**White Paper**

# Cybersecurity: Priorities & Proposals for Small ISPs

Prepared by

Patrick Donegan
Chief Analyst, Heavy Reading
www.heavyreading.com

on behalf of

www.infoblox.com

www.paloaltonetworks.com

www.sonus.net

www.wedgenetworks.com

**July 2016**

## Small ISPs Differ From Their Larger Peers

The world of communications services tends to look quite different from the perspective of large, household-name Internet service providers (ISPs), on the one hand, and smaller ISPs on the other. Large ISPs are publicly quoted companies, have large workforces, are technology leaders across fixed and mobile networks, and often serve millions or tens of millions of subscribers – including many government users and large businesses.

Small ISPs are often the exact opposite: They are more likely to be privately owned, usually don't have their own cellular operating licenses, and tend to have small (or very small) technical and operations teams. They serve smaller subscriber bases, and while they may serve the small and medium-size business (SMB) sector, they are a lot less likely to compete in the market for large enterprise and government customers. A lot of small ISPs are focused on regional markets, rather than nationwide plays. With some notable exceptions, they are also less likely to be technology leaders. Many small ISPs in rural markets are also dependent on government subsidies to render them financially viable.

The first half of this white paper describes the threat landscape from the perspective of small ISPs. It also proposes a six-point plan for driving higher cybersecurity investment into these businesses. The second half of the paper looks at three specific areas of cybersecurity risk, explaining what they are as well as why and how small ISPs should evaluate and address them.

The final part of the paper examines the case for small ISPs to sell security as a service – not just as a source of revenue generation, but also as part of a coherent strategy for increasing investment in the security of their own network infrastructure and their broader customer base.

## Cyber Threats Look Different When You're Small

Unsurprisingly, the perspective that management in small ISPs tends to have on the communications landscape, and its opportunities and challenges, tends to differ significantly from their larger peers, almost irrespective of the aspect of the business one considers. Cybersecurity is one such area where the perspective and security stance of small ISPs tends to be very different from that of their more illustrious competitors.

Large ISPs are much more likely to have among their customers a lot of large and medium-sized businesses, government departments and agencies, as well as some high-net-worth individuals. A clear consequence of that is that the most advanced threats are more likely to make their way onto their networks than the networks of smaller ISPs.

Take phishing attacks, for example. In the case of random "spray and pray" attacks, the customers of small ISPs may be just as vulnerable as those of large operators. But in the case of targeted spear-phishing, where attacks target groups of individuals such as employees of a specific company, small ISPs are less likely to carry that traffic. The same is true of distributed denial-of-service (DDoS) attacks. Large ISPs tend to offer a much more attractive attack surface of enterprise customers for attackers to target than smaller ISPs. So, again, when it comes to the most sophisticated types of target attacks, on balance large ISPs are more likely to be carrying them.

Moreover, large ISPs tend to be more of a direct target in their own right than smaller ISPs. There is much more money, or more valuable customer data, to be gleaned from the enterprise customers of large ISPs than from those of smaller ISPs. And the larger the customer base, the greater the disruption that can be created – that also makes the larger ISP a more interesting target from an attacker's perspective.

### The Disparity in Cybersecurity Resources

Faced with what appears to be greater risk, and having relatively large revenues driving their growth, larger ISPs have tended to find it easier to justify investment in cybersecurity, whether that be in terms of security hardware and software or in terms of dedicated security personnel and security training of other personnel.

Look under the hood at the cybersecurity setup of smaller ISPs, by contrast, and in the case of many of the smallest among them, you won't find much more than a firewall in terms of dedicated security hardware and software. You'll find that many of these companies don't even have a full-time person dedicated to security.

In many cases, the security role is bundled in with a broader operational role – indeed, in some cases that person may even be the only person responsible for operations in the whole company. Unsurprisingly, some of these companies aren't even able to keep up with regulatory compliance requirements, let alone invest in the additional capabilities required to protect themselves and their customers comprehensively against cyberattacks.

## Cyber Threat Realities for Small ISPs

We believe that the above description of how small ISPs often view cybersecurity threats, and the limited resources they commit to protecting against them, is quite well represented in **Figure 1**, which is taken from a 2Q14 Heavy Reading survey on DDoS Attacks in Service Provider Networks.

**Figure 1: Small ISPs See Fewer DDoS Attacks But Suffer More Severe Consequences**

| Specific Attack Type | Experience of Attacks | % of Large ISPs | % of Small ISPs |
|---|---|---|---|
| Flood attacks | Report seeing almost daily | 31% | 13% |
| Amplification attacks | | 21% | 10% |
| Flood attacks | Report as having disruptive, severe or catastrophic impacts | 25% | 55% |
| Amplification attacks | | 24% | 43% |

*Source: 2Q14 Heavy Reading survey on DDoS Attacks in Service Provider Network, #97*

These data points show two things: First, it confirms that small ISPs do indeed see fewer DDoS attacks than their larger counterparts. Just 13 percent and 10 percent of small ISPs reported seeing flood and amplification attacks almost daily, compared with 31 percent and 21 percent of large ISPs who reported seeing these attacks almost daily.

### Fewer Attacks & Yet More Severe Consequences

The second takeaway from **Figure 1** is that, while small ISPs do tend to see fewer incidents, attacks tend to have a significantly more damaging effect when they do get through. Only 25 and 24 percent of large ISP respondents cited flood attacks and amplification attacks as having disruptive, severe or catastrophic impacts on their business. Three quarters of large ISP respondents referred to these attack types as having either no significant impact or a manageable impact. In the case of small ISP respondents, however, 55 and 43 percent cited flood and amplification attacks as having disruptive, severe or catastrophic impacts.

The reason for this apparent asymmetry in the experiences of ISPs of different sizes is clear, and indeed has already been alluded to. Small ISPs tend to consider themselves less vulnerable to cyber threats, hence they tend not to invest enough in cybersecurity. And then when attacks do get through, the consequences of that under-investment by smaller ISPs do tend to make themselves felt in the form of longer time to detection, longer time to mitigation, and more disruption compared with their larger peers, who are much more likely to have invested adequately.

## A Six-Point Plan to Raise Cybersecurity Spend

Heavy Reading proposes the following six-point plan to help raise cybersecurity spending on the part of small ISPs as a platform for reducing customer churn and increasing service revenues.

Heavy Reading's six-point plan for small ISPs comprises the following:

1. Better understanding of the cyber threat environment
2. Getting lower costs and more attractive financial terms for network security hardware and software
3. Squeezing the most security value out of existing network infrastructure
4. Relief from some over-burdensome regulations
5. Better support for cybersecurity from industry associations
6. Selling security as a service

Each of these points is now dealt with in the following sections.

### 1. Better Understanding of the Cyber Threat Environment

This paper has already dealt with the asymmetry in DDoS attacks in which smaller ISPs tend to see comparatively fewer attacks, yet also tend to suffer greater impacts from an attack that gets through. This is an important starting point for a better understanding of the threat environment that small ISPs face.

A second key point is that in the absence of the right threat monitoring and detection capabilities small ISPs simply do not know how much or what kind of malicious traffic is in their network. Hence they likely don't know the full extent to which this traffic is already impacting network efficiency, network availability or the security of their customer's information.

A third point is that while large ISPs are a lot more likely to be affected by major, high profile attacks, small ISPs are arguably more vulnerable to lower level attacks such as ransomware attacks which are growing in number. One such was flagged recently by the authorities in the U.S. In April 2016, the U.S. Secret Service issued an Advisory Alert warning of attackers threatening to trigger a network outage unless they paid a ransom of 5 bitcoins (US$2,000 at then-current market rates).

To begin with, such threats are less likely to be blocked by a small ISP as it is less likely to have the security solutions in place to detect and mitigate it. Second, successful low-level attacks of this kind have the potential to do a lot more damage to the brand image of a small ISP than a large one. The larger one will have the greater scale, the greater security savvy, as well as the PR and legal machinery with which to brush them aside as trivial "drop in a bucket" across a base of subscribers in the hundreds of thousands, millions, or even tens of millions. A smaller ISP with a few thousands or tens of thousands of customers may find it a lot more challenging to contain the immediate incident or the longer term reputational impact. And these days, of course, it's not just a question of the ISP's association with the incident in the mainstream media but on social media as well.

Whether it's "right" or "wrong," "fair" or "unfair," the tendency for users to blame their ISP for the effects of cyberattacks should be well understood now. And with the ISP business emphasis rebalancing in many markets from a focus purely on acquisition of new customers, in favor of greater attention to customer retention, it's easy to see how successful attack impacts pose at least as great a threat to small ISPs – if not greater – compared with larger ones.

## 2. Lower Costs & More Attractive Financial Terms From Vendors

A common barrier to small ISPs investing in network security equipment is that the costs of network security hardware and software are too high. A lot of hope in the small ISP community is rightfully being placed on virtualization to lower the cost of investing adequately in security.

Part of the issue here has been that while most vendors serving the ISP market focus on scaling their products up, they haven't necessarily invested in reducing their form factors so that they are optimized for the needs of small ISPs and at truly affordable cost points. There is evidence of progress here on the part of some security vendors but that momentum needs to continue.

Also, the traditional front-loaded capex model for acquiring a security appliance simply doesn't work for many small ISPs. Their budgets simply can't stretch to accommodate that, even in the case of form factors that are scaled down and cost-optimized to their needs.

Many security vendors have already adapted the front-loaded capex model to extend and distribute capex payments over the duration of a contractual term, and this is helping. The near- to medium-term goal, however, must be for vendors to leverage virtualization to the fullest and extend software-as-a-service-based consumption billing models to small ISPs. This enables them to be billed once a month or once a quarter according to the exact amount of security software they have consumed during the billing period, measured against the relevant metric for that vendor's solution. This should make an even bigger difference.

Consumption-based billing models can certainly be challenging for vendors and ISPs alike to implement. They can be challenging for both parties from a technical

implementation perspective, as well as challenging for vendors from a business-model perspective. We note that a very small handful of vendors, often relatively new startup companies, are already delivering on this capability. We expect that the pressure on other vendors to start to deliver on that model will also grow over the next 18 months.

### 3. Extracting Security Value From Existing Network Infrastructure

Small ISPs aren't always deriving the full security benefits of the existing infrastructure that they already have in the network. Exploiting this can also help strengthen an ISP's security stance. That could mean better exploiting security features built in to existing switches and routers, or those built into other basic network infrastructure. This can yield security features at much lower cost than investing in dedicated security equipment. A variant on this approach consists of driving multiple security applications off the same security platform, rather than just the one. Some specific examples are provided further on in this paper.

Small ISPs do need to be watchful, though, that these approaches deliver worthwhile defenses, and don't just tick a notional box among security requirements without actually protecting themselves adequately.

### 4. Relief From Overly Burdensome Regulations

All ISPs necessarily need to comply with government regulations. Due to the vulnerability that many small ISPs have in their security postures, and lower revenue bases, there may be grounds for providing concessions to them relative to the requirements imposed on larger ones.

An example of this kind of thinking is in the U.S. with the passing in March 2016 by the House of Representatives of the Small Business Broadband Deployment Act. According to this Act, ISPs with fewer than 250,000 subscribers would be exempt for five years from enhanced FCC transparency rules that require ISPs to publicly disclose information about network management, performance and commercial terms. Such concessions help free up the ISP's time and resources for higher priorities, which could include security. Depending on the local market, regulatory concessions could also be tied to progress in other areas such as cybersecurity.

### 5. Better Support From Industry Associations

Small ISPs don't have the resources to pull together all the relevant market information and shared experiences with peers that any business needs to succeed. They must rely in part on industry associations – and the subscription dues they pay to these organizations – to do that for them. Hence, small ISPs should be lobbying their industry associations to do more in terms of coordinating education in cybersecurity with other peers. This will create enhanced networking opportunities for smaller ISPs with cybersecurity vendors, consultants and other specialists that can support them.

### 6. Leveraging Virtualization to Sell Security as a Service

A key element in any strategy to enhance a small ISP's security stance can actually be to begin selling security as a service, especially to enterprise customers, via a virtual security appliance. As discussed in more detail further on in this paper, a security-

as-a-service play is a lot more feasible for small ISPs now that virtualized network security software and turnkey "as a service" security solutions are widely available from leading vendors.

The virtualized model also ties in nicely with Point #2 in this six-point plan, in that virtualization should provide lower cost points and therefore lower the barrier to entry. It also aligns well with Point #3, relating to reusing infrastructure, in that small ISPs can consider using the same vendor's virtualized software for protecting their own infrastructure as well as protecting enterprise customers as a direct revenue generating service. Where security as a service is successful in lowering churn and driving revenue, stronger financial performance can also serve as a driver for investing further in network security.

## Stronger DNS Security in a Small ISP Network

In an ISP context, the basics of security don't get any more basic than the Domain Name System (DNS), the naming system that translates easily recognized domain names into numeric IP addresses, enabling servers and other computing and networking resources to look up and associate with one another.

Precisely because of its critical importance, the DNS infrastructure is one of the favorite targets for cyberattacks. The attack type traditionally associated with the DNS has been the DDoS attack, which overloads the servers with an overwhelmingly large volume of communication requests.

As an example, metropolitan Detroit customers of WOW, a small ISP operating in the Midwest and Southeast of the U.S., suffered outages throughout an entire weekend during the summer of 2015. These arose from DDoS attacks on its DNS servers. Other DNS attack variants include cache poisoning for redirecting traffic to rogue sites where malware is unwittingly downloaded and DNS tunneling for carrying out fraud against ISPs.

ISPs don't just host their own DNS infrastructure for their consumer customers. To be successful in the enterprise segment, many need to be able to host their enterprise customer's DNS infrastructure as well, including in virtualized formats.

The number of queries per second supported by the DNS infrastructure is still important today, but it has been surpassed in importance in recent years by how well the DNS infrastructure is protected from a security standpoint. This involves investing in properly protecting DNS servers with a rich suite of capabilities.

This should potentially include leveraging the gateway function of the DNS between the end user and the Internet to monitor DNS threats worldwide; tracking and correlation against known threats from the source IP addresses of DNS requests; the application of offline packet inspection of the DNS packets themselves; and automatic updates of DNS security rule sets.

An April 2014 Heavy Reading survey on DDoS Security in ISP networks found that only 30 percent of small ISPs had integrated DNS appliances capable of supporting a full suite of their DNS server vendor's own security features. Fifty two percent had open source (typically BIND) DNS servers. These depend on the ISP layering on their own security features, which means that in practice security is often inadequate. In the same survey, the status reported by large ISPs was almost the exact reverse.

While protecting the DNS infrastructure itself against DDoS attacks and exfiltration attacks is self-evidently important, ISPs also have the option of leveraging the same DNS resources to achieve other security goals as well. Serving as a good example of #3 in this paper's six-point plan, the DNS can be used for control plane-based content filtering to better protect end users against malware and accessing malicious web site. This can be a lower-cost alternative to investing in dedicated deep packet inspection (DPI) solutions to that same end.

## Threat Detection Throughout L4-L7

The importance of protecting the DNS is just one example of the growing importance of protecting the ISP infrastructure not just at the network layer, but at L4 through L7 as well. One of the challenges facing all ISPs – and therefore one where small ISPs can look to differentiate – is to establish a brand as not just a provider of high-capacity pipes at competitive prices. The challenge is to differentiate on the basis of the quality with which they deliver an ever increasing variety and volume of applications, including a growing number of delay sensitive applications.

In essence, software-defined networking (SDN) and network functions virtualization (NFV) enable operators to load applications onto the network faster, at lower cost, in greater volumes and with better performance. These days, providing a consistently high-quality application experience across PCs, tablets and other devices requires much closer monitoring and detecting of malicious activity at the application layer.

This is because attackers are increasingly targeting the application layer. They are shifting their emphasis from attacks focused solely on taking out network resources at the network layer. Increasingly, they are focusing on application-layer attacks to breach the network and steal and expose customer information or exploit vulnerabilities in different signaling protocols to carry out data exfiltration, resource exhaustion or fraud. These target specific vulnerabilities in server resources impacting both real-time and non-real-time communications. Among the primary targets are the Domain Numbering System (DNS), HyperText Transfer Protocol (HTTP) and Session Initiation Protocol (SIP).

These days, malware can also be found embedded in all manner of end-user devices, websites, browsers, applications and adware. Whether it be through exposure of private information or disruption to application performance, monitoring and detecting threats at the application layer is becoming increasingly important.

L3/L4 security solutions such as firewalls remain important for protecting against conventional network-layer attacks. But application-layer attacks tend to be difficult for many of these solutions to detect. Attackers long ago figured out how to write apps that defeat L3/L4 policy controls. And since conventional L3/L4 solutions can often miss these attacks, a network security strategy needs to follow in that same direction and be aimed at detecting and mitigating these application-layer attacks.

An evolution in next-generation firewall architecture that allows multiple security functions from L4 to L7 to be carried out with just one inspection of each packet – rather than multiple inspections per security function – has interesting potential. It has the potential to eliminate a lot of the processing performed in sequential inspection architectures, with potential gains in terms of improved security, while freeing up capacity and keeping latency low.

From a security standpoint, leveraging a universal threat detection engine across the layers and across multiple protocols gives a single packet inspection platform the potential to scan traffic for multiple application-layer threats at once.

## Secure Real-Time Communications

Consistent with the need to differentiate with services and applications, real-time communications are an increasingly key offering with which many ISPs are looking to differentiate themselves. Depending on the type of market they serve, and the segments of that market they are targeting, these services can be a real differentiator for small ISPs. That could be via VoIP, including VoWiFi; or increasingly via video, real-time collaboration, or browser-to-browser applications, potentially using Web Real Time Communication (WebRTC).

Where small ISPs choose real-time communications to differentiate with, they need to consider specific network security solutions to protect the network and their customers. An obvious option is to consider using session border controllers (SBCs) to protect against security threats that exploit vulnerabilities in SIP, the most common signaling protocol used in real-time communications.

Conventional security solutions such as traditional firewalls can't do some of the things they're designed to do in a real-time communications context. For example, because SIP traffic is encrypted, most traditional firewalls can't identify malware embedded in the payload whereas an SBC is designed to do that.

There's an additional vulnerability where exposure to DDoS attacks is concerned. For example, a traditional firewall will typically close a port based on a simple timing mechanism that may leave it open for a period following an application being admitted by the device. An SBC, on the other hand, will open and close ports dynamically, closing them immediately as soon as SIP session has ended so that the vulnerability to DDoS attacks is closed off.

Among the other threats know to arise in real-time traffic are eavesdropping, caller ID spoofing, theft of service and toll fraud. Toll fraud has a particularly high profile in some markets, because of the demonstrable financial costs to the enterprise that arise from it. Failure to provide protection against toll fraud can serve as a good enough reason for some IT managers not to select an ISP in favor of a more security-savvy ISP that does.

Protecting against these threats to the real-time communications environment – and the incremental revenue that it promises – requires security solutions that are capable of detecting and mitigating these unique threats via a rich feature list that provides security around the SIP protocol, such as physical or virtual instances of an SBC solution.

## Security as a Service: For Growth & Security

The previous sections have focused on areas of security that ISPs need to protect their own infrastructure as well as their customers at generic, high level. Consistent with point #6 in our six-point plan, this section focuses on the case for small ISPs to enter the security-as-a-service market.

Security as a service can offer compelling benefits over the level of security that most SMBs and consumers will achieve on their own, at lower cost and according to a model that is easier to use and administer. By offering such services an ISP can increase its competitiveness, generate profitable incremental revenue, and establish an advanced security platform that will also provide security for its own infrastructure and services.

Charging for providing additional security as a service – especially to enterprises – can form a critical element in a small ISP's strategy for improving competitiveness, increasing revenues, as well as hardening its own network security stance.

Many small ISPs already do this, and momentum behind others entering the market appears to be building steadily now. As shown in **Figure 2,** 60 percent of a sample of 36 small ISPs surveyed a year ago were intent on rolling out virtual firewalls to enterprise customers. Around 50 percent of these respondents were intent on doing the same with virtualized Web security and virtualized intrusion detection systems (IDS) and intrusion prevention systems (IPS). Most of the respondents who indicated an intent to deploy any one of these individual services, also indicated an intention to deploy others, so as to be able to offer a suite of security services for customers to choose from.

**Figure 2: Small ISPs Planning to Offer Security VNFs to Enterprises**

| Type of Security VNF | # of Respondents | % of Respondents |
|---|---|---|
| Firewall | 21 | 60% |
| Web Security | 18 | 52% |
| IDS/IPS | 17 | 49% |
| DDoS Protection | 13 | 38% |
| Security Management | 12 | 34% |
| Identity & Access Management | 11 | 31% |
| Malware Detection | 10 | 29% |

*Source: Subset of 36 small ISP respondents – 12 with revenues of $200M-$500M, 12 with $50M-$200M, 12 with less than $50 million – from Heavy Reading's May 2015 survey on "Network Security In The SDN and NFV Era"*

There are a number of reasons behind this momentum for small ISPs to roll out security as a service. Enterprises – especially SMBs – are in a similar position to some ISPs in that they themselves are facing mounting security threats, lack some of the basic security protections, and sometimes face similar capex constraints to the ISPs themselves.

As suggested by **Figure 2**, and as alluded to in point #2 of our six-point plan, virtualization has potential to materially alter the business case for security as a service. It does that in terms of the speed to market that it promises with security services as well as in terms of the more favorable cost models that vendors should increasingly be able to extend to small ISPs – and which they, in turn, should then be able to pass on to their customers.

The security-as-a-service business model is now being reinvented with virtualization. No one – neither the ISP nor the SMB – should need to invest up-front capex in a dedicated security device that must necessarily be over-provisioned to allow for future growth. This requirement in the traditional security-as-a-service business model has long been a barrier to adoption of security as a service for both small ISPs and for SMBs.

With virtualized, cloud-based, software solution delivery models, ISPs are increasingly able to subscribe to security software on a pay-as-you-use basis. The ISP can then sell this capacity on to SMB customers according to the exact same pay-as-you-use model. Vendor solutions are increasingly available to ISPs that can be hosted on the ISP's own cloud or in a third-party cloud. They can even be hosted on their own premises as an entry-level "cloud-in-a-box" with enough compute, storage and network resources to get a new revenue stream in security services off the ground.

If the business model is designed correctly, the additional potential of a software-as-a-service model of this kind is that neither the ISP nor the end SMB customer needs be tied into a long-term contract. This too has been a major barrier to adoption in the past. Because neither party takes on a dedicated hardware investment in a cloud-based virtualized solution, both parties should be able to pay to consume indefinitely or until they decide to cease buying, without penalty.

It's a misnomer to think of the security-as-a-service model as somehow different or separate from the ISP's own security stance with respect to its own infrastructure. A successful security-as-a-service business is proven to reduce churn, drive additional revenue, or both. Improved business performance provides a platform on which additional investments can be made, including in the ISP's own security. Moreover, and consistent with point #3 in our six-point plan, ISPs that invest in security as a service should also be looking to leverage economies of scale by taking the exact same security solutions they are selling to SMBs and applying them to securing their own infrastructure.

## Summary

While the cyber threat landscape is universal, small ISPs experience it in ways that are unique and different from large ISPs.

With limited resources in capital and expertise, there is a problem of under-investment in cybersecurity among small ISPs. This paper has put forward a six-point plan to address that problem, focusing on better awareness; lower costs and more flexible financial terms; leveraging existing infrastructure; regulatory relief; better support from industry associations; and selling security as a service.

This paper provides examples of security improvements that small ISPs can make in the area of application layer security generally and with respect to real-time communications and DNS in particular. It also shows how selling security as a service can serve as a core element in protecting a small ISP's own network infrastructure from security attacks.

## About Infoblox

Infoblox enables ISP, mobile, cable, broadband, and managed service providers to offer a safe, reliable, and fast first-connection impression to subscribers and enterprise customers with the most scalable and secure DNS platform. Security is one of the top criteria for subscribers and enterprises when they are choosing service providers.

Unsecured devices put network assets at risk, and dissatisfied subscribers can damage a trusted, valuable brand and reputation. Infoblox solutions provide highly cost-efficient control, improved subscriber experience, and deep protection from a wide range of DNS attacks and malicious website access.

Infoblox delivers the intelligence, performance, and proactive protection service providers need to safeguard their networks, subscribers, and brand. All Infoblox solutions include patented Infoblox Grid™ technology, which provides optimal operator visibility and control across the entire Infoblox DNS infrastructure, enabling quick detection of service-threatening attacks while easing operational costs and increasing manageability. Service providers can leverage secure DNS caching, authoritative DNS, IP address management (IPAM) and managed DNS/DHCP/IPAM offerings.

## About Palo Alto Networks

Palo Alto Networks is the next-generation security company maintaining trust in the digital age by helping tens of thousands of organizations worldwide prevent cyber breaches. With our deep cybersecurity expertise, commitment to innovation, and game-changing Next-Generation Security Platform, customers can confidently pursue a digital-first strategy and embark on new technology initiatives, such as cloud and mobility. This kind of thinking and know-how helps customer organizations grow their business and empower employees all while maintaining complete visibility and the control needed to protect their critical control systems and most valued data assets.

Our platform was built from the ground up for breach prevention, with threat information shared across security functions system-wide, and designed to operate in increasingly mobile, modern networks. By combining network, cloud and endpoint security with advanced threat intelligence in a natively integrated security platform, we safely enable all applications and deliver highly automated, preventive protection against cyberthreats at all stages in the attack lifecycle without compromising performance. Customers benefit from superior security to what legacy or point products provide and realize a better total cost of ownership.

ISPs can combine the power of our Next-Generation Security Platform with the industry's best people and programs to secure their own networks and also meet a wide range of customer needs with tiers of threat prevention capabilities tailored to different industry verticals and use cases, including Governments, Financial Services, Healthcare, and the Internet of Things (IoT).

# About Sonus

Sonus brings the next generation of Cloud-based SIP and 4G/VoLTE solutions to its customers by enabling and securing mission critical traffic for VoIP, video, IM and online collaboration. With Sonus, enterprises can intelligently secure and prioritize real-time communications, while service providers can deliver reliable, secure real-time services for mobile, UC and social applications. Sonus offers an award-winning portfolio of hardware-based and virtualized Session Border Controllers (SBCs), Diameter Signaling Controllers (DSCs), Cloud Exchange Networking Platform, Policy/Routing servers and media/signaling gateways. Visit www.sonus.net or call 1-855-GO-SONUS. Follow Sonus on Twitter, Facebook, LinkedIn, YouTube and Instagram.

# About Wedge Networks

Headquartered in Calgary, Canada, Wedge Networks is recognized as an innovator and a disruptive market leader in the rapidly growing Security-as-a-Service and service provider security market. With deployments spanning 17 countries, protecting tens of millions of end points, Wedge offers a proven network security platform that is 100 percent virtualized for operation in the network operator's data center or hosted cloud. The platform inspects data streams in real-time and applies security policies as data flows through the network. This cloud-based operational model is further enhanced with a Pay-as-you-Sell subscription licensing model that allows service providers to synchronize security licensing fees with customer subscriptions for a dramatically improved business model.

The platform, known as Wedge Cloud Network Defense™, represents the industry's first Orchestrated Threat Management platform (OTM). It combines Wedge's patented elastic scale hyper-inspection engine with industry leading third-party security technologies to provide a variety of high-performance security services. Available services include virtualized secure web gateway, secure email gateway, IPS/IDS, Sandboxing, DDoS mitigation, Server and IaaS protection, mobile security, and more. These security services can protect the network operator's network as well as provide Security-as-a-Service to service subscribers, leveraging multi-tenancy support.

Providing the ultimate in packaging flexibility, Wedge Cloud Network Defense is available for deployment as a virtual machine, as an application running in an OpenStack or VMware cloud compute environment, as a pre-packaged Cloud-in-a-Box, or as an appliance running on industry standard x86 server hardware. Please visit www.wedgenetworks.com for more information. Also, be sure to download our white paper on Security-as-a-Service.