Vantio™ ThreatAvert protects networks against new threats that rely on DNS and originate inside provider networks such as stealthy DNS-based DDoS attacks or bot based malware. ThreatAvert Application provides reporting facilities using network-wide security data gathered from ThreatAvert servers distributed across a network.

Preconfigured reports offer instant access to information for evaluating security posture. Graphical views of all forms of DNS-based DDoS and botnet activity offer instant access to data for day-to-day monitoring, establishing trends, or spotting emerging problems and troubleshooting. Drill-downs to any level of detail allow better characterization of DDoS activity and bot behavior, or deeper analysis of more subtle threats. Dynamic searches provide additional visibility.

Threat data and analytics remain within the operator’s network for ease of access and to fulfill regulatory mandates covering data privacy.

ThreatAvert At a Glance
Security staff need data to understand the current and historical posture of their network. ThreatAvert’s preconfigured reports provide instant data access for supporting day-to-day monitoring needs, evaluating anomalous behaviors, and spotting potential emerging threats. Real-time graphical displays of query data obtained from Vantio Caching DNS servers are combined with threat information from Nominum Global Intelligence Xchange (GIX) to create graphs that can be displayed with a click.

Simple Security Data Navigation
ThreatAvert Application offers real time graphical displays of data obtained from servers. A Threat Dashboard shows DNS-based DDoS activity and botnet threats as well as infected clients. Additional preconfigured graphs can be displayed with a few clicks:

- Threats – by Type, IP, Subscriber, QPS, and Query Count
- Domains – Blocked (based on matches against GIX Threat Lists), DNS Amplification, Random subdomain DDoS Attacks, and Rate Limiting Statistics
- Client and subscriber statistics – Infections, Blocked, MX queries (typically bots sending spam)
- Query Statistics – Blocked (based on matches against GIX Threat Lists), Infected Query Rate, Percent Random Subdomain Queries

Pull down menus can be used to shape charts: define time frames, select servers (one, all, or any portion), and specify query parameters to chart. External analysis is supported through data export functionality.

Scheduled “Push” Reports
Security staff, DNS administrators, and Operations regularly require security data. The ThreatAvert Application makes it simple to automatically generate reports to support technical and business requirements based on the statistics described in the previous section. Reports can be scheduled and mailed to management stakeholders with a mouse click.
**Scalable Application**

Intelligence provided with ThreatAvert is based on best practices for data collection, aggregation, transformation, and presentation. Nominum development and operations engineers have decades of combined knowledge gained from experience managing more than 1.1 Trillion DNS queries around the world every day.

The ThreatAvert application is enabled with Nominum’s N2 Platform. The Nominum Data Aggregator feeds query data into ThreatAvert, providing a centralized data repository, filtering, and data processing facilities. Dozens of distributed servers can connect and upload their DNS data to the Data Aggregator. Role-based access ensures network operations staff only see data for which they are granted rights. N2 integration speeds deployment and makes it simple to implement other additional subscriber-facing applications.