

September 14, 2016

Marlene H. Dortch
Secretary
Federal Communications Commission
445 12th Street, S.W.
Washington, D.C. 20554

Re: *Notice of ex parte meeting from Nominum, Inc.
Protecting the Privacy of Customers of Broadband and Other
Telecommunications Services, WC Docket No. 16-106*

Dear Ms. Dortch:

Pursuant to Section 1.1206 of the Commission's rules,¹ Nominum, Inc. (Nominum) provides notice of an ex parte meeting on September 12, 2016. Sandy Wilbourn (Senior Vice President of Engineering) and the undersigned as counsel for Nominum, met with Stephanie Weiner (Office of the Chairman), Matt DelNero, Lisa Hone, Brian Hurley, Daniel Kahn of the Wireline Competition Bureau and Jeffery Goldthorp, Nicole McGinnis, Peter Strayer and Emily Talaga of the Public Safety and Homeland Security Bureau. Attached to this ex parte is a presentation that was provided to Commission staff that further explains Nominum's DNS-based products and their role in enhancing security and reliability of broadband Internet access service (BIAS) providers' networks and their use in providing consumers innovative tools so they can exercise greater control over their Internet experiences. Nominum, which was founded in 1999, provides its services to more than 100 BIAS providers in more than 40 countries, representing more than 500 million subscribers processing more than 1.6 trillion transactions daily.

The principal purpose of the meeting was to discuss Nominum's comments and reply comments that were filed in response to the above captioned proceeding.² Specifically, we addressed Nominum's concerns related to network security and reliability and to the continued ability to develop innovative consumer controls. We also discussed the opportunities for real-time notification as an option for providing notice in light of the questions the Commission raised in the NPRM regarding effective notice and innovation. In addition, we discussed two joint statements filed in the above-captioned proceeding by Internet researchers and technologists that Sandy Wilbourn joined and that discuss some partially overlapping issues.³

¹ 47 C.F.R. § 1.1206.

² See Nominum comments (available at <https://ecfsapi.fcc.gov/file/60002081097.pdf>) and Nominum's reply comments (available at [https://ecfsapi.fcc.gov/file/107070984023238/Nominum%20Reply%20Comments%20FCC%20Broadband%20Privacy%20NPRM%20\(filed\).pdf](https://ecfsapi.fcc.gov/file/107070984023238/Nominum%20Reply%20Comments%20FCC%20Broadband%20Privacy%20NPRM%20(filed).pdf))

³ Letter from Prof. Nick Feamster, in his personal capacity, and others to Tom Wheeler, Chairman, Federal Communications Commission, Docket No. 16-106, filed June 27, 2016 (available at <https://ecfsapi.fcc.gov/file/1070642992845/BroadbandPrivacyNPRM-ResearchExemptionLetter.pdf>); Letter from Prof. Nick Feamster, in his personal capacity, and others to Tom Wheeler, Chairman, Federal Communications Commission, Docket No. 16-106, filed Aug. 6, 2016 (available at [https://ecfsapi.fcc.gov/file/1080654886605/FCCPrivacyNPRMResearcherExemption%20\(3\).pdf](https://ecfsapi.fcc.gov/file/1080654886605/FCCPrivacyNPRMResearcherExemption%20(3).pdf)).

Network Security and Reliability. Consistent with its comments, Nominum reiterated its position that the Commission should provide greater clarity that collection and use of DNS and other network-based data is valuable to enhancing the overall security and reliability of a broadband Internet access service (BIAS) provider's network. In the *BIAS Privacy NPRM*, the Commission notes that Section 222(d) provides a basis for an exception to any notice and consent regime for BIAS providers to use, disclose or collect customer proprietary network information (CPNI) to "protect the rights or property of the provider, or to protect users and others from fraudulent, abusive, or unlawful use of, subscription to, broadband services."⁴ In seeking comment on how to interpret this provision to permit BIAS providers to protect themselves and their customers from cybersecurity and other threats, the Commission proposes to permit use or disclosure when "reasonably necessary" to achieve those ends.⁵ Nominum said it is important that BIAS providers have reasonable discretion in advancing these ends and not be inhibited or discouraged from taking steps to do so. Nominum cautioned that the ambiguity and uncertainty added by the word "necessary" might in fact result in less protection and security by inhibiting activity BIAS providers engage in today to enhance the security and reliability of their networks. As Nominum explained, while it may seem like semantics, the phrasing "reasonably necessary" could call into question the use, disclosure or collection of such information that is reasonable because, for example, a BIAS provider might be concerned that it could be second-guessed as to whether the protections that might result were sufficiently certain or imminent to meet the "necessary" portion of the guidance or pertained to research that might not necessarily prove successful. BIAS providers could be questioned on whether there might have been an alternative path to the result and whether the approach taken might not therefore be considered "necessary."

In this way, the Commission might inhibit ongoing practices that are reasonable and have led in the short or long term to improved network security and to the creation of innovative tools offered by BIAS providers to customers. Nominum asked that the Commission make clear in the explanatory text or in final rules that reasonableness is the standard for considering whether a practice fits within the statutory exception of Section 222(d) for BIAS providers when adopting practices designed to enhance the security and reliability of their network and in protecting their customers.

Innovations Promoting Consumer Control. Nominum also discussed the important products it has developed that many BIAS providers offer to consumers and provide consumers greater control over their Internet experience. As Nominum explained, the products allow for greater parental control over the Internet their children encounter and have proved popular where offered; they also allow users to better protect their devices and household networks from botnets, phishing and malware threats; and they help protect against the accessing of illegal content, such as child pornography. Many of these services rely on Nominum being able to access Internet traffic at the DNS level across the Internet to help ensure the tools work as intended and are kept up-to-date to prevent new or modified attacks from succeeding.

⁴ *Protecting the Privacy of Customers of Broadband and Other Telecommunications Services*, WC Docket No. 16-106, Notice of Proposed Rulemaking, 31 FCC Rcd. 2500, 2540 para. 115 (rel. Apr. 1, 2016) (*BIAS Privacy NPRM*) (internal quotations omitted).

⁵ *Id.* at 2541, para. 117.

Access to only some of the DNS data it now has would inhibit the protection of all of the BIAS providers and consumers that Nominum and others provide today in several respects. For example, because Nominum serves so many BIAS providers in the U.S. and around the world it can potentially see and recognize certain threats more quickly than a single BIAS provider. This is also consistent with the well-known benefits to security of more information, as through information sharing.

As Nominum mentioned to the Commission staff, the data it uses is anonymized.⁶ The *BIAS Privacy NPRM* calls into question whether data can be thought of as truly anonymized, noting that “advances in computer science, however, have demonstrated that seemingly anonymous information can often (and easily) be re-associated with identified individuals. Our proposal incorporates this modern understanding of data privacy.”⁷ Nominum is concerned that the Commission’s understanding of what might be considered reasonably anonymous will be too narrowly drawn and urged the Commission to reconsider the standard outlined in the *BIAS Privacy NPRM*.⁸

Notice. Consistent with its comments and reply comments⁹, Nominum also discussed questions the Commission raised in the NPRM about how consumers should be notified of certain BIAS provider privacy and data security practices and about any innovative means for doing so. Nominum highlighted that newer in-browser messaging technologies have some benefits and should be among the options for notice available for BIAS providers to choose among.

Researcher Exception. Nominum also mentioned to staff the importance of including in the final rules an exception for researchers. Nominum is a member of and supports efforts by a group of Internet researchers and technologists, led by Professor Feamster of Princeton University. That group is seeking to ensure that the Internet research, which has gone on for decades and provided many beneficial uses that promote innovation, security, stability and reliability of networks should be allowed to continue.¹⁰ Absent a specific provision, as offered in the letter, we are concerned that such activities would be called into question.¹¹ Nominum urged the Commission staff to consider adopting the rule language contained in Professor Feamster’s August 2016 letter.¹²

⁶ Nominum comment at 5.

⁷ *Id.* at 2520, para. 60.

⁸ In looking at this issue in the context of the Video Privacy Protection Act (VPPA), the Third Circuit Court of Appeals upheld a District Court decision in *In re Nickelodeon Consumer Privacy Litig.* concerning the disclosure of PII to third parties. In dismissing the VPPA claim relating to video-watching habits, the Third Circuit found that the VPPA must allow for the identification by an ordinary individual of a specific person’s identity. Such a standard is worth consideration by the Commission. *In re Nickelodeon Consumer Privacy Litig.*, 2016 U.S. App. LEXIS 11700 (3d Cir. N.J. June 27, 2016).

⁹ Nominum comments at 6-7

¹⁰ Letter from Prof. Nick Feamster, in his personal capacity, and others to Marlene H. Dortch, Secretary, Federal Communications Commission, Docket No. 16-106, filed Aug. 6, 2016 (available at [https://ecfsapi.fcc.gov/file/1080654886605/FCCPrivacyNPRMResearcherExemption%20\(3\).pdf](https://ecfsapi.fcc.gov/file/1080654886605/FCCPrivacyNPRMResearcherExemption%20(3).pdf)).

¹¹ See *Revisions of Part 15 of the Commission’s Rules to Permit Unlicensed National Information Infrastructure (U-NII) Devices in the 5 GHz Band*, ET Docket No. 13-49, 29 FCC Rcd. 4127 (2014); *Clearing the Air on Wi-Fi Software Updates*, Julius Knapp, Chief, Office Engineering and Technology, available at <https://www.fcc.gov/news-events/blog/2015/11/12/clearing-air-wi-fi-software-updates> (Nov. 12, 2015).

¹² *Supra* n. 3.

Nominum appreciates the time and interest of the Commission staff in its services and the potential impact the BIAS Privacy NPRM could have. As Nominum mentioned, it looks forward to a continuing dialogue with the Commission. Please direct any questions to the undersigned.

David Turetsky
Gregory W. Guice

Akin Gump Strauss Hauer and Feld LLP
1333 New Hampshire Avenue, NW
Washington, DC 20036
(202) 887-4565
Counsel for Nominum, Inc.



FCC NPRM

September 12, 2016



Summary

- Nominum
- Nominum Products
- Nominum Architecture
 - Why DNS data is important

Subscribers Are Our Focus

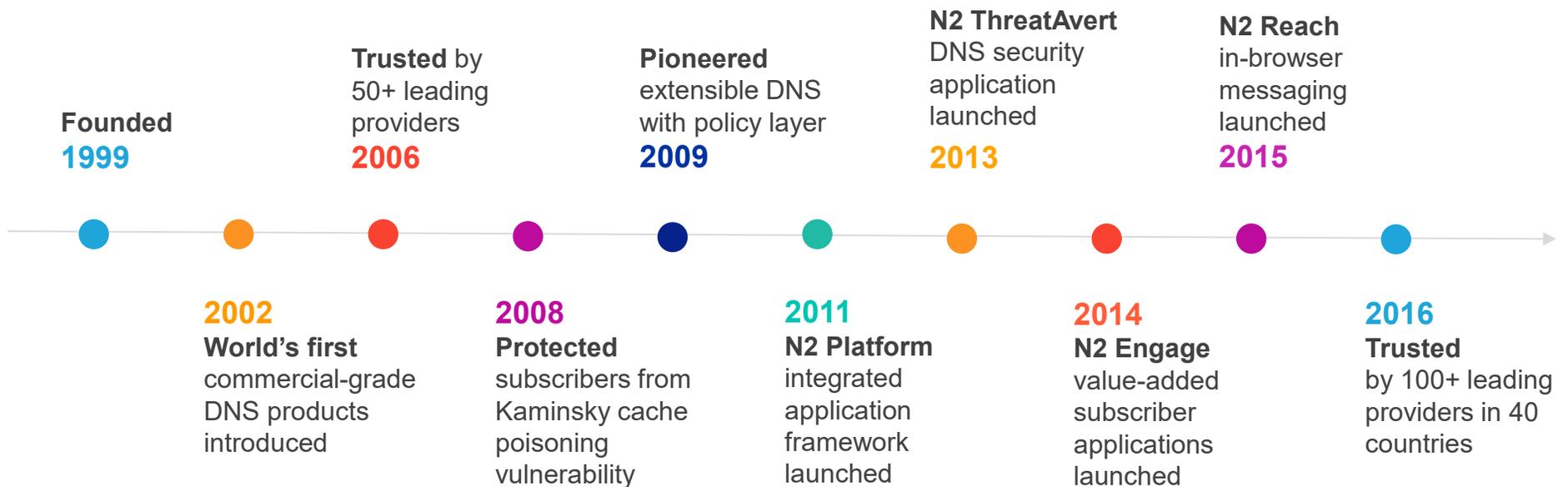
Nominum optimizes the internet experience through DNS.

From performance to personalization, every Nominum solution works *together*.

The result? Teams working in sync to deliver personalized services *faster*.



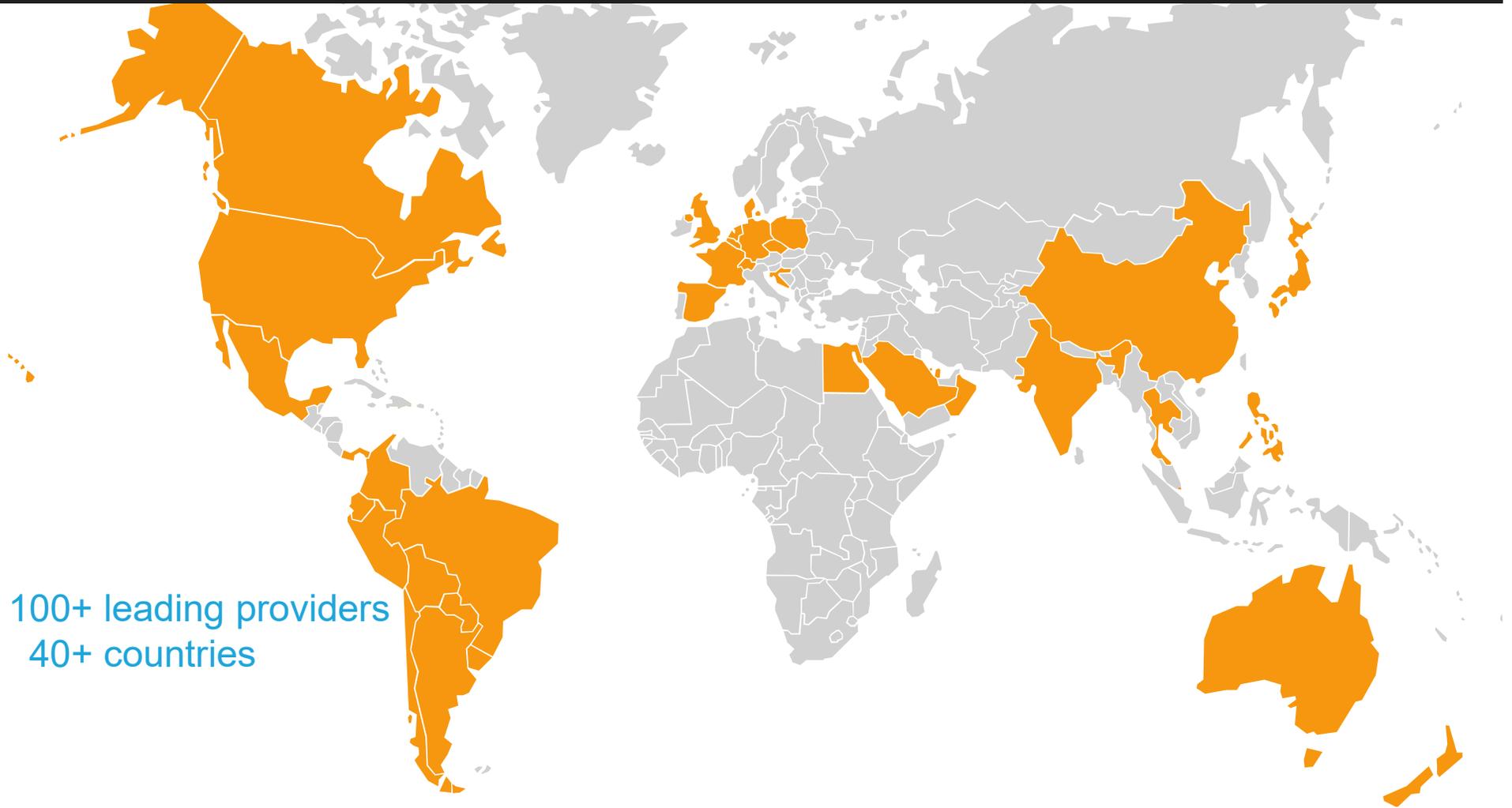
The DNS Innovation Leader



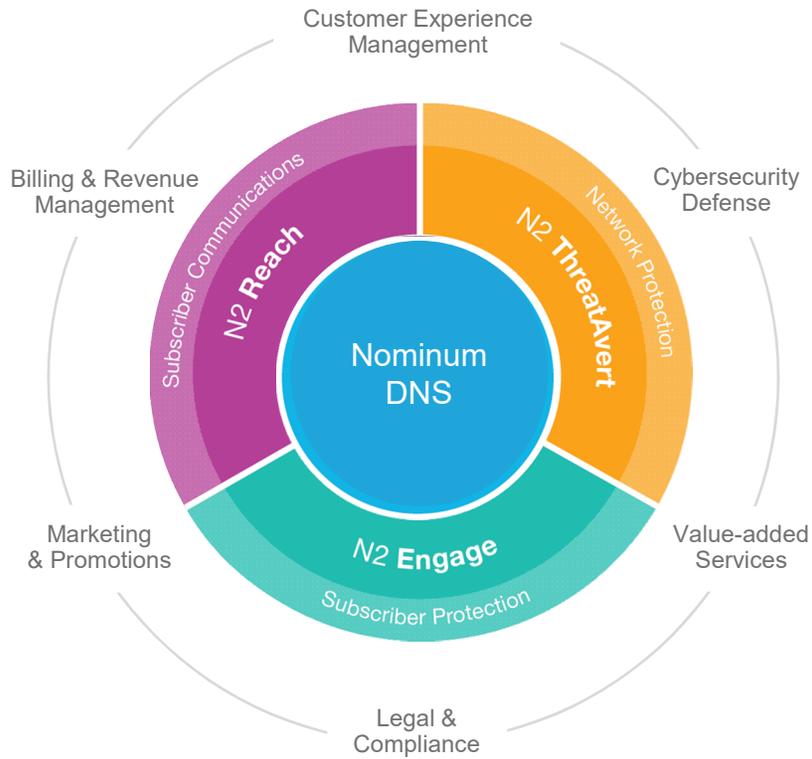


Nominum DNS processes
1.6 trillion queries every day.

More than 100x the
combined daily volume of
Tweets, Facebook likes, and
Google searches.



100+ leading providers
40+ countries



Extensible DNS

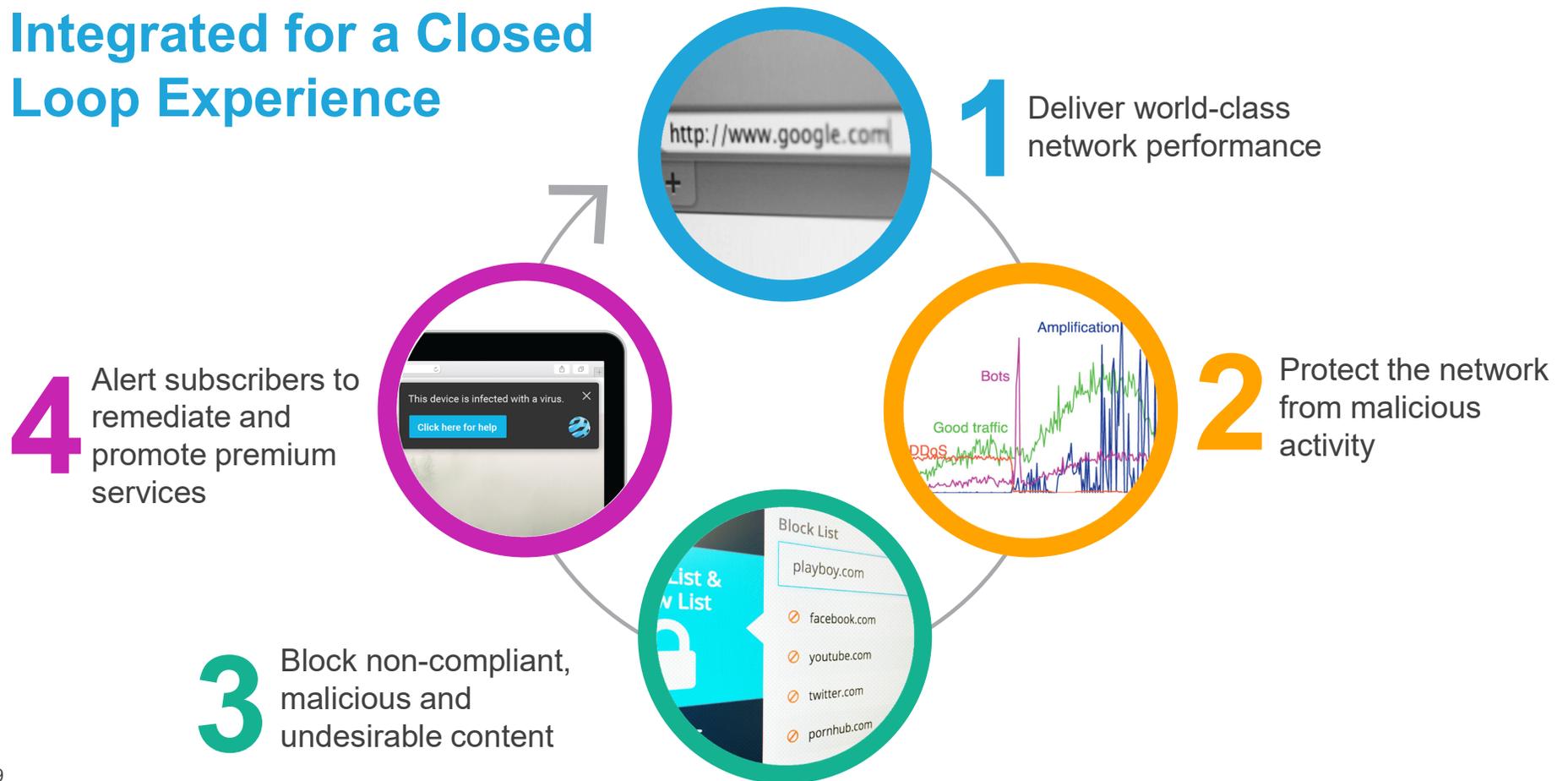
Integrated Applications

Infinite Use Cases

Nominum Products

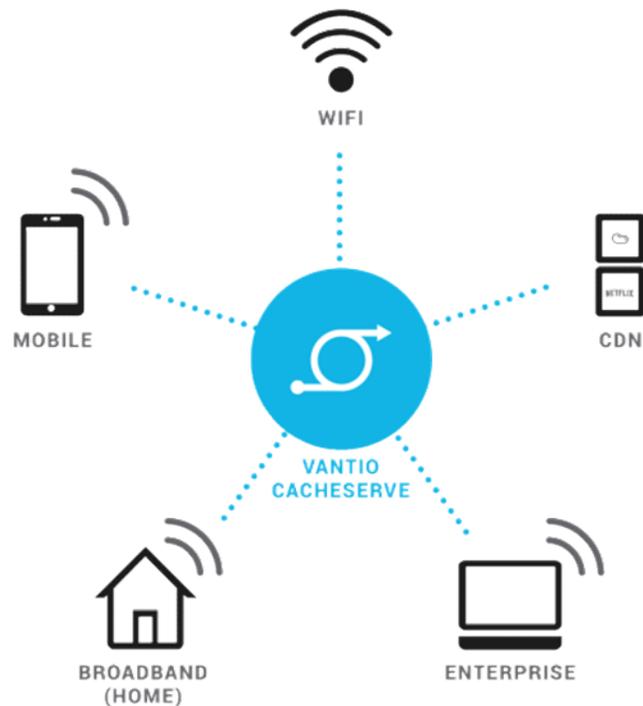


Integrated for a Closed Loop Experience





Industry's Best DNS Resolution



Policy-driven Architecture

Industry-leading policy framework provides security, helps optimize content delivery and is the foundation for additional services.

Flexible Reporting

Real-time logging, aggregation reporting provide visibility into key operational metrics.

Scalable and Future-proof

Over 2 million QPS on commodity hardware allows you to consolidate equipment. Software-based, API-driven solution is NFV-ready.



Protect against DDoS, botnets, DNS tunneling and toll fraud queries



Precision Policies

Finely-tuned filtering blocks malicious queries while allowing good traffic to preserve the online experience.

Backed by Data Science

Nominum Data Science analyzes over 100 billion DNS queries every day to continually update threat lists.

Data Driven Insights

Create reports with ease for insight into all malicious activity, including infected subscribers.



End-to-End Content Control



Content Compliance

Allows compliance with mandates and social responsibility commitments.

Subscriber Safety

Protects the entire household and all connected devices from phishing, viruses, spyware, adware and malware—with a single click.

Personal Internet

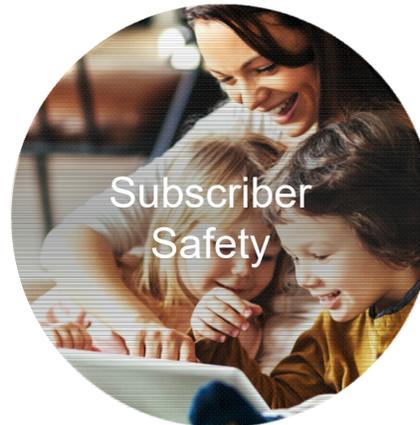
Allow subscribers to choose what internet content is accessible. Tailor access for each family member. Can be deployed household-wide or per device.



A Wide Range Of Uses



- Protect households from illegal content
- Block prohibited online content



- Shield household networks
- Protect subscriber devices
- Protect subscribers from cyberthreats including phishing and malware
- Security breach notifications

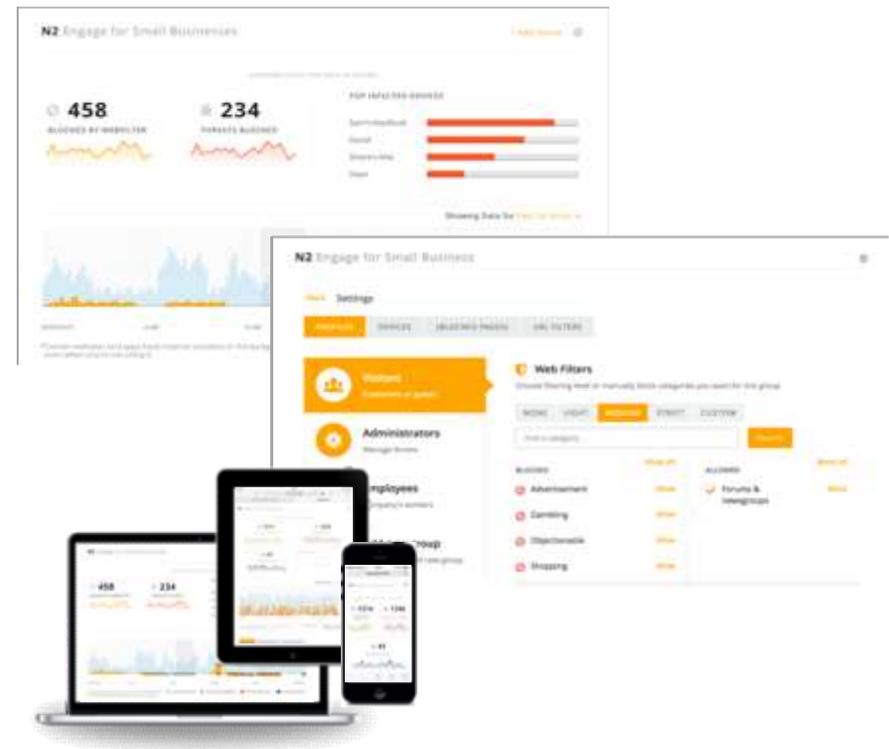


- Enable subscriber-defined content control
- Provide parental controls and monitoring
- Protect children online and alert parents as appropriate



Engage for SMB is ideally Suited for Today's Threats

- N2 Engage for Small Business (Phase I)
 - DNS-based network and device protection
 - Designed for businesses without IT Departments
 - Sold white labeled through carriers
- Robust group policy controls ensure appropriate web access for:
 - Employees
 - Guests
 - Sensitive devices like credit card readers
- Competitive Advantages to ISPs
 - ISPs keep the traffic on their network
 - More competitive price points
 - Easier deployment and lower support costs
- Move up stream to larger enterprise customers



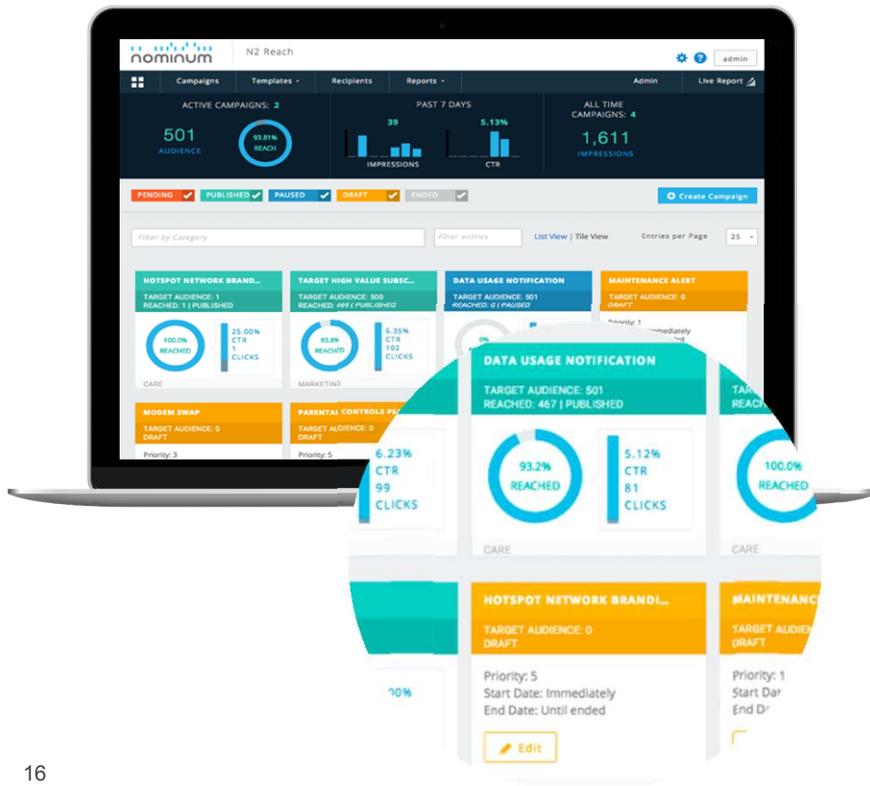
N2 Reach

A powerful communication medium that displays media-rich messages in a subscriber's web browser.





Media-rich, In-browser Messaging



Easy Campaign Creation

Business units can easily design and launch campaigns in minutes without burdening IT.

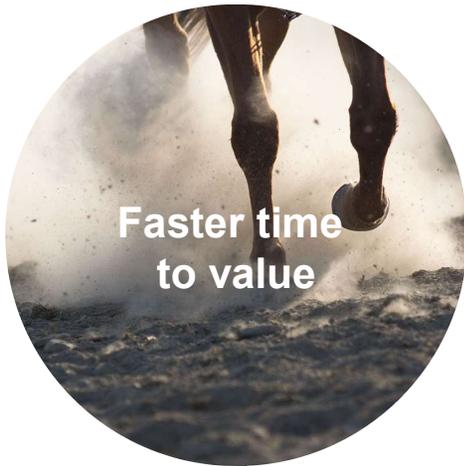
Dynamic and Adaptive

“Set and forget” capabilities automatically add or remove subscribers based on attributes such as billing cycles and data limits.

Measure and Optimize with Ease

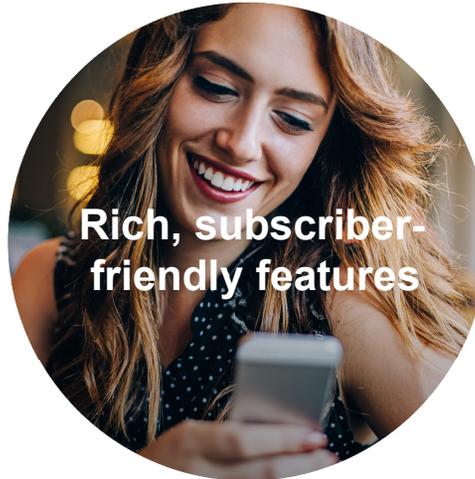
Live dashboard metrics and intuitive reporting help providers fine-tune campaigns for exceptional results.

Summary of Benefits



**Faster time
to value**

Integrated suite allows fast rollout of services without burdening IT



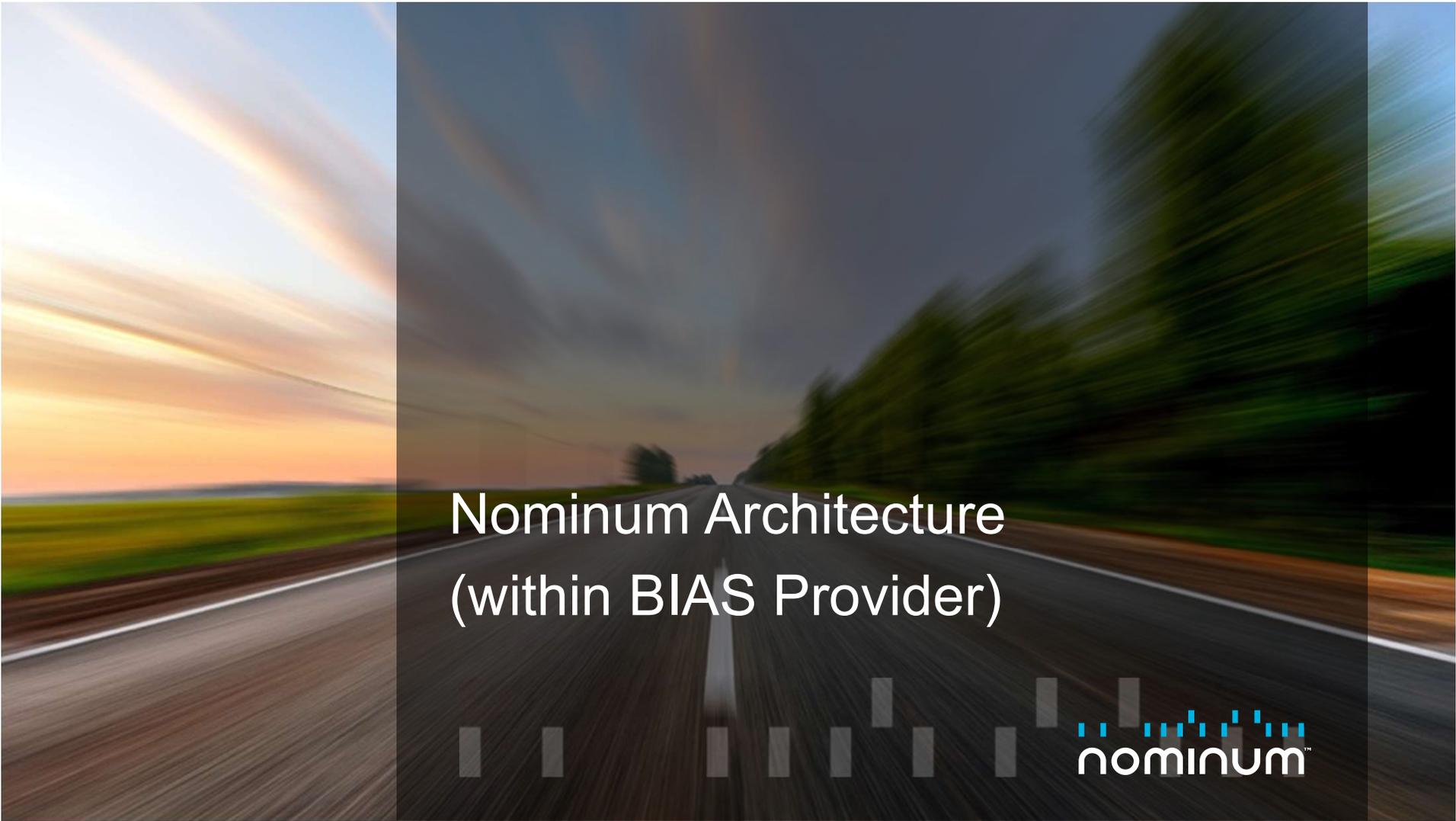
**Rich, subscriber-
friendly features**

Fast and reliable internet, cyberthreat protection, content controls and enhanced communications



**Lower total cost
of ownership**

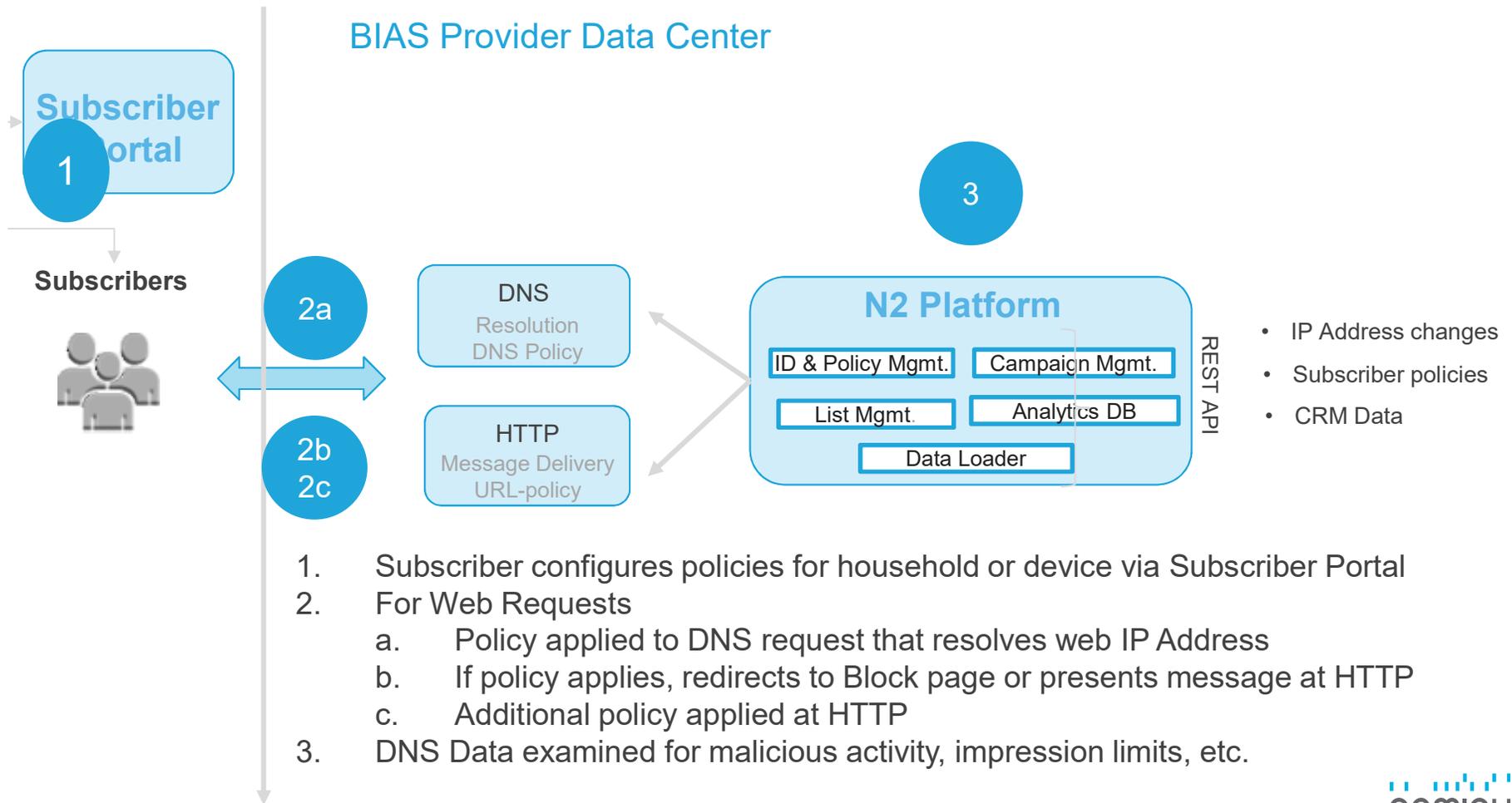
No separate training, integrations, support, troubleshooting, installation, patches or upgrades



Nominum Architecture
(within BIAS Provider)



nominum™



Why DNS Network data is required

- Analyzing networking data (primarily DNS) across the BIAS network is important for the functioning of Nominum products. Some examples include:
- DNS DDoS reflection attacks come from many computers (unknown to their owners).
- Need to understand 'normal' DNS traffic to avoid blocking valid subdomains during a DDoS attack.
- Millions of 'new' domains are queried for from many clients every day. Almost all of these 'new' domains are fraudulent, leading to phishing attacks. These come from all clients.
- 'Ransomware' (e.g. Locky) use new 'seeds' regularly. We detect these seeds so that we can block C&C communication. These can come from any client.
- Analysis of DNS traffic yields better classification for parental controls.
- Analysis of messaging traffic ensures that messaging functions correctly in the face of a changing web.

How DNS Network data is collected

- DNS Data is collected in real-time from CacheServe
- Aggregated at the N2 platform level
 - Raw DNS Data is aggregated into 10 minute chunks
 - Raw DNS Data is expired
 - IP Addresses are anonymized. ISP owns the keys
 - Data never leaves the control of the ISP
- The platform is designed to enable specific analyses for the Nominum products