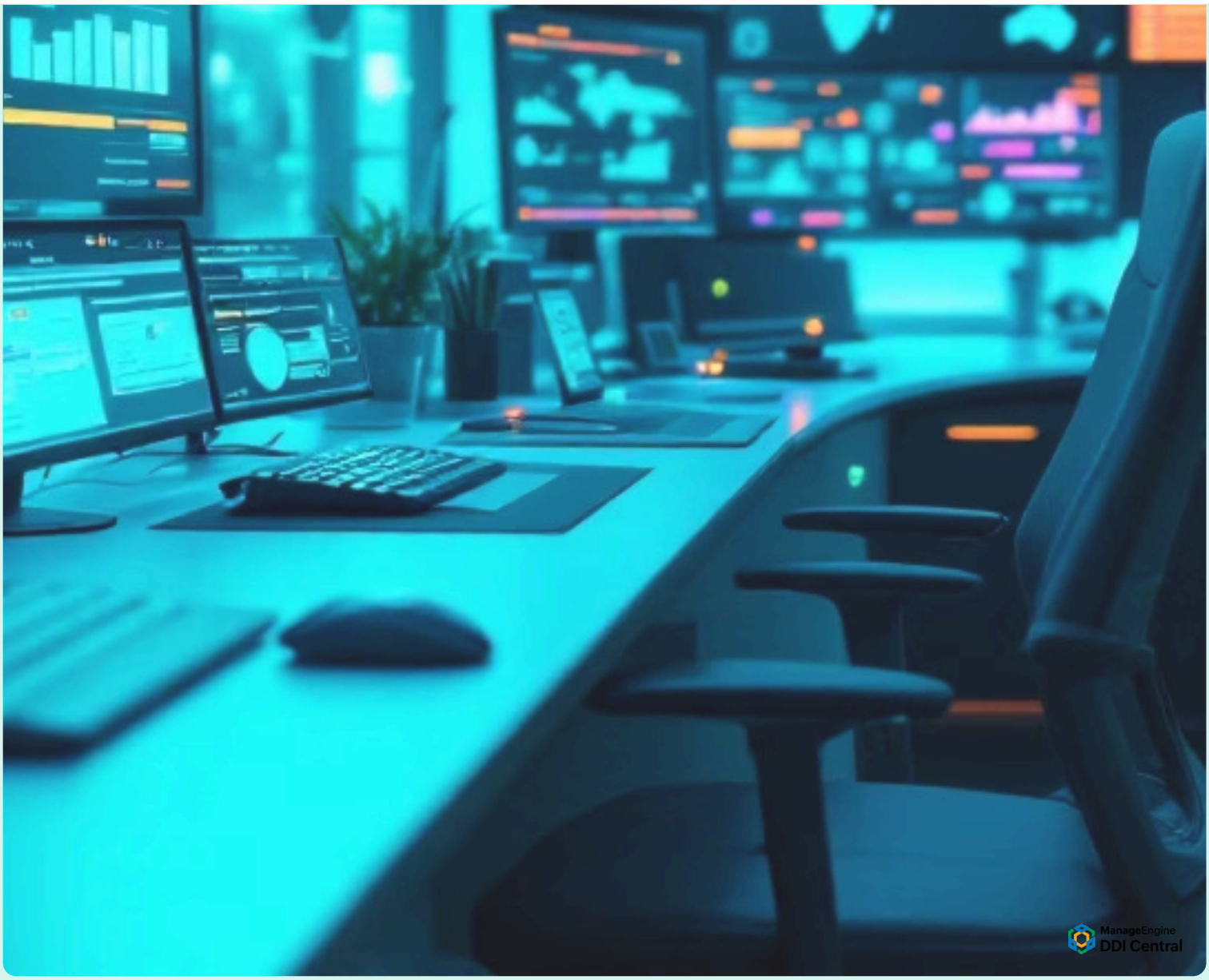
Detecting Hidden Threats in Enterprise Networks with DDI Central



Introduction

Modern enterprise networks have increasingly complex infrastructures, consisting of multiple clusters, branch networks, and segmented environments, all monitored and managed by network administrators. Despite implementing DNS- and DHCP-based security features and policies, certain cyberthreats can still infiltrate the network without the awareness of IT teams. These threats may compromise devices, spread laterally, and cause significant network disruption, leading to the loss of confidential data, operational delays, and reduced network reliability.

The Scale of the Threat

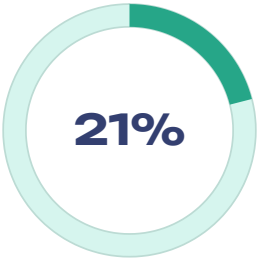
Malware, ransomware, and lateral movement attacks are among the most common and complex threats to detect and remediate in modern enterprise environments.

Average Data Breach Cost

A record high — a 10% increase over the prior year and the largest single-year spike since the pandemic, per the IBM Cost of a Data Breach Report 2024.

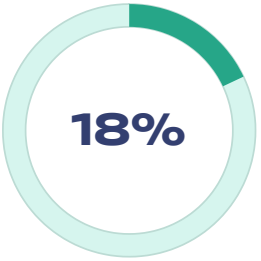
Organizations Hit by DNS Attacks

90% of organizations suffered DNS attacks in the past year, with each attack costing an average of USD 1.1 million, per the 2023 IDC Global DNS Threat Report.



Leverage DNS for Threat Intel

Only 21% of organizations currently leverage DNS data as part of their cyberthreat intelligence strategy, leaving a critical detection gap that threat actors continue to exploit.



DNS Attack Growth in 2023

DNS-based attacks increased by 18% globally in 2023, making network-layer visibility tools like DDI Central essential for early threat detection.

Organizations often find it difficult to detect lateral movement attacks because distinguishing between legitimate and malicious network traffic or user behavior is challenging. Organizations take close to **six hours on average** to mitigate each DNS-based attack, underlining the urgent need to move from reactive measures to proactive, purpose-built detection.

Key Challenges Enterprise Networks Face from Silent Cyberthreats

Enterprise networks face four critical security challenges that create opportunities for hidden threats to take hold and spread undetected.

1

Visibility Gap in Hybrid Environments

According to a press release by AlgoSec on its State of Network Security Report 2025, **71% of IT security teams** struggle with maintaining visibility across their organization's network security, especially in hybrid environments.

This challenge is largely driven by the increased adoption of cloud services, remote access tools, and third-party applications, which makes it difficult for network administrators to track what devices, users, and services are connected to the network.

This lack of end-to-end visibility and the presence of network blind spots create opportunities for attackers to breach the environment more easily, spread malicious activity across devices, and gain unauthorized access to confidential data.

2

Increasing Complexity of the Threat Landscape

The threat landscape is evolving rapidly, and the volume of cyber threats continues to grow in today's fast-moving digital world. Enterprise networks are becoming more vulnerable to modern cyberattacks that involve multiple, highly sophisticated techniques.

Although organizations are increasingly adopting artificial intelligence (AI) and machine learning (ML) technologies to strengthen their cybersecurity posture, attackers are also leveraging these technologies to exploit network vulnerabilities more efficiently.

This dual use of advanced technologies increases the risk for enterprises, as it becomes more challenging to predict, identify, and mitigate emerging threats and potential data breaches.

3

Lack of Effective Data Management

Network infrastructures across all sectors generate a massive volume of cybersecurity data on a daily basis. It is essential for organizations to collect, correlate, and analyze this data to detect threats and take timely remediation actions.

However, without the right tools for log management and data analysis, processing this information can become overwhelming and inefficient.

Many organizations struggle to prioritize critical alerts and derive actionable insights due to the absence of a centralized and structured data management system capable of handling large volumes of logs and alerts from multiple sources.

4

Implementation of ML for Cybersecurity

Organizations must prioritize the implementation of ML-based solutions to detect cyberthreats in real time across different network segments.

The use of ML techniques enables continuous learning from network behavior, helping enterprises identify anomalies and zero-day threats more effectively.

In addition, enabling automation for responding to real-time threats is crucial to minimize network exposure and reduce the manual effort required to differentiate between legitimate activity and malicious behavior. Automated, ML-driven systems significantly enhance proactive defense capabilities and improve overall security resilience.

How DDI Central Helps Detect Cyberthreats and Anomalies

DDI Central's **DNS Threat Intelligence and Anomaly Detection** features play a crucial role in strengthening an organization's DNS security posture by delivering a multilayered defense approach. It enables organizations to detect and mitigate cyberthreats proactively, preventing them from entering or spreading within the network in the first place. With ML-based threat intelligence mechanisms, DDI Central helps enterprises remain secure and resilient against increasingly complex cyberthreats.

Below are the key features DDI Central offers for DNS multilayered security:

DNS Threat Intelligence

Real-time threat feeds from ManageEngine CloudDNS and external vendors, automatically enforced across all DNS servers.

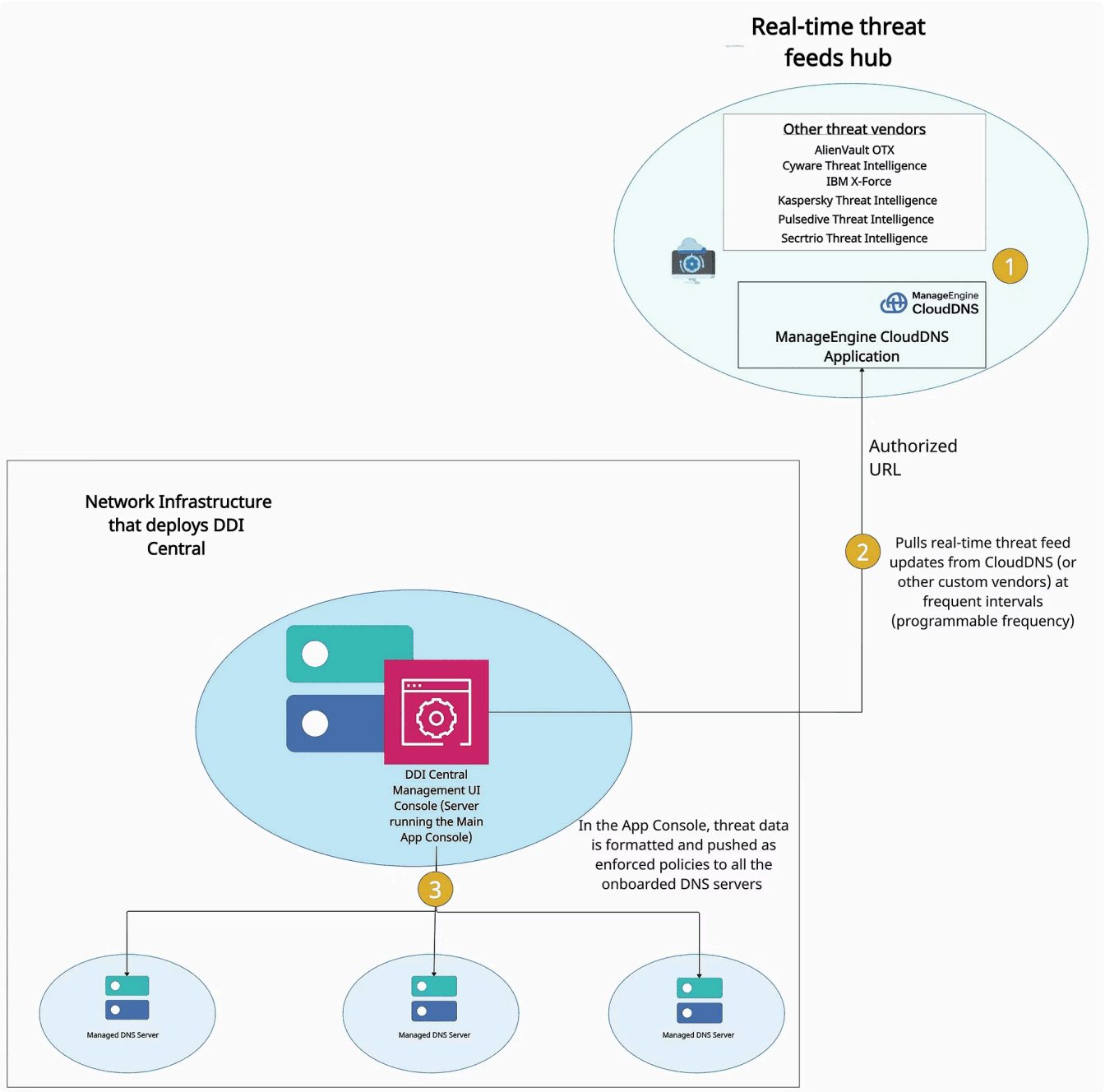
Anomaly Detection

Dual-layered detection using built-in rules and Zoho's Zia AI engine to identify DGA patterns and advanced threats in real time.

DNS Detection and Response

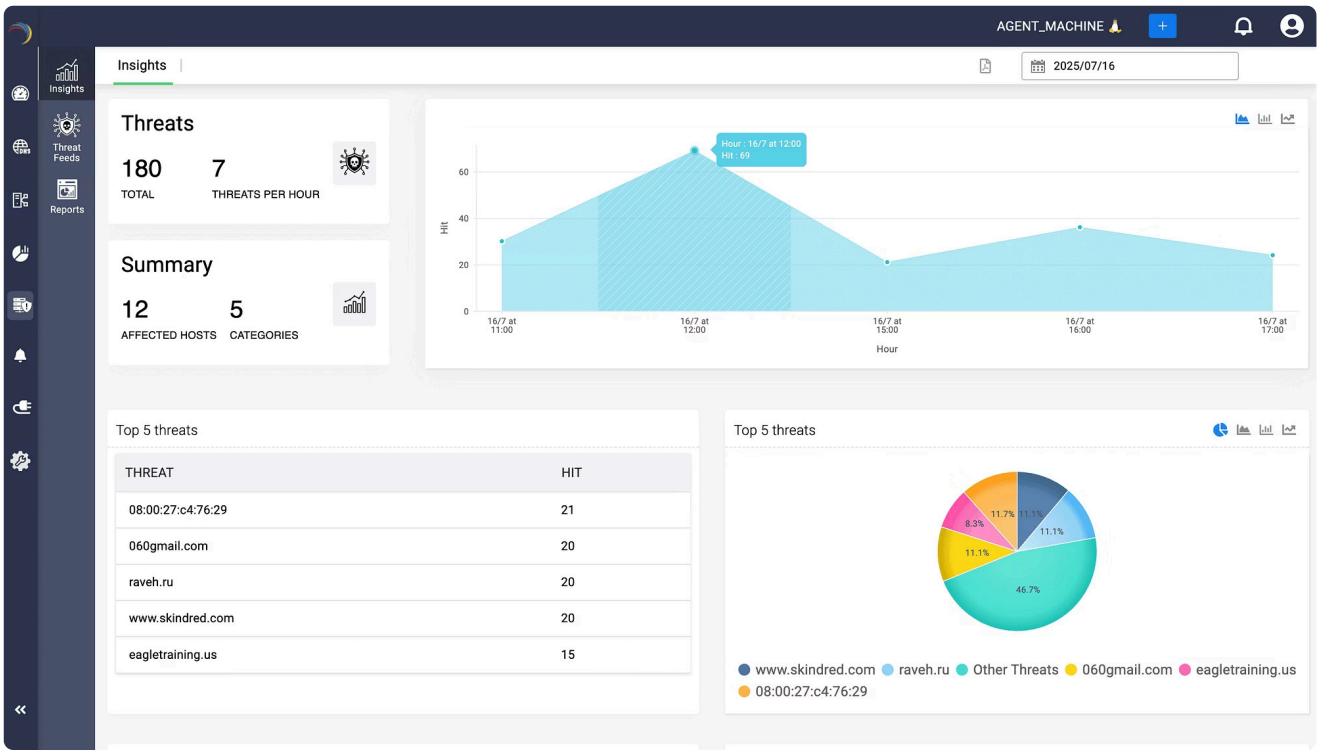
Continuous monitoring of DNS traffic and DHCP interactions with automated quarantine of compromised hosts and subnets.

DNS Threat Intelligence



Real-time threat feeds hub

DDI Central utilizes threat feeds from ManageEngine CloudDNS to implement DNS-level threat defense across all DNS servers within the network environment. These threat feeds are dynamically updated at regular intervals to ensure protection against emerging threats. Network administrators can view live threat feed data pulled from CloudDNS through a centralized dashboard, providing clear visibility and real-time summaries of DNS-based threats.



Supported Threat Intelligence Vendors

In addition, DDI Central supports the ingestion of live threat feeds from external vendors. The platform facilitates onboarding of threat intelligence from the following vendors:

- AlienVault OTX
- Cyware Threat Intelligence
- IBM X-Force
- Kaspersky Threat Intelligence
- PulseDive Threat Intelligence
- Sectrio Threat Intelligence

Standardized Feed Support

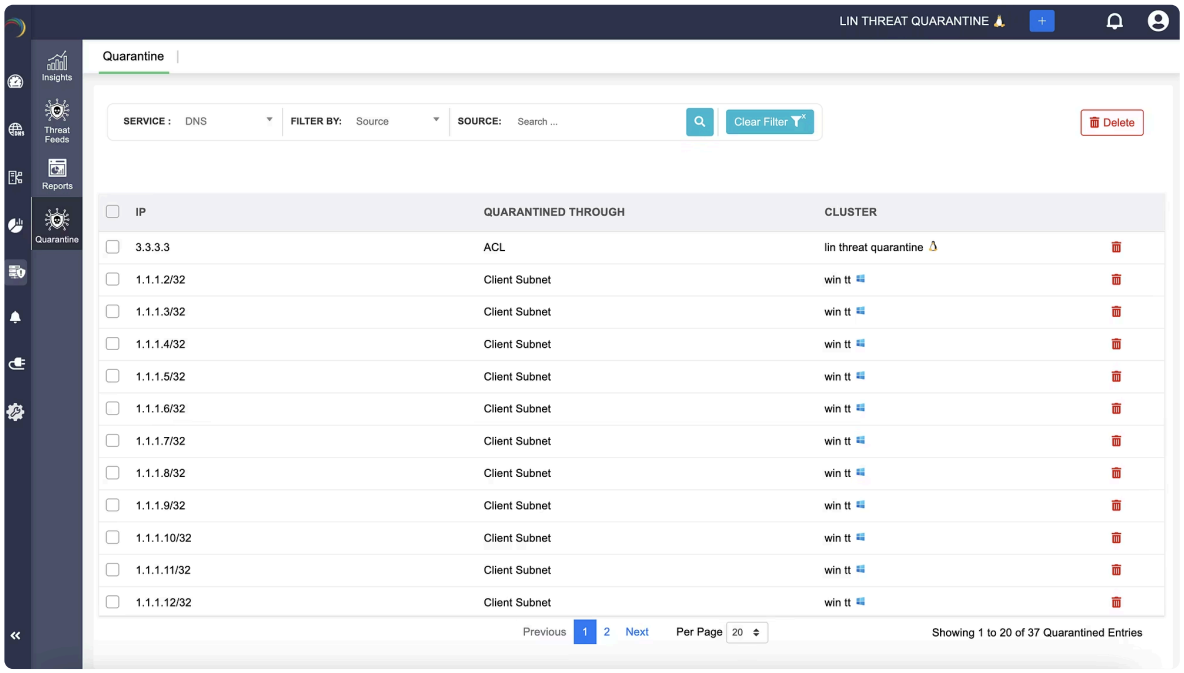
DDI Central also supports **Structured Threat Information Expression (STIX)** and **Trusted Automated eXchange of Indicator Information (TAXII)** servers for fetching standardized threat feeds.

Network administrators simply need to add the feed server details of their respective threat intelligence vendor within the application, or they can retain CloudDNS as the default threat source.

DDI Central automatically classifies and enforces policies on malicious domains based on a **confidence score**. Each threat entry is assigned a score derived from the vendor's advanced analytics and telemetry correlation. This confidence score reflects the likelihood that a domain is malicious.

All ingested threat feeds are automatically converted into **Response Policy Zone (RPZ)** or **access control list (ACL)** rules and pushed to all DNS servers, enabling them to take immediate action on malicious DNS requests.

DNS Detection and Response



DNS Detection and Response (DDR) in DDI Central continuously monitors DNS traffic and DHCP interactions across the network. It analyzes query patterns and flags suspicious behavior, such as an unusual volume of DNS requests originating from a specific IP address to domains listed in the active threat feed repository.

Upon detecting suspicious activity, DDR leverages predefined threat feeds and policy rules to automatically quarantine the compromised IP address or host using one of the configured response mechanisms:

ACL (DNS)

Blocks further DNS queries from the suspicious IP address directly at the DNS-server level.

Client Subnet (DNS)

Isolates the subnet generating the malicious DNS requests from the rest of the network, preventing lateral spread.

Host (DHCP)

Automatically isolates the compromised host by assigning it to a restrictive DHCP scope.

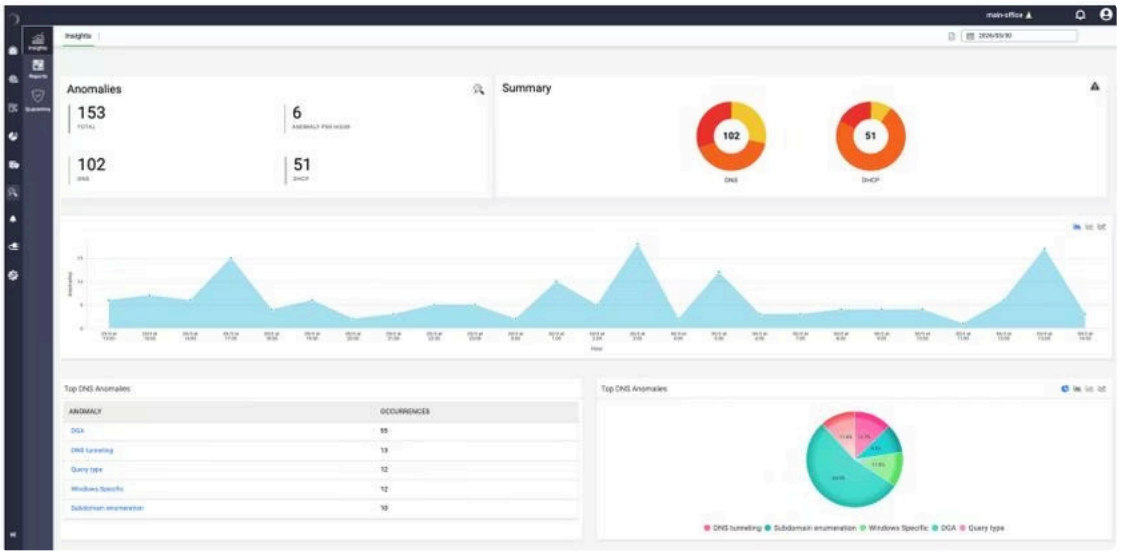
Filter (DHCP)

Completely blocks the compromised host from obtaining new DHCP leases through MAC-based filtering.

Administrators can easily identify which DNS Detection and Response (DDR) mechanism triggered the quarantine via the **Quarantine Dashboard**. The dashboard clearly displays the isolation method used, enabling precise diagnosis and streamlined remediation.

This intelligent and automated response framework empowers network administrators with rapid containment capabilities, significantly reducing risk, minimizing manual intervention, and improving overall network resilience.

Anomaly Detection



DDI Central's Anomaly Detection provides real-time identification of unusual DNS and DHCP behavior through a dual-layered approach:

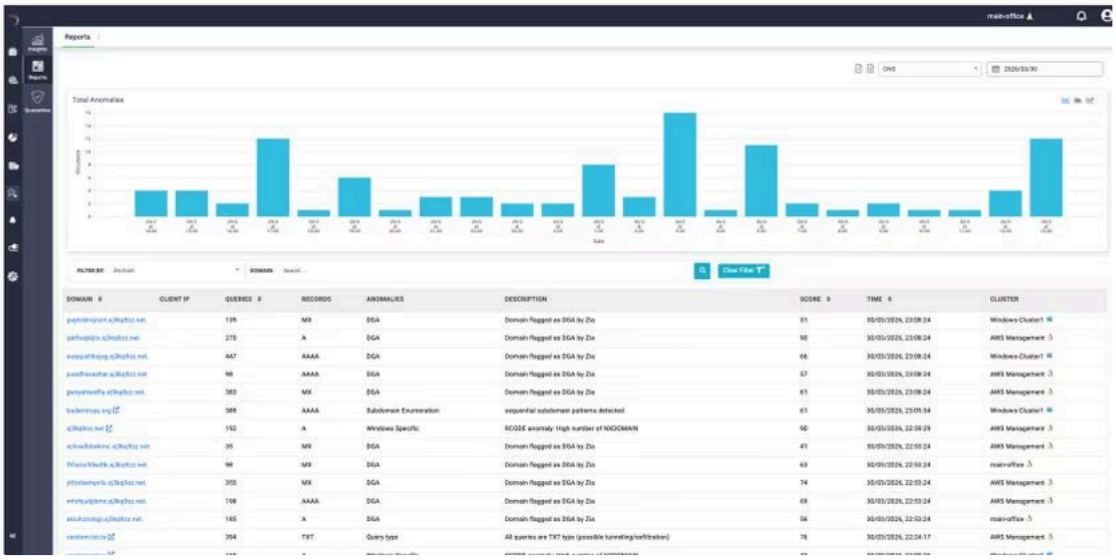
1 Built-in Detection Rules

A comprehensive library of built-in detection rules designed to identify known protocol-level anomalies.

2 Zoho's Zia AI Engine

Applies ML models to detect advanced threats such as Domain Generation Algorithm (DGA) patterns and other sophisticated attack techniques.

By associating behavioral patterns and traffic anomalies early in the attack life cycle, the engine enables timely containment and deeper analysis. This proactive detection model prevents the propagation of malicious activity within the network and ensures administrators can respond before service integrity or security is compromised.



Each detected anomaly is assigned a **severity score** to help security teams quickly assess its potential impact. DDI Central classifies anomalies into **four severity bands**, enabling administrators to prioritize investigations based on clear, quantifiable thresholds. This structured approach ensures that high-risk patterns stand out immediately, allowing for rapid validation and response.

Use Case: Detecting a Hidden DDoS Attack in an Enterprise Network

Let's take an IT organization that operates within a complex network environment consisting of multiple IoT devices such as CCTV cameras, routers, employee work devices (laptops and BYOD devices), and other connected systems. However, the organization lacks strong end-to-end visibility and centralized controls, making it difficult for network administrators to monitor all connected assets continuously.

In this scenario, a vulnerability in one of the outdated devices is exploited by an attacker. The compromised device begins communicating with a botnet infrastructure, receiving remote instructions from command-and-control servers. As a result, a distributed denial-of-service (DDoS) attack is silently initiated from within the network—without the awareness of the IT team.

Step-by-Step Response Walkthrough

1

DNS Threat Intelligence Detects Suspicious Activity

DNS threat intelligence in DDI Central detects suspicious activity when the compromised device starts sending frequent DNS queries to malicious or suspicious domains. The platform analyzes these DNS query requests against internal and external threat intelligence feeds.

2

Threat Classification

Upon matching the queried domain with known malicious indicators—based on confidence score and severity rating—the system classifies the activity as a verified threat.

3

Automated Containment via DDR

Immediately, the DDR mechanism initiates automated containment. The compromised device's IP address is quarantined before the attack can spread across other devices in the network. The client subnet and affected host are isolated from the rest of the environment, further DNS query requests are blocked, and the device is prevented from acquiring new DHCP leases to reconnect to the network.

4

Anomaly Detection Identifies Advanced Threats

At the same time, Anomaly Detection continuously monitors DNS and DHCP behavior in real time. If a device suddenly begins generating high-frequency DNS queries, resolving newly registered domains, the built-in detection rules instantly flag this behavior as abnormal.

5

Zia AI Catches DGA Patterns

Simultaneously, Zoho's Zia AI engine applies ML models to detect exhibiting DGA-like patterns and subtle behavioral deviations that may not match predefined threat signatures, ensuring advanced threats are identified at an early stage.

Through this multilayered and automated approach, DDI Central enables proactive detection, rapid containment, and effective mitigation of hidden threats within enterprise networks.

Conclusion

> Hidden threats in modern enterprise networks rarely announce themselves. They operate quietly within trusted services such as DNS and DHCP, blending into legitimate traffic before escalating into larger security incidents. In highly distributed and segmented environments, relying solely on traditional monitoring and manual troubleshooting is no longer sufficient.

By leveraging DDI Central's integrated threat intelligence, DDR, and AI-driven anomaly detection, organizations can transform their core network services into an active security layer. This approach enables the early identification of malicious domains, suspicious query behavior, and compromised hosts while automating containment through intelligent enforcement mechanisms.

With this unified and proactive strategy, DDI Central empowers organizations to stay ahead of evolving threats. As a result, your network becomes not only operationally efficient but **inherently proactive and defensively resilient**—capable of detecting hidden risks early and preventing them from disrupting business continuity.