
# CCTV

# NETWORK THREAT DETECTION SYSTEM

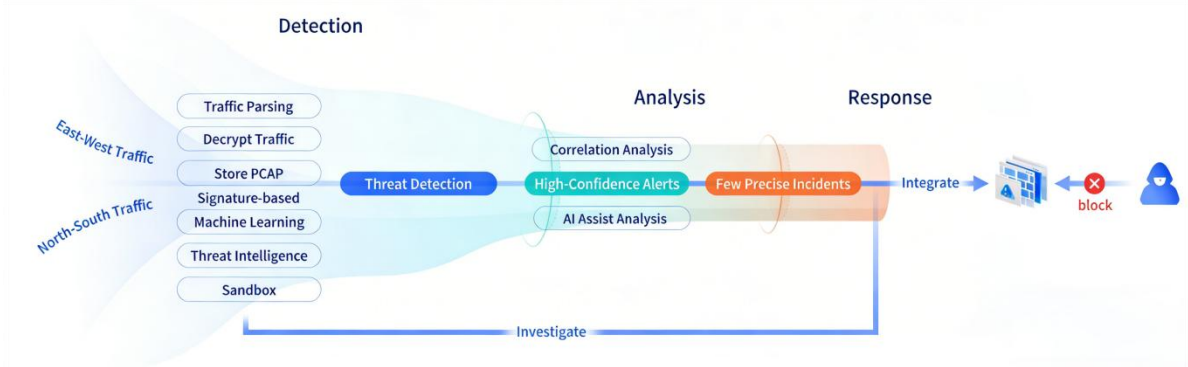
# 1. Product Overview

The Viruni CCTV Network Threat Detection System (CCTV-NDR) is an advanced threat early warning system that integrates traffic threat detection, malicious file detection, analysis and tracing, and coordinated response. Relying on a rich feature library, comprehensive detection strategies, and accurate in-depth analysis models for rule-based detection and combining advanced threat detection technologies such as intelligent machine learning, dynamic sandboxing, semantic analysis, and threat intelligence.

It can instantly detect various known and unknown threats in users' networks. Its detection capabilities fully cover the entire APT attack chain and support the detection of more than twenty types of attacks, including various malicious code attacks, remote control, WEB attacks, email attacks, vulnerability exploitation, tunnel communication, etc.

It helps users identify advanced threats such as APT arsenal fingerprints, abnormal encrypted traffic, fileless attacks, anti-traceability C&C attacks, 0-day attacks, etc.

The platform presents the threat situation within the network through visualization technology, could store complete data packets and conduct retrospective analysis and forensic investigation, can provide real-time warnings of network attacks, and enhance users' awareness of network attacks.




# 2. Key Benefits

### Incident Monitoring and Response

CCTV-NDR is capable to detect security incidents such as mining, ransomware, botnets, data breaches, host compromises, and lateral attacks. It can also collaborate with firewalls, WAFs, and EDRs to handle and respond to these incidents.

### Attack Forensics and Tracing Analysis

CCTV-NDR can not only identify existing threats but also record information such as the source of the threat, attack methods, attack process, attack targets, and attack impacts.

### Detection of Known and Unknown Threats

CCTV-NDR can conduct comprehensive detection and analysis for various known and unknown threats. Its detection scope covers the entire APT attack chain.

## 3. Features

### Network Traffic Detection

CCTV-NDR can capture and analyze network traffic in real-time. The product uses AI security detection technologies such as threat intelligence, machine learning, and semantic analysis, combined with sandbox-based malicious file detection, to accurately detect known and unknown cyber threats

It supports 1-click switching between operation mode and expert mode for flexible threat investigation. Operation mode allows analysts to filter events by commonly used fields such as event type, risk level, attack status, rule ID, Packet ID, payload, CVE/CNNVD ID, etc.

Expert mode supports compound query expressions with logical operators including but not limited to: AND, OR, NOTIN, ==, and! =. It also provides at least 7 built-in investigation templates and allows users to create and save custom templates based on historical filter conditions for future use.

It supports status-level inspection of traffic, including analysis of individual packets, session connections, retransmission packets, and overall network payloads. It can generate alerts on abnormal behaviors in business network traffic transmission.

It includes 30 or more deep detection modules, covering high-risk web attack techniques such as Shiro deserialization and webshell variants including AntSword, Godzilla, Behinder 3.0 and Behinder 4.0. It can be capable of identifying covert tunneling and proxy tools used for Command and Control, including but not limited to: Shootback, TunnaProxy, dnsat2, reGorg, reDuh and Cobalt Strike.

### Phishing Email Detection

CCTV-NDR employs the XGBoost model trained with a large number of malicious samples to conduct phishing email detection from multiple aspects including email headers, email contents, URLs, and QR codes. It checks for deception in email headers, sensitive information in email contents, and factors like the number of hyperlinks, redirects, and specific characters within URLs. These features are evaluated comprehensively. Once the score of a detected email surpasses the set threshold, it is identified as a phishing email.

### Dynamic Sandbox Detection

CCTV-NDR incorporates dynamic sandbox analysis technology, which is capable of detecting malicious behaviors in files. These malicious behaviors include registry actions, operations in

sensitive paths, process - related behaviors, import table information, resource information, segment information, string information, and behaviors such as taking screenshots during the file's operation.

It supports mainstream operating systems including Windows XP, Windows 7, Windows 10 and Linux as Sandbox environments. The sandbox module is built with independently developed technologies and patents.

### Intelligent Semantic Detection

CCTV-NDR is equipped with the intelligent semantic detection function. It can conduct in - depth analysis by associating with the context, deeply understand the semantics of the code, restore the attacker's intentions, and detect attacks that traditional intrusion detection systems cannot identify, such as SQL injection, XSS, OGNL, JSP scripts, PHP scripts, and other attacks.

### APT Attack Detection

CCTV-NDR detects APT attacks in multiple ways. It captures intruder traces across the APT attack chain via traffic detection. Using threat intelligence on 500+ APT groups, it spots their activities. A powerful file sandbox and the new Orca Sandbox analyze files to find unknown APT threats. Also, it identifies connections to known APT groups from communication traffic.

### Customized Detection and Analysis

The product is equipped with a customized detection and analysis module. Through user - defined configurations, it can detect various abnormal behaviors in the traffic, including the transmission of sensitive information in emails (such as emails containing sensitive content, emails sent or received during login from a different location , emails sent or received at special time periods or by specific senders), abnormal logins (such as logins from different locations, logins at special time periods, logins of specific accounts, or logins to specified business servers at specific times or locations), unauthorized connections (such as communication with IPs in specified geographical locations, communication during specified time periods), abnormal network sessions (such as abnormal network transmissions), periodic abnormal attacks (such as slow brute - force attacks, Distributed Denial of Service (DDoS) attacks, abnormal multi - frequency access to IPs/domains), and characteristic - based abnormal attacks.

### In-depth Web Attack Detection

CCTV-NDR achieves in-depth Web attack detection by conducting in-depth inspection of HTTP traffic. It performs multiple operations such as Web address translation, decrypts encrypted messages to detect wehshell attacks, collaborates with WAF (Web Application Firewall) and NGFW (Next-Generation Firewall) to protect against attacks and block risky IPs and domains. It detects

abnormal access and locates attackers by analyzing various dimensions like access accounts, utilizes static script analysis technology to detect attacks exploiting common Webmail vulnerabilities, and also filters normal Web business access based on machine learning.

### In - depth File Attack Detection

CCTV-NDR focuses on in - depth file attack detection. Aiming at file - based APT attacks, it uses file intelligent recognition algorithms to separate and identify files in the traffic. It can quickly and accurately (with an accuracy rate of 99%) detect malicious threats such as viruses and Trojans, covering various malicious behaviors like CVE vulnerability exploitation. Meanwhile, CCTV - NDR analyzes the threat trends and indexes of hosts, grasps the spread patterns of malicious samples, and warns of network security threats.

### Encrypted Traffic Detection

For APT (Advanced Persistent Threat) detection, decryption can be carried out by uploading private key certificates. It supports SSL protocols such as TLS1.1 and TLS1.2, but does not support TLS1.3 and the DH algorithm.

### Automated Incident Response

CCTV-NDR can coordinate with other products, such as firewall, WAF, EDR, for defense and response to security incidents. It generates protection policies by calling API interfaces of other products and supports bypass blocking by sending Reset packets to servers.

### Intelligent Reports

CCTV-NDR offers five types of intelligent reports, including comprehensive threat analysis, host threat analysis, file threat analysis, external threat analysis, and asset risk analysis. The generation and analysis functions of these intelligent reports effectively replace traditional manual threat analysis, providing users with more efficient and accurate risk assessments.

## 4. Advantages

### AI-powered Threat Analysis

CCTV-NDR leverages AI and advanced machine learning algorithms to analyze network data, to accurately detect known and unknown cyber threats.

### All IN ONE

CCTV-NDR integrates functions such as traffic collection, threat detection, high - performance sandbox, large - screen display, and threat analysis. It features simple deployment, high reliability, and effectively avoids issues caused by poor coordination among multiple devices, thus saving construction and maintenance costs.

### Leading High - Performance Architecture

It adopts the VPP high - performance technology architecture such as vector packet processing, protocol linear parsing, and multi - mode feature matching. The performance of APT product category is far ahead. The maximum throughput performance can reach 100G.

### Precise Detection for Reducing False - Alarm Rate

CCTV-NDR uses a machine - learning - based detection model to score SQL commands and XSS script behaviors from normal business operations, determining their normality to lower false - alarm rates. It also accurately identifies attack states by analyzing context and response content. Leveraging over 12 million pieces of high - precision intelligence, such as malicious address libraries, CCTV - NDR organization information, and details of malicious families, it precisely warns of incidents like compromises, remote control, ransomware attacks, DDoS attacks, tampering, and network scans.

It supports alarm deduplication and convergence with entity-based classification. Top30 abnormal clients IPs and their event frequencies shall be visualized via color-coded bar charts, with 1-clisk drill-down to view original alerts and attack statuses. Exported event reports shall include, at minimum: Client IP, Server IP, number of successful attempts, number of risk events, total event count, event name, risk level, attack status, 1$^{st}$ occurrence time and last occurrence time.

### Deep Protocol Analysis

Collected by the platform is processed by a traffic analysis engine, which parses IP packet fields and flow characteristic information, analyzes application layer protocols, and determines the presence of applications in the traffic. Protocol parsing is performed from multiple dimensions:

- It supports bidirectional traffic auditing, enabling auditing of both request and response content.
- It supports parsing protocol messages such as HTTP, FTP, SMTP, POP3, SMB, IMAP, DNS, HTTPS, SMTPS, POP3S, IMAPS, RADIUS, KRB5, SNMP, NEFLOW, TFTP , HTTP2, and NNTP (HTTPS, SMTPS, POP3S, and IMAPS encrypted protocols requires importing the server's private key certificate), and provides port number configuration for auditing protocol types, which can be changed as needed.
- It supports parsing and auditing of 5G related protocols, including GTP, PFCP and NGAP.
- It supports login behavior recognition for commonly used protocols and applications, including QQ, Web, LDAP, FTP, Telnet, SMPT, POP3, SMB, Radmin, Oracle, MSSQL, Sybase, MySQL, DB2, PostgreSQL, Redis and MQTT.
- Source IP address, destination IP address, source MAC address, destination MAC address, source port, destination port, protocol number, message length, packet length, etc.

- The initial occurrence time and end time of the traffic, and the duration of the traffic.
- Based on protocol behavior feature analysis.
- based on the behavioral characteristics and patterns of each protocol.

## 5. Specifications

| CCTV-NDR- Physical Appliance | | | |
|---|---|---|---|
| Model | CCTV-NDR-E2000 | CCTV-NDR-E10000 | CCTV-NDR-E50000 |
| **Performance** | | | |
| Traffic Handling Capacity (Network Layer) | 2Gbps | 10Gbps | 50Gbps |
| **Technical Specifications** | | | |
| Memory (GB) | 32 | 128 | 256 |
| Data Hard Drive Capacity | SATA 2TB*1 | SATA 4TB*1 | SATA 8TB*2 |
| **Hardware specifications** | | | |
| Dimension (L x W x H) (mm) | 550*435*89 | 550*435*89 | 729.8*482*87.8 |
| Rack Height | 2U | 2U | 2U |
| Gross Weight (kg) | 15kg | 20kg | 35KG |
| Power Supply | Dual | Dual | Dual |
| Maximum Power (W) | 300 | 350 | 800 |
| Bypass | N/A | N/A | N/A |
| Management Network Port | USB2.0*2<br>RJ45*1 | USB2.0*2<br>RJ45*1 | USB3.0*4 |
| Network Port | GE*6 | GE*6<br>1GbE SFP*4<br>10GbE SFP+*2<br>Port Expansion Slot: 2 | GE*4<br>10GbE SFP+*4 |