Product Brief

N2™ THREATAVERT

Protect vital DNS assets and identify malware

Service Providers recognize network security drives brand equity because it directly impacts subscriber satisfaction. Secure networks are also easier and less expensive to operate since distractions and fire drills are minimized. But new threats that leverage DNS and originate inside provider networks are forcing a rethink of how to protect essential DNS resources and the networks they support. Investments in traditional security solutions and Best Practices won't work against:

- Stealthy DNS-based DDoS attacks that use millions of home gateways with open DNS proxies; or infected Internet "Things" (IoT) that are designed to compromise network integrity.
- Sophisticated bot malware secretly loaded onto consumer devices that impacts the subscriber experience and satisfaction by sending spam, stealing financial and personal data, and more.
- DNS tunnels using special client software that carries other protocols inside DNS to steal services.

DNS Security Belongs in DNS Servers

DNS queries are a leading indicator of malicious activity because resolving the address of a malicious resource - C&C server, malware download, exfiltration site, etc – is the first step in enabling most forms of malicious activity. DNS resolvers are an ideal place to embed intelligence to target DNS-based threats because they see all the queries on a provider network. Malicious activity can be detected by matching incoming queries against entries on dynamic threat lists.

N2 ThreatAvert is powered by Nominum's leading Vantio CacheServe resolver, equipped with Global Intelligence Xchange (GIX) dynamic threat feeds described below. ThreatAvert leverages the DNS control plane to secure networks, which makes it highly efficient because there is no need for additional inline or offline data plane packet processing. Since it is network-based every device is covered, and clients and hosts don't require security software installation or updates. There are numerous other benefits:

N2 ThreatAvert protects networks and subscribers from lurking cyberthreats with accurate, adaptive and automated technology combined with data science.

KEY HIGHLIGHTS

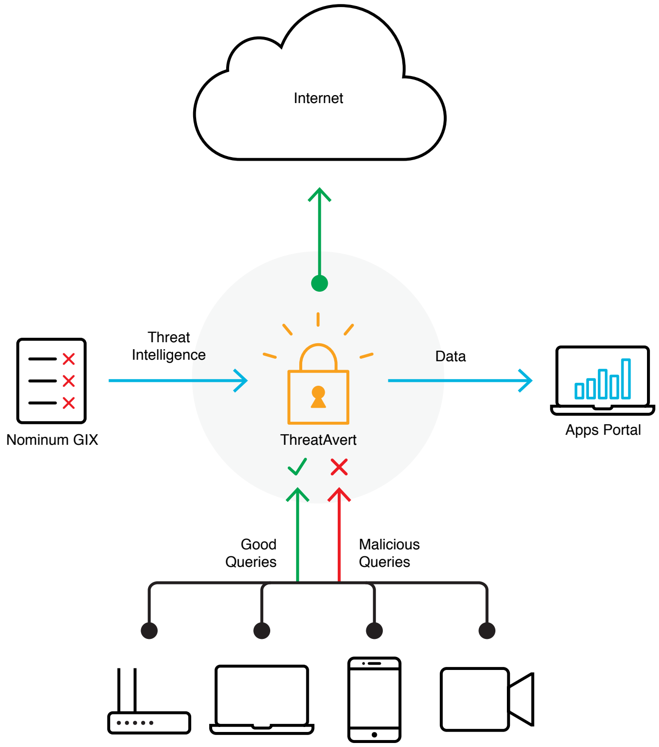
- Global Intelligence Xchange (GIX) threat feeds stream updated protections 24x7
- Precision Policies block malicious queries and ensure good traffic is never dropped
- Integration with N2 Platform data architecture offers real-time access to threat and telemetry data
- Reporting dashboards provide an at-a-glance view of malicious activity, and drill-downs to details
- Based on leading DNS technology to ensure the best possible subscriber experience

Accurate. Provides superior depth and breadth of coverage based on leading DNS threat research.

Agile. Disrupts malware very early in the cycle by detecting and blocking malicious DNS queries.

Automated. Implements a “set it and forget it” deployment model, and is simple to maintain

Adaptive. Updates threat feeds continuously to maintain protections as exploits change



85% of threats detected by GIX were not detected by other 3rd party malware feeds

Superior accuracy, depth and breadth of threat coverage

Nominum Security Research produces GIX threat feeds by processing more than 100 Billion anonymized DNS queries, live-streamed from Communications Service Providers (CSPs) worldwide. This real-time visibility into global DNS traffic uncovers cyberthreats more quickly and comprehensively than security researchers using traditional techniques such as honeypots. Superior results come from investments in:

- Patent-pending algorithms to instantly detect anomalous behavior, correlate disparate threats, and identify new Domain Generation Algorithms used by bots.
- Advanced techniques for auto-whitelisting names to ensure “good” DNS queries are always protected.
- Research staff with years of security experience and a deep understanding of malware and DNS data.
- Worldwide network and data centers for real time processing of live data streams.

The large data stream processed by Nominum experts offers a comprehensive picture of malicious activity across the Internet, as well as localized attacks. Finely tuned algorithms flag anomalous queries in real-time for further analysis. DNS-based DDoS traffic, bot activity, and DNS tunnels can be identified within minutes of their first appearance anywhere in the world.

Machine learning and correlation of incoming queries with 3rd party sources broaden coverage by revealing patterns that reflect subtle variations in exploits that honeypots or other traditional forensics techniques miss. Predictive analysis is also used to target future malicious activity, by reverse engineering Domain Generation Algorithm (DGA) seeds for instance. GIX threat feeds are continuously benchmarked against other sources and typically show substantial increases in threat coverage. Nominum research has shown 85% of threats detected by GIX were not detected by other 3rd Party malware feeds. Data sharing is encouraged to expand GIX data and improve the detect rate even more. Targeted threats unique to a provider network or geopolitical area may also be detected.

GIX eliminates false positives using domain validation algorithms developed over years of research. These algorithms rate candidate domains against more than 90 name related attributes. Threat data from reputation lists, honeypots, and other sources is also incorporated in the validation process. Manual review is undertaken if there is any doubt about the maliciousness of a domain. After validation Precision Policies (see below) for managing unwanted traffic are associated with each exploit and incorporated into GIX feeds which are streamed to resolvers throughout the world.

Reports can be shared amongst DNS operations, security and executive stakeholders

Precision Policies

Precision Policies are incorporated into GIX feeds to manage unwanted DNS traffic. A broad and deep feature set allows fine grained filtering to target only malicious queries and always protect (answer) legitimate queries:

- Precision Policies can be applied to incoming queries or outgoing answers
- Filters or rate limits can be set based on: IP, Query Type, FQDN or many other query parameters
- Filters or rate limits can use multiple query parameters: QTYPE AND FQDN, IP AND FQDN, etc
- Logical operators can be used: AND, OR, NOT
- Filters or rate limits can match against GIX dynamic threat lists or operator supplied lists
- Policies and threat lists can be combined: MATCH against BLOCKLIST AND NOT on WHITELIST
- Multiple policy actions determine how queries are handled: drop, synthesize answer, answer with truncate, NXD, NOERROR, and much more
- Policies can be combined and nested, making them even more powerful

Scalable data management and rich telemetry

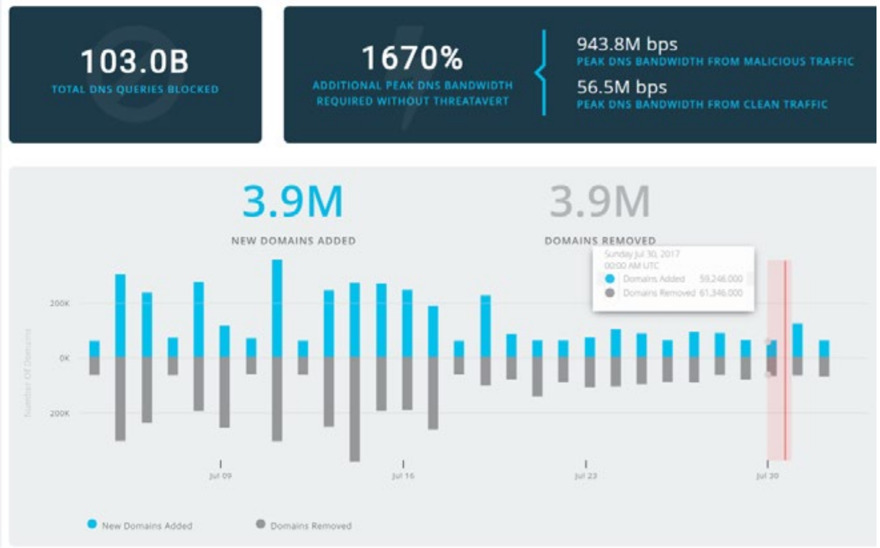
ThreatAvert is integrated with the N2 Platform data architecture which offers real-time access to threat and telemetry data to enable richer ThreatAvert reporting (shown below). Because the data is streamed using an open platform (described above) it's simple to integrate into open analytics and visualization tools.

The new architecture is resilient through failures to provide non-stop availability and it supports optional connections to Big Data systems (Splunk, Hadoop) or purpose-built applications, to create additional security 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.

Security Threat Essentials

ThreatAvert reports have been completely rebuilt to offer an instant assessment of security posture. An Executive Dashboard, shown below covers:

- DNS queries blocked – malicious and unwanted activity deterred
- Peak DNS Bandwidth Saved – costs avoided
- Top Malware in Network – threat landscape at a glance
- Infected Subscribers – window into network and customer exposure
- Threat Intelligence Updates – snapshot of continuously updated protections


103.0B
TOTAL DNS QUERIES BLOCKED
1670%
ADDITIONAL PEAK DNS BANDWIDTH REQUIRED WITHOUT THREATAVERT
943.8M bps
PEAK DNS BANDWIDTH FROM MALICIOUS TRAFFIC
56.5M bps
PEAK DNS BANDWIDTH FROM CLEAN TRAFFIC
3.9M
NEW DOMAINS ADDED
3.9M
DOMAINS REMOVED
Sunday Jul 30, 2017
00:00 AM UTC
● Domains Added 59,246,000
● Domains Removed 61,346,000
200K
0K
200K
Number Of Domains
Jul 09
Jul 16
Jul 23
Jul 30
● New Domains Added
● Domains Removed

TheatAvert dashboards provide a high-level view of threat activity.

An additional Security Dashboard provides graphs of each of the categories of exploits.

- DNS-Based DDoS: 4 graphs showing QPS and Top 10 Domains for DNS Amplification and Pseudo-Random Subdomain Attacks (PRSD)
- Malware: 2 graphs showing Queries and Infected Client IP Addresses

One click displays finer granularity of DDoS attacks (5 minute intervals) and more information about domains and clients that were involved. Successive layers of detail about Malware and Infected Clients can also be obtained with a click.

Leading DNS engine reduces operating costs and delivers the best subscriber experience

N2 ThreatAvert is built with industry-best DNS technology, developed and supported by the leading engineering team with decades of experience and an unmatched track record of innovation. The largest, most complex networks in the world rely on Vantio CacheServe's robust design and advanced features:

- Leading performance (2.5 M queries/second) means fewer servers, reducing CAPEX and OPEX
- Lowest latency ensures the best possible subscriber experience
- Unique layered DNS cache poisoning defenses protect subscribers from compromised DNS data
- High performance recursive resolution & specialized algorithms ensure availability during attacks

Better Protection, Better DNS, Better Network

Stealthy, powerful DNS-based DDoS attacks and more sophisticated malware are a strong motivation to deploy new layers of defenses against attacks that originate inside provider networks. DNS resolvers are an ideal place to embed intelligence to target DNS-based threats because they see all the queries on a provider network. Nominum Security Research processes massive volumes of live streamed DNS data to uncover and validate emerging threats far faster than traditional research techniques. The Global Intelligence Xchange (GIX) incorporates this work into a continuously updated real time threat feed that is automatically distributed worldwide. Fed by GIX, Precision Policies target malicious traffic and protect good traffic. Together these capabilities deliver agile, accurate, automated and adaptive defenses against fast changing threats.

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