DNSSight
with HYAS inside

USE CASE

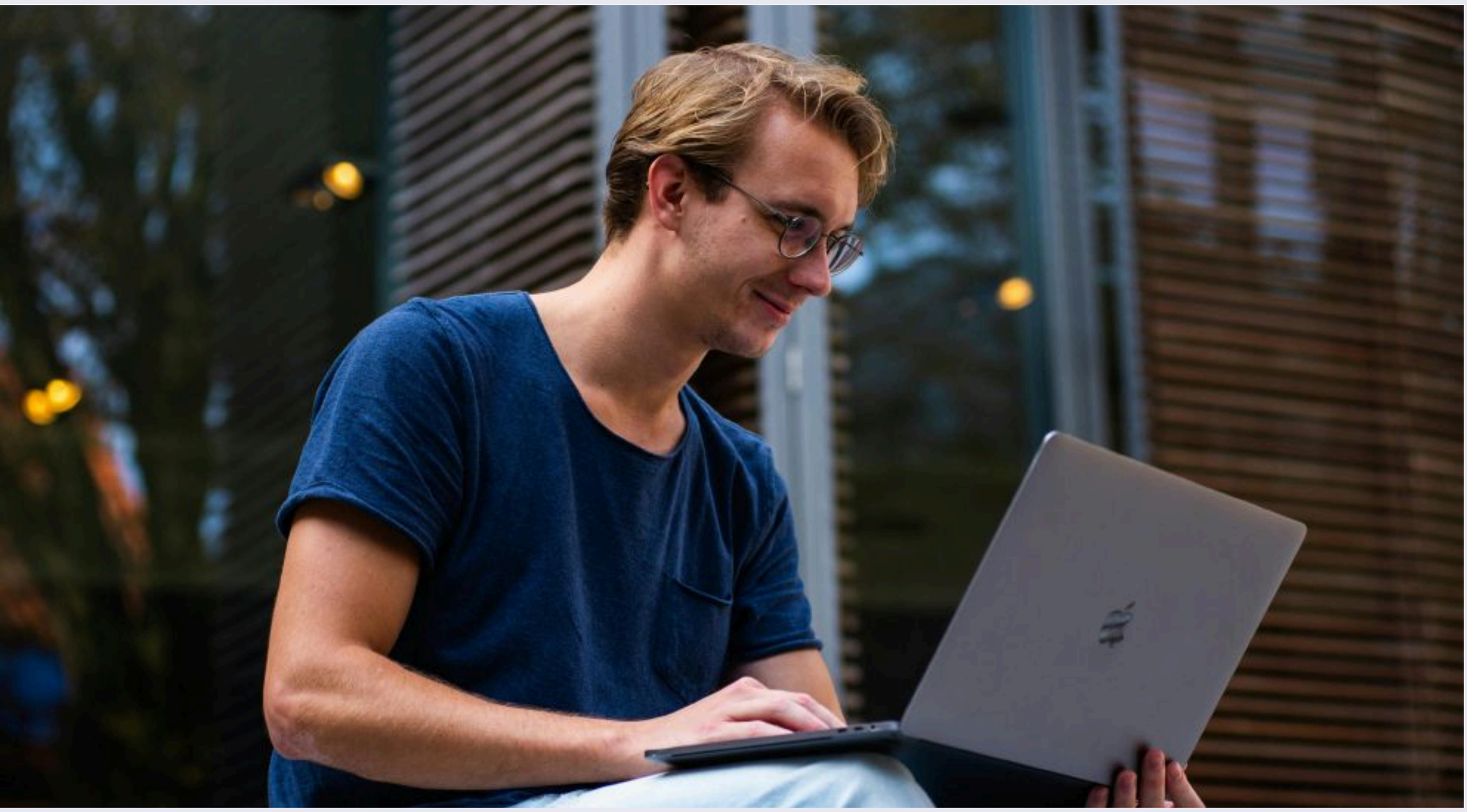
Gaining Visibility Behind the VPN

Empowering Remote Workforces Without Losing Control Over DNS Security

BACKGROUND

A global consulting firm boasts a highly mobile workforce spread across multiple continents. Employees regularly connect to the corporate network via virtual private network (VPN) clients, ensuring confidentiality for sensitive projects.

However, this arrangement introduces a challenge: once employees are **behind the VPN**, traditional DNS monitoring solutions often fail to identify the specific device or user generating suspicious DNS queries.



The firm’s security and IT teams already use a robust firewall, a SIEM platform, and endpoint antivirus solutions. Yet correlating DNS queries with individual remote devices remains a time-consuming puzzle, particularly when IP addresses are dynamically assigned by the VPN. They need a way to maintain unified oversight, even as employees hop between on-site and remote environments.

DNSSight provides a game-changing layer of DNS visibility that extends behind the VPN, allowing the security team to pinpoint potential threats to any remote or roaming endpoint, all without overhauling the existing infrastructure.

CHALLENGE

LIMITED REMOTE VISIBILITY

Dynamic IP Assignment

Remote endpoints receive ephemeral IPs from the VPN, complicating attempts to trace malicious DNS queries back to specific machines.

Fragmented Logs

Traditional DNS logs show only inbound or outbound connections at the gateway, failing to link suspicious queries with the device or user behind them.

COMPLEX INFRASTRUCTURE

Diverse Endpoints

Laptops, mobile devices, and specialised contractor machines span different OS versions, making uniform agent deployment or software installs problematic.

Existing Tools

An investment in firewalls, SIEM, and endpoint security needs to be preserved—another “rip and replace” solution isn’t feasible or cost-effective.

OPERATIONAL DISRUPTION RISKS

Zero Tolerance for Downtime

Consultants rely on seamless connectivity to client sites and internal resources; any network disruptions harm productivity and customer trust.

Security vs. Accessibility

Overly strict measures could block legitimate traffic or hamper the user experience, reducing compliance and fuelling workarounds.

SOLUTION

DNSSight for Comprehensive VPN Visibility

FULL DNS CORRELATION

VPN-Aware Insight

DNSSight integrates with VPN-compatible firewalls, capturing DNS requests passing through the tunnel and automatically linking them to user credentials or machine details in real time.

Agentless Monitoring

No need to deploy additional software on every device—DNSSight leverages existing IAM, and DNS logs to match the query to the correct endpoint.

END-TO-END THREAT DETECTION

Malicious Domain Alerts

Short-lived or suspicious domains commonly used by attackers are flagged instantly, whether the user is working from the office, home, or a remote client site.

NX Domain Tracking

Even if a malicious domain is offline, DNSSight still captures and highlights the attempt, ensuring no hidden threats escape notice.

OPERATIONAL EFFICIENCY

Seamless SIEM Integration

Enriched DNS data flows into the organisation's SIEM, enabling swift correlation with other alerts (firewall, endpoint, or user activity).

Minimal Network Impact

Deployable on a virtual machine without reconfiguring the entire VPN or network topology, preserving uptime for mission-critical tasks.

RESULTS

ENHANCED REMOTE SECURITY

Pinpoint Attribution

Security analysts can instantly see which remote device generated a suspicious DNS query, speeding up incident triage and containment.

Proactive Defence

With continuous DNS visibility behind the VPN, emerging threats—like newly spun-up phishing domains—are caught before they propagate across the network.

STRONGER ROI ON EXISTING TOOLS

SIEM & Firewall Synergy

DNSSight boosts the effectiveness of the firm's firewall and SIEM investments, delivering detailed and actionable DNS insights to existing dashboards.

No Major Upgrades

Avoid expensive hardware or forced migrations, letting IT teams focus on strategic improvements instead of operational firefighting.

STREAMLINED INCIDENT RESPONSE

Faster Investigations

Automated correlation ensures that once a malicious domain is flagged, the investigating team sees immediately who attempted the connection and when.

Reduced Alert Fatigue

Intelligent filtering cuts down extraneous logs, ensuring each alert that hits the SOC is rich with context and ripe for immediate action.

OPTIMISED USER EXPERIENCE

No Intrusive Agents

Users remain productive without extra software or repeated updates.

Consistent Connectivity

Consultants keep the frictionless VPN access they need to serve clients around the globe, with no loss of security oversight.

CONCLUSION

In an era when remote work and global collaboration have become core pillars of enterprise operations, retaining robust DNS visibility behind the VPN is vital. DNSSight ensures that every query—whether from the corporate office or a home-based consultant—gets captured, correlated, and analysed in real time.

For security teams grappling with dynamic IP addresses, limited insight into remote user activity, and a patchwork of endpoint devices, DNSSight offers peace of mind.

By extending **DNS visibility behind the VPN, the firm gains unified oversight, swift incident response, and a better return on their existing security investments,** all while delivering the uninterrupted connectivity that staff and clients demand.