DNSSight
with HYAS inside

USE CASE

Transforming Distributed Retail Networks with Centralised DNS Control

Enhancing Security, Efficiency, and Visibility across Branch Stores and Warehouses

BACKGROUND

A major retail chain, with dozens or even hundreds of physical locations spanning multiple regions, faces a mounting challenge: maintaining consistent network security standards across a diverse and distributed environment. Each store typically has its own networking stack—**routers, POS terminals, IoT sensors**—creating a complex web of devices and logs that are difficult to monitor centrally.

To complicate matters further, retail environments deal with large volumes of daily transactions, rely heavily on third-party vendors for services like payment processing, and are prime targets for cybercriminals hunting for customer data. Despite employing various security tools—firewalls, endpoint protection, and payment compliance solutions—**the retailer struggles to gain comprehensive visibility into DNS queries that could signal malicious activity.**

Enter DNSSight: a solution designed to bring **centralised DNS visibility and control to a geographically dispersed retail enterprise,** while aligning with compliance obligations and maintaining high availability for in-store operations.

CHALLENGE

DISTRIBUTED ARCHITECTURE

Complex Store Networks

Each store or warehouse often has its own local network, making it difficult to standardise DNS logging and threat detection.

High Device Diversity

From POS terminals and inventory scanners to security cameras and IoT sensors, a myriad of devices generates DNS requests.

LIMITED REAL-TIME VISIBILITY

Fragmented Logging

DNS queries might be partially captured by on-site systems, but these logs aren't always centralised or correlated with user or device data.

Manual Investigations

Suspicious queries require labour-intensive cross-referencing of firewall logs, DHCP records, and possibly third-party vendor reports.

HIGH-VALUE TARGET

Data-Rich Environment

Retailers process large volumes of customer information and payment data, making them prime targets for phishing, credential theft, or supply-chain attacks.

Compliance Pressures

Stringent data protection laws and PCI DSS guidelines mandate robust monitoring and alerting to protect sensitive financial information.

OPERATIONAL & COST CONSTRAINTS

No Downtime Tolerance

Retail outlets cannot afford network outages or performance bottlenecks that disrupt transactions.

Minimal On-Site Tech Resources

Staff in remote store locations may lack the expertise to manage complex, localised security solutions.

SOLUTION

DNSSight for Retail Networks

CENTRALISED DNS VISIBILITY

Unified Log Collection

DNSSight automatically gathers DNS logs from each store location and correlates them in real time with IAM Directory, and other relevant data.

Cloud or On-Premise

Depending on preference and compliance requirements, the retailer can deploy DNSSight in a central data centre or hybrid cloud, seamlessly pooling DNS traffic from all locations.

REAL-TIME THREAT DETECTION

Key Device Malware Alerts

Filtered suspicious or blocked domain query from key devices triggers an instant alert to SIEM. The SOC identifies the requesting device and user within seconds.

NX Domain & Anomalies

Short-lived, malicious domains—often used in phishing or command-and-control channels—are detected even if they don't fully resolve, drastically reducing attack dwell time.

LOW-IMPACT DEPLOYMENT

Agentless Architecture

DNSSight doesn't require installing software on every POS terminal or IoT device. Instead, it leverages existing DNS infrastructure and log sources without rearchitecting.

Scalable Management

New store locations can be quickly folded into the system by adjusting DNS logging configurations—no significant hardware or software upgrades needed.

ENHANCED OPERATIONAL EFFICIENCY

SIEM Integration

DNSSight's alerts and reports feed directly into the retailer's central SIEM or security dashboard, enabling seamless correlation with other threat intel and incident data.

Detailed Reporting

Management gains insights into the volume and type of DNS queries each store generates, highlighting potential vulnerabilities and improving threat-hunting efforts.

RESULTS

CONSISTENT NETWORK SECURITY

Multi-Site Standardisation

Regardless of location, each retail branch follows the same DNS monitoring and alerting processes, closing visibility gaps across the organisation.

Uniform Policy Enforcement

Centrally defined policies—like blacklists or whitelists—apply immediately to DNS traffic everywhere.

PROACTIVE THREAT DETECTION

Reduction in Manual Investigations

Automated, real-time correlation means security analysts no longer spend hours sifting through scattered store logs.

Faster Incident Response

SOC teams can zero in on compromised devices or users almost instantly, whether the threat surfaces in a flagship store or a remote branch.

OPTIMISED OPERATIONAL COSTS

Minimised Downtime

No sweeping network reconfigurations or constant manual interventions—the solution is designed for in-place integration.

Lower Resource Requirements

Centralised log collection and analysis reduce the need for IT staff at each branch, saving on labour costs.

COMPLIANCE & AUDIT READINESS

PCI DSS Alignment

Comprehensive logging of DNS queries helps the retailer demonstrate compliance by maintaining a clear record of all network activity around payment systems.

Easier Reporting

DNSSight’s dashboards and exports provide quick access to data required for internal and external audits, ensuring a smooth compliance process.

CONCLUSION

In a sector where **point-of-sale performance** and **customer trust** are paramount, DNSSight offers a non-disruptive path to **centralised DNS visibility** across widely distributed retail operations.

By unifying DNS data under one platform, it delivers:

- **Real-Time Alerting** on malicious or anomalous domain queries.
- **Streamlined Incident Response** that extends to every store and warehouse.
- **Robust Compliance** with industry regulations like PCI DSS.

For retail executives seeking to modernise security without introducing friction to daily operations, **DNSSight stands out as a strategic enabler—transforming a fragmented network into a cohesive, well-defended enterprise.**