

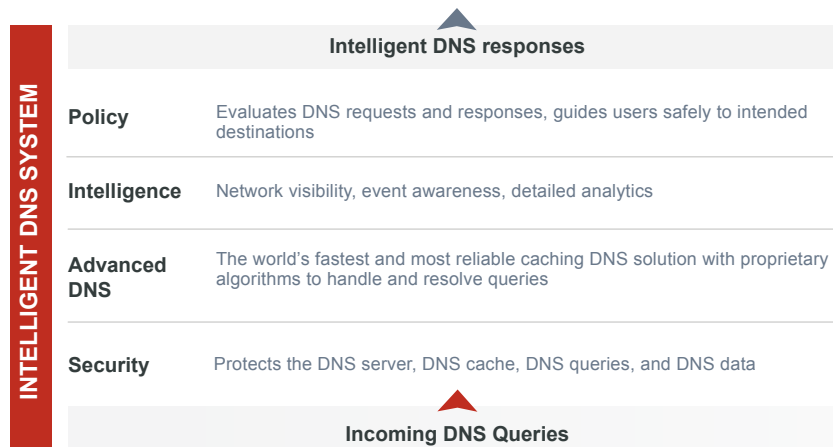
Vantio™ Intelligent DNS System

THE FOUNDATION FOR A BETTER INTERNET

The Domain Name System (DNS) plays a central role in every IP and has a major impact on the end user's Internet experience. Caching DNS is the first IP service Internet users touch when they browse the Web, watch a video, send an email, or make an IP phone call. If the DNS goes down, the Internet goes down. If the DNS is slow, end-users perceive the "network" as slow. If the DNS is compromised, anyone can be silently redirected to an attacker's site and have their identity stolen or worse.

The **Vantio** Intelligent DNS System is an In-Network, software-only, solution that provides a faster, safer more useful Internet experience for more than 500 million fixed and mobile broadband users around the world. The system architecture features a unique policy layer for service creation to enhance Internet navigation, protect networks from botnets and other forms of malware, and more. Embedded intelligence adds a level of event awareness and network visibility that has never been available before. Additionally, Vantio offers complete remote monitoring and online diagnostics.

Vantio security defenses remain unmatched in the industry, maximizing protection against cache poisoning attacks that can expose end users to identity theft and fraud. Robust DNSSEC and **Nominum's** proprietary DNSAUTH provide cryptographic protection for DNS data. Advanced query processing algorithms yield the industry's highest performance and lowest latency and deliver attack dampening features to provide extraordinary resilience to DDoS events. Because it runs on open hardware and operating systems Vantio can easily be deployed on existing hardware with no changes to the network architecture.



Advanced Query Processing

The core Vantio caching engine is completely optimized and delivers far better caching performance, and operational data than any alternative solution. Nominum developed two entirely independent solutions for caching (Vantio) and authoritative (ANSP) DNS functions. By focusing Vantio exclusively on the caching function in the product design, Nominum was able to achieve levels of performance and scalability not possible in dual-purpose name servers.

KEY FEATURES

- Special purpose, software-only recursive DNS server
- Advanced query handling for proven performance and headroom
- Attack dampening and on-the-fly configuration for ZERO downtime
- Layered defense mechanism to defend against cache poisoning
- Full DNSSEC support with optional DNSAUTH to secure DNS communication links
- Full IPv4/IPv6 support
- Advanced architecture to support policy layer for service creation
- Dynamic priority assignment— in-line priority determination among policy modules
- Intelligence layer for remote monitoring, on-line diagnostics, and dynamic improvement
- Full network visibility and event awareness
- Support for multiple OS and hardware platforms

Numerous memory management, cache management, and query management techniques enable this superior performance:

- Vantio stores DNS responses in efficient data structures to enable the fastest possible look-ups regardless of the cache size
- Special algorithms identify and prefer the fastest responding authoritative servers
- Vantio makes maximum use of idle time (the time spent waiting for incoming queries or replies from authoritative servers)
- Cache entries that are about to expire can be pre-fetched (the pre-fetch timer is settable)
- Incoming queries are pooled if multiple requests for same domain arrive in succession only one authoritative query is sent, eliminating redundant queries
- When memory usage starts to reach predefined thresholds, Vantio removes the least recently used data from cache
- Memory allocations for caching and recursion contexts are settable, in systems with a lot of memory the size of the cache can be increased

Collectively these optimizations improve the cache hit rate, which increases responsiveness to end user queries and results in fewer recursion contexts which greatly improves the resiliency of the server and reduces the load on other network elements.

Beyond performance, addressing latency provides an immediate and noticeable impact on the speed of the Internet, or more aptly described as the user's connection to the Internet. As latency increases, so does the time it takes for users to receive a requested web page or complete the process of sending an email. To achieve these latency improvements, Nominum regularly assesses Round-Trip-Time (RTT) for servers and chooses the fastest one for resolving queries. There is also a configurable pre-fetching process that greatly reduces the time to resolve a query via a proactive process for keeping the cache populated with current information prior to a customer query forcing the recursive process.

Embedded Intelligence for Network Visibility

Leveraging the high performance design of the underlying caching engine, Vantio has advanced capabilities that provide network visibility and event awareness. Extremely fine-grained DNS query data can either be collected for offline analysis or analyzed in real time. An extremely powerful built-in analysis tool provides facilities to examine query data to identify security threats such as bot activity on the network, or to accurately characterize subscriber and application performance trends. No other DNS server has similar capabilities.

Alerting, Thresholding, and Advanced Anomaly Detection

Awareness of network events is greatly enhanced with Vantio advanced anomaly detection capabilities that use the extensive event and network-level information gathered by Vantio. This allows for tight monitoring of the DNS with immediate alerts when there are major changes in network behavior. For example, malicious activity from hackers such as the onslaught of a DDoS attack can be recognized and signaled instantly. At the same time valuable or sensitive network resources like Web sites or mail servers can be closely monitored and when activity levels exceed or drop below normal operating ranges network staff can be proactively alerted to the change. This is not possible to do with other caching DNS servers.

NETWORK OWNER BENEFITS

- Fastest and most stable Internet experience
- Flexibility to choose the hardware and OS for your network
- Market-leading solution that is in production at 140+ top ISPs worldwide
- Full network and end-user security against all known DNS attacks
- Real ROI—lower opex, decreased capex, no architectural changes
- Platform for service creation—Network Protection, Navigation Assistance, etc.
- Industry-relevant innovations designed for owners of large networks
- Event awareness—real-time alerts to network owners and administrators
- Network visibility—full-featured real-time reporting of DNS traffic and trends
- No network upgrade required to support DNSSEC and other advanced protocols

Policy Layer for Service Creation

Vantio was specifically designed to accommodate policy software modules, deployed individually or together, that allow network owners to offer new services quickly and easily. The optional software modules evaluate incoming DNS requests in real time and enforce policies to enhance Internet navigation or improve network security. Extensive policy controls allow network owners to define services tailored to their specific end user, network, market, and operational requirements. All policy software is completely integrated in the Vantio Intelligent DNS System, and as such, there is no need to add new equipment to the network or change the network architecture in any way.

Dynamic Priority Assignment

The value of Intelligent DNS Systems is being proven in networks every day and network owners are taking advantage of multiple policy modules. Dynamic Priority Assignment (DPA) makes certain that when multiple policies are applied to a DNS query they are always evaluated in the most optimal order.

As the network environment continually changes, DPA automatically updates the order in which policies are applied. For example, when Vantio is updated with a non-existent domain (NXD) that was determined to be malicious, the order in which policies are evaluated is changed on the fly. Security policies are evaluated before Navigation Assistance policies to make optimal use of server resources and ensure networks and end users are always protected.

DPA also lets network owners efficiently and optimally run the caching DNS service, provide network visibility and event awareness, and offer advanced anomaly detection, simultaneously on the same server. In the case of multiple servers, the technology allows for balancing processes across multiple cores. Even with intensive data gathering and analysis operations the industry-leading performance of the essential caching DNS service is maintained.

Layered Security Defenses

Vantio layered security defenses offer the best protection available against DNS cache poisoning and completely deter the exploit discovered by security researcher Dan Kaminsky. No other vendor offers all of these critical layers of protection.

- The Deterrence Layer includes Nominum's industry-leading UDP Source Port Randomization implementation and domain case randomization (0x20) to make it harder for attackers to correctly guess query parameters.
- The Defense Layer detects spoofing attempts and re-queries Authoritative servers over a secure connection (TCP), greatly slowing the progress of an attack (by 100 times or more)
- The Resistance Layer employs Glue Segregation and Query Response Screening to ensure that certain data in DNS query responses is not cached.
- Finally, the Remediation Layer sends alerts when an attack is underway and records parameters associated with the attack.

Robust DNSSEC

DNSSEC is the industry standard for using cryptography to secure data published in the DNS. Nominum engineers have tremendous depth of experience with DNSSEC, having participated in the definition of the original protocol specification more than a decade ago. Nominum's DNSSEC implementation integrates and automates all of the functions and processes needed for deployment. This eliminates operational overhead and more importantly the risk associated with deploying DNSSEC.

END USER BENEFITS

- Always available, fastest Internet experience
- Freedom from site spoofing and identity theft (i.e. No cache poisoning)
- More value to existing Internet service
- Applications work as optimally intended (i.e. DNS not a bottleneck)
- Support for next generation applications (IPv6, DNSSEC, etc.)
- Additional, integrated service offerings from your ISP

DNSAUTH

DNSAUTH is a protocol developed by Nominum for securing DNS data links while maximizing compatibility with existing DNS infrastructure. It extends Nominum's layered defenses by securing communication links between Vantio caching servers and Nominum authoritative servers (ANS and ANSP). DNSAUTH authenticates authoritative servers and optionally encrypts DNS responses in transit between caching and authoritative servers. Cryptographic protection of DNS links introduced with DNSAUTH makes it statistically impossible for an attacker to compromise DNS data. It is fully compatible with DNSSEC.

Attack Dampening

Vantio is far more resilient to extreme query loads – such as DDoS attacks. Efficient design (discussed above) ensures Vantio uses far fewer resources to process queries, allowing it to withstand higher query volumes than any other server on the market. Vantio also will not exceed its maximum memory, which is one of the main reasons other caching servers fail under attacks. Instead, Vantio remains responsive under attack or other load conditions, serving legitimate queries, and providing the ability to take the actions necessary to deflect the attack or otherwise manage the event.

A rate limiting feature establishes a global threshold that limits incoming queries from individual clients (an exclusion list allows specified devices to be exempted from the threshold), shielding the server from abuse. Vantio also manages outbound connections to authoritative servers so that it is not possible to DoS with barrages of recursive queries.

In-Network and Off-Network Services

Best practices for caching DNS deployment call for in-network DNS supplemented with Off-Network hosted services. Vantio In-Network services along with SKYESM Resolution hosted services improve system diversity, resilience, and availability, and deliver on-demand capacity to meet peak loads with high performance. Vantio is the only In-Network caching DNS solution that is seamlessly integrated with hosted network services which are based on the same underlying software technology.