Nominum
Shaping the New Internet

DATASHEET

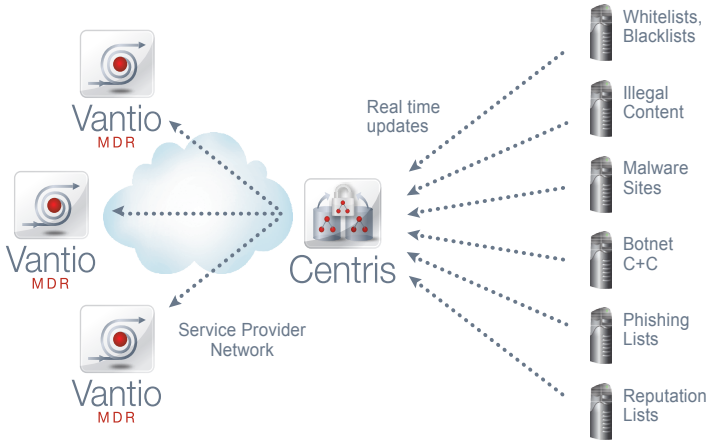
Nominum Centris™

THREAT AGGREGATION AND PROVISIONING SERVER

Web based exploits, malware, and spam raise network owner costs by increasing the need for bandwidth, networking hardware, and support, as well as reducing end user satisfaction and creating public relations problems. Government mandates or voluntary agreements are also beginning to require that providers block access to illegal content such as web sites hosting child exploitation images.

Existing solutions for dealing with web based threats and spam are showing their limitations. They are proving costly to scale, have difficulty keeping up with the rapidly growing array of threats that change constantly, and for newer devices such as smartphones protections may not be available at all. The result is many threats go undetected so networks degrade, end users are exposed and unhappy, and network owners have to deal with higher costs and peer networks that may take action against spam originating from their networks.

Nominum **Centris** threat aggregation and provisioning server is an in-network multi-protocol database that is part of a complete solution to stop more threats and more spam more effectively than any alternative. Centris purpose-built high performance database aggregates, stores, and serves information about Internet threats or reputation lists at unprecedented scale (more than a billion records). Information stored by Centris is centralized, in-network, and can be used by any network device or application to: clean up networks by identifying botnets and other malware, target illegal content, and cost effectively deter more spam.



Centris is a software only solution that can be deployed rapidly on commodity hardware platforms without any changes to the underlying network architecture. There is no change in network performance or latency and no change in DNS performance or reliability. Combining Centris, SKYE℠ Network Protection Service, and Vantio™ Malicious Domain Redirection (MDR) policy software offers network owners a completely automated solution to protect their networks and ensure end users have a safe, secure and productive web experience regardless of what device or application they are using.

KEY FEATURES

- High performance threat aggregation and secure provisioning database
- Multi-environment support (broadband, email, location-aware security services)
- Multi-application support (network security, compliance, anti-spam, etc.)
- Secure data transfer to/from multiple sources simultaneously
- Scalable to handle millions of threat categories and a billion records with zero latency impact
- Advanced policy control for multi-format whitelisting
- URL and other non-domain identifier support
- Optimized integration with SKYE Network Protection Service
- Scalable integration across multiple Vantio MDR servers
- Patented data synthesis algorithm for fast response and load optimization

© 2010 Nominum, Inc. All rights reserved. Nominum, Navitas, Vantio, Centris and TRUE Architecture are registered trademarks of Nominum, Inc.

Cost Effectively Clean up Networks and Deter Spam

Because of the large number of web sites hosting malicious content, and massive volumes of spam generated by infected hosts, no single threat data "source" can always find, track and be up-to-date with them all. Centris allows network operators to clean up their networks and protect end users by dramatically improving the effectiveness of malware and spam deterrence efforts through integration of multiple threat data sources, such as **SKYE** Network Protection Service, or reputation lists. Threats or spam missed by one source but tracked by another will be reflected in the Centris database, yielding a higher overall success rate when the data is used for enforcing policies. Centris can also be used as compliance solution for meeting government mandates to protect Internet users from illegal content. It is simple to integrate into any network and offers essential security mechanisms to handle this sensitive data.

Diverse Threat Data Sources Validated by Nominum

Centris can be configured to receive real-time threat updates over a secure communications channel from SKYE Network Protection Service (NPS). NPS provides a real-time feed of bot-related and other malicious domains gathered over the Nominum Global Network. Threat data is aggregated and validated with proprietary systems developed at Nominum.

Instant Updates Across the Network

Threat data stored in Centris is instantly made available in real time to enforcement points such as Nominum's Malicious Domain Redirection (MDR), as well as email gateways, firewalls or other network devices. This minimizes the time from when a threat is discovered, to when it is available to network devices that act on the data, taking away a major advantage that attackers have enjoyed in the past.

Composite Zones Greatly Increase Efficiency

A unique feature, composite zones, allow network devices to send a single query to Centris and get a response about whether an IP address or domain is listed among any of the multiple lists supported. This reduces the number of DNS queries required and cuts the response time for each query. This in turn reduces load on the clients sending queries to Centris, caching name servers, and other network elements.

Secure Downloads of Threat Data

Centris "commercial-grade" features make it more secure and easier to manage than any alternative. Sensitive records can be securely downloaded from the list provider using https and automatically hashed and stored in a secure format on the Centris server. TSIG support for zone transfers ensures integrity of threat updates.

Greater Network Efficiency and Control

With Centris, all threat data is stored locally in-network. There are two methods of distributing the data across the network. Enforcement points such as Nominum's MDR can pull dynamic updates from the Centris database at preconfigured intervals, in which case, the distribution is completely automated and instantaneous. Alternatively, network devices can push queries to Centris. In either case there is no need for enforcement points to send queries to remote resources "in the cloud" so latency and possible outages are avoided.

NETWORK OWNER BENEFITS

- Central repository for all threat data across the network
- Open platform with secure channels for provisioning and propagation
- Standard interfaces and flexible data formats improve broad range of services
- Simplified architecture for complex & distributed protection
- Ease of deployment—software only solution, multiple hardware OS support
- Simplified provisioning and management
- Automatic updates without service impact
- Data control and privacy—in-network data aggregation and anonymization
- Tracking, reporting, and transaction visibility
- Application and site safeguarding to ensure availability

END USER BENEFITS

- Enables your ISP to deliver network based services that protect you
- Less spam, less botnets and rapid protection against fast changing threats
- Unified protection model for all applications
- Gain protection without service degradation through distributed threat data
- Leverages the natural path for Internet resolution to provide new services
- Protects user privacy—no transfer of personally identifiable information to 3rd parties

© 2010 Nominum, Inc. All rights reserved. Nominum, Navitas, Vantio, Centris and TRUE Architecture are registered trademarks of Nominum, Inc.

"Future-Proof" Platform Optimized for Scaling, Performance and Availability

Threat data from today's leading sources already comprises hundreds of millions of records and they are growing rapidly. Centris was engineered to simultaneously store more threat records and handle frequent database updates without sacrificing performance or availability. The proprietary, persistent, and highly optimized database is stored both in-memory and on-disk offering far better performance than text files or a general purpose database backend. Even with a billion records stored in a production system Centris offers the fastest response to queries and handles very high query volumes without service degradation.

Server downtime is eliminated by loading new data without a restart. Full, incremental or "one-off" updates are intelligently batched and written to disk. Configuration changes can be made on the fly without restarting the server. Centris' optimized data structures deliver fast startup to reduce latency during both cold and warm boot to minimize planned maintenance windows. Patented algorithms monitor and manage system resources to ensure availability and consistently high performance even under extreme loads.

Multi-protocol Support

Centris simultaneously incorporates data from diverse threat databases using common protocols including RBLDNSD, RSYNC, incremental zone transfers (IXFR), full zone transfers (AXFR) and SOAP/XML.

Multi-Environment Support

Centris is suitable for fixed and mobile broadband as well as other network environments and security applications. Support of standard protocols also allows Centris to be used for data distribution to email gateways, firewalls or other network devices.

Highly Manageable

Nominum's Command Channel API, or interfaces for PERL, JAVA, C, Python and SOAP/XML provide secure remote management. SNMP support allows administrators to easily monitor Centris using their preferred management framework.

© 2010 Nominum, Inc. All rights reserved. Nominum, Navitas, Vantio, Centris and TRUE Architecture are registered trademarks of Nominum, Inc.