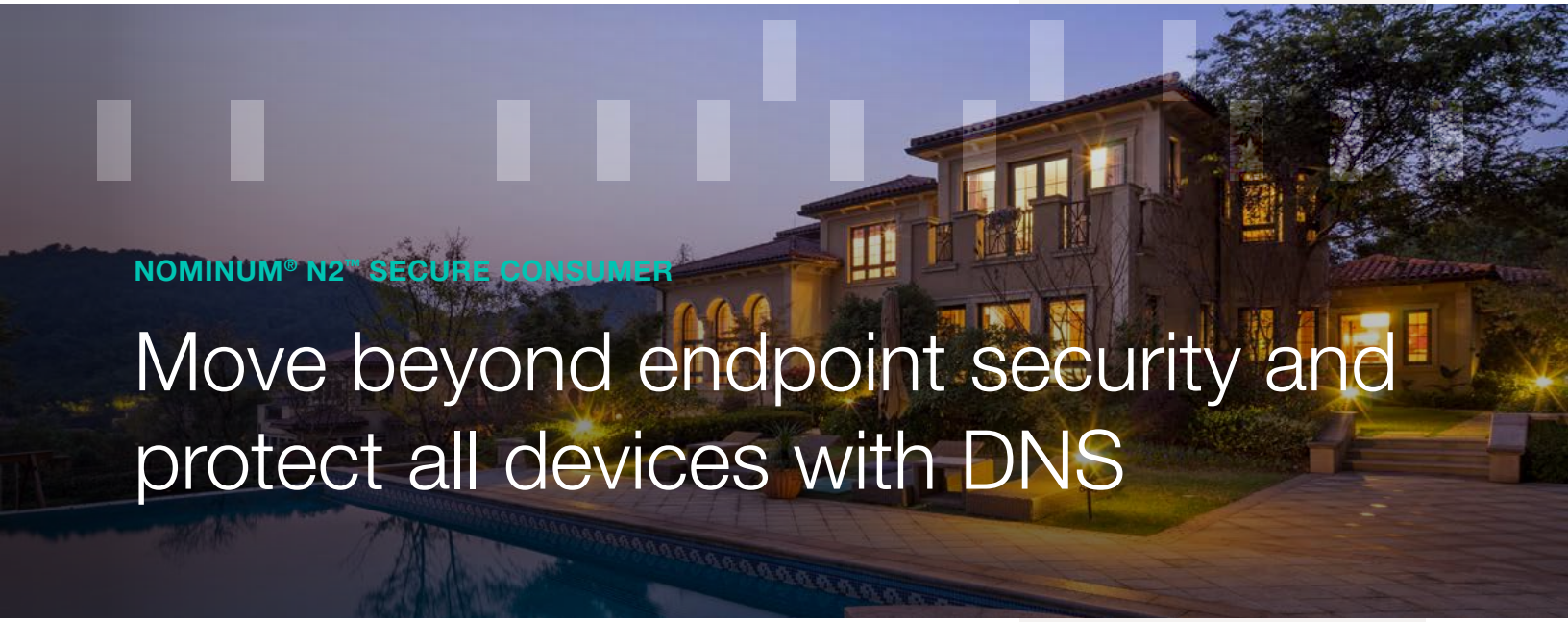
Solution Brief



NOMINUM® N2™ SECURE CONSUMER

Move beyond endpoint security and protect all devices with DNS

Introduction

Internet usage is at an all-time high, with more and more devices being added to household networks. At the same time, subscribers face cyberthreats that are agile, sophisticated and dangerous. Advanced security solutions must be implemented that protect subscribers proactively and around the clock.

The number of IoT devices in the home continues to increase, yet IoT manufacturers rarely make safety features a priority. Contemporary threats are configured to prevent detection, making them ever more complicated to find and avert, giving cybercriminals an advantage that Communications Service Providers (CSPs) cannot afford to ignore. When a subscriber's personal information is endangered, it has a negative impact on individuals and households. Subscribers often blame their provider for lack of security and are 3.8 times more likely to churn and eight times more likely to call customer support, according to Nominum research.

DNS-based security

N2 Secure Consumer is a DNS-based, network-hosted security solution that provides protection from phishing, viruses, ransomware and malware for any internet-enabled device in the household with a single click. It helps providers enhance essential online services and dramatically improves subscriber satisfaction with advanced cybersecurity protection that guards against identity and financial theft. Providers can also optionally offer parental controls from Nominum, cloud-based content filtering that protects children and entire households from inappropriate content.

Nominum built a caching DNS server from the ground up based on extensive knowledge and industry expertise. Built-in intelligence is a fundamental component of the Vantio® CacheServe product, and its layered defense capabilities. DNS is

N2 Secure Consumer leverages DNS to protect subscribers from today's advanced cyberthreats.

KEY HIGHLIGHTS

- Protects from phishing, viruses, ransomware and other malware.
- Guards against personal and financial theft.
- Attractive pricing with no cap on the number of connected household devices.
- Network-wide protection means no per-device configuration or updates needed.
- Zero performance degradation.
- Network-wide visibility into all infections.

used in the CSP network to return the IP address for a domain so the subscriber's request can be completed. DNS can block network-level threats like DDoS and amplification attacks while protecting subscribers from malicious activities on all connected devices. Because DNS sees all internet network calls, it offers a first line of defense against cyberthreats.

Endpoint security solutions

The traditional approach to home device protection is to install security applications when and if required on each device. This solution worked when the internet was limited to a few personal computers in each household. Endpoint security solutions such as anti-virus are now incomplete and ineffective because they are unable to protect subscribers across devices such as smart TVs, security cameras, gaming consoles and many other devices.

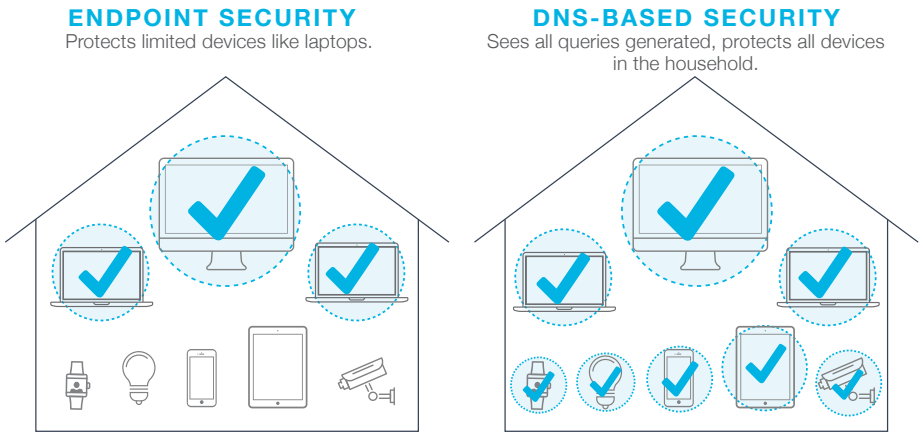
Endpoint solutions offer products that must be downloaded and configured for each device that needs protection. Once installed, devices need to be updated periodically. According to CSPs, this installation and update process dramatically reduces adoption rates, resulting in loss of revenue, low customer satisfaction and unprotected subscribers.

Comparison

Endpoint security platforms are unable to provide complete, dynamic threat detection that protects against the fastest-changing cyberthreats. According to Damballa, 70 percent of threats are not detected by anti-virus within an hour of their appearance and it takes six months for 100 percent of threats to be detected. Nominum security solutions are backed by an experienced data science team that detects both known and unknown threats within minutes.

DNS Network Security	Endpoint Solutions
Network-wide security protects the entire household.	Limited protection. Requires separate installation and updates.
Detects both known and unknown threats in less than 20 minutes.	Time to detect threats and update threat lists can be long.
Attractive pricing—deploy network-wide and scale as needed.	Expensive monthly fees with a cap on number of protected devices.
No software installation required for subscribers.	Complex configurations and updates.
Network-wide visibility. Automatically detects and allows providers to notify infected users and direct them to remediation services.	No network-wide visibility as installation is limited to a few devices. Usually doesn't work on smart TVs, game consoles, etc.
Zero performance degradation.	Potential performance degradation. Software consumes CPU resources.

70 percent of threats are not detected by anti-virus solutions within an hour, according to Damballa.



DNS-based security can protect multiple devices, managed through one central portal.

Hardware-based protection

In the recent past, security providers have brought to market router-based solutions. This feature has several pitfalls. Users must adhere to router specifications (which raises compatibility issues) and operating system requirements, then configure settings, which may require administrative credentials. A hardware investment as well as monthly or annual fees is involved. The cost can easily exceed $250 to get started and protection is limited to the home network. With Nominum, subscribers are protected on fixed lines, mobile and even a provider's public Wi-Fi network. Advanced protection is turned on universally with a simple button from a web page.

Protects from ransomware and other threats

Ransomware is a denial-of-access style of attack that encrypts data on infected devices and prevents users from retrieving the data unless they have a decryption key, which they must pay for. The first level of attack is usually a downloadable Trojan file from a website or personal email. After the download, a payload is run that encrypts the files and holds them for ransom until the desired price is paid in cash or through Bitcoin.

Given the nature of the malware business, ransomware emerged recently as the fastest and most efficient way to turn virtual assets into real money. Since individuals and organizations are often willing to pay the medium-level price (on average about $679, according to CIO Magazine) to retrieve their information, cybercriminals are encouraged to expand their capabilities and networks to offer more sophisticated attacks. N2 Secure Consumer stops ransomware from communicating with its Command and Control (C&C) servers before it can cause harm. When malware or phishing is detected, Nominum blocks malicious queries for all subscribers on all devices through continually-updated blacklists.

Mobile and IoT devices

A vast network of IoT devices, coupled with the increasing sophistication and speed of cyber-attacks, is proving a fundamental challenge to traditional security solutions. With N2 Secure Consumer, all devices in the household can be shielded with a single click and settings apply to all connected devices without installation, hardware or updates. There is no limit on the type of devices, so the subscriber does not need to worry about IoT devices or new mobile devices. All devices that connect to the

internet are protected without any configuration—including smart TVs, smartphones, laptops, gaming consoles and more.

The closed-loop solution for preventative DNS security

If an infected device enters the network, N2 Secure Consumer can detect malicious domains by identifying IP addresses that query domains. Since malware often performs lookups to C&C servers to get their next set of instructions or to download a malicious payload, Nominum will detect the communication attempt and disable it before it connects to C&C servers.

The next step is to identify what subscribers are infected with what type of malware. Based on the domain names queried, Nominum identifies the type of malware and the extent of the damage to the subscriber. The information is made available through a centralized graphical reporting interface to service provider personnel and can be used to automatically generate in-browser messages to the infected subscriber.

Conclusion

Considering infected subscribers are much more likely to churn and/or call customer support, sending them a message that identifies the infection (and also provides remediation advice) turns a negative experience into a positive one. In conjunction with Nominum, 451 Research indicates that 86% of subscribers prefer in-browser messages for important security alerts and advice on how to fix security-related problems. With a limited license for N2 Reach, CSPs can automatically alert infected subscribers with in-browser messages that typically reach 90% of the target audience within 24 hours of being sent.

Effective security is not just about detecting infected users and removing malware, but also about preventing subscribers from becoming infected by blocking access to malicious domains. N2 Secure Consumer is capable of redirecting subscriber requests from malicious sites to a provider-branded messaging page that includes a description of why the site is blocked, and how the provider is helping subscribers maintain online safety. Whether you offer it as a free add-on for valued customers or package it with parental controls as a safety bundle, it helps to increase brand loyalty and increase revenue.

451 Research indicates that 86 percent of subscribers prefer in-browser messages for important security alerts.

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