Nominum Closes the Loop with 'Security as a Service' - A Network-based Paradigm

Networks and Service Platforms

Report Snapshot

Cyberthreats have evolved and become costly. A new approach is needed.

Hackers and cybercriminals no longer simply attack web sites and spread malware and viruses directly. Phishing attacks capture user data and software for future use; botnets take control of user devices to make them active participants in a threat network; and compromised IoT devices participate in Distributed Denial of Service (DDoS) attacks so diffuse that they look like user traffic - until it is too late.

The latest WannaCry and Petya based ransomware attacks are just some of many that exemplify the cost of SMB attacks that has more than tripled over the last 4 years.

To 'Close the Security Loop' we need a new Paradigm.

A 'Network Centric' paradigm that detects threats and protects both Small and Medium Businesses (SMBs), Public Wi-Fi users and the network itself.

DNS based network solutions can block the growth of botnets and the spread of ransomware centrally rather than relying on busy SMB end users - who have no IT in-house staff - to keep software up to date. For CSP Managed Security as a Service (SECaaS) can pre-empt attacks before SMB end users are even aware they have a problem.

While Domain Name Systems (DNS) have long been used to block DDoS and network-based threats, they can now be the best way to offer 'SECaaS' to safeguard SMBs from cyberthreats as they emerge in real time.

Networks

www.strategyanalytics.com

July 2017

Sue Rudd
email: srudd@strategyanalytics.com

Executive Summary

SMB Security Demands a new 'Network-centric' Paradigm

Cyberthreats have evolved and become costly. A new approach is needed.

Hackers and cybercriminals no longer simply attack web sites and spread malware and viruses directly. Phishing attacks capture user data and software for future use; botnets take control of user devices to make them active participants in a threat network; and compromised IoT devices participate in Distributed Denial of Service (DDoS) attacks so diffuse that they look like user traffic – until it is too late.

The May 2017 'WannaCry' and June 2017 Petya-based ransomware attacks are just a few of many that have escalated the cost of Small and Medium Business (SMB) attacks by more than threefold over the last four years.

We need a New Paradigm that Closes the Security Loop

A new 'Network-centric' paradigm could detect threats and protect both Small and Medium Businesses (SMBs), Small Office Home Office (SOHO) users and the network; and in addition, block the growth of botnets and the spread of ransomware centrally. SMBs will never be fully protected if they rely on busy users to always keep software up to date.

New Opportunity for CSPs to offer SMBs Security as a Service (SECaaS)

Exacerbated security attacks and the need for a network-based security approach have created an opportunity for Communications Service Providers (CSPs) to offer Security as a Service (SECaaS) to *preempt threats before end users are even aware they have a problem*. While Domain Name Systems (DNS) have long been used to block Distributed Denial of Service (DDoS) and network-based threats, they can now offer 'SECaaS' to safeguard SMBs from cyberthreats as they emerge in real time while preventing unprotected SMB devices from joining network-based attacks.

CSPs can leverage their existing CAPEX Investment in DNS infrastructure to offer managed SECaaS at a price point that is attractive to millions of SMB subscribers.

This paper describes:

- Dynamic threat landscape
- Requirements to address security threats
- Network-based solutions to meet network-based threats
- DNS-based solutions that leverage CSP strengths
- SMB market opportunity for CSP Managed Security Service
- How CSPs are positioned to offer SMB Security as a Service (SECaaS)

Table of Contents

1. Introduction

Competitive pressures are forcing Communications Service Providers (CSPs) to evolve beyond connectivity and offer incremental value-added, hosted and managed services to sustain revenue growth. Security services are now becoming a candidate for a CSP managed service as awareness of the need for security protection has skyrocketed following recent Internet attacks.

Threat trends and strong alignment with large customer segments have created an opportunity for CSPs to offer a foundational layer of web protection for every Internet access. CSPs can provide a previously unavailable level of web security to reduce the risk their customers face, without imposing any new configuration or management burden.

Stories about ransomware and machines that infiltrate systems to destroy data have spread rapidly around the world. The number of phishing attacks reached an all-time high in 2016 according to the Anti-Phishing Working Group.[1] Phishing is the basis for unwanted software downloads that lead to monetary or data losses. Botnets are escalating too; bots lurking on devices are trained to find valuable data like credit card information, login or other credentials for financial transactions, and can quietly export those inputs for 'monetization'.[2]

Traditional security solutions such as endpoint client software or expensive Universal Threat Management (UTM) appliances are challenged to keep up with dynamic web threats that change constantly to avoid detection. Those approaches are not well-suited for protecting the rapidly expanding base of botnets and Internet-connected 'things' that are being installed everywhere. The right endpoint protections are often not even available for many devices and hardware. As a result, a number of Over the Top (OTT) cloud-based security companies have emerged to offer their cloud network for managed security services.

CSPs are in fact exceptionally well-positioned to offer cloud-based security solutions *themselves* since network-based solutions leverage a CSP's deployment and operating strengths. CSP services also align well with CSP customer segments like Small and Medium Businesses (SMBs) that can be poorly served by large enterprise firewall and other enterprise security vendors.

CSPs now have an opportunity to leverage existing relationships to target two markets:

- ***Small and Medium Businesses (SMBs)*** often lack IT resources and security expertise, yet nearly three-quarters (73%) of senior managers in these companies report cybersecurity as a high priority[3] and are looking for ways to reduce their risks. Capital constraints, however, limit what they can spend, but a subscription model with a modest incremental managed security service fee on a monthly bill could overcome these budgetary barriers.

[1] Anti-Phishing Working Group Global Phishing Survey: Trends and Domain Name Use in 2016
http://docs.apwg.org/reports/APWG_Global_Phishing_Report_2015-2016.pdf

[2] Botnets overshadowed by ransomware (in media)
https://www.welivesecurity.com/2017/06/07/botnets-overshadowed-ransomware-media/

[3] Cyber Security Breaches Survey 2017
https://www.gov.uk/government/statistics/cyber-security-breaches-survey-2017

- Public Wi-Fi hotspots also want to ensure Wi-Fi users aren't exposed to web threats or undesirable content when working remotely. Public Wi-Fi hotspot deployments are usually remote facilities, e.g. storefronts, with the same constraints as SMBs, i.e. no IT expertise, limited budgets, etc.

The new network-based security approach described in this paper will allow CSPs to deliver an essential foundational layer of protection 'as a service' for these use cases. CSPs can today create network-based subscriber security service experience and outflank the OTT cloud-based security players. Because it is lightweight, easy to use, and cost-effective, new DNS-based managed security services can be positioned as necessary for every Internet access connection.

2. Dynamic Threat Landscape

Today's cyberthreats are characterized by innovation, and are designed to propagate, and bypass detection and controls by continually 'changing their complexion.' No one is immune because they spread randomly using software flaws or social networks. SMBs are especially vulnerable because they frequently do not have a dedicated IT professional on site. As of June 2016 the Ponemon Institute reported that "55 percent of SMBs say they experienced a cyberattack in the past 12 months and 50 percent of SMBs had a data breach during the past year."[4]

The Internet of Things (IoT) is emerging and there is every reason to believe more and more 'things' will get 'smart' and 'connected'. IoT devices have a wide range of capabilities that can be 'hijacked' to create diverse security vulnerabilities. These include:

- ***Intelligence*** - processor/memory/networking stack
- ***Instrumentation*** – cameras, microphones, speakers, sensors
- ***Susceptibility to compromise*** – NATed (Network Address Translation) - always-on or polled
- ***Accessibility*** - open ports and agents, unpatched vulnerabilities

This massive pool of IoT devices creates a new playing field for attackers. The potential for harm was demonstrated in October 2016 when a Mirai botnet delivered the largest DDoS attack in history leveraging a relatively small number of 'dumb' devices.[5] Attackers have begun to explore IoT vulnerabilities as part of the 'weaponization of IoT devices'.[6]

The cost of these attacks for SMBs is escalating. The FBI estimated that the total cost of ransomware in the U.S. was $24 million in 2015 and increased to $209 million in just the first three months of 2016.[7] Those numbers could be conservative since many transactions are never reported due to business concerns about public disclosure. The Small Business Association survey referenced above also showed that attack costs for SMBs averaged nearly $9,000 with losses from hacked bank accounts averaging slightly less than $7,000. Since SMB cost of capital is often high, these losses are even more painful.

[4] http://www.ponemon.org/blog/smbs-are-vulnerable-to-cyber-attacks

[5] https://www.malwaretech.com/2016/10/mapping-mirai-a-botnet-case-study.html

[6] https://www-01.ibm.com/common/ssi/cgi-bin/ssialias?htmlfid=SEL03128USEN&

[7] http://www.reuters.com/article/us-usa-cyber-ransomware-idUSKCN0X917X

3. Network-based Solutions to Meet Network-based Threats

To meet these new network-based threats and the risks introduced by mobile devices, a new strategy is needed. SMBs cannot wait until an attack reaches end user PCs, tablets or smartphone devices and hope that each termination will respond appropriately to promptly block a threat, stop an attack or refuse to join a botnet. SMBs need to preempt threats before they jeopardize end user devices, applications or corporate databases. A new approach that handles the problem from the network perspective is required, SMBs cannot rely on millions of busy end users to update software that would classify, isolate or redirect the incoming flood of attacks on every different device.

IT security professionals and their Internet and Communications Service Providers (ISPs and CSPs) need to work together to:

- **Stop attacks at a distance** as they develop
- **Block emerging threats and attacks within seconds of identifying them,** e.g. by rejecting unregistered *phishing* URLs as fast as they pop up rather than relying on end users to avoid clicking on bad links
- **Assume that some users will always become infected** and automatically prevent them from spreading an infection, virus or ransomware software across the network
- **Prevent unknowing users whose resources have been hijacked from participating in botnets** and becoming threats themselves

Network-based threats demand we scan proactively for threats and attacks as they arrive in the network. Service providers operating DNS network-based security services can see everything that is coming in real time and with the right software instantaneously trigger network-based solutions to fight ***both network- and end user-originated attacks***.

DNS is the 'always on' threat protection mechanism that can close the security loop by detecting and preempting threats to SMBs or other end users even before they are aware they have a problem.

4. Requirements to Address Today's Attacks

As attackers innovate, CSP and SMB defenses must adapt in parallel. This demands four key requirements:

1. **Defenses must respond fast to fast-changing malware**

   SMBs need simple ways to reduce their exposure to web attacks. Enforcement points must be network-based so that they are always available and updated in real time – i.e. no "Decline" or "Later."

   Threat feeds should be streamed so that the latest protections are always active.

   Real-time enforcement is essential to narrow the window of viability for attacks and reduce the success rate of attackers.

2. **Defenses must be device-agnostic**

   The diversity of individual devices renders client-based security software protection impossible or impractical.

   A common layer of protection is required to insulate the multitude of diverse devices that are connected to networks to minimize risk exposure. This common layer of defense can not only block threats, but also offers a useful baseline so that subtle deviations from normal behavior are detected instantly across all categories of devices.

3. **Security upgrades need to be simplified, automated or eliminated**

   End users frequently ignore, defer, or disable automated client or application updates that may impact their security. Even SMB staff charged with managing security may delay those efforts in favor of urgent revenue-generating business activity.

   Business applications and servers must all have specialized protections and management, but minimizing dependencies on end user and IoT devices will reduce SMB staff load and ensure more robust, continuously updated protection.

   Users must be made aware of malicious activity that is within their 'span of control.' When infections are discovered on end user devices, or users attempt to navigate to known malicious destinations, e.g. websites that download malware, they need to be warned instantly of the dangers of proceeding and prompted with suggestions for remediation. Messages not only alert subscribers but motivate appropriate immediate action.

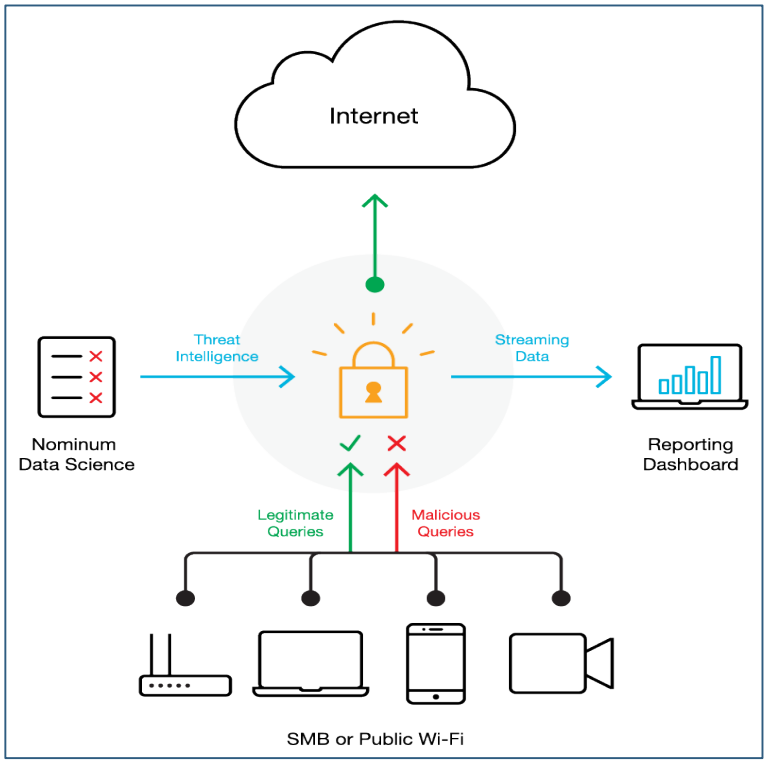
CSPs are uniquely positioned to meet these requirements with DNS to enable 'Closed Loop' Security.

5. DNS-based Defenses Enable Closed Loop Protection

Domain Name System (DNS) can provide the 'foundational layer of protection' to address the SMB and public Wi-Fi web security challenges described above. Nominum has recently announced its Closed Loop solution for CSPs and their SMB customers that can be deployed in fixed, mobile, and converged networks as well as on public Wi-Fi networks. This solution – shown in the diagram below – relies on intelligent filters and policies that are applied to DNS queries generated by SMB subscribers equipped with the service.

Since both malicious and legitimate applications use the DNS it is essential to identify the presence of malicious activity with real-time threat intelligence feeds and to process legitimate DNS queries normally. As malicious queries are flagged by the Nominum solution, special treatment is immediately applied. For example, a user query to a phishing domain will be redirected to prevent the user from going to that phishing site. Alternatively, a botnet Command and Control (C&C) query will be immediately blocked to prevent botnet malware from getting instructions. Virtually every device and application uses the DNS so nearly all devices and applications can be protected with minimal user action. Because DNS is already in the real-time flow, no additional latency is introduced for the secure query processing and the user experience is maximized.

Exhibit 1. DNS is the Most Efficient Place to Match Queries to Threat Intelligence

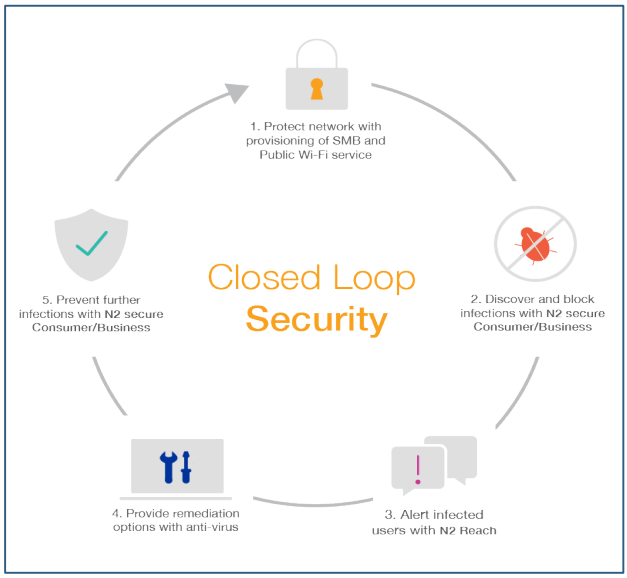


Source: Nominum

As indicated in the chart above, managing security via DNS queries sent from applications and devices is the most efficient and effective way to identify malicious activity. Since all traffic requires a DNS lookup, malicious activity can be detected by comparing incoming DNS traffic against all known threat feeds in real time. Blocking malicious queries stops attacks dead.

The complete Closed Loop solution is depicted in the diagram below. It consists of tightly integrated applications that protect SMBs and Wi-Fi users from web threats while a parallel messaging application keeps them informed and engaged.

Exhibit 2. Complete Security Demands a Closed Loop Solution



Nominum's DNS-based Closed Loop solution offers a new foundational layer of protection for every SMB Internet access connection. Tightly integrated applications like this that leverage existing DNS infrastructure are cost-effective for CSPs to deploy and end users to use, while they keep subscribers informed and engaged.

Five Steps to a Closed Loop Solution

Below we summarize what occurs at each of the steps shown in the chart above.

Exhibit 3. Five-step Process

Step	*Functionality*	*Description*
1.	***Protect the Network***	SMBs or public Wi-Fi locations are provisioned with either cloud-based or on premise DNS servers and integrated to connect each new site.
2.	***Discover and Block Infections***	Activated subscribers are protected as all DNS queries they send as part of their normal web browsing/internal IT experience are evaluated by a Nominum DNS resolver. DNS tracks malware or bots that steal valuable personal information in real time. • Protections are network-based so there is no client software to be installed. • Completely automated, every device in business is covered and subscribers never have to deal with updates. • Service is always-on with up-to-the-minute threat information. • SMBs and public Wi-Fi administrators can use a graphical portal to set preferences on content allowed at workplaces and remote locations/homes.

Exhibit 3. Five-step Process (Continued)

Step	*Functionality*	*Description*
3.	***Alert Infected Users***	If a device is identified as infected, e.g., after visiting an unprotected network, an integrated application will notify the infected user. CSP-branded in-browser messages personalized for every SMB or public Wi-Fi customer are sent to reflect specific details of the infection. Tools for managing these messages are built into the software.
4.	***Provide Remediation Options***	Links to remediation tools and advice included in end user messages. Providers present branded web pages recommending tools from partners. Message pages point to advice and other information.
5.	***Prevent Further Infections Proactively***	To deter email or web-driven phishing, users are notified with an in-browser message before they attempt to navigate to malicious destinations where malware or ransomware may be lurking. Messaging sent to end users while they're actively engaged. Preventative approach saves time and money and reduces stress.

Source: Nominum

Automated dynamic threat lists for these Closed Loop services are based on intelligent algorithms developed by Data Science experts at Nominum and updated in real time as threats are identified around the globe. Additional lists can be created to automatically filter unwanted content.

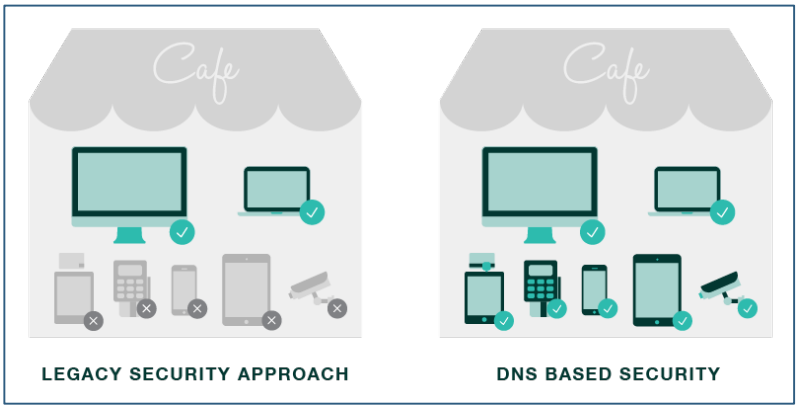
Nominum processes over 100 billion DNS queries per day and applies analytics to identify new threats quickly and to derive unique insights for algorithm development. A sophisticated, multi-step validation process minimizes false positives that can significantly increase operational overhead and reduce subscriber satisfaction.

Deploying SECaaS in CSP Cloud

CSPs can deploy the infrastructure needed to support the service within their own facilities, in the cloud, or hosted as a managed service. DNS servers used by SMBs on the customer premise or at public Wi-Fi sites can be operated in the cloud as part of the managed service.

The alternatives for CSPs that do not offer subscribers a 'Closed Loop' security solution are less efficient, less effective and more limited in scope. For example, one major drawback of today's endpoint security solutions is that protection must be applied to every individual device, rather than to the entire network and all associated devices. Endpoint solutions leave holes in the network and firewalls explicitly allow many 'port holes' that cybercriminals can take advantage of. On the other hand, network level DNS security requires no software downloads, no port configuration and no user-initiated updates – and still every device on the network is automatically protected.

Exhibit 4. DNS-based Security Covers Every Device Automatically



Source: Nominum

Nominum's Closed Loop DNS-based approach therefore delivers a new foundational layer of protection for every Internet access connection. CSPs that deploy it will have a sustainable competitive advantage that is:

- ***Lightweight*** - No client software means every device is protected automatically. No on-premise hardware means less CAPEX and OPEX for CSPs.
- ***Personalized*** - Each workplace or public Wi-Fi administrator can customize the service to match unique needs without any major configuration or operational burden on the CSP.
- ***Simplicity -*** SMBs or Wi-Fi administrators can set up the service in minutes via a portal.
- ***Engaging*** - Integrated messaging app creates opportunities to inform and engage subscribers.
- ***Agile*** – DNS-enhanced platform ensures rapid time to market with continuing upgrades for CSPs based on tightly integrated, software-only applications, deployable in the cloud, 'as a service' or as a combined CPE and 'as a service' solution
- ***Automated*** -Threat detection and protection enforcement points are automatically and instantaneously updated with the real-time inputs.
- ***Scalable*** - DNS control plane-based processing analyzes all queries without introducing additional latency and was designed from the start for carrier-scale operations.

6. SMB Markets Offer Significant Managed Service Opportunity for CSPs

As CSPs move to offer cloud-based managed services, one source estimates that the global opportunity for Telecoms Managed Services, including *Managed Data Centers, Networks, Data and Information, Mobility, Communications and Managed Security,* is likely to be almost $12 billion in 2017 and will grow at a Compound Annual Growth Rate (CAGR) of 13.7 percent to over $22 billion by 2022.[8]

Separately, it is estimated that the total market for Managed Security Services (MSS) could grow to almost $41 billion by 2022, increasing at a CAGR of 16.6 percent from last year.[9] Even if telecoms capture less than one-third of the total MSS market, this represents a huge opportunity. And cloud-based MSS are expected to be especially attractive to SMBs that have the potential to drive a substantial share of that revenue.

SMBs Need Managed Security Services (MSS)

A July 2016 report by Osterman Research 'IT Security at SMBs: 2016 Benchmarking Survey' describes the results of a survey of SMB security managers and indicates that 55 percent of SMBs have an IT staff of three or fewer people, and 29 percent have an IT staff of one or less. This means SMBs either contract for expensive IT security people or purchase security-as-a-service or forgo protections altogether. The report notes that "while a slight majority of SMBs reported their current web security capable of stopping malware infiltrations, fewer than half of respondents expressed confidence in their ability to protect against the most advanced threats like ransomware, phishing and targeted attacks, or stopping a breach of sensitive data." The table below shows IT managers' level of concern compared to their assessment of their current protections. It also indicates concerns about managing access to content at work that can undermine productivity, consume bandwidth, and create HR exposure.

Exhibit 5. Comparison of SMB Concerns vs. Perceived Level of Protection

Issue	Perceived Protection	Level of Concern	Security Gap Index
A breach of sensitive or confidential data	45%	70%	1.56
Phishing attacks	47%	68%	1.45
Targeted attacks/zero-day exploits	45%	65%	1.44
Malware infiltration through web surfing	55%	74%	1.35
Ransomware	49%	65%	1.33
Malware infiltration through email	57%	75%	1.32
Malware infiltration through SSL web surfing	50%	60%	1.20
Botnets	44%	52%	1.18
Malicious activity from insiders	45%	50%	1.11

Source: Osterman Research Inc. 'IT Security at SMBs: 2016 Benchmarking Survey'

[8] Research and Markets: http://www.businesswire.com/news/home/20170524005464/en/

[9] Allied Market Research: https://www.alliedmarketresearch.com/managed-security-services-market

7. CSPs are Well-positioned to Offer Closed Loop Security

Recent attacks have greatly increased awareness of security, and as SMBs recognize they need outside help, Managed Security Services (MSS) will become a significant market.

CSPs – both telecoms and cable operators – are able to service a large number of relatively small customers very efficiently, and an attractive bundle of high-speed bandwidth, mobile services Wi-Fi and MSS should allow them to dominate the SMB market for SECaaS.

Mobile Users Want to Buy Security Services from their Service Provider

A recent survey by Allot indicates that 61 percent of their global end user respondents said they would like to buy a mobile security service from their service provider even though only 11 percent currently pay for mobile protection. "The gap between demand and fulfillment for mobile security services presents a significant and immediate opportunity for CSPs." See Exhibit below.

Exhibit 6. Mobile Security Buyer's gap by Region

	Europe	Australia	Asia	North America	LATAM	Africa
Demand	67%	60%	60%	63%	59%	50%
Fulfillment	15%	13%	11%	11%	8%	5%
Gap	52%	47%	49%	52%	51%	45%

Source: Allot

Six Out of 10 Users Would Look to CSPs for a Security Solution

When asked who they would like to buy a security solution from, six out of 10 opted for their CSP.

Exhibit 7. Percentage of End Users Who would Buy Mobile Security Services from their CSP

Europe	Australia	Asia	North America	LATAM	Africa
67%	60%	60%	63%	59%	50%

Source: Allot

8. Conclusion - Business Benefits for CSPs and their SMB Customers

DNS-based managed security solutions not only provide significant IT benefits for CSPs and their SMB customers, they also deliver significant business and operational benefits to both parties. These are summarized below:

Significant Benefits for CSPs

The DNS-based SECaaS offers significant benefits for CSP operations and service delivery including:

- Control of a complete security solution
- Real-time monitoring and control of live security threats
- Configurable and flexible options that can support variable CSP service offers
- Full visibility into both user and network events
- Managed Service Option for SMBs and SoHo users and even consumers
- Ongoing support from Nominum Data Science experts for updates on malicious sites/activities

SMBs Benefit from Managed Security as a Service (SECaaS)

SECaaS ensures that SMBs have:

- Instantaneous user communications and interaction
- 'Inherent' security
- Simple activation and updates - 'No Assembly Required' and no software to install or update repeatedly
- Protection for all devices and all network access connections

Overall Benefits of Delivering Security 'From the Network'

Several unique overall benefits accrue from this network-centric approach.

- ***Breadth of Security Coverage:*** All users and all devices anywhere over any access technology are automatically protected by software that is instantaneously updated for the latest threats.
- ***Depth of Protection:*** More timely, reliable and robust than traditional device app software that depends on users for upgrades.
- ***Cost-effective for both CSPs and their SMB Customers:*** No expensive security platform or separate probes are required for the CSPs. SMBs will avoid paying expensive IT staff/contractors as well as save on the cost of acquiring, maintaining and updating expensive CPE software. Costs are projected to be at 40-50 percent of traditional customer-based solutions to create the most affordable premium SMB solution available.

The Bottom Line

DNS-based Security as a Service allows CSPs to deliver 'Always On,' instantly threat-aware, highly reliable yet totally transparent proactive protection for SMBs.

Appendix A. Differentiators for DNS Network-based 'Security as a Service'

Six Key Differentiators - Simplicity, Scalability, Service Offer, 'See Through', Seamless and Simultaneous Communication

Below we summarize the six key differentiators that make DNS-based SECaaS the preferred solution for a CSP managed service for SMBs.

Exhibit A.1. DNS-based SECaaS - Six Differentiators that Deliver Unique Benefits to CSPs and SMBs

	Six Differentiators	Delivered Benefit for CSP	Delivered Benefit for SMB
1.	*Simplicity*	▪ Reduces complexity of cloud and SMB security package solutions	▪ Makes personal control and lightweight solution simple yet powerful
2.	*Scalability*	▪ Reduces linearly increasing firewall costs ▪ Scales complex network security mechanisms and number of events processed seamlessly	▪ Scales threat and attack support dynamically as needed 'on demand'
3.	*Service Offer*	▪ Service bundle options make service 'sticky' and reduce churn for CSPs	▪ Security bundle is attractive for SMBs that can add options in future - e.g. customer/guest Wi-Fi security & HTTPS proxy termination
4.	*'See Through'*	▪ CSPs have 'see through' visibility and big data analytics for threat and attack handling as well as subscriber awareness and personal profile analytics	▪ Everything is transparent to the SMB and its end users ▪ 'Opt-in' for analytics options
5.	*Seamless*	▪ SECaaS operates cross fixed, mobile and Wi-Fi access networks	▪ Authentication and blocking operate anywhere locally, regionally and potentially globally ▪ Secure Wi-Fi/hotspot access for SMB and shared/public Wi-Fi sites ▪ Secure guest Wi-Fi on business sites ▪ (Future) Secure roaming for employees on untrusted Wi-Fi or across service providers - with DNS roaming agent and/or redirection to monitor inputs from other DNS platforms
6.	*Simultaneous Communication*	▪ Two-way Interaction can be initiated with customers as soon as threat is detected	▪ SMB has tools for proactive interactive problem resolution and communication with CSP

Source: Strategy Analytics Networks and Service Platforms

These six key differentiators allow both telecoms and cable CSPs to compete not only with traditional app and firewall-based competitors but also with OTT and cloud managed service providers.