

Case Study

CUSTOMER PROFILE

COLT is an award winning provider of data, voice and managed services to major businesses, SMEs and wholesale customers across Europe.

BUSINESS SITUATION

- Highly reliable, extremely low latency pan-European IP Backbone
- DNS infrastructure based on Nominum
- Regulatory changes mandated blocking child sexual exploitation content and illegal gambling sites

SOLUTION

Nominum's TRUE architecture Nominum Vantio™ Base Server and Vantio Malicious Domain Redirection Service Delivery Module

KEY BENEFITS

- No new equipment and no changes to network architecture
- Proven stable and reliable platform allowed for very rapid deployment – concept to production in days
- No impact on network performance
- Users redirected to different web pages based on what site they are trying to access
- Activity logs maintained for compliance with regulatory requirements

COLT

COLT is a leading European provider of business communications. COLT specializes in providing data, voice, and managed services to major businesses, SMEs and wholesale customers across Europe. COLT operates a 13-country, 25,000km secure and reliable network that includes metropolitan area networks in 34 major European cities with direct fibre connections into 15,000 buildings and 18 COLT data centres. COLT is widely acknowledged for superior technology and award winning customer service. COLT Telecom Group S.A. is listed on the London Stock Exchange (COLT). Information about COLT and its services can be found at www.colt.net.

Nominum Trusted Response and Universal Enforcement (TRUE) architecture™

Nominum's new Trusted Response and Universal Enforcement (TRUE) architecture allows providers to deliver a safe and secure Internet experience. It offers real time protection for subscribers, restricting access to illegal or malicious content on the web, or defending against rapidly expanding web based threats such as spam, phishing, or botnets. With the TRUE architecture, providers can enhance the subscriber Internet experience and generate new high margin revenue streams without impacting network operations, changing the network architecture, or introducing any new equipment into the network.

The TRUE architecture is built on Nominum's core DNS technologies that provide superior security, performance and availability for more than 170 million broadband households connected by more than one hundred large service providers globally. It starts with a secure DNS foundation based on unique layered defenses that provide the industry's most advanced protections against all forms of DNS attacks, including cache poisoning attacks.

The newest element of the TRUE architecture is the Malicious Domain Redirection (MDR) enforcement point which provides real time protection for subscribers; and the Centris server which is a massively scalable, in-network threat database that is synchronized in real-time with external and internal threat lists. TRUE incorporates the Vantio Base Server, an advanced DNS caching server with a modular design that supports Service Delivery Modules such as MDR that enable network-based subscriber services defined and controlled by the provider.

COLT recognized very early that deploying best of breed technologies in their network would provide them a substantial advantage in offering leading edge, high performance services. In particular they realized that a scalable and resilient DNS infrastructure would offer long term benefits in the form of network responsiveness and stability, which would contribute directly to ongoing customer satisfaction, retention, and growth.

Challenges

Network Providers regularly face the challenge of exceeding customer expectations for service availability and quality while carefully managing costs and improving network performance. At the same time they must also ensure they are in compliance with legal requirements in the countries where they operate and work cooperatively with influential non-governmental organizations that advocate for various issues.

Recently there has been universal agreement on the need to introduce measures to restrict access to the most insidious content on the Internet – sites featuring child sexual exploitation. Governments around the world have either already enacted laws, or service providers have worked on a voluntary basis with judicial authorities and law enforcement to proactively implement solutions to eliminate this scourge. In some countries legislation has also been passed to prevent access to illegal services on the Internet such as unlicensed gambling. These regulations and others that will inevitably follow place an additional burden on service providers: how to comply without adversely impacting the user experience or network operations.

Reliable, High Performance DNS Foundation

Starting in 2004, COLT built out their DNS infrastructure with Nominum caching name servers, which were selected on the basis of performance and reliability. They were able to build a highly redundant pan-European DNS network with servers close to their customers, and experienced 100% uptime and consistently fast response times for DNS queries.

COLT was recently informed of a new Italian government mandate that required network operators to block access to online gambling sites that are not licensed, as well as a subsequent initiative to block access to child sexual exploitation content that introduced new requirements.

Blocking access to child sexual exploitation content was an especially complex problem because there was a need to update the DNS much more frequently (within 6 hours after updates were issued) so any kind of static provisioning was unworkable. Furthermore, there were thousands of sites that had to be blocked and the list was likely to grow over time. Finally, there was a need to meet regulatory requirements to log addresses of users attempting to access illegal sites.

Scaling, Automating with Vantio MDR

COLT realized that a scalable and automated solution was needed to address these problems and decided to evaluate Nominum's Malicious Domain Redirection (MDR) Service Delivery Module (SDM) as a solution. MDR runs as a module on top of Nominum's Vantio Base Server and as a software-only solution, can be installed on a multitude of standard hardware platforms and operating systems already in place in the network.

MDR examines DNS requests and redirects users to a web page if a request to access a targeted site is identified. For instance, MDR can be configured with records to identify sites hosting illegal gambling or child sexual exploitation content. When a request to access such a site is identified rather than offering the address of the site, MDR offers the address of a teaching page that has information about why the user was redirected. Different teaching pages can be presented depending on the list that the query matches. In other words someone trying to reach a gambling site can be presented with a different page than someone trying to reach a site with child sexual exploitation content.

MDR is configured and continuously updated on an automated basis using the Nominum APIs. This allowed COLT to comply with the regulatory requirements to update records quickly after they were published and also allowed them to move away from the tedious, labour intensive, and

disruptive manual process they had used earlier. Since MDR scales to support tens of millions of records, accommodating the lists mandated by existing regulations was straightforward, with room to support growth and the addition of many more lists.

Simple Installation and Reporting

For COLT, MDR provided the perfect solution to their problem. The favourable experience with Nominum's first generation caching server made their evaluation brief and they moved into production quickly. Upgrading their existing Nominum caching servers to Vantio and MDR was straightforward, with no disruption to services and no need for any kind of hardware upgrades. All of the existing operational and control applications and procedures were preserved and Vantio specific monitoring and control were easily configured. They also set up MDR to generate reports on IP addresses attempting to access sites targeted by the lists.

Summary

"At COLT, we're working cooperatively with the regulatory agencies in Italy to prevent access to illegal gambling and content on the Internet as a value to the community of users we serve," said Stefano Maifreni, Product Manager for Internet Access Services at COLT. "With Nominum's new products, we can comply with new requirements quickly without any changes to the network or user behaviour. We plan to leverage these products to deliver ongoing security and safety from other threats."

COLT's desire to block illegal websites and work cooperatively with regulatory agencies motivated them to find a cost-efficient way to block access to sites hosting child sexual exploitation content. They identified Nominum's MDR as a solution that would not require any new equipment or changes to their network. MDR also reduced their workload by allowing automatic mass updates to the system without any service disruption. Reporting capabilities that were part of MDR were an added bonus that again reduced operational overhead. COLT's MDR deployment was implemented on an expedited basis as a result of years of favourable experience with existing Nominum products and the customer support organization.

ABOUT NOMINUM

Nominum's network naming and addressing solutions are the foundation of the always-on broadband Internet, supporting more than 150 million households connected by more than one hundred service providers in every region of the world - North America, Europe, Asia-Pacific, and Latin America. Nominum's Domain Name System (DNS) and Dynamic Host Configuration Protocol (DHCP) products lead the industry in security, performance, and reliability. Nominum innovations allow providers and enterprises to leverage DNS to deliver a Trusted Internet Experience; creating an environment where individuals can browse, interact and transact online without fear of identity theft or exposure to illegal or malicious content. It preserves the freedom to explore, create and share content, while maintaining privacy and removing the immense burden on Internet users to provide and maintain the technology needed to protect themselves from an increasingly complex and continually changing range of online threats.

.....

Nominum, Inc.

2000 Seaport Boulevard, Suite 400
Redwood City, CA 94063 USA

Phone: +1.650.381.6000

Fax: +1.650.381.6055