White Paper

Intel® Xeon® 6 Processors

Intel® Ethernet 810 Network Adapters

Powered by Intel® Xeon® 6 Processors, H3C SecCenter CSAP-NDR Enables Enterprises to Build Comprehensive and Accurate Security Threat Detection and Operations Management Platforms

Authors

Yiwen Li

Dong Wang

Intel Corporation

Table of Contents

1. Introduction

With the increasing complexity of network environments and the advancement of cyberattack techniques, enterprise data increasingly faces severe threats. Traditional single-point network security protection tools have exposed problems such as frequent false positives in threat analysis, difficulty in tracing and collecting evidence, and inefficient response and disposal. In this context, Extended Detection and Response (XDR) and Network Detection and Response (NDR) are gaining widespread adoption. By centralizing the collection and correlation of data from multiple security layers, they enable more efficient and accurate security protection.

H3C has launched the H3C SecCenter CSAP-NDR security threat discovery and operations management platform. This integrated hardware and software solution utilizes servers equipped with Intel® Xeon® 6 processors and Intel® Ethernet E810 Network Adapters. It leverages tools and technologies such as Network Traffic Recorder (NTR) and Data Plane Development Kit (DPDK) optimized for Intel platforms to build XDR and NDR platforms. This platform provides users with network threat detection, in-depth threat analysis, and full-packet tracing and forensics capabilities, improving the security of network and business systems and incident handling efficiency, providing in-depth network security protection.

2. XDR and NDR Have Become Essential Tools for Enterprises to Deal with Complex Security Threats

As digital transformation progresses, the scale and variety of enterprises' digital assets are rapidly expanding. While digital applications distributed across cloud, mobile, and other locations drive business growth, they also expand the cybersecurity attack surface, potentially putting enterprise data assets at risk. In traditional security architectures, various security devices and applications typically operate independently, lack correlation analysis, and rely on manual intervention. This makes it difficult to cover heterogeneous environments across multiple sources, including cloud, end-point devices, and networks. Enterprises urgently need a holistic threat detection solution.

XDR provides unified security management and coordinated response capabilities, integrating security-related endpoint detection data with telemetry from various security and business tools, such as network analytics and visibility (NAV), email security, identity and access management, cloud security, and security information and event management (SIEM). As an emerging security platform, XDR, built on a big data infrastructure, provides security teams with exceptional visibility, flexibility, and scalability, ultimately enabling them to automate various functions. As a key product category within the XDR space, NDR focuses on network-related detection and response, encompassing traffic

processing, threat detection, source analysis, and coordinated response mitigation. This helps accurately identify threats, generate alerts, and leverage other security capabilities for remediation.

For enterprises, NDR provides the following important capabilities:

- Process multi-source traffic and conduct coordinated analysis of the threat data
- Identify various security threats and then automate responses through security orchestration, shortening the response time
- Provide a unified security dashboard, offering global visibility and displaying attack paths, impact scope, and trends
- Supports threat detection in multi-cloud environments, meeting compliance requirements for data localization or cloud storage

To successfully deploy NDR solutions in enterprises, multiple challenges must be overcome, including performance and traffic analysis. Regarding performance, big data-based data analysis is a core component of NDR, involving workload processing such as data matching, network packet encryption and decryption, and data compression. Enterprise customers require NDR platforms to quickly and efficiently process and analyze large amounts of real-time data. However, as the amount of threat data they need to process continues to grow, NDR platforms are facing increasing performance pressure.

3. H3C CSAP-NDR Solution Based on Intel® Xeon® 6 Processors

3.1 H3C SecCenter CSAP-NDR Security Threat Detection and Operations Management Platform

H3C has launched a suite of security products and solutions for advanced persistent threat (APT) attack detection and prevention, specifically the H3C SecCenter CSAP-NDR Security Threat Detection and Operations Management Platform (H3C SecCenter CSAP-NDR). These products and solutions are designed for APT detection, disposal, and tracing.

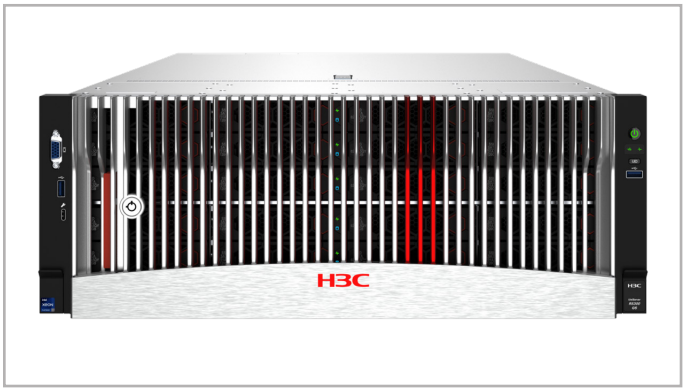

Figure 1. H3C SecCenter CSAP-NDR Security Threat Detection and Operations Management Platform

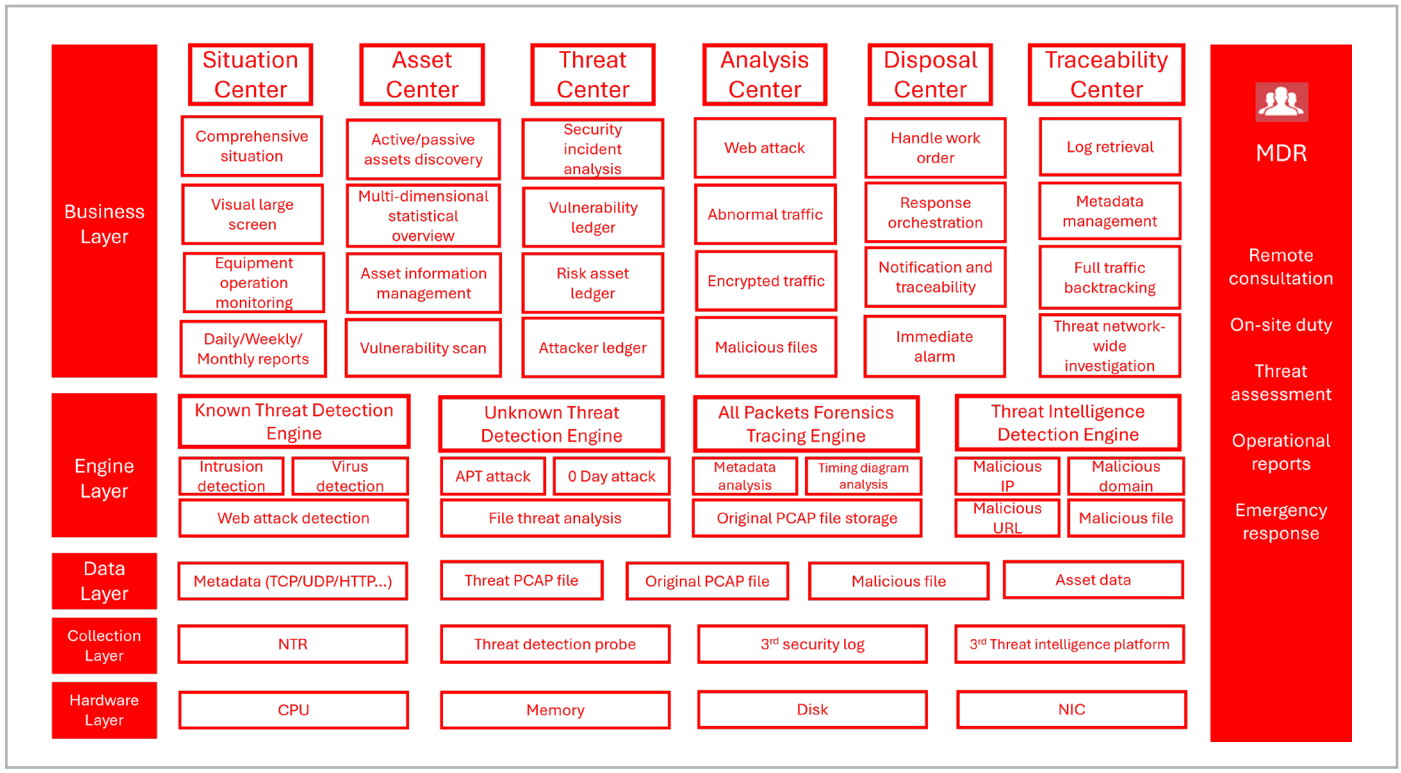

Figure 2. HC3 SecCenter CSAP-NDR Architecture

H3C SecCenter CSAP-NDR can conduct in-depth analysis of data flows on key paths by mirroring network traffic, including:

- Threat detection capabilities based on a million-level threat intelligence library, IPS signature library, AV signature library, and application signature library
- Perform AI in-depth analysis based on association analysis and behavior analysis models
- Identify complex attacks based on CAPEC and ATT&CK technical and tactical attack methods
- Provide comprehensive traceability capabilities based on panoramic attack chain analysis, in-depth analysis of alarm events, and full-packet storage backtracking technology
- Based on Security Orchestration, Automation, and Response (SOAR) technology, network devices, security devices, and terminal devices are linked to achieve rapid response

The platform provides customers with a set of advanced threat detection, source tracing analysis and response integrated systems. This can be widely used in attack and defense drills, security activities and other scenarios, improving the security of network systems and business systems and the efficiency of incident handling, and deeply protecting network security.

Focusing on "deep threat detection and tracing," H3C SecCenter CSAP-NDR integrates key technologies such as deep metadata analysis, full logging, file threat identification, UEBA behavior analysis, PCAP full-packet storage, real-time attack and defense monitoring, and precise tracing and evidence collection. It provides network threat detection, deep threat analysis, and full-packet tracing and evidence collection capabilities, helping customers enhance their decision-making and preemptive judgment, quickly identify and resolve issues, and improve security operations efficiency.

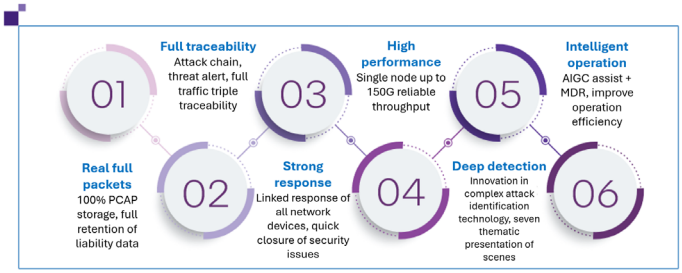

Figure 3. H3C SecCenter CSAP-NDR Platform Advantages

3.2 H3C and Intel Collaborate to Provide a One-Stop Shop NDR Hardware and Software Deployment Solution

H3C has partnered with Intel to provide a one-stop shop deployment solution for H3C SecCenter CSAP-NDR, combining both hardware and software. This solution can be configured with servers powered by Intel Xeon 6 processors, providing powerful computing power for workloads such as analyzing massive amounts of traffic data.

This solution integrates the NTR (Network Traffic Recorder) framework optimized for Intel platforms, which enables real-time reception and storage of zero-packet-loss network traffic. It meets functional requirements such as network packet indexing, network packet filtering, network packet data compression, data encryption, and network packet search and query, accelerating XDR/NDR load processing.

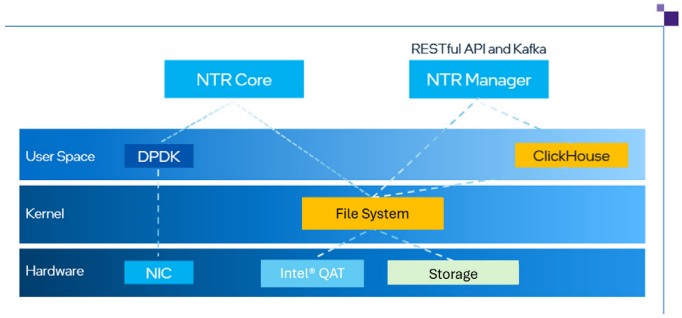

Figure 4. Network Traffic Recorder (NTR) Architecture

Intel Xeon 6 processor can be equipped with up to 144 efficient cores (E-cores) and supports 8 DDR5 memory channels.

Intel Xeon 6 processors not only have a rich core count but can also take full advantage of built-in hardware acceleration technologies such as Intel® QuickAssist Technology (Intel® QAT), which allows for better response to rapidly changing workloads and integrated deployment requirements in edge and network areas, help users achieve higher energy efficiency and deployment density.

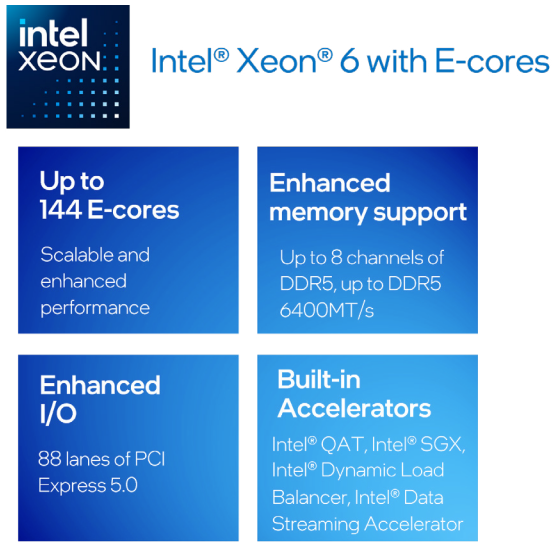

Figure 5. Intel® Xeon® 6 Processor empowers network and edge applications

The Intel® Ethernet E810 Network Adapter offers 100GbE performance and supports single or dual-port connections, providing excellent performance in PCIe 4.0 x16 slots and supports advanced features, such as Application Device Queues (ADQ), Dynamic Device Personalization (DDP), RDMA iWARP, and RoCEv2. It can effectively meet the stringent bandwidth and latency requirements of various workloads.

In addition to the hardware, the H3C solution also leverages various software optimization libraries from Intel such as DPDK and Hyperscan, and hardware accelerators such as Intel QAT for performance optimization.

- **DPDK**

DPDK is a high-speed network packet software development kit, able to read and write directly to the network interface card by bypassing the Linux system network protocol stack, combining the network interface card receive queue with the binding of different cores in a multi-core processor. The use of large page memory can achieve line-speed transmission and reception of high-throughput network traffic. DPDK with optimizations from Intel can significantly improve data processing performance and throughput, giving data plane applications more time to run.

- **Hyperscan**

Hyperscan is an open-source high-performance multi-regular expression matching library developed by Intel, for use on Intel® processors. Hyperscan provides a flexible and easy-to-use library that can match a large number of regular expressions simultaneously, has high performance and good scalability, and also provides unique features for network packet processing. In ClickHouse, Hyperscan supports the acceleration of regular expression matching, fuzzy query, and search in data analysis work. It significantly improves data analytics performance on the latest Intel processors.

- **Intel QAT**

Intel QAT is a hardware acceleration technology for high-performance security, private key protection, and compression/decompression scenarios. It can offload related workloads from the CPU to the Intel QAT device, effectively improving application and platform performance. For compression/decompression, Intel QAT supports compression for file systems and databases, supporting popular algorithms such as ZSTD and Zlib. Intel QAT compression can help customers effectively save storage space and cost.

When NDR platform stores the network traffic data, to better save storage space, it can leverage Intel QAT compression technology, to achieve fast and efficient data compression.

3.3 Test Setup and Reference Performance Results

To verify the performance of the H3C SecCenter CSAP-NDR one-stop shop deployment solution for hardware and software under typical network loads, H3C and Intel jointly conducted tests in a carrier network operator's project. The traffic model used is shown in Figure 6. The main traffic for this project is Real-time Transport Protocol (RTP) traffic.

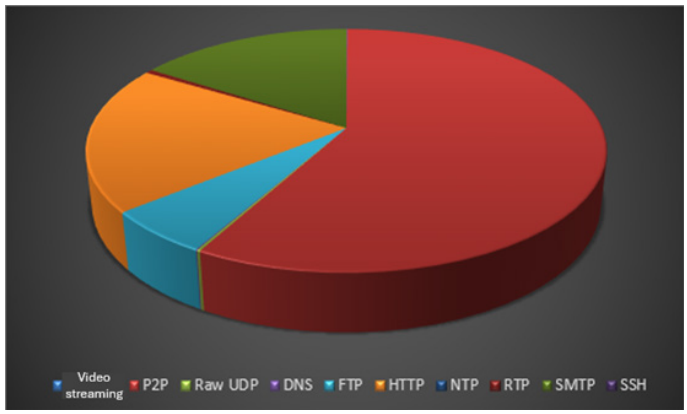

Figure 6. Traffic model used in a certain carrier project

The traffic trend of this project is shown in figure 7, under the single throughput of 100Gbps environment, the network traffic keeps stable, and the performance remains reliable.

In addition, H3C and Intel also jointly tested Intel QAT compression. Based on the performance data, Intel QAT compression was able to achieve compression ratio of 73.76%[1] for ClickHouse.

Figure 7. 100 Gbps Single Throughput Trend Chart[2]

[1] Data based on Intel test results on July 2025. Test Setup: Dual Intel® Xeon® 6740E processors @ 2.4 GHz, 192 cores, 512 GB memory (16x32GB DDR5 6400 MT/s), 11 x 3.5 TB Solid-State Drive, 1 x 1.7 TB Solid-State Drive, Ubuntu 24.04.1 LTS. Performance varies by use, configuration and other factors. Learn more at www.Intel.com/PerformanceIndex.

[2] Data based on H3C test results on July 2025. Test setup: Intel® Xeon® 6766E processor, 256 GB memory, NingOS V3 (1.0.2403); Virtual machine setup: Intel Xeon 6766E, 120 GB memory, NingOS V3 (1.0.2403). Intel does not control or audit third-party data. You should consult other sources to evaluate accuracy.

4. Future Opportunities

NDR has become a key tool for enterprises to deal with advanced threats by breaking down network security data silos and improving the automation level of security incident detection and handling. The H3C SecCenter CSAP-NDR security threat detection and operations management platform based on Intel technologies leverages software and hardware optimization acceleration, along with Intel data encryption and decryption technology, to efficiently analyze and process large-scale, real-time traffic data, providing users with leading NDR security services.

Intel Xeon 6 SoC is based on performance cores (P-cores), a cutting-edge product for network and edge. It not only inherits the excellent Intel® Advanced Vector Extensions (Intel® AVX) and Intel® Advanced Matrix Extensions (Intel® AMX) acceleration technologies, as well as powerful AI acceleration capabilities from the previous generation Intel Xeon processors, but also focuses on the deep integration of connectivity, computing power and AI features. It provides a variety of dedicated IPs in the I/O chip, including vRAN Boost, 200Gbps Ethernet, and media transcoding accelerators, which can more efficiently support NDR.

Figure 8. Intel® Xeon® 6 SoC delivers powerful performance and connectivity

In addition, H3C and Intel continue collaborating to optimize performance for real application scenarios and use a spectrum of security technologies from Intel to build a multi-level security protection system, thereby helping enterprises better protect the security of data centers and safeguard the digital transformation process.

Terminology

Abbreviation	Description
CPU	Central Processing Unit
XDR	Extended Detection and Response
SQL	Structured Query Language
NDR	Network Detection and Response

For More Information

H3C

Intel® Xeon® 6 Processor

Intel® Ethernet Products

Data Plane Development Kit (DPDK)

Hyperscan

Intel® Industry Solution Builders

About H3C

As a leader in digital solutions, H3C Group is committed to becoming a trusted partner for customers' business innovation and digital transformation. H3C possesses comprehensive digital infrastructure capabilities in computing, storage, networking, 5G, security, and terminals, and provides a one-stop shop of digital solutions including cloud computing, big data, artificial intelligence, industrial Internet, information security, intelligent connection, edge computing, etc. and end-to-end technical services. The network security product line is one of H3C's oldest product lines, with 20 years of development. H3C's active security solutions have extensively served customers in various industries, including government, operators, finance, energy, education, and healthcare, and are fully trusted by customers for their excellent products and high-quality services. To learn more information about H3C, please visit H3C's official website: h3c.com.

About Intel

Intel (NASDAQ: INTC) is an industry leader that creates world-changing technology, drives global progress, and enriches lives. Inspired by Moore's Law, Intel is committed to advancing semiconductor design and manufacturing to help customers meet their greatest challenges. By embedding intelligence into the cloud, network, edge, and various computing devices, Intel unleashes the potential of data to transform business and society for the better. For more information about Intel, please visit Intel's official website: www.intel.com.

1025/YL/PDF 367310-001US