Independent market research and competitive analysis of next-generation business and technology solutions for service providers and vendors

HEAVY READING WHITE PAPER

Security-as-a-Service in the Carrier Cloud: How CSPs Can Capture the SMB Opportunity

A Heavy Reading white paper produced for Nominum

AUTHOR: JIM HODGES, PRINCIPAL ANALYST, HEAVY READING

INTRODUCTION

The ongoing adoption of cloud computing by communications service providers (CSPs) continues to fundamentally reshape their business models and technology strategies on several levels. One such area that is garnering significant attention is the impact of the cloud on security services. This is because security services and the vital tools they encompass can be empowered through the adoption of a carrier cloud model. This, in turn, better positions CSPs to meet the demands of their customers, including those in the small to medium-size business (SMB) market segment.

The timing of this migration is optimal, since many SMBs now recognize the threats they face and realize that given their limited IT budgets and lack of security expertise, CSPs are well positioned to protect them from cyberattacks.

While the opportunity for CSPs is significant, many are hesitant to make a move in this area because they want to ensure they can address SMBs' needs and maintain control of the service in a carrier cloud. We believe the answer lies in focusing on the implementation of a seamlessly integrated suite of security-as-a-service (SECaaS) capabilities that make it simple for SMBs to adopt services and operationally efficient for CSPs to deploy and manage them at any scale.

Accordingly, this paper examines the business opportunities associated with cloud-based SECaaS for SMB customers, as well as the technical and architectural considerations that CSPs must embrace to create a cohesive and viable SECaaS delivery model that allows them to maintain control.

In addition, this paper discusses the impact of the changing threat landscape on SMBs, as well as the opportunities for CSPs to address SMB requirements through the introduction of SECaaS managed services. Further, the paper documents the interworking of the Domain Name System (DNS) and Big Data and Analytics (BDA) systems to deliver robust and effective SECaaS.

SMB THREAT LANDSCAPE SPELLS CSP OPPORTUNITY

With news reports regularly covering ransomware exploits that extract tens of thousands of dollars from innocent victims, such as hospitals, or sophisticated phishing schemes that capture financial accounts, SMBs are increasingly aware of the cybersecurity threats they face.

To substantiate, the U.K. government recently released a Cyber Security Breaches Survey with several important findings:

- Senior managers in nearly three quarters (73%) of micro/small businesses say that cybersecurity is a high priority.
- 45% of all micro/small businesses having identified a cybersecurity breach or attack in the last year.
- Micro/small businesses are less likely than medium/large firms to have cybersecurity measures in place, such as formal policies (32% vs. 61%) or cybersecurity training for staff (19% vs. 47%).

The report concludes that even the smallest businesses of two to nine employees are targeted by attacks, likely because reconnaissance is automated and indifferent to the size of an organization.

Research in the U.S. offers similar findings. For example, an article in CIO magazine reported the following:

- SMBs are a lucrative and vulnerable victim for cybercriminals simply because many of them are not attentive to the steps needed to protect themselves.
- The average direct cost to a small business for a single attack in 2013 was almost $9,000, excluding brand damage and other soft costs.
- SMBs incur nearly four times the per-capita costs of cybercrime than larger firms.

Although some of these findings are a few years old, the problem has continued to grow.

While these statistics only cover the U.S. and U.K., there is no reason to believe that SMB security exposure is different in any other country, since Internet-based attackers do not respect boundaries. As a result, CSPs worldwide have a significant opportunity to extend existing customer SMB relationships to upsell SECaaS.

While the market appeal and acceptance of SECaaS is growing year over year, it's important to assess implementation alternatives. One option that is getting more attention recently is DNS-based security services. DNS is a foundational protocol; virtually every application depends on it to initiate client/server transactions, including both legitimate applications (such as email, customer relationship management, databases and more) and malicious applications (such as phishing and malware). Due to this inherent visibility into every legitimate and malicious transaction, DNS occupies an excellent vantage point.

With the addition of simple policies to decide how individual DNS queries should be handled, it's possible to implement extremely efficient security services: legitimate DNS queries can be processed normally, while malicious queries are flagged for special treatment. DNS also lends itself to cloud deployments, since properly-designed software does not need any specialized packet processing; clouds built with commodity hardware deliver acceptable performance.

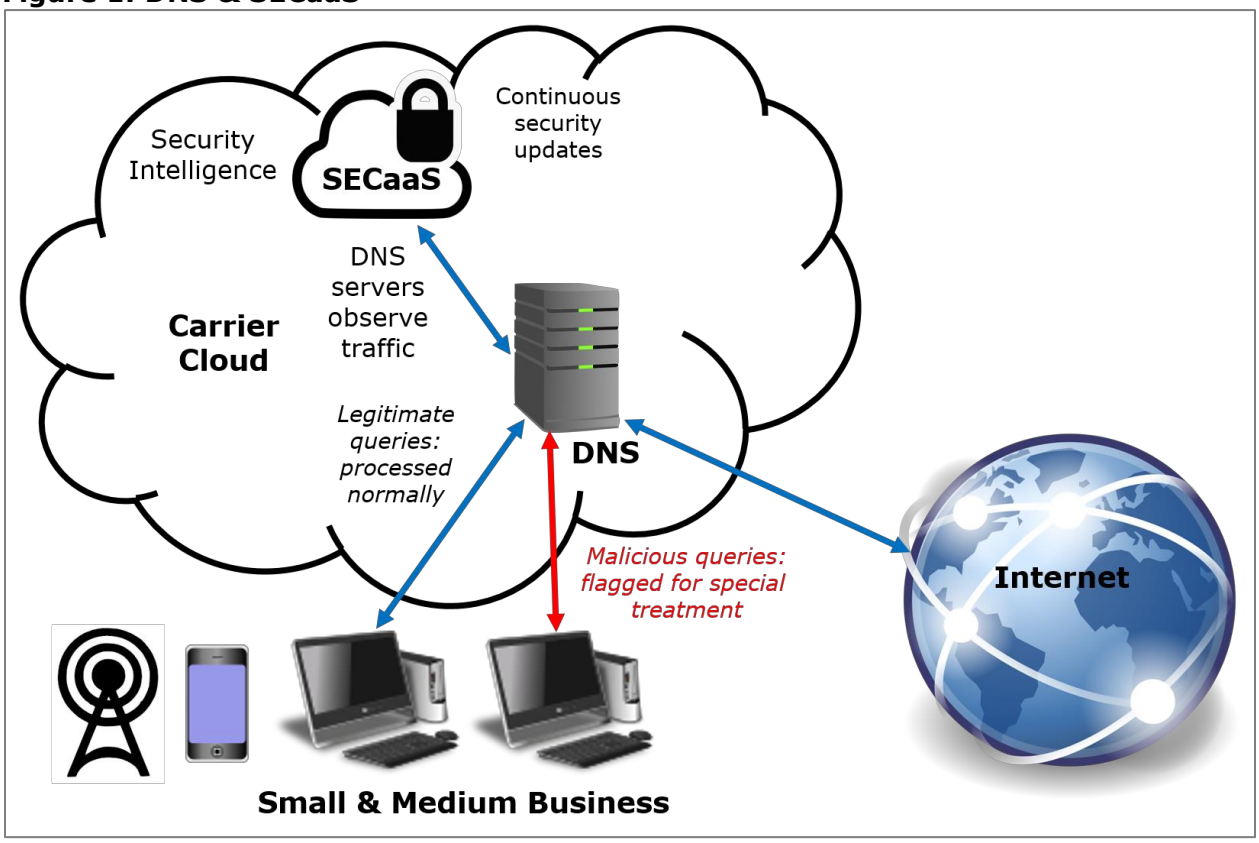
DNS-based security capabilities can provide an effective line of defense against fast-changing cyber threats that can now manifest themselves on a broader scale due to the greater number of intrusion points introduced by the cloud.

For example, using DNS to block phishing or bot/malware Command & Control (C&C) communications offers better protection than solutions that remediate post-infection. DNS data collected from servers protecting customers can be analyzed in conjunction with data science-based tools to iteratively develop defenses for new threats (discussed later in this paper). A DNS-based security solution is shown in **Figure 1**, and existing DNS infrastructure can be used to deliver robust SECaaS applications using a cloud architecture that gives providers control.

The DNS-based SECaaS solution depicted here is notable on both a business and a technical level. From a business perspective, it is simpler to deploy and manage than other security solutions because it supports a common carrier cloud-based software fabric, which negates the need for on-premises hardware or software. There's also never a truck roll (or mail drop)

for customer premises equipment (CPE) installation or repair. This means CSPs can enter SMB markets quickly, using relationships they already have within a very large customer base.

Figure 1: DNS & SECaaS



Source: Heavy Reading

Services can also readily be extended to consumer markets. Providers can deploy a sticky service that leaves them in control and extend the level of SMB trust with a robust security product, which pays considerable dividends from a customer loyalty, relationship and upsell perspective. Finally, upselling services is more straightforward and consistent in an SECaaS environment because software upgrades are done centrally and deliver the most current level of up-to-date coverage for all users.

SECaaS has other inherent technical advantages. Every device on the SMB premises is covered, and there are never any CPE or client software updates. This is especially important given the increasing use of bring-your-own-device (BYOD) mobile terminals, which may not have connected to the business network before and introduce new risks and vulnerabilities.

It is also relevant to the rapid growth of the Internet of Things (IoT), where we see higher-speed access driving more powerful and more connected devices that will effectively push out the borders and bring threats closer to the user. Guest or public WiFi services can also be covered.

Adding more refined filtering of DNS traffic (policies) opens up opportunities to extend the range or value of packaged SECaaS solutions. One common use case is to present SMBs with a simple webpage to configure contextually aware content filtering to block users from

visiting inappropriate sites (e.g., adult content) or sites that consume excessive bandwidth during work hours.

In many cases, existing infrastructure can be used to effectively and efficiently scale, although the DNS must continue to evolve to respond to changing requirements. Security policies can also be adapted on the fly to align with evolving threats.

There are substantial benefits for SMB customers that typically lack IT resources and have limited budgets. These include:

- Breadth: coverage of diverse threats across all internet-connected devices
- Depth: highly effective defenses
- Absolute ease of use: zero-touch after optional customization, no maintenance or updates
- Attractive price point: modest incremental increase in communications services costs

As a result, DNS has emerged as a vital and foundational SECaaS network element enabling CSPs to offer SMBs scalable and extremely flexible security services whether hosted in the carrier cloud or in a third-party cloud from ecosystem partners that preserves CSP control.

THE RISE OF BIG DATA & DNS

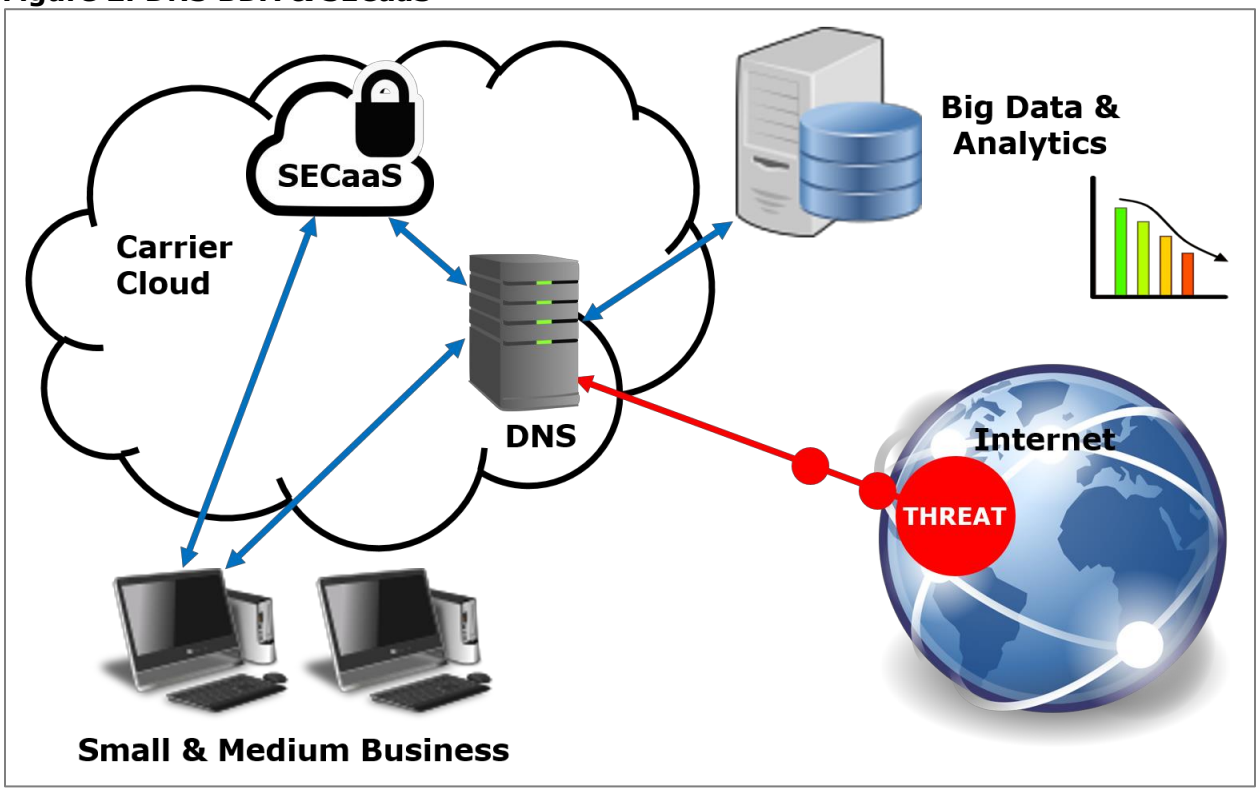
New service delivery is the lifeblood of CSPs – as is the need to continually evolve as requirements change and technology advances. However, innovative approaches to data management are needed to support these new demands. Since DNS data provides CSPs with insights into user consumption patterns, it is perfectly suited for interworking with BDA-based data science-based techniques – in fact, given security and service needs, we believe it is a requirement.

As illustrated in **Figure 2**, DNS becomes the logical first place to enforce security policies by taking advantage of the BDA data pattern analysis that identifies and confirms the presence of malicious DNS activity. Anomalous activity can be detected in seconds, and after algorithmic processing validates newly discovered threats or threat variants, that activity can be fed into DNS servers. This approach delivers the true power of a DNS-based SECaaS solution: rapid protection against highly dynamic threats.

As an example of the results that can be derived from intensive DNS data analysis, Domain Generation Algorithms (DGAs), a common tool used by cybercriminals to obscure their exploits, can be discovered and characterized. This is incredibly valuable security information because it enables *proactive* protections. Distributing a threat list with DNS domain names an exploit will use *in the future* disrupts the proper functioning of malware. Businesses worldwide that are exposed to cybersecurity incidents can be protected before they have breaches.

Since SMBs are often the "test bed" for cyberthreats targeted at enterprises, *trust* is crucial – particularly when users are paying and counting on their SECaaS providers to defend their valuable data and applications on a 24/7 basis. This real-time protection would most certainly positively impact the perception of an SECaaS provider, building an even stronger trust model, and measurably improving the customer experience.

Figure 2: DNS BDA & SECaaS



Source: Heavy Reading

To maximize the value of their SECaaS investments, many CSPs will adopt a collaborative model, working with ecosystem partners, such as Nominum, that can deliver turnkey SECaaS solutions enhanced by the BDA efforts of a dedicated data science team.

This eliminates a substantial burden for the CSP – managing and validating threat data – and thereby optimizes CSP operational efficiency. This arrangement can be expanded even further when the ecosystem partner maintains responsibility for all functions of the SECaaS and DNS platforms on a daily basis, including real-time publication, distribution and management of threat lists.

BDA and DNS together are needed for a robust and effective SECaaS that is operationally efficient for CSPs to manage and control. Stated differently, BDA working in collaboration with DNS amplifies the value proposition of SECaaS capabilities that CSPs can, in turn, offer to their SMB customers without the need to commit time and money integrating on-premises hardware or software.

The addition of policy-based content filtering allows for customization of services, which enhances the customer experience even more. Looking ahead, we believe several considerations will drive this linkage between customer experience and security.

The most important is the evolution path of analytics itself. BDA-driven capabilities will only get better at predicting cyberattacks, which will positively enhance the reach and adoption of SECaaS. CSPs will ultimately end up with a powerful tool to dominate SMB markets by proactively mitigating the threat landscape.

CONCLUSION

Security and cloud services have arrived at an interesting intersection. Existing security solutions, such as client software or specialized CPE, face capacity challenges at a time when elastic scale and agility is vital to mitigate security threats. CSPs can take advantage of this opportunity with targeted products to address large and attractive SMB markets.

Similarly, SMBs are aware of the threats they face and realize that given their limited IT budgets and lack of security expertise, CSPs are better positioned to protect them from cyberattacks.

The technical and business impacts of the carrier cloud are, without question, profound. Therefore, in response to these new security-driven demands, the industry is adopting a forward-looking stance in service delivery that encompasses support of security capabilities on a much broader scale, a scale in which the scope of security services is expanded to optimally leverage the ease of management, agility and scale the cloud embodies. Progressive CSPs have already learned that in order to thrive in this environment, SECaaS is a sensible way to address the fluid needs of SMB customers.

CSPs will get greater peace of mind when their security interests are met by an ecosystem partner that possesses BDA capabilities for analyzing massive amounts of DNS data per day, and the ability to execute targeted policies. For CSPs, this means not only embracing carrier cloud solutions that provide them with control, but also expanding relationships with ecosystem partners, such as Nominum, that can deliver a complete and cost-effective DNS cloud-integrated solution.