a widely used threat intelligence platform and intelligence cloud API services dedicated to helping the security operations team to work more efficiently on compromise detection and alert noise reduction, allowing them to focus and take action on the real threats.

Data Collection	Analysis/Extraction	Quality Control	Threat Intelligence
Basic data	Cloud Sandbox	Black and white list	IP profiles/ Hacker profiles
Sample data	Traceability system	8 AI models	Attack tool/ attack method
Attack data	Threat hunting system	etc.	IoA Intelligence/ Yara intelligence
Cyberspace mapping data	Algorithm models		High Value C2/ Phishing intelligence
Open source intelligence	Graph database		300+ APT groups being tracked



World's Leading Threat Intelligence

High-Fidelity: Up to 99.9%

ThreatBook provides high-fidelity intelligence collected from alerts from real customer cases. Our R&D team uses it as a critical indicator to evaluate our intelligence extraction and quality control work. Meanwhile, we continuously assess the data based on any relevant alerts from timely cyber incidents.

Efficient: More than Context

No more worries about mass alerts! ThreatBook threat intelligence aggregates data and information with a clear verdict, behavior conclusions, and intruder portraits. It enables the SOC team to spend less time on irrelevant or harmless activities,boosting the operation's efficiency.

Actionable: Detection and Response

The core value of threat intelligence is detection and response, that is, enterprises can carry out compromise detection with high-fidelity intelligence, figuring out if a device has been attacked or if a server has been infected and respond based on the investigation to prevent threats, isolate or avoid risks in a timely manner and reduce the likelihood of serious consequences.

Capabilities

TIP

An on-premise threat intelligence platform that offers lifecycle management for intelligence querying, analysis, production and sharing, empowering SecOps teams to expedite threat detection and incident resolution.

API

We offer Premium API to help enterprises with threat detection and analysis, fully utilizing the existing security devices. By detecting compromises and reducing alert noises, it can help the security operation team to find any kind of threats, including APT, remote control, theft, mining, ransome and etc.

Key Benefits

Detection

Leveraging 99.9% high-fidelity of ThreatBook threat intelligence, we can help you accurately find compromised hosts and emerging threats from massive event alerts and logs, such as Mining pool, Ransomware, APT, etc., drive rapid analysis and disposal, and increase the efficiency of responding to threats.

Protection

Through threat intelligence, we can figure out who the adversary is, what his or her behavior is like, where they've been hacked, what methods they've adopted, etc. Therefore, users will be able to quickly fix its weak points, strengthening the whole security system.

Efficiency

With high-fidelity intelligence data, enterprises can quickly figure out their weak points in their security establishment. With ThreatBook threat intelligence and the relevant cyber-security products covering cloud+network+endpoint, the enterprises can build up a strong defense system that is not only low-cost but also highly efficient.

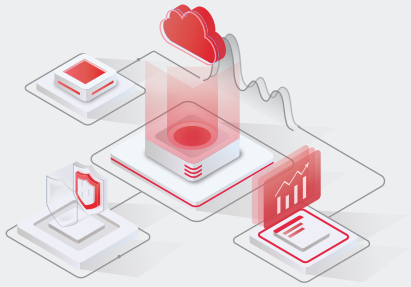
Welcome to explore our global threat intelligence and API service!
Experience high-fidelity intelligence for free!

→ **web: www.threatbook.io**

THREAT INTELLIGENCE PLATFORM-TIP

Centralizing Security Intelligence for Proactive Security

ThreatBook TIP is an on-premise threat intelligence platform that offers lifecycle management for intelligence querying, analysis, production and sharing, empowering SecOps teams to expedite threat detection and incident resolution.



Capabilities

Security Operation Empowerment

- Provides a vast repository of up-to-date and accurate IP reputation, IOC, and vulnerability intelligence.
- Deeply empowers threat analysis, risk identification and mitigation, and automated orchestration in security operations.

Multi-source Intelligence Management

- Enables flexible integration with various intelligence sources, including commercial, regulatory, self-generated, and custom.
- It supports field-level fusion of multi-source intelligence to greatly enhance intelligence usability.

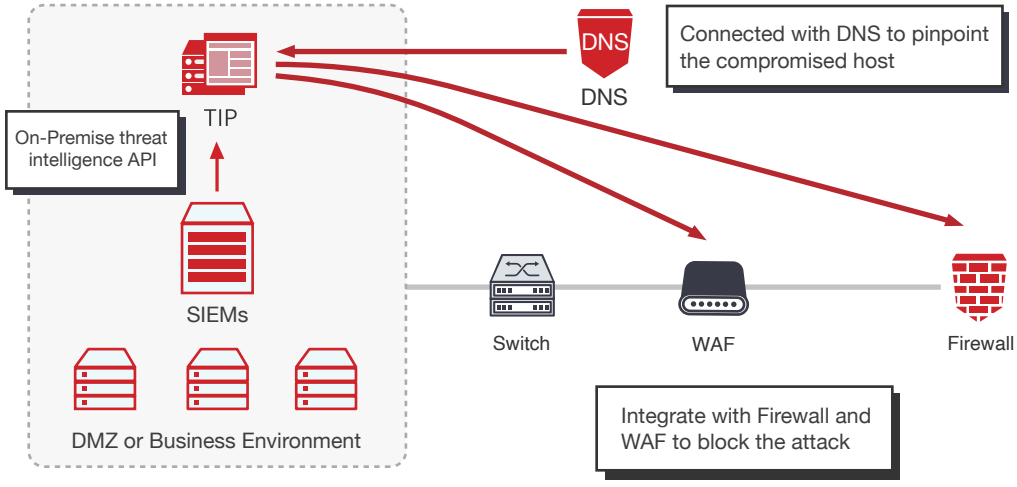
On-premise Intelligence Production

- Based on local alert logs and sample data, leveraging ThreatBook's powerful intelligence production system, to produce custom IP reputation and IOC intelligence.

Intelligence Cascading and Sharing

- Building an intelligence sharing ecosystem within the industry/group to enable seamless intelligence sharing among affiliated organizations, achieve a "one hit, all immune" security posture.

“Integrate With SIEMs”



Key Use Cases

- **Alert Noise Reduction and Response**
- **Compromise Detection and Response**
- **Phishing Email Analysis**
- **Vulnerability Risk Assessment**
- **Unified Management and Operation of Intelligence**
- **Host Malicious File Hash Detection**

THREATBOOK SAAS API

We Deliver Operational Threat Intelligence

Threatbook SaaS API provides full-coverage, high-fidelity, rich context and up-to-date threat intelligence for security operation teams of all sizes to streamline threat analysis and speed up response to potential attacks.

Capabilities

INTEGRATED INTELLIGENCE

- Millions of high-fidelity IOC intelligence
- 4.2 billion global IP reputation and labels
- More than 200+ global APT groups tracking
- Millions of domain names added daily
- Millions of malicious samples added daily
- More than 10 yeas of PDNS data collected
- More than 20 years of Whois data collected
- Minute-level intelligence updates

BENEFITS

- Threat discovery and compromise detection for office network hosts / production networks and DMZ servers
- Risk identification of external IP of applications or services that are accessible over public networks, such as web, mail and SSH
- Analysis of suspicious files/processes on endpoints/servers for identification of malicious programs
- Threat detection cooperates with internal SOC/SIEM big data platforms or analysis logs from security devices such as WAF/IPS/NGFW
- Correlation analysis of internal and external security incidents

API Capabilities

	IP Detection Capability	Domain Name Detection Capability	File Analysis Capability	URL Analysis Capability
Basic analysis API	IP analysis IP reputation Compromise detection	Domain analysis Compromise detection	File analysis File reputation report Anti-virus engine detection	URL analysis URL reputation report
Advanced query API	Advanced IP query	Advanced domain name query Subdomain query Domain context		

DNS-BASED SECURE WEB GATEWAY --OneDNS®

Product Overview

ThreatBook OneDNS® is a DNS-based Secure Web Gateway fusing threat intelligence, while tackling network threat effectively and operating user-friendly.

With OneDNS®, various office terminals can connect to the internet without threats, anytime and anywhere. It effectively protect against new network threats such as malicious mining, blackmail virus, APT attack, phishing and malicious software, and realizing a closed loop of detection, interception, location and evidence collection.

Capabilities

Secure, Fast and Stable DNS Resolution for Enterprise

With DNS filtering, OneDNS can offer a secure DNS resolution, which provides an SLA up to 99.999% detecting rate. While securing your queries against tampering, the speed of internet access will be guaranteed to ensure fast and stable network connection.

Advanced Threat Intelligence for Advanced Protection

ThreatBook's threat intelligence has been listed on Gartner Threat Intelligence Market Guide Report for four consecutive years. The cloud database can be updated online in minutes, with a detecting rate of 99.99%. With threat intelligence, OneDNS can comprehensively block new cyber threats such as malicious mining, ransomware, phishing, APT, etc.

Unified Management on Multi-layer Branches

Via SaaS services, the security configuration of a company can be managed by one account through a visible way, while hierarchical customized management is supported for all branches.

Experience New Security of Your Office Network

Easy

You can configure OneDNS completely only in minutes without any additional hardware fees, and the dashboard is also easy to understand and use. Via SaaS services, our customers do not need to upgrade and maintain software manually.

Security

OneDNS protects all your workplaces with outstanding threat intelligence. A huge cloud database with hundreds of millions intelligence updates automatically in minutes to keep pace with the newest threats.

Steady

OneDNS has ever kept 100% persistent service for more than 10 years, provides backup capabilities, distributed decentralized architecture, automatic load balancing and fault self-healing with service nodes. We promise an SLA up to 99.999% for a steady DNS resolution.

Cost-friendly

OneDNS makes a one of the best prices on the global market right now. With fewer cost, you can experience an excellent DNS security service.

Recommended and favored by 5,000+ companies,
widely accepted by ten millions of end users.
Internet security provider with professional domain name resolution service certificate.

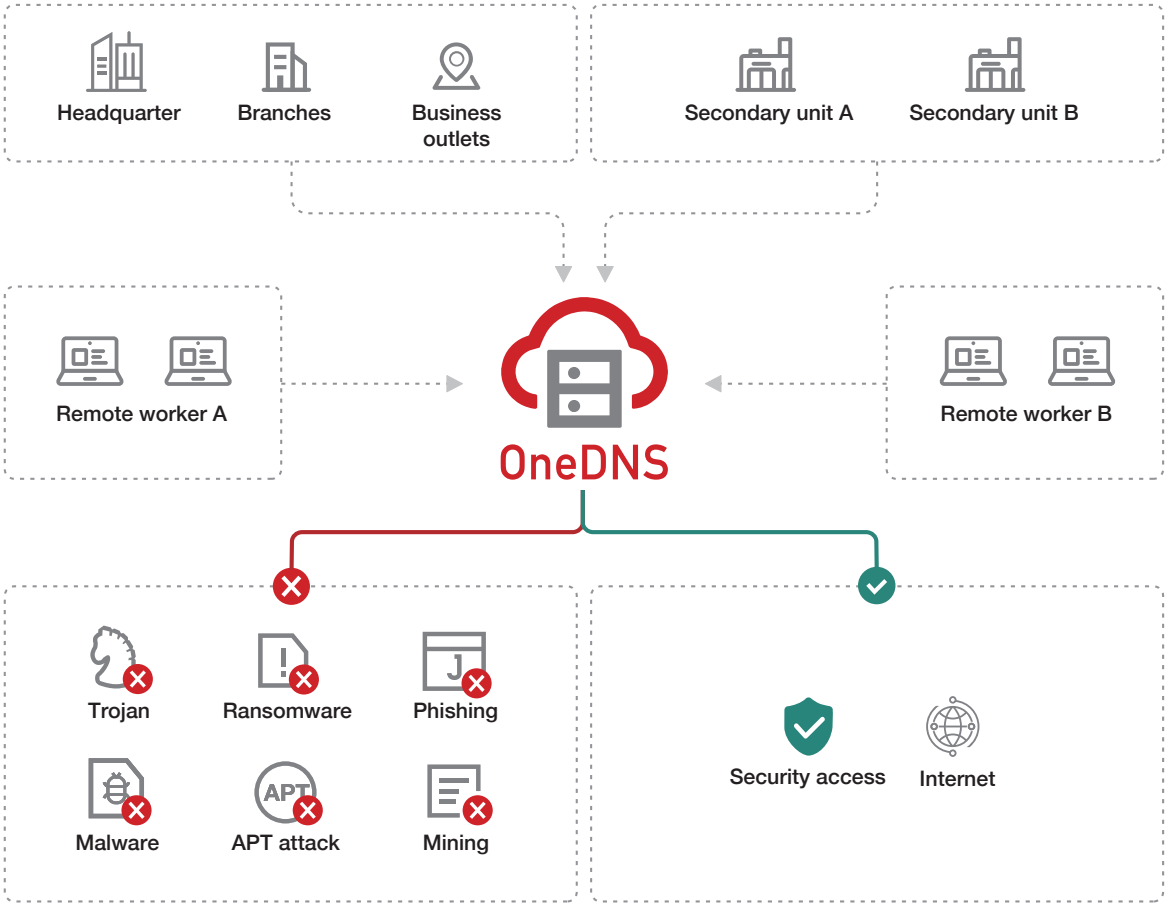
Case Study

Challenges

A mega financial and insurance enterprise of 30,000 branches all over the country: they are large in number, deep in hierarchy and have scattered employees, which made it very difficult to conduct an unified control. Meanwhile, the level of security teams in different places is uneven, and it is difficult to ensure the effectiveness of security measures, resulting in many hidden dangers and high risks for the whole group.

Benefits

With OneDNS of built-in high-quality threat intelligence, it provides secure internet access services for 200,000+ terminals in 30,000+ branches, avoiding malicious mining, ransomware, APT, etc. Meanwhile, OneDNS has created a province-based two-level control strategy for enterprises through flexible and powerful management functions. Each provincial team is responsible for the safety monitoring and management of its own region, and the headquarters security team manages tens of thousands of branches through a single console.



Managed Detection and Response (MDR)

Service Overview

Managed Detection and Response (MDR) service provides cloud-based security capabilities in a cost-efficient manner, allowing users to obtain a security team that is online 24/7, fully equipped with security skills, and capable of continuous iterative upgrades.

Detection

Attack Detection
Compromise Detection

Precise detection of complex attacks, efficient capture of unknown risks

Analysis

Threat Profiling Analysis
Threat Severity Analysis

Deep support from security experts, original system traceability and tracking

MDR

Early Warning

Vulnerability Warning
Security Incident Warning

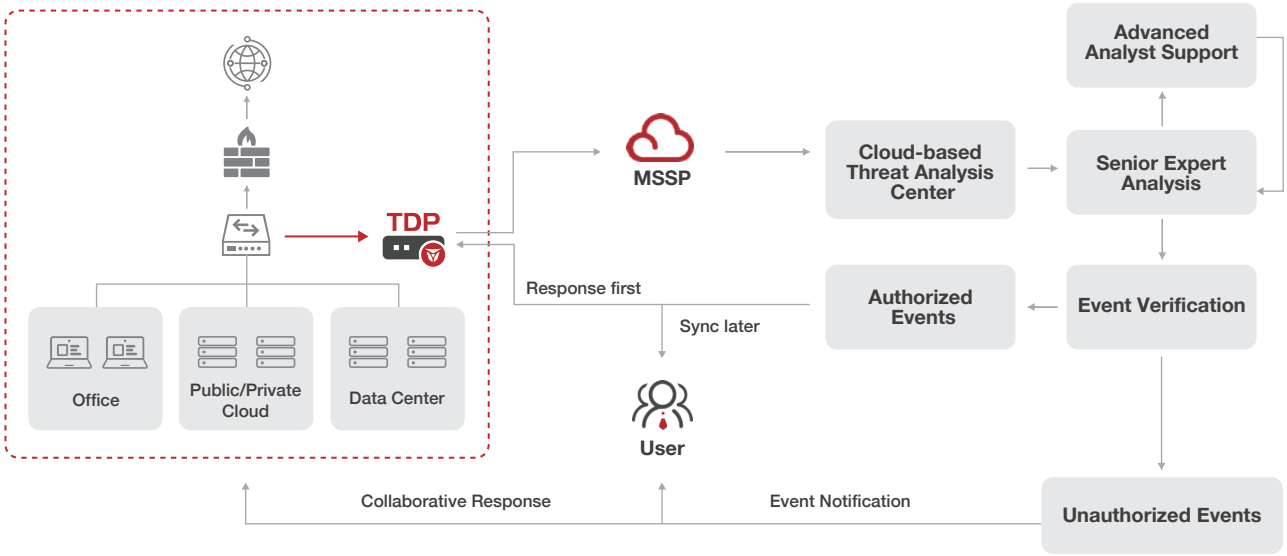
Timely warning of emergent threats, in-depth analysis of hot events

Response

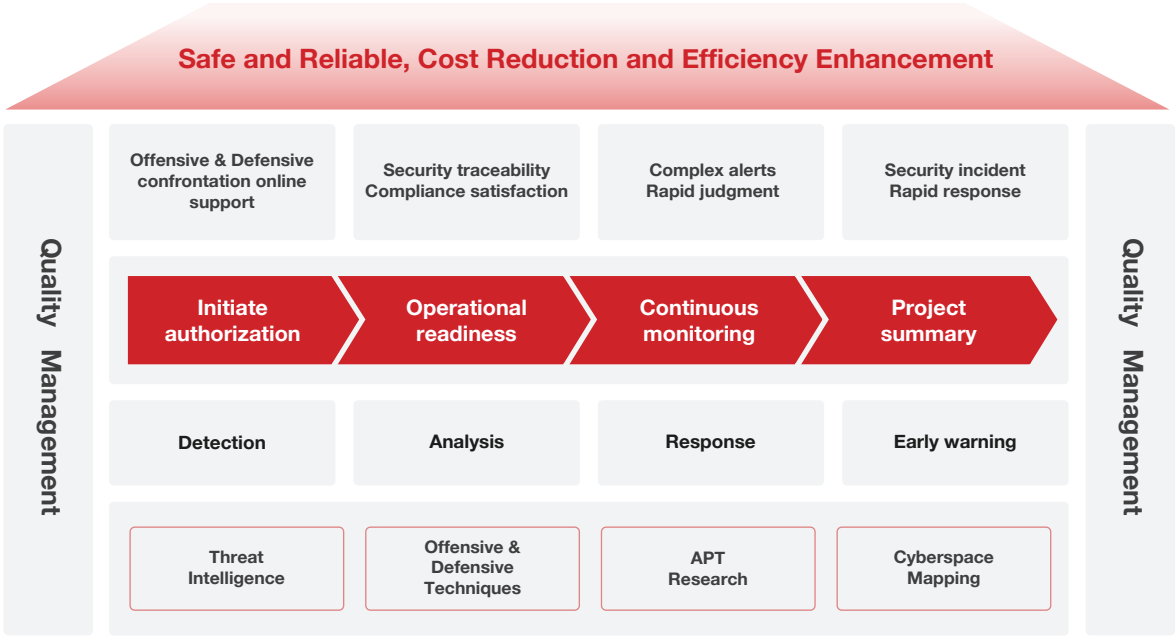
Threat Response
Vulnerability Verification

Thorough and complete threat handling, full adaptation to diverse scenarios

Service Mode



Service Capability Framework



Service Benefits

01

Before the Attack

Powerful intelligence capability, providing early warning for new network risks

02

During the Attack

Service experts quickly identify and locate threats, communicate timely, and assist in response

03

In-depth Analysis

Multi-dimensional deep support for emergency response, offensive and defensive operations, and sample analysis, providing comprehensive security protection on network and endpoint levels

04

After the Attack

Complete recording of the confrontation process, real-time accumulation of security experience

THREAT TRAP HONEYPOT SYSTEM - HFish

Product Overview

By using secure, agile and reliable medium- to low-interaction honeypots, HFish enhances users' capabilities in the fields of compromise detection and threat intelligence. HFish has been adopted by over 4,000 enterprises with 30,000 deployed nodes, making it one of the most widely used free honeypot products.

Product Features

Accurate Threat Detection

- Attack signatures can be timely updated from cloud.
- Support users to customize signatures for detection flexibly.
- Built-in traceability module can be enabled on demand.

Secure Cloud Honeynet

- Network traffic traction, no local risk.
- Non-local network, no need to worry about being breached.

Multi-scenario Support

- Support mixed deployment of physical machine, virtual machine, cloud environment and IoT.
- Resolve the pain points of unawareness of cyber security for remote branch office intranets, cloud edge and cloud intranets.

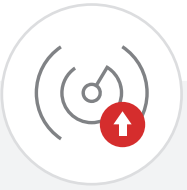
Intelligence Integration and Collaboration

- Free inquiry of honeypot intelligence on HFish.net.
- Accurate and stable intelligence production unit.
- Native support for interfacing with ThreatBook intelligence management platform TIP.

Use Cases

Compromise detection

Challenge: device take-out, USB device access, employees downloading illegal software, client vulnerability, VPN account theft and many other reasons will increase the risk of intranet compromise.
Solution: HFish nodes are widely deployed in various areas of the intranet at a low cost. Once an attacker who penetrates into the internal network touches the honeypot node of the intranet, the node immediately transmits an alert to the HFish management terminal. The management terminal notifies the user/administrator of the internal host. If it has been compromised, the administrator can immediately check the emergency response.



External threat perception

Challenge: cyber attack methods are constantly being upgraded, and encrypted protocol traffic attacks, multi-layer encrypted file attacks, new advanced threat attack methods, etc. often make enterprises unaware.
Solution: HFish is divided into management end and node end. It can deploy nodes in multiple areas, which is equivalent to the integration of assets into the environment. As a threat probe, it is monitored in the management end interface. On the one hand, the honeypot can attract firepower; on the other hand, when the management end finds an attack, it can intercept and block the blocking device in time to prevent further proliferation.

Threat intelligence production

Challenge: at this stage, many network traffic detection equipment or situational awareness have a large number of alerts every day. There are too many attacks to be processed and analyzed, and the number of false alerts is large, which is not conducive to analysis.
Solution: HFish can be deployed in the external network environment to form self-generated intelligence, and the alet is the threat. It can reduce the noise of TDP, situation awareness platform and SIEM alerts through syslog or api calls, improve the analysis efficiency, and these intermediate devices can be linked with firewalls to intercept and block, so as to prevent attacks from spreading.

Offensive and defensive combat drills

Challenge: in recent years, there have been more and more demands for offensive and defensive drills and major events protection, and enterprises are paying more attention to the construction of network security in practice, in order to truly deal with high-intensity hacker attacks.
Solution: HFish has actual combat capability, including accurate identification and capture of attack tactics; Sensing an external network attack situation, positioning intranet compromised host, and preventing the lateral movement of threats from infecting the core business; Capture attacker data and obtain the hacker's fingerprints, social, geographic, and other information; Transfer attacks to the cloud honeynet to ensure asset security; Capture 0day, find unknown high-level threats, etc.

→ Visit **https://hfish.net/** to start deployment with one click

WEBSHELL DETECTION EXPERT– SHELLPUB

Product Overview

SHELLPUB is a well-known free webshell detection and killing tool. It has massive webshell samples, as well as independent webshell killing technology. It integrates multi-engine technologies such as AI, deep scan, traditional features, and cloud big data. It has fast killed speed, high precision, low false alerts and other advantages. Since its launch in 2017, it has been downloaded more than 300,000 times, has scanned over 30 billion files, and has detected over 30 million malicious samples.

Product Features

Convenient online scanning and removal

It could detect webshell quickly and accurately through a browser and access the latest detection capabilities.

Powerful memory webshell kills

With the patent of an efficient memory webshell detection algorithm, it has little intrusion to business, supports memory webshell detection of Java 6 + or higher in the Linux version, and automatically identifies the three mainstream middleware of WebLogic, Tomcat and Jboss. Windows version is the earliest IIS. NET memory webshell detection tool in China, with a wide application range and exceptional detection performance.

Flexible SaaS API

Webshell can be detected in any scenario as long as the API can be called. The API has a good effect in scenarios that are sensitive to resource overhead, such as IOT devices.

Free kill client terminal

The program is small, scans quickly, and works with multiple versions of Windows and Linux. In 2022, it is compatible with mainstream domestic hardware and effectively supports localization substitution.

Product Advantages

Cloud Engine

Relying on massive webshell samples, quickly and accurately detect known webshells.

AI Engine

99.95% detection rate, low false positives.

Deep Engine

Anti-Obfuscation, Anti-AntiVirus.

Feature Engine

Fast detection and low system overhead.

→ For details, please log on to n.shellpub.com ››

Web: www.threatbook.com
Email: contactus@threatbook.com
Singapore | Hong Kong | Beijing