DNSSight

DATASHEET

DNSSight: Empowering Secure, Hybrid and Non-Cloud Networks

A Seamless On-Premise DNS Visibility Solution for the Enterprise

Executive Overview

As organisations grow and evolve—whether through acquisitions, legacy infrastructures, or regulatory constraints—cloud-based solutions aren't always the ideal fit. DNSSight offers on-premise DNS visibility without forcing disruptive network overhauls or installing endless software agents. This single platform monitors, correlates, and enriches DNS data in real time, providing actionable insights for Security Operations Centres and maximising existing security investments.

The Visibility Gap in DNS

- Protective DNS solutions are essential; they block malicious queries effectively. But they often fail to identify which device or user initiated those queries without significant steps.
- Network Firewalls and URL Filtering struggle with off-network or inactive domains (e.g. phishing sites that are already down). Without DNS visibility, you never know who attempted a risky connection.
- Agent-Based Approaches create deployment headaches: legacy devices may be incompatible, IoT endpoints remain invisible, and constant updates consume resources.

Why On-Premise and Why Now?

- Non-Cloud & Hybrid Environments: Cloud inflation, data sovereignty, and compliance demands often push organisations to keep data and operations on site.
- Zero Disruption: DNSSight integrates seamlessly with existing DNS, DHCP, and authentication logs—no forklift upgrades or network remapping.
- Comprehensive Coverage: By staying inside your network, DNSSight sees all DNS queries, including IoT devices, offline malicious domains, and VPN clients.

Four Critical Use Cases

1. Pinpointing Attack Sources

Protective DNS might block DNS tunnelling attacks, but which machine is infected? DNSSight shows you in seconds, eliminating guesswork and manual correlation.

2. Catching NX Domain Threats

Up to 80% of malicious domains are already down when queried—no HTTP/S traffic ever occurs. DNSSight intercepts these invisible NX Domain requests, swiftly linking them to specific devices or users.

3. Advanced Anomaly Detection

If a crucial server requests unfamiliar domains—breaking its usual pattern—DNSSight flags the irregularity and notifies your SOC. You discover threats before they escalate (Example: SolarWinds-style compromises).

4. Access Guard for Comparative Analysis

DNSSight can query multiple protective DNS databases in parallel, letting you compare results from different solutions. You gain data-driven insights on which security tools perform best in your environment—no guesswork.

Business and Security Benefits

- Immediate ROI: No expensive rebuilds or disruptions—just a virtual machine that correlates DNS logs in real time.
- Universality: Every device (IoT, mobile, legacy) is covered. No agent needed.
- Reduced SOC Workload: Alerts flow directly into SIEM systems, so analysts swiftly identify threats without sifting through disjointed logs.
- Regulatory Alignment: On-premise deployment ensures total ownership of data, ideal for industries with strict compliance demands.
- Future-Proof: As your network evolves, DNSSight scales effortlessly, keeping pace with new devices, branches, and infrastructure changes.

Aspect	Agent-Based DNS Security	DNSSight (Agentless)
Deployment Complexity	High overhead for large organisations where thousands of endpoints must be configured individually. Must account for diverse OS versions and legacy systems.	Centrally deployed on a virtual machine, with no need to install or manage agents on endpoints. Quickly scales without rewriting or replacing existing infrastructure.
IoT & Legacy Support	Often incompatible with legacy operating systems, IoT devices, and specialised hardware. Leaves critical non-standard devices unprotected.	Monitors DNS traffic from all devices on the network without requiring OS-level support. Captures data from traditional endpoints as well as specialised or legacy systems.
Maintenance & Updates	Requires frequent version updates on each endpoint. Can cause downtime or interruption during rollouts, especially in sensitive operations (e.g., ambulances).	Updates and maintenance apply only to the centralised platform, not individual machines. Virtually no endpoint downtime or manual patching needed.
Operational Disruption	Agent conflicts, performance overhead, and user interruptions are common. Requires more extensive approval and change-control processes to meet enterprise policies.	Invisible to end users; no performance penalties on individual devices. Minimal disruption and lower bureaucratic overhead for deployment.
VPN & Remote Users	DNS agents are often overwritten or bypassed by existing VPN clients, weakening visibility. Requires extra configuration to maintain consistent coverage.	Integrates directly with firewalls and VPN solutions to ensure DNS traffic (including remote queries) is fully monitored and correlated, without additional endpoint software.
Visibility & Context	Captures limited data if traffic never reaches a higher-level protocol (e.g., an offline malicious domain).Correlation with DHCP and AD logs is typically manual.	Automates correlation among DNS, DHCP, and AD logs in real time, pinpointing specific users and devices behind each query—even if the domain is offline.
Log Retention Compliance (M-21-31)	Manual and inconsistent long-term storage of logs; often lacks structure, retention planning. or archival accessibility.	Supports M-21-31 directives with configurable log retention: 12 months live access + 18 months archive. Enables retrospective investigations with searchable correlated DNS/DHCP/AD records.

Conclusion

DNSSight brings clarity to the often-overlooked DNS layer, turning every blocked domain and NX response into an actionable data point—without complex network upgrades or agent sprawl. For large, hybrid, and on-premise environments seeking robust threat detection, DNSSight is the streamlined, cost-effective solution that boosts your existing security stack and delivers immediate, tangible value.