DNSSight
with **HYAS** inside

USE CASE

Strengthening Financial Compliance and Security with DNSSight

Meeting PCI DSS, GDPR, and Long-Term Log Retention Requirements without Disrupting Operations

BACKGROUND

A large financial institution, operating under both **PCI DSS** (Payment Card Industry Data Security Standard) and **GDPR** (General Data Protection Regulation), faces heightened scrutiny over data protection and security practices. On top of these regulations, new guidelines—such as M-21-31—emphasise the importance of storing DNS logs for extended periods, often a year or more, to assist in investigations and maintain a strong incident response posture.

The institution already runs a multi-tiered security framework, featuring SIEM tools, firewalls, and endpoint protections. However, it has yet to find a non-disruptive way to:

- **Capture and retain** extensive DNS data for all internal queries.
- **Demonstrate compliance** with strict regulations on data logging and privacy.
- **Correlate high-volume DNS logs** with user and device details, enabling timely investigations.

CHALLENGE

REGULATORY PRESSURE

PCI DSS mandates secure handling and monitoring of payment-related data; DNS traffic can provide early indicators of compromise or unauthorised data transfers.

GDPR requires strict protection of personally identifiable information (PII). Any security breach can lead to severe penalties, especially if customer data is exposed.

M-21-31 & Extended Log Retention:
Recent guidance calls for retaining DNS logs for at least one year, introducing new storage and management demands.

VISIBILITY SHORTFALLS

Standard DNS solutions block suspicious domains but often do not show which user or device made the request.

Linking ephemeral IP addresses to specific systems (including IoT and legacy platforms) can be cumbersome, resulting in incomplete investigations.

DATA OVERLOAD & FRAGMENTATION

High transaction volumes typical in financial institutions generate vast amounts of DNS data every second.

Storing and making sense of this volume—especially under one-year retention guidelines—requires efficient indexing, correlation, and search capabilities.

OPERATIONAL COMPLEXITY

Traditional solutions may require overhauling DNS infrastructure or deploying agents on every endpoint—impractical for a global bank managing thousands of devices.

Any downtime or reconfiguration risk interrupting critical financial services, from card transactions to internal accounting.

SOLUTION

DNSSight for Compliance and Control

COMPREHENSIVE DNS LOGGING & RETENTION

Long-Term Storage

DNSSight automatically ingests DNS logs and securely stores them, meeting year-long (or longer) retention requirements without manual overhead.

Indexing & Search

A robust database structure supports quick lookups, allowing compliance teams to retrieve historical DNS records with minimal effort.

REAL-TIME CORRELATION & VISIBILITY

Unified Data Sources

DNS logs are enriched with IAM data in real time, pinpointing the exact user or device generating suspicious requests.

Full Coverage

By working at the network level, DNSSight monitors every DNS query—whether from on-site desktops, IoT systems, or remote employees.

REGULATORY ALIGNMENT

PCI DSS & GDPR

DNSSight's on-premise deployment ensures sensitive data remains within controlled environments, preserving privacy and integrity.

Incident & Forensic Readiness

Aligned with M-21-31, DNSSight's extended logging capacity ensures compliance teams can efficiently review DNS activity from months past, facilitating smoother audits and investigations.

SEAMLESS INTEGRATION

SIEM & Security Stack

DNSSight forwards critical DNS events to existing SIEM tools, enabling deeper correlation with other logs (firewall, endpoint, etc.).

Reduced Overhead

Deployed as a virtual machine, DNSSight requires no complex network redesign or agent installations—preserving day-to-day banking operations without disruption.

RESULTS

ENHANCED REGULATORY COMPLIANCE

Proof of Retention

The bank demonstrates to auditors and regulators that DNS logs are retained safely for a year or more, satisfying PCI DSS, GDPR, and new M-21-31 guidelines.

Audit-Ready Reports

Customisable dashboards and automated reporting reduce the burden of compliance documentation.

RAPID INCIDENT RESPONSE

Early Threat Detection

A single DNS query to a known malicious domain raises alerts, allowing security teams to isolate compromised systems before data loss occurs.

Accelerated Investigations

Analysts can quickly trace DNS queries back to the originating endpoint, dramatically reducing time spent correlating logs across multiple systems.

LOWER COSTS & STREAMLINED OPERATIONS

No Rip-and-Replace

DNSSight leverages the institution’s existing DNS structure and SIEM investments, minimising capital expenses.

Centralised Management

Fewer manual processes for collecting, storing, and searching DNS logs free up valuable staff time.

FUTURE-PROOF SECURITY STANCE

Adaptable Architecture

As regulations evolve or volumes of DNS traffic grow, DNSSight scales seamlessly without end-user disruption.

Unified Risk Visibility

Holistic insights into network behaviour help anticipate emerging threats and proactively address compliance requirements.

CONCLUSION

Financial institutions facing stringent data protection mandates and lengthy log-retention guidelines need a solution that delivers both **deep visibility and ease of compliance.**

DNSSight addresses these challenges by automatically collecting, correlating, and retaining DNS logs in an on-premise environment—ensuring alignment with PCI DSS, GDPR, and even evolving regulations like M-21-31.

By preserving critical DNS data for extended periods, DNSSight enables swift threat detection and thorough forensics without burdening the organisation with excessive storage or disruptive network changes.
The result is a future-ready, audit-friendly solution that protects sensitive financial data, fortifies regulatory compliance, and elevates overall security maturity.