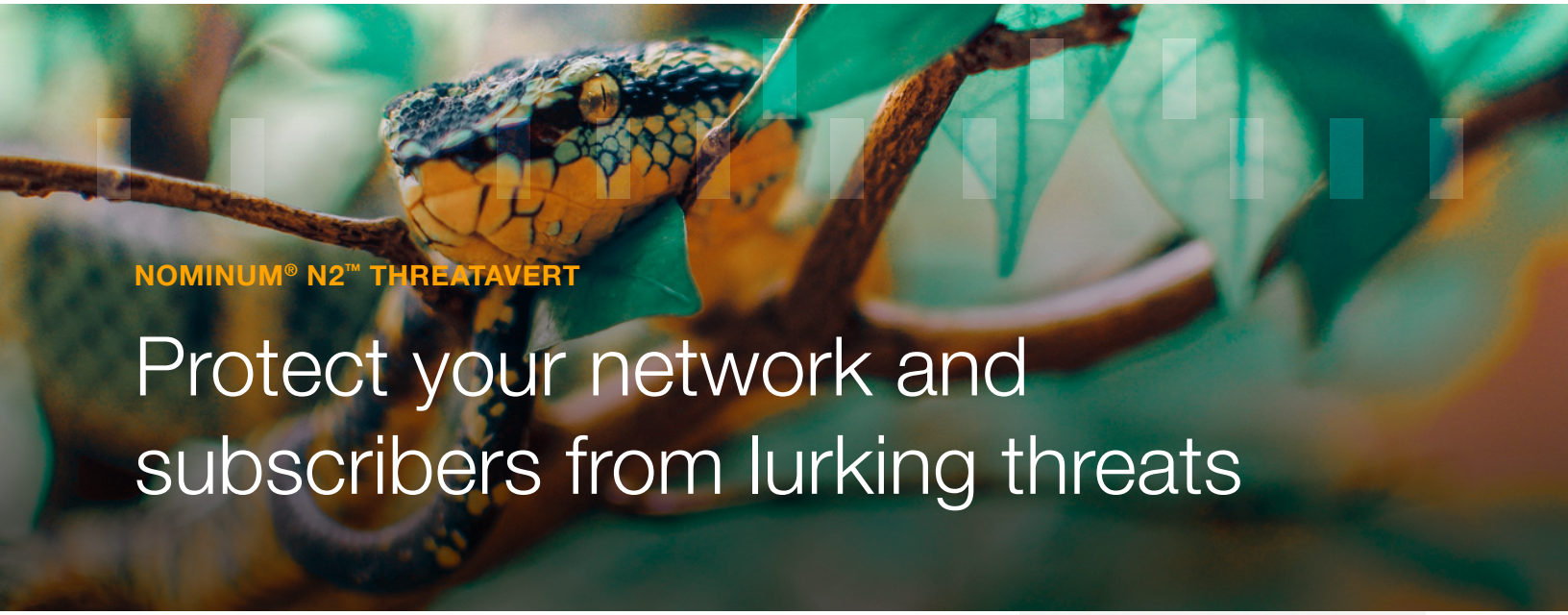
Product Brief



NOMINUM® N2™ THREATAVERT

Protect your network and subscribers from lurking threats

N2 ThreatAvert provides real-time protection against threats originating from within service provider networks that degrade a subscriber's online experience. It delivers unmatched accuracy and up-to-the-minute data that is validated by Nominum Data Science, removing the potential for false positives that block legitimate subscriber traffic. The solution is highly adaptive, with a proven track record in deterring fast-changing exploits. It is completely automated, meaning the operations team can "set it and forget it" with assurance that the network's DNS servers are fully protected.

Advanced software and Nominum Data Science protect your network from vulnerabilities

New threats are forcing service providers to rethink the best way to protect essential DNS resources and the networks they support. Such threats include:

- DNS-based DDoS attacks that use more than 10 million home gateways with open DNS proxies, or bot-infected devices that compromise network integrity
- Sophisticated bot malware, secretly loaded onto consumer devices, that rely on DNS to trigger spam, financial/personal data theft and more
- DNS tunnels carrying other protocols that use special client software to steal service

DNS resolvers help facilitate nearly every internet transaction, making them an ideal place for cybercriminals to embed malicious code. Nominum identifies attacks that are not published elsewhere or before they are made public, embedding intelligence to target "inside" threats. ThreatAvert effectively blocks DNS-based cyberthreats to maintain network availability/uptime and improve subscriber experiences without taxing servers.

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 lists and algorithms provide up-to-date, 24x7 protection
- Dashboards provide at-a-glance view of all malicious activity, with drill-down capability
- Precision policies target malicious queries used for DNS-based attacks, botnets and tunnels
- Allows good traffic while filtering bad traffic
- More than 100 billion queries analyzed each day by data scientists for anomaly detection

Data Science analyzes 100 billion queries daily to keep networks protected

Nominum identifies cyberthreats more quickly and comprehensively than other security software products. That's because Nominum Data Science analyzes more than 100 billion anonymized DNS queries each day to publish threat lists in real time. Unique algorithms detect anomalous behavior, correlate threats that share common underlying characteristics and identify new Domain Generation Algorithms used by bots. Once identified, malicious domains are blocked while "good" DNS queries are auto-whitelisted, so subscribers reach their intended destination with the best possible internet experience.

Integrated threat lists keep your network protected 24x7, 365 days per year

Nominum updates its Global Intelligence Xchange (GIX) lists continuously to track DDoS, malware activity and DNS tunnels. GIX algorithms identify DDoS activity quickly—new threats can be identified within 5 minutes and validated/published within 20 minutes of their first appearance anywhere in the world. When attack activity subsides and is no longer seen in real-time traffic streams, threat list entries are aged out. However, a "recent list" is instantly invoked if ThreatAvert detects a query for an earlier attacked domain within a week of its first appearance.

The large data set processed by Nominum data science every day offers a comprehensive picture of malicious activity in local attacks and across the internet. GIX has a consistent track record of detecting DDoS, malware and tunnels where other security technologies have failed. Nominum research has shown that 85% of threats detected by GIX were not detected by third party malware feeds.

By using domain validation algorithms that have been developed from years of research, GIX eliminates false positives. More than 90 name-related attributes are corroborated along with threat data from reputation lists, honeypots and other sources. Manual review is undertaken if there is any doubt about the legitimacy of a domain, assuring that highly accurate protection takes place at all times.

Fine-tuned filtering blocks attacks, protects subscriber internet experiences

Precision policies protect the DNS, subscribers and networks from abuse by precisely targeting malicious DNS queries used for DNS-based DDoS attacks, botnets, or tunnels. These policies are fed by GIX data. A broad and deep feature set allows fine-grained traffic filtering including rate limits, query handling instructions and nesting of queries (for more powerful filtering). DNS network operators also have the ability to whitelist and blacklist specific domains, based on local information.

Integrated dashboards provide insight into malicious activity

ThreatAvert provides an intuitive, at-a-glance dashboard that details malicious activity. Graphs display DNS-based DDoS and bot activity, infected subscribers and other attack-related details. Data for reports is continuously fed, without impact to a subscriber's internet activity.

With drill downs to details, deeper forensics are just a click away. Reports can be scheduled and automatically emailed so status can be shared amongst DNS operations, security and executive stakeholders.

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

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

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

Extensible platform for digital transformation

ThreatAvert is an integrated component of the Nominum N2 application suite. N2 leverages the company's market-leading Vantio™ DNS engine. Applications include **N2 Reach** in-browser messaging which alerts subscribers of possible infections while providing remediation instructions and **N2 Engage Subscriber Safety** which provides proactive, single-click security capabilities that can be set from any device to keep home networks and all connected devices safe from data and identity theft.

ABOUT NOMINUM

Nominum is the world's DNS innovation leader and the first company to create an integrated suite of DNS-based, subscriber-centric applications that digitally transform service providers while personalizing the online experience for subscribers. More than 100 providers in over 40 countries trust Nominum software to protect their networks and deliver greater value to subscribers.

Nominum Data Science is a worldwide team with expertise in internet security, machine learning, artificial intelligence, natural language processing and neural networks. Previous projects of team members include quantum physics and data analytics used to discover the Higgs boson at CERN and some of the earliest investigations into the structure and propagation of botnets.

CORPORATE HEADQUARTERS

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

+1 (650) 381-6000

hello@nominum.com