ThreatBook

LEADER IN THREAT DETECTION AND RESPONSE

Threat Detection Platform

Threat Intelligence Platform

OneDNS Cloud

ThreatBook SaaS API

X Intelligence Community

Cloud Sandbox

Managed Detection and Response

www.threatbook.cn

E-mail: contactus@threatbook.cn

Tel: +8610-57017961

Company Introduction

ThreatBook

Founded in July 2015, growing up as the leader of the next generation security provider. ThreatBook is in forefront of protecting hundreds of organizations in China by delivering innovative products and services base on the Threat Intelligence. With 5 years research and development, ThreatBook has empowered customers with threat intelligence and analysis through professional and easy-to-use product capabilities to help them establish comprehensive threat awareness systems. ThreatBook was the only Chinese representative vendor listed by Gartner's Market Guide for Threat Intelligence Products and Services in 2017 and 2019. It was repeatedly named on the CyberSecurity 500 list from 2017 to 2019 and was selected to be the 2019 Red Herring Top 100 Asia Winner.

Products and Services:

OneDNS Cloud

A secure cloud platform focus on DNS resolution, providing SaaS-based DNS query inspection and access management service

TDP-Threat Detection Platform

Intelligence-driven threat awareness platform which focus on real threat, pinpoint compromised hosts and empower security manager with closed loop security.

Threat SaaS API

Threat detection and analysis API

TIP-Threat Intelligence Management

On-premise deployment multi-source CTI management, production and ditribution platform.

X-Open CTI Community S-Cloud Sandbox

X community: Most popular and active CTI community in Asia

S Platform: Threat Intelligence empowered open cloud sandbox

Managed Detection and Response

Provide enterprises with security services including threat inspection, incident response, on-site cyber security protection services, expert consultation, advanced intelligence subscription and external asset monitoring.

Our Customers:

ThreatBook have provided products and service to hundreds of enterprise customers in different verticals including energy, securities, bank, government, internet and manufacturing industry.

Gartner

The only Chinese representative vendor listed by Gartner's Market Guide for Threat Intelligence Products and Services

CYBERSECURITY VENTURES

Named on the CyberSecurity 500 list from 2017 to 2019

ENTERPRISE SECURITY

Top 10 AI Security Solution Provider by Enterprise Security Magazine

RED HERRING ASIA 100 WINNER 2019

2019 Red Herring Top 100 Asia Winner

INFOSEC AWARDS WINNERS CYBER DEFENSE MAGAZINE 2020

Winner of Best Product for Threat Intelligence and Cutting Edge SaaS/Cloud Security 2020 CDM InfoSec Awards

WORLD ECONOMIC FORUM

The designated cyber security vendor of The Summer Davos World Economic Forum from 2017 to 2019

Threat Detection Platform

TDP

Product Overview:

ThreatBook’s Threat Detection Platform (TDP) enables in-depth full analysis of bidirectional traffic with an intelligence-driven threat detection kernel and a risk analysis module that fully considering the customer’s perspective. It serves as a strong foundation for the security team to have a good awareness of network security situation, discover hidden risks, focus on real threats, strengthen the ability of incident response and improve operational efficiency.

Core Capabilities:

Identify successful External Attacks and Pinpoint Compromised Hosts

Accurately identify successful external attacks through bidirectional network traffic detection;

Present threat situations in multiple dimensions and perspectives with data visualization technology;

Rely on ThreatBook’s professional threat intelligence data capability and analytical skills to accurately pinpoint compromised hosts in the intranet.

Discover Assets and Identify Risk Exposure

Use traffic monitoring to identify enterprise’s open ports and running applications and help the enterprise understand the cyber exposure status of assets and carry on targeted and reasonable management.

Use the real-time detection module to inspect the enterprise portal access, weak passwords usage, anomalous API behavior, and file transfer into or out of the enterprise, and help the enterprise understand the security weak points.

Eliminate Threats through cooperation of Access Control and Endpoints

Security teams can make informed remediation decisions with the help of the rich context of threat intelligence regarding the incidents.

Support blocking network access of the compromised host, and provides endpoint tools that connected to the platform to identify malicious processes, block network access, and automatically wipe out common malware.

Product Features:

01

Synchronize with ThreatBook’s professional threat intelligence database on minute basis

02

Scientifically classify threat events and provides a rich contextual information for threat events

03

Support flexible deployment at any network node in a bypass manner

04

Complete cyber-attack path discovery and present threat situations in multiple dimensions and perspectives

05

Provide endpoint remediation tools to identify malicious processes and block threats

06

Support bidirectional traffic monitoring for rapid detection of successful attacks and APT.

“Focus on Real Threats”

Threat Intelligence Platform

TIP

Product Overview:

ThreatBook’ s Threat Intelligence Platform (TIP) is the first threat intelligence management and distribution platform in China. It supports integrate multi-source intelligence to achieve unified management and distribution, help enterprises produce proprietary threat intelligence locally and conduct intelligence correlation analysis and deep mining, and integrate with existing security systems to enhance threat awareness and response capabilities.

Core Capabilities:

Integrate and Distribute Multi-source Intelligence

ThreatBook’ s machine-readable/advanced intelligence report, third-party business intelligence, open source intelligence and corporate proprietary intelligence are seamlessly integrated to conduct standardized and multi-dimensional quality assessment of multi-source threat intelligence, achieve unified management of intelligence, and facilitates threat intelligence query and distribute across the organization.

Empower Organizations to Produce Proprietary intelligence

TIP incorporates miniaturized versions of ThreatBook’ s leading threat intelligence production algorithms and processes, which can automatically produce threat intelligence targeted at raw data from the user’ s environment and standard data from ThreatBook.

Localized Threat Intelligence API

Based on ThreatBook’ s industry-leading threat intelligence data, localized high-frequency intelligence query APIs are provided to assist corporate security teams in business risk assessment and conducting focused protection in business areas with the support of intelligence data.

Collaborate with Security Devices

Collaborate with firewalls, WAF, IDS/IPS and other security devices downstream are achieved with custom policies and plug-in to enhance automatic response and strengthen protection capabilities.

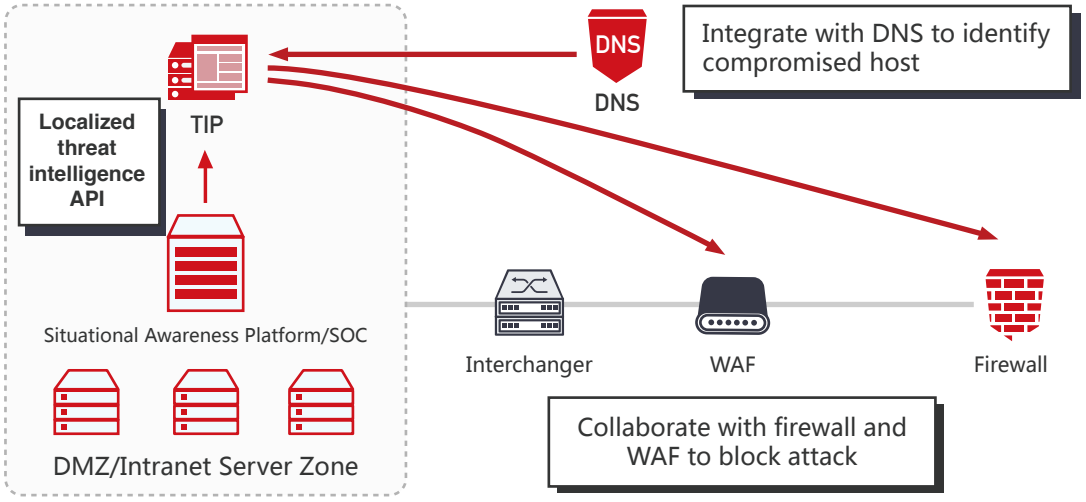
API Implementation with Situation Awareness, SOC and SIEM Platforms

Based on TIP’ s unique modules, connection with situation awareness, SOC and SIEM platforms are implemented to enable data correlation analysis, in-depth intelligence mining, and alert prioritization, and improve the intelligence detection and analysis capabilities of the security operation system.

Support Cascading Deployment in Multiple Sites

Enable centralized management of threat events and distribution threat intelligence with cascading deployment.

Integrate With Situational Awareness Platforms



Product Advantages:

01

Carry with ThreatBook's high-value machine-readable intelligence from all over the world

02

Support local production of proprietary threat intelligence

03

Seamlessly API implementation with popular domestic and international situation awareness / SOC / SIEM / big data platforms

04

Support SaaS and on premise deployment to address requirement for cloud environment and corporate data privacy needs

05

Provide customized plug-in to meet the needs for real-time threat blocking

06

10,000 level QPS for threat intelligence query

OneDNS Cloud

Product Overview:

OneDNS Cloud is a secure cloud platform focus on DNS resolution, providing SaaS-based DNS query inspection and access management services. OneDNS Cloud blocks connection between network devices and malicious IP addresses in real time to prevent subsequent attacks. Security management teams can flexibly apply policies on the OneDNS cloud based control panel to perform access Control & Audit. This SaaS based service can easily adapts to various IT architectures, enabling unified security protection for corporate headquarters, branches, roaming devices, even cloud applications

Core Capabilities:

Precisely Block Malware Attacks

91% of the malware use DNS protocol. Based on ThreatBook' s high-quality threat intelligence, OneDNS Cloud can accurately block malware communication and prevent further attacks.

Protect Web Browsing

OneDNS Cloud will automatically block users' access to malicious websites such as phishing websites and websites embedded with Trojans, and then send risk warnings pages to users.

Access Control and Audit

The security management team can configure content classifications or network addresses to be blocked/allowed for headquarters and branch offices according to the corporate security policy.

Provide a Holistic View of Security

The OneDNS cloud based control panel provides enterprises with multi-perspective data reports, presenting the content classification of websites visited, detected internal security threat alerts, and non-compliant browsing behaviors. Optionally, a Virtual Appliance (VA) can be installed locally to pinpoint internal host behaviors.

Product Features:

Stable And Fast Resolution Service

The OneDNS Cloud has a DNS caches covering ten regions and three major operators across the country, and a comprehensive disaster recovery plan allowing for high availability switching failover in seconds.

Simple Deployment Without Hardware

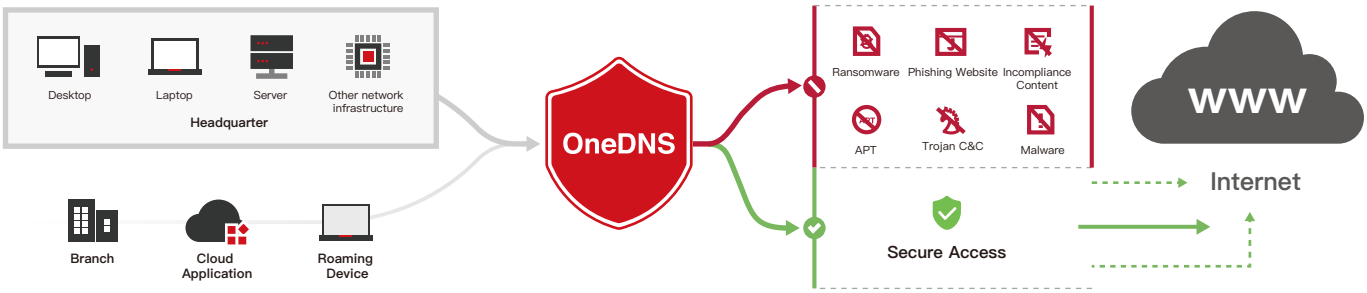
Full deployment across the enterprise network can be completed within half an hour by simply setting the default DNS server of the computers, servers or network devices to access the IP address pointing to OneDNS services

Unified Management and Control Of Head-quarters, Branches and Remote Offices

With support for diverse access scenarios such as network egress, dynamic IP and roaming hosts, administrators can perform unified management from the cloud console.

Comprehensive Threat Protection

Threat intelligence is updated on minute basis to accurately and timely stop malicious behaviors of malware, trojans, worms and ransomware, block employee' s access to phishing websites, and protect corporate network security.



Since its establishment in 2013, OneDNS has been serving millions of users. OneDNS is one of the few professional vendors with Internet domain name resolution service qualifications.

ThreatBook X Intelligence Community

Product Overview:

The X Intelligence Community is the first comprehensive threat analysis platform and intelligence sharing community in China. Based on threat intelligence query, analysis and sharing, it provides security practitioners around the world and enterprises with a convenient one-stop analysis tool, and aims at helping community users improve the ability to quickly analyze and respond to security incidents through real-time analysis and detection results and shared information such as IOCs, hacking resources, TTP, clues and events, and providing enterprise users with enterprise-level services such as security operations tools, external asset monitoring and industry-specific threat intelligence, thereby assisting individuals and enterprises in quickly locating and eliminating potential security risks.

Product Features:

Open Threat Intelligence from Community Users along with Attractive Intelligence Sharing Rewards Program

In addition to open intelligence shared by users, the X Intelligence Community is the first to launch the intelligence sharing program with rewards of tens of millions RMB to encourage intelligence sharing across the security industry, attaching importance to discovery of high-quality Intelligence and sincerely rewarding community members and business customers.

Comprehensive Threat Types and Analysis Results

Focuse on data accuracy and abundant, deliver extensive data sources and visualize the correlation analysis results to help users quickly and promptly eliminate potential network security risks. Support security analysis and visualized analysis of asset monitoring / domain name / IP / Hash / URL for event identification, threat level analysis, threat impact analysis, and correlation and traceability analysis.

Powerful Enterprise-level Tools and Services

Provide enterprise-level batch intelligence query tools and external asset monitoring services to help enterprises quickly discover asset threats, data leakage risks such as password leakage, sensitive file leakage and mailbox leakage, and service exposure risks such as exposed web portals, services and ports.

Accurate Scenario-based Threat Intelligence API

Obtain all data from ThreatBook’ s threat analysis platform through private APIs tailored for your application scenarios, which can be deeply integrated with your products and services.

ThreatBook SaaS API

Product Overview:

ThreatBook SaaS API relies on the powerful raw data collection system in the cloud, combined with a variety of independently developed core intelligence extraction systems with dozens of extraction methods, to quickly and automatically produce high-coverage, high-accuracy, context-rich intelligence data, providing unique value for a variety of business.

Data Accumulation:

- Raw data of tens of billions of domain names records accumulated with millions of newly registered domain names everyday
- PassiveDNS data over 8 years
- Historical Whois domain data records over 18 years
- Billions of malicious samples accumulated along with 1 million new newly captured malicious samples
- 400,000 high confidence IOCs
- Reputation and labels of 4.2 billion global IP addresses
- Tracing Attacks of more than 180 famous hacking groups around the world on an hourly basis
- Intelligence updated on minute basis

Business Values:

- Threat discovery and compromise detection for office network hosts / production networks and DMZ servers
- Risk evaluation 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 hosts/-servers for identification of malicious programs
- Threat detection cooperates with internal SOC/SIEM big data platforms or analysis logs from security device such as WAF/IPS/NGFW
- Correlation and traceability 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 name Compromise detection	Hash query File reputation report	URL analysis URL reputation report
Advanced Query API	Advanced IP query	Advanced domain name query Subdomain name query Domain name context		

ThreatBook Cloud Sandbox

Product Overview:

Unlike traditional malware detection method, ThreatBook Cloud Sandbox provides a comprehensive multi-dimensional detection service, which collects and analyzes static and dynamic behavior data of files by simulating their execution environment and using these data in combination with Threat Book' s threat intelligence cloud to discover unknown threats in minutes.

Product Features:

Rapidly detect threats in both Windows and Linux environment. More than 20 types of files are supported

Enable automated and customizable behavior analysis of malicious files with virtual sandbox deep analysis technology for detection of unknown threats

Integrate ThreatBook's multi-core advanced intelligence analysis system to intelligently identify threats among network and host behaviors during file execution, producing IOCs that can be used directly for compromise detection and incident analysis

Support identification and detection of anti-sandbox malware to prevent malware from bypassing virtual machine checks

Product Advantages:

1 Supports file uploading API for automatically detection of know and unknown threats.

2 Combines more than 700 high-quality behavior signatures to better identify and classify key behaviors of malware.

3 Continue to capture millions of newly created malicious samples in real-time through multiple sources such as honeypot networks around the world to achieve full coverage of threats across global.

Managed Detection and Response

MDR

Service Overview:

The support from senior security experts enable timely discovery, alert, response and remediation of internal and external threats, as well as hackers' profile analysis and traceability analysis of attackers. In-depth analysis is performed on events such as mainstream threats, major security incidents, and high-risk APTs. Recommendations are provided on early warning, prevention, response and remediation. Threat intelligence and security incidents in key industries such as finance, energy, and government are refined and analyzed to provide best practices for response and remediation, helping enterprises improve security ability.

Service Introduction:

Threat Inspection

Conduct periodic (such as monthly/quarterly) monitoring and inspection on office hosts/production servers through dedicated threat detection devices, investigates and identify security issues and hidden risks, and provide recommendations on rectification and remediation

Incident Response

Provide fast and professional incident response services for emergencies or major security events such as business unavailability, internal network compromised and production network intrusion, locate, fixe and trace security events to guarantee normal operation of business

On-Site Cyber Security Protection Services

During major events and cyber-attack drills, designate on-site security experts to assist the security team in responding to real/simulated external attacks.

Expert Consultation

Provide auxiliary analysis and remediation services for suspicious threats and security device alerts in daily operation, and provide suggestions for improving security operation capabilities and efficiency.

Advanced Intelligence Report Subscription

Deliver high-value security protection intelligence, methods and advices with regard to in-depth analysis reports on typical security incidents in key industries and the latest global epidemic threats, external assets and risks.

External Asset Monitoring

Discover external assets of the enterprise from an external perspective, collect external exposure data, analyze and identify related threats and potential risks, and provide early, comprehensive, accurate, and effective intelligence data for timely response of related security threats and risks.

Leader in Threat Detection and Response

ThreatBook

E-mail: contactus@threatbook.cn Tel: +8610-57017961

Beijing: 3rd Floor Suzhoujie Street, Yingzhi Plaza,49-3 Suzhoujie Street, Haidian District,Beijing

Shanghai: Room 306, 6th Floor, Lane 88, Rongsheng Road, Pudong New District, Shanghai

Shenzhen: CRO7, 15th Floor, Block B, East Block, Nanshan Coastal Building, Shenzhen