allot
See. Control. Secure.

Position Paper

World-leading Network-native Security

January 2024

Contents

Executive Summary

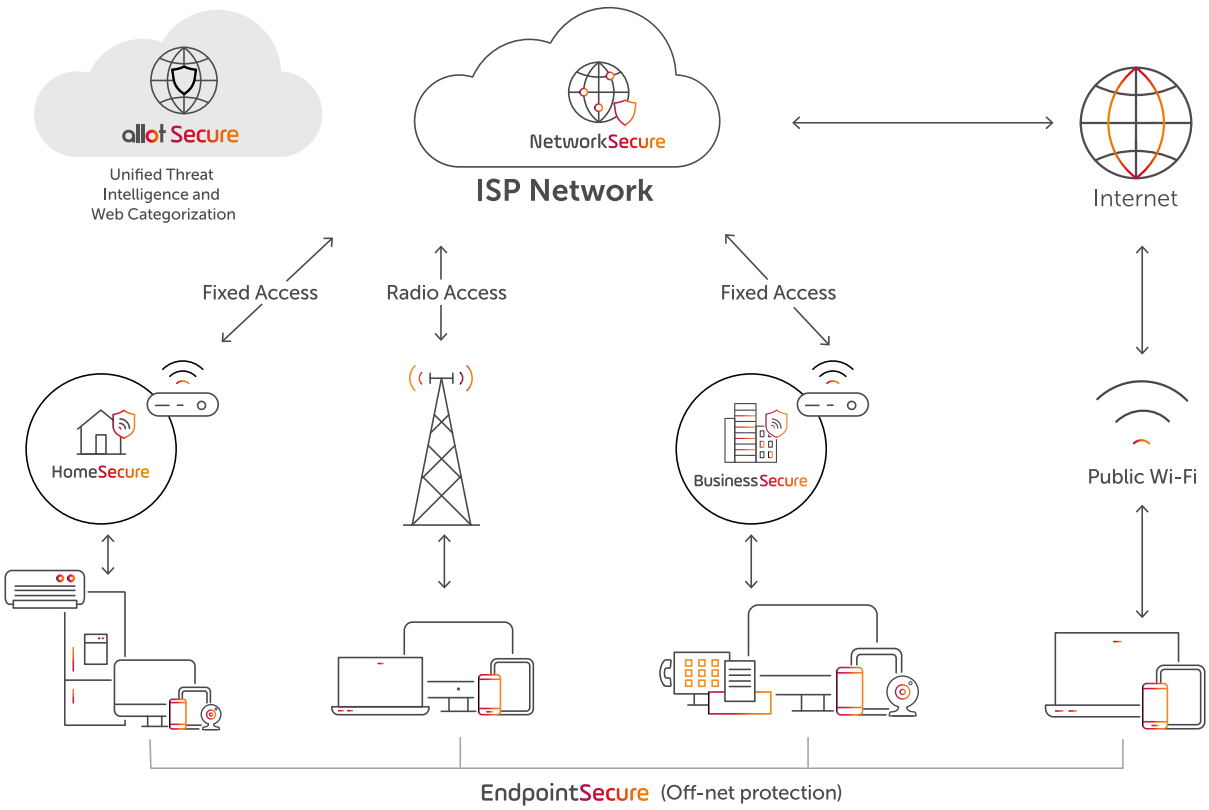
For years, CSPs have offered their consumer and small business customers client-based endpoint security solutions. The benefits of these solutions are limited to the small number of subscribers who successfully deploy them – usually less then 5% of the subscriber base. The low adoption rates for such solutions do not translate into significant benefit for the CSPs. Among the many reasons that make network-native security services the new gold standard for CSPs is that they are easy to deploy, easy to provision and easy to use, leading to high service adoption rates.

Recent statistics from live Allot network-native security implementations show that Allot has successfully detected and blocked 66% more cyber threats in 2023 compared with the previous year. By all measures, the number of worldwide cyberattacks against consumers and small businesses continues to rise. Bad actors target them with malware, ransomware, phishing attacks and a host of threats that range from annoyances to significant life interrupters. The people who suffer from these threats, and who fear them, are all customers of communication service providers (CSPs). They access their internet data through telecoms and ISPs who are increasingly under pressure to provide security services to all of their customers.

In fact, according to a 2022 global survey conducted by Coleman Parkes Research for Allot, 68% of CSP customers are more likely to buy additional products or services if a CSP offers security. This rises to 70% for customers aged 18-44, 72% for heavy data users (making up 51% of subscribers), and 74% for subscribers who were previously victims of cyber attacks. This puts the question to rest of whether CSP customers want security solutions. What remains to be answered, however, is what type of solutions will satisfy the customers' demands while offering sufficient benefit to the CSP, as well?

An alternative to client-based endpoint security is network-native security for consumer and small business customers. With network-native solutions deployed in the CSP's network, the CSP can offer high-quality security services as part of the core offering along with connectivity. As a network-native solution, security services can be zero-touch – no installation and no provisioning hassle for the customer.

This has led to CSPs seeing adoption rates of up to 30% (and more in some cases) when they deploy network-native security services. Along with other advantages for the customer and the CSP, network-native security services are a mutually beneficial offering that take into account the reality of today's security environment plus the needs of the CSP. This all leads to network-native security being the new gold standard for CSPs security solutions for consumer and small business customers.



Typical Allot Network-native Security Deployment

Endpoint Solution Limitations

While CSPs often provide client-based security solutions to their consumer and SMB customers, these solutions come with limitations that can lead to frustrated customers, lost revenue and unnecessary expenses.

Provisioning

One disadvantage of client-based solutions is the difficulty in provisioning them. If the CSP succeeds in convincing the customer to take advantage of a client-based solution, the customer needs to download, install, accept terms and conditions and configure the client before using it. Once it is configured, it needs to be updated periodically – also the responsibility of the customer. This process, while commonplace for IT professionals and tech savvy individuals, is a hassle, if even possible, for most consumer and SMB customers. Hassle inevitably leads to low solution adoption and retention rates, meaning less revenue for the CSP and little, if any, improvement in the CSP's image.

Support Costs

Another sticking point for CSPs, when it comes to client-based solutions of any type, are the customer service calls that accompany the provisioning of such solutions. When an app is provisioned by the CSP, customers will naturally turn to the CSP for help when they run into issues with the app. In some markets, a service call can cost the CSP between $8 and $15. For a troubleshooting call, that cost can rise to as much as $35. For a service that brings in $3 or so of monthly revenue for the CSP, a single call can be the difference between annual profit and loss for a customer. For these, and other reasons, CSPs are reticent to introduce new endpoint solutions. In the end, endpoint solutions, from convenience to pricing to service, are not designed to properly serve the needs of the CSP, and their vendors are not invested in the success of the CSP.

Network-Native Security Advantages

Network-native security services are deployed as a part of the CSP's network infrastructure. Similar to client-based endpoint security solutions, network-native solutions block cyber threats that can negatively impact the customer's data, device and digital experience. The main difference lies in the fact that the network-native solution blocks threats in the network, before the threats attack the end user's devices. Network-native security solutions can block adware, various types of malware, ransomware, phishing attacks and other types of threats. In addition, network-native solutions can deliver content controls for safe parenting and content category filtering for small businesses.

The advantages of network-native security are many. While there are some advantages that seem obvious, others might surprise you. When the solution is not installed on the customers' devices, one basic advantage includes OS independence. In addition, running in the network means that network-native security also has no impact on battery life or device performance the way client-based solutions do. It cannot be accidentally deactivated or deleted and there is no need to install it on multiple devices. Beyond these customer pleasing advantages, below is a broader sample of why network-native security is an ideal choice for both CSPs and their consumer and small business customers.

Advantages for the CSP

Pricing

Endpoint security solutions often come with a fixed pricing model set by the vendor without consideration for the CSP's pricing model. The CSP must then integrate that cost into their packages based on the price set by the vendor, leaving little flexibility for the CSP. With Network-native security, CSPs can expect a revenue sharing model where the vendor gets a part of the incremental monthly revenue and the vendor gets its share, as well. This model puts the vendor into a position where it is invested the success of the CSP's service, offering support to the CSP to ensure that success. In this model, the pricing is controlled by the CSP, leaving room for the flexibility that the CSP requires to ensure that the service is profitable.

Provisioning

Network-native security simplifies the provisioning process from initial engagement, to the backend billing engine and through the zero-touch end-customer deployment. When all the customer needs to do to start using the service is to accept it through the CSP's UI, portal, promotion or point of sale, the likelihood of adoption increases significantly compared with client-based solutions.

Customer Support

Resource-intensive support calls incur high costs, as described earlier. When a client-based solution is introduced to the mass market through the CSP's marketing system, it can generate a large number of support calls to address common (and sometimes complex) issues that arise when the customer needs assistance with installation and configuration. The investment in support on the part of the CSP can be far lower when implementing a network-native security solution where the solution is zero-touch since it sits on the network instead of on the customer's device.

Go-to-Market

Resulting from its zero-touch simplicity, network native security frequently achieves a high adoption rate of up to 30% (and higher in some cases) while endpoint security sees limited adoption success, with low single digit market penetration when marketed by CSPs. When customers are given tasks, especially technical tasks, they can be put off by the perceived complexity. This is often the case with client-based endpoint security, which has never achieved strong success for CSPs. Because of the strong go-to-market proposition of network-native security for the customer, high adoption rates can be achieved quite rapidly, with higher-than-expected retention rates, as well.

Exclusively built for CSPs

Network-native security is, by necessity, designed, built and implemented exclusively for CSPs. This ensures that the solution is aligned with the integration and marketing demands of the CSP. Endpoint security products are sold through competing channels, and even through competing CSPs, reducing their uniqueness and rendering the CSP as simply one more channel for the vendor. Network-native security solutions offer the CSP the opportunity to be unique in their security offering.

Branding

One of the goals of network-native security is to achieve uniqueness for the CSP. A CSP with a branded security solution has an advantage over its competitors. Running in the network, the CSP can control the user experience of their network-native security offering which is white labeled by design. The UX of other solutions is controlled by the OEM, leaving little space, if any, for CSP branding. While this benefits the OEM, it only serves to create parity with competing CSPs without delivering the competitive advantage of network-native security.

Convergence roadmap

Traditional security solution providers are mostly siloed in their own ecosystems, without considering the marketing and deployment plans of the CSP. Network-native security has an open approach to integration, and is convergence-ready. Convergence, in this context, refers to creating a single, unified security experience for the customer whether they are at home or out and about, as long as they are connected to the CSP network. For customers who get their home and mobile data access from a single CSP, a converged experience is a great advantage that simplifies security on all the customers' devices. Converged billing for home and mobile security can also simplify the experience for the CSP. Because the network-native solution sits in the network, this is all possible.

Reach

Network-native security is designed for mass-market deployment. Because it achieves very high adoption rates, the CSP can expect a large number of customers to subscribe to the service. As a network-native service, the CSP has an opportunity to communicate with customers through the UX of the service. This usually happens when a dangerous link is blocked or at monthly reporting time, or whenever the CSP chooses to inject a message, as appropriate. More frequent customer communication with more customers translates into better customer retention. That cannot be achieved through endpoint solutions.

Advantages for the end-user

Software and definitions updates

For the small number of customers who manage to download and install a client-based security solution, even a smaller number manage to keep the software and definitions updated. Without updated threat definitions a client-based security solution is blind to the constant string of new threats that are generated by bad actors who target people's data and privacy. On the other hand, network-native security keeps definitions updated constantly from within the network. Drawing from a cloud-based library which is constantly updated, the network-native solution ensures that all subscribers who use the solution are protected from even the newest threats, without their needing to lift a finger.

Management

The CSP is ultimately responsible for the management of the solutions that they supply to their customers. Spending time to keep software and various parameters updated on multiple devices is not an attractive feature for customers who want hassle-free services. For large businesses, with IT departments, this is less of an issue. But for the average consumer or even for small businesses wo have no IT personnel or expertise, the last thing they want to do is configure software. Network-native security solutions are easy to manage and keep up to date since all the IT configuration happens in the CSP network. There is nothing for the end customer to do but to enjoy their digital experience without cyber threats.

Background operation

As mentioned earlier, customer service calls are expensive. A CSP will try to reduce the number of service calls, especially costly troubleshooting calls, as much as possible. Client-based solutions which require customer intervention are likely to generate service calls when customers with low to no IT experience engage with them. Network-native security solutions operate in the background, requiring no intervention on the part of the customer. This reduces the likelihood of customer service calls which are required for endpoint security solutions that need to be properly installed by subscribers who do not have IT expertise.

End user experience

As opposed to a client-based solution, where the end user is required to become familiar with a complex set of tools in order to properly manage the solution, the network-native solution requires very little of the end user with an interface that is used only for reporting purposes and does not demand any interaction on the part of the customer. Since the bulk of the technology sits in the

network and not on the device with a network-native solution, the non-technical end user experiences a much easier-to-use tool.

Parental control/Content filtering

The nature of network-native security makes it possible to implement parental control services for consumer customers and content filtering services for small business customers. These services can be implemented at the time of provisioning in a single solution, and again, with no installation necessary.

Conclusion

The threat of cyber attacks is rising. While traditional client-based endpoint security solutions face low adoption rates and provisioning challenges, network-native security solutions deployed within the CSP's network have emerged as a promising alternative. With adoption rates of up to 30% and various advantages such as simplified management, background operation, and revenue-sharing pricing models, network-native security is positioned as the new gold standard for CSPs' security solutions. Allot is at the forefront of this market, offering the world leading network-native security solution.

Client-based endpoint security solutions present limitations for CSPs, including provisioning difficulties, high customer service costs, and low adoption rates. In contrast, network-native security solutions offer advantages such as constant, zero-touch updates, simplified management, and reduced customer service calls. The pricing model allows for revenue sharing, providing flexibility for CSPs to control costs and ensuring vendor support for the success of the service. Network-native security simplifies the provisioning process, enhances end-user experience, and achieves higher adoption rates compared to client-based solutions.

Exclusive to CSPs, network-native security enables branding opportunities and a convergence roadmap, supporting a unified security experience for customers across home and mobile devices. With its mass-market focus, network-native security proves advantageous for customer communication, parental controls, and content filtering services, making it a comprehensive and mutually beneficial solution for CSPs and their customers.

About Allot

Allot Ltd. (NASDAQ: ALLT, TASE: ALLT) is a provider of leading innovative network intelligence and converged security solutions for service providers and enterprises worldwide, enhancing value to their customers. Our solutions are deployed globally for network and application analytics, traffic control and shaping, network-native security services, and more. Allot’s multi-service platforms are deployed by over 500 mobile, fixed and cloud service providers and over 1000 enterprises. Our industry-leading network-native security-as-a-service solution is already used by many millions of subscribers globally.