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.

Core Capabilities

ADVANCED COMPREHENSIVE THREAT PROTECTION

PROTECTION FOR ROAMING ENDPOINT

LIGHTWEIGHT SAFETY CLOSED LOOP

CUSTOMIZABLE AND FLEXIBLE CONFIGURATION

CENTRALIZED MANAGEMENT MULTIPLE WORKPLACES

New experience of enterprise office security

Light

Light deployment, light operation and maintenance, light management

No hardware investment, zero operation and maintenance costs, and complete access in 10 minutes.
An integrated close loop of detection, interception, positioning, evidence collection, simplifying the security operation process.

Full

Full intelligence, full scene, full coverage

Threat intelligence updates in time, covering all scenarios of centralized work, multiple branches, and remote work. All types of terminals are fully supported, like Host/PC, Windows/Linux, and IoT.

Accurate

Analysis accuracy, detection accuracy, interception accuracy

100+ accelerated sites, ten-year intelligent link optimization.
Hundreds of millions of levels of intelligence coverage, 99.99% detection rate, automatic interception without human intervention.

Steady

Professional qualifications, enterprise-level SLA and QoS

Internet Domain Name Resolution Service Qualification Certificate, 100% uninterrupted service for nine years.
National 100+ acceleration sites, distributed decentralized architecture, automatic load balancing and fault self-healing, and 99.999% availability.

i-Sprint
Trust without Boundaries

ThreatBook

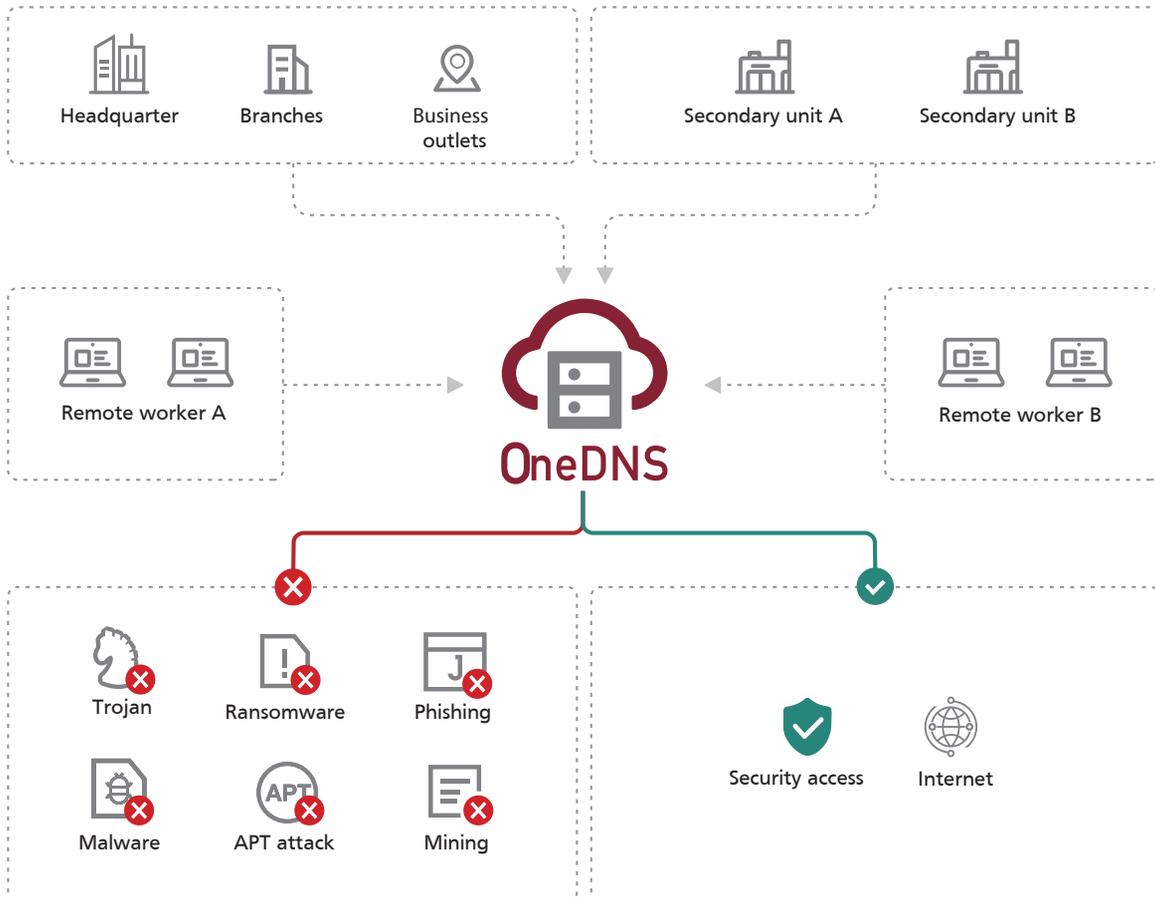## ⭐ Typical cases and scenarios

CASE STUDY

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.

| Headquarter | Branches | Business outlets | | Secondary unit A | Secondary unit B |

Remote worker A

OneDNS

Remote worker B

| Trojan | Ransomware | Phishing |
| Malware | APT attack | Mining |

| Security access | Internet |