VANTIO™ CACHESERVE

Deliver fast, reliable and secure Internet with the DNS leader

For more than 15 years, Vantio CacheServe has offered exceptional availability, extraordinary stability, and superior security. CacheServe technology maximizes the power of server hardware and is consistently ahead of alternatives with numerous innovations that make networks more responsive, and less costly to operate:

- A comprehensive policy framework enables granular control over query traffic for security and services
- Embedded features enable efficient capture, filtering, and offload of DNS data for use by reporting, planning, and big data systems
- Integration with N2 Platform enables value added services, and management of DNS data and policies at massive scale
- Resolution enhancements optimize interactions with DNS clients and authoritative DNS servers to maximize the subscriber experience

Coupled with responsive 24x7 commercial support, staffed with experts steeped in provider requirements, networks built with CacheServe always deliver the quality Internet experience subscribers demand. Hundreds of millions of internet users in over 40 countries rely on it every day for fast, reliable and safe internet access.

Sizzling performance and rock solid stability reduce costs and deliver a superior subscriber experience

A single CacheServe 7 instance running on commodity hardware can answer more than 2.5 million queries per second. This supports business imperatives to reduce costs through server consolidation and simpler operations. Overall cost reductions (CAPEX and OPEX) of nearly 40% can be obtained in centralized topologies. OPEX reductions are even more compelling. Benchmarks comparing rack/power/cooling and management costs show savings of more than 50% with centralized POPs and more than 35% for distributed POPs. Low latency query responses deliver the best possible subscriber experience.

For over a decade, Vantio CacheServe has formed the foundation for the world's fastest and most reliable Internet networks by enabling self-defending DNS infrastructure that shields networks and subscribers from cyberthreats.

KEY HIGHLIGHTS

- Leading performance, low latency DNS resolution
- Unique cache poisoning defenses
- Policy framework for fine-grained control over query traffic
- Real time system and operational data in easy to read reports
- Efficient collection of DNS data

Scalable data management

CacheServe is integrated with the N2 Platform data architecture which offers:

- Real-time access to detailed DNS query and other telemetry data to enable richer Network View reporting (shown below)
- Resilience through failures to provide non-stop availability to power a non-stop customer experience
- Optional connectors to open Big Data systems (Splunk, Hadoop) or purpose-built applications, to create additional operational, security and business insights

The same data architecture is used by all N2 Platform components. It's based on open solutions that have been proven in the world's largest networks, delivering operational excellence at web scale and speed.

Rich telemetry empowers operations

CacheServe streams detailed telemetry data for reporting or use by other operational systems. Data is divided into component streams, with hundreds of metrics covering all aspects of query activity and system state. Because the data is streamed using an open platform (described above) it's simple to integrate into open analytics and visualization tools. Nominum customers are using open solutions like Grafana and Kibana for very low cost, small footprint, monitoring integrations. When their operational requirements change, or new data is added to telemetry streams, it is easy to upgrade dashboards to incorporate it.

Integrated N2 applications

Nominum N2 applications are fully integrated with CacheServe so it's easy for providers to quickly and easily offer security services purpose built for businesses and consumers. A companion messaging application can be used to notify subscribers of security issues, and extended to a broad range of communications use cases such as late bill pay, service upgrades and offers, and notifications of network status or changes.

N2 Secure Consumer protects all connected devices in the home from phishing, ransomware, and malware. Households can also define filters to block inappropriate content, for peace of mind and a more satisfying digital lifestyle.

N2 Secure Business is a SECurity as a Service (SECaaS) offering that protects businesses from ransomware, phishing, botnets and zero-day malware attacks.

N2 Reach provides in-browser messaging, a powerful communication channel that boasts far greater engagement and conversion rates than email or direct mail.

Precision Policies protect networks

Precision Policies enable value added services and protect networks from abusive queries while protecting legitimate traffic. Fine grained policies (all the way down to the individual device level) precisely target unwanted traffic and ensure good queries are always answered. Policy triggers operate on incoming queries or outgoing answers for comprehensive coverage. Software designed for extremely high performance means providers get sophisticated policies, massive capacity, and low latency. Other solutions impair resolver performance, miss unwanted traffic, and cause collateral damage by over-filtering queries and disrupting the subscriber experience.

Today, hundreds of millions of internet users in over 40 countries rely on CacheServe daily for fast, reliable internet.

It's simple to upgrade CacheServe to ThreatAvert which integrates Global Intelligence Xchange (GIX) dynamic threat feeds. GIX is based on streaming threat intelligence gathered by Nominum security research experts who analyze over 100 billion DNS queries every day, live streamed from provider networks worldwide. The combination of GIX and Precision Policies delivers automated, agile, and adaptive defenses against highly dynamic DNS based DDoS attacks, and identifies subscriber devices infected with bots.

Leading DNS cache poisoning defenses protect subscribers

Cache poisoning defenses remain the most effective in the industry. Vantio stood up against Kaminsky's infamous attack that compromised other resolvers in minutes. Nominum shipped defenses for the new cache poisoning vulnerability announced by JPRS (JPCERT-AT-2014-0016) months before details were disclosed.

Data-driven operational insights

Extensive reporting capabilities offer statistics and system data for instant verification that servers are operating within normal ranges, and to anticipate capacity requirements. If unusual activity appears on a graph, operators can easily drill down to identify the cause. Using Network View, they can see the top domains or clients responsible for a traffic spike, the clusters or servers involved and the

CacheServe reports use real time telemetry to display high level operating status. Detailed data is a click away.
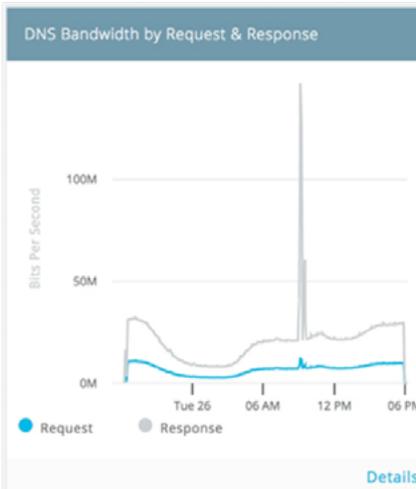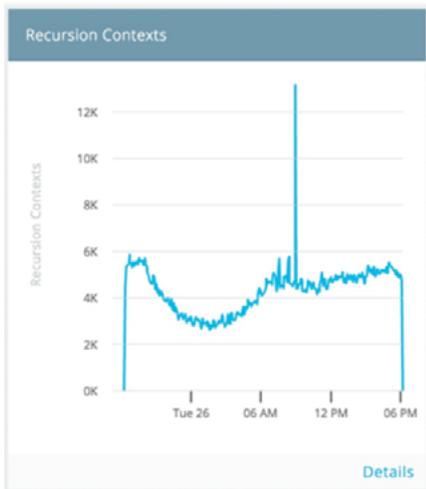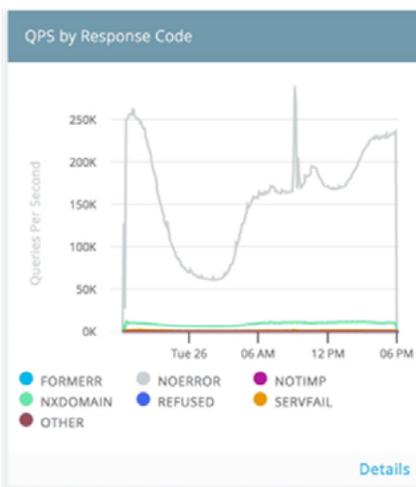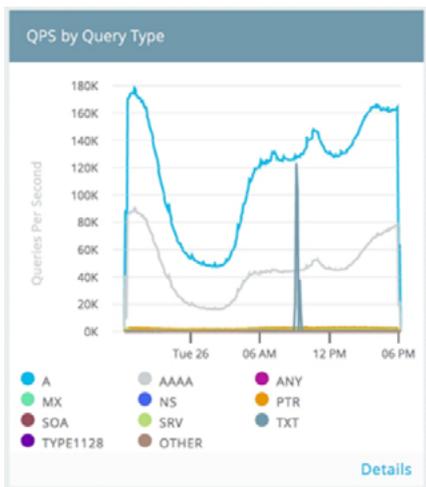
CacheServe reports provide valuable trend and network data.

relationship between different statistics and metrics being displayed. For forensic use, query analytics tools such as built in nom-kafka-search provide the ability to search, filter, group and post process the stored DNS logs for low level, detailed access to the entire query stream.

Custom dashboards and reports can be created, organized, and formatted to reflect operator priorities and requirements. Tag based reports enable user defined views of - DNS servers - fixed/mobile, city/region, IPv4/IPv6 - to better match network topologies, access technology, or other internal processes/workflows/tools. These capabilities simplify navigation and analysis in complex networks. All types of reports can be scheduled and mailed to stakeholders.

Improved availability of authoritative servers under adverse conditions

DDoS attacks targeting DNS nameservers have been some of the most powerful ever recorded and attackers continue to innovate. When authoritative DNS servers become unavailable the web resources they serve also become unavailable. CacheServe prefetch features allow cached records for popular web resources to be retained when authoritative servers are unavailable, and automatically refreshed when authorities come back online. Other enhancements allow preferential access to recursive queues under heavy load conditions for a list of "good" domains configured by the operator.

Success Based Rate Limiting reduces stress on Authoritative Servers under attack by dynamically rate limiting recursive queries when NXD responses reach a threshold value. Traffic can be rate limited at both the nameserver and domain level so only traffic to names that are under attack can be rate limited, while other traffic is managed normally.

Content-aware DNS resolution

For service providers that are considering deployment of distributed Content Delivery Network (CDN) caches across their networks, EDNS0 client subnet (ECS), a draft RFC, can potentially improve the alignment of content sources with preferred network capacity to reduce transit path costs. Equivalence class, a unique CacheServe feature incorporates the respective provider and CDN network topologies to substantially reduce the load on resolvers (cached entries) that would otherwise be introduced with ECS.

ABOUT NOMINUM

Nominum, now part of Akamai, provides an integrated suite of carrier-grade DNS-based cloud solutions that enable fixed and mobile operators to enhance and protect their networks, strengthen security for consumers and business subscribers, and offer innovative value-added services. The result is improved service agility, increased revenue, greater brand loyalty and a strong competitive advantage. More than 130 providers in over 40 countries use Nominum software.

CORPORATE HEADQUARTERS

Nominum, Inc.
800 Bridge Parkway, Suite 100
Redwood City, CA 94065

+1 (650) 381-6000

hello@nominum.com