opensystems

COMPARISON REPORT

THE ROI OF SASE SD-WAN: SAVINGS THAT GO BEYOND SWITCHING FROM MPLS

open-systems.com

“Gartner predicts that by 2024, at least 40% of enterprises will have explicit strategies to adopt a converged networking and security model known as SASE. The architectural flexibility and cost savings of the model are simply too attractive for organizations to ignore.”

Introduction

Gartner coined the term “secure access service edge” (SASE, pronounced “sassy”) when analysts outlined a strategy whereby network and security functionality converge into a consolidated, cloud-native service. Gartner defines SASE as “an emerging offering combining comprehensive WAN capabilities with comprehensive network security functions… to support the dynamic secure access needs of digital enterprises. SASE capabilities are delivered as a service based upon the identity of the entity, real-time context, enterprise security/compliance policies and continuous assessment of risk/trust throughout the sessions.”[1]

Speaking about the importance of the new architecture, Gartner analysts wrote: “SASE will be as disruptive to network and network security architectures as IaaS was to the architecture for data center design.” They concluded, “Digital business transformation, adoption of cloud-native computing and increasing adoption of edge computing platforms will require SASE.” [2]

Despite the futuristic portrait of SASE as “emerging,” implementations of this strategy have existed in some fashion since well before the analyst firm’s seminal 2019 research report. In fact, Open Systems, which was founded in 1990 as a security integrator and managed security services provider (MSSP), has been delivering an intelligent edge and cloud access platform – the foundation of SASE – for over a decade with best-of-breed SD-WAN technology, embedded security at every layer, and 24x7 global operations support. A true SASE pioneer, Open Systems delivers a complete solution of network and security to thousands of companies around the world today.

Our experience with these customers has shown a plenitude of ROI benefits to a SASE SD-WAN strategy. Thus, the purpose of this paper is not to make a technical case for SASE – we've outlined those arguments in our SASE e-book – but to explain the financial case for SASE SD-WAN, and where organizations can expect to find the savings (or cost avoidance) in an Open Systems SASE strategy relative to an SD-WAN-based solution from a traditional telco or managed services provider (MSP).

The Comparison

This document compares the Open Systems Secure SD-WAN – a SASE solution – to a generic SD-WAN solution from a more traditional MSP; for example, a telco with an integrated SD-WAN offering. Gartner refers to this latter offering as a "SASE alternative" utilizing a software-based branch office. "By using a software-based blade approach to an on-premises branch CPE, a vendor with a set of partners could deliver many of the services in [the SASE identity-centric architecture]. Alternatively, the CPE could call out to cloud-based services when and where needed (for example for security inspection)."[3]

Numerous telcos and MSPs/MSSPs worldwide offer this alternative type of solution, often building off existing communication links provided by the service provider, with a cloud-managed SD-WAN solution and security layered on top. Such solutions often use components from multiple third-party vendors to create the overall offering. As an example, these components might include SD-WAN from vendors such as Viptela, VeloCloud, Silver Peak, or Masergy, and security functions from Palo Alto Networks, Fortinet, Check Point Software, SonicWall, Bitglass, and/or others. As a result, the network, SD-WAN and security functions may be integrated but they are not truly converged – or as Gartner says, they are "stitched together" – which only leads to costly complexity.[4]

In contrast, Open Systems has implemented a very comprehensive security stack. It includes functions to cover the entire kill chain – next generation firewall, intrusion detection, secure web gateway, email gateway, DNS filter, web proxy, endpoint security, and AI-driven network threat detection and response. The vast majority of the stack is our own technology, and we have built automated monitoring and alerting capabilities into the stack to accelerate resolution of issues and incidents.

Open Systems' security is converged with the network functions and everything is monitored 24x7 by our world-class NOC/SOC centers, which are staffed by expert-level engineers. This allows us to simplify the total experience for customers and deliver the outcomes that they want.

To look at the ROI of Open Systems' SASE SD-WAN solution versus that of SD-WAN from an MSP, we'll compare the relative costs and complexities in areas that tend to have a major impact on solution costs: Network, Security, Technology, Setup, Operations, and Organization.

NETWORK

There are two aspects of the network itself to consider in this comparison: Connectivity, which concerns the communication links and who provides them; and Application Focus, which is the process by which applications are identified and treated by the network.

Connectivity

One of the advantages of any SD-WAN is the ability to employ multiple types of access connections. For the price of a single MPLS line, an organization can install multiple broadband and/or 4G/5G links that can be used as failover or concurrent lines to increase bandwidth and availability over SD-WAN.

The savings of using MPLS-alternative links can be substantial. In the US, Gartner saw organizations with savings as much as 378%; 225% in EMEA; and 184% in APAC when moving from MPLS to hybrid/internet connectivity.[5] In the majority of cases, the cost per incremental bit is lower on SD-WAN. Thus, by deploying SD-WAN, enterprises have reported that marginal costs for bandwidth have gone down, and access speeds have gone up.[6,7]

Challenges of traditional MSP

- Connectivity lock-in (i.e. MPLS)
- Provider lock-in
- Multi-provider management and complexity

Cost

$ $ ◐

Complexity

● ● ○

With any type of networking solution provided by a telco, a customer is going to be locked into expensive, long-term contracts for services such as MPLS. There will be no choice of who provides the link, as that's the core business of a telco. What's more, if the customer is a global enterprise, the MSP will need to manage MPLS or other connections offered by different service providers in other regions of the world, given there is no telco today that can provide global service coverage on its own. This requirement for multi-provider management adds complexity and costs to the solution.

Cost

$ ○ ○

Complexity

● ○ ○

Benefits of Open Systems SASE

- Connectivity agnostic (MPLS, internet, 4G/5G)
- Provider agnostic
- Management of 1000+ providers for our customers

The Open Systems SASE solution is agnostic in terms of connectivity – both as far as the type of connectivity (MPLS, internet, 4G/5G, etc.) as well as the provider(s) of the communication services. Open Systems has experience in managing the relationships with more than a thousand communication providers for our customers. The existing relationships and coordination capabilities lower both complexity and cost.

Open Systems' SD-WAN has auto-failover mechanisms for reliable connectivity and performs active load balancing for optimal application performance. These features mitigate against the often considerable cost of downtime and help minimize poor end-user and customer experiences.

Application Focus

All applications on any network must be accurately identified so that they can be prioritized, routed and steered to the proper communication link, all according to policy. There are thousands of application identification engines on the market that perform this function, and how they work can vary greatly. For example, some look at packets while others look at protocols. Some look at context to help identify applications. Some engines can't identify all applications and simply process them as “unknown.”

Challenges of traditional MSP

- Applications are not shared across the platform
- Prioritization, routing and optimization options focus on protocols only
- No application performance insights

Cost

$ $ $

Complexity

● ● ●

In a traditional MSP solution offering, multiple application identification engines are often used. Not only does this drive up costs, it also can create conflicts with how the app IDs are resolved because one engine detects an application completely differently than another. Many simply rely on the less accurate protocols of the applications. This approach creates a heterogenous view of applications that can cause complexity with resolving policies. Further, the organization gets no application performance insights to help with optimization.

Cost

$ $ ◐

Complexity

● ● ○

Benefits of Open Systems SASE

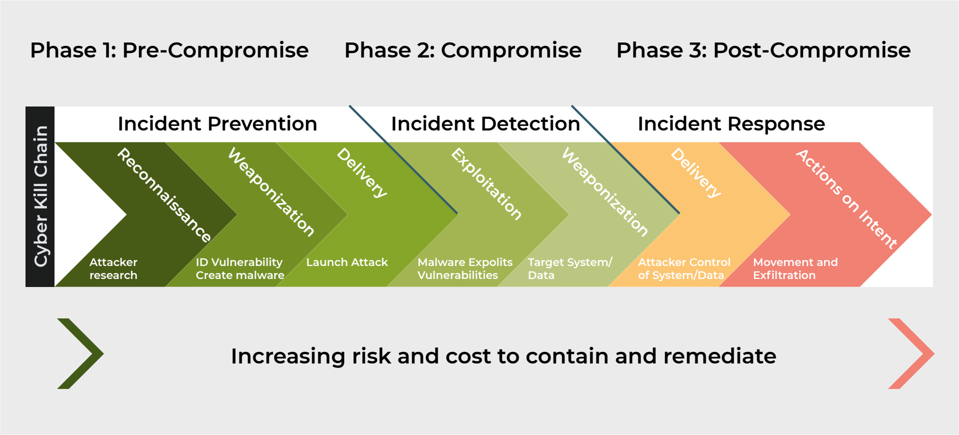
- Shared and custom applications are consistent across the platform
- App-based visibility, prioritization, routing, and optimization
- Application performance visibility

The Open Systems SASE solution provides one homogeneous view of applications, along with the option to identify custom apps as well. Thus, shared and custom applications are identified consistently across the entire platform. In addition, the Open Systems engine provides application performance visibility. This information can be used to further optimize enterprise applications. There's much more flexibility – and much less cost – with the Open Systems approach than in having many different point solutions that are layered on top of each other to provide complete coverage for application identification.

SECURITY

Two major aspects of security that are important considerations of a SASE SD-WAN solution are Coverage, meaning how much of the cyber kill chain is covered by the embedded security functions; and Integration, which refers to how unified the security functions are.

Lockheed Martin introduced the seven steps of the cyber kill chain in 2011



Based on image source:
Internet Security Alliance

Coverage

The model describes how organizations can detect, deny, disrupt, degrade and deceive the actions of attackers to provide a stronger security posture of the organizations' systems. The concept of the kill chain is, the sooner that malicious activity can be detected and mitigated, the less physical and financial damage the organization will experience from the attack. For instance, the inclusion of email security in the security stack will enable detection of phishing campaigns that are often the start of cyberattacks. (According to the Verizon Data Breach Investigations Report of 2020, most malware is still delivered by email.)[8] If a malicious message can be detected and blocked before it's even opened, that prevents an attacker from gaining a foothold in the environment. The cost to contain the attack at this early stage is minimal.

Challenges of traditional MSP

- Disjoint point solutions which include security vendor management and inhomogeneous and distributed security logs
- Either network or endpoint focused with very limited cloud coverage

Cost

$ $ $

Complexity

● ● ●

Oftentimes, MSPs and even MSSPs simply manage whatever security tools customers ask them to manage. It's really a disjointed collection of solutions with heterogenous and distributed security logs. What's more, these tools tend to be either network- or endpoint-focused with very limited cloud coverage. Some traditional security vendors are pushing into the managed detection and response (MDR) space. However, their coverage may be lax because they are working from logs rather than actual network flows, so they aren't seeing everything in context that could be indicative of a threat.

Cost

$ ○ ○

Complexity

● ○ ○

Benefits of Open Systems SASE

- Broad unified security portfolio to cover the whole kill chain (firewall, web, email and endpoint security as well as XDR)
- Endpoint, edge or in the cloud

Open Systems has a broad unified security portfolio that covers the entire cyber kill chain, from reconnaissance on systems to taking actions to mitigate the threat. What's more, the security functions operate on the endpoint, at the edge or in the cloud for maximum coverage. Because Open Systems has the ability to detect and mitigate threats earlier in the kill chain, the cost of an attack is substantially less than if it were to happen at a later stage. Thus, the ROI/cost savings come from damage avoidance.

Integration

The degree of integration affects various aspects of the cost and complexity of a SASE solution: integration in general is expensive as synergies of technologies and features can't be leveraged and organizations are forced to buy functionalities twice, embedded in solution offerings of two different vendors. On the other hand, complexity increases with each isolated security functionality due to integration and orchestration tasks. For example end-to-end quality assurance to the entire security stack, even as changes are made to the code during update or patch cycles.

Challenges of traditional MSP

- Product stitching
- End-to-end functionality assurance is up to the customer
- High functionality overlap from different providers

Cost

$ $ ○

Complexity

● ● ●

Cost

$ $ ○

Complexity

● ○ ○

Benefits of Open Systems SASE

- Unified on one platform
- End-to-end quality assurance
- Optimal leverage of synergies (i.e. MDR and Secure SD-WAN)

Solutions from traditional MSPs typically include discrete security tools that are stitched together to create a “complete” offering. The MSP may not even test the end-to-end functionality of the range of tools; that is left up to the customer organization. If one component has an update or patch, it can cause a problem across the board because no one is truly testing the security stack end-to-end. And because the tools are discrete, there is often high functionality overlap – or worse, gaps – in the products provided by different vendors.

A critical shortcoming of this jigsaw puzzle of a security stack is what happens to the traffic flowing through it. Each security function has its own engine. The traffic will be decrypted before going through a single engine for inspection, then re-encrypted before moving to the next engine, where it is decrypted, inspected and re-encrypted again – and so on, down the line of security tools. This creates tremendous complexity and latency, and impacts performance overall.

The security functions in the Open Systems SASE SD-WAN solution are unified on one platform. The vast majority of the security stack is our own code, which eliminates the issues of stitching products together. This gives Open Systems a single set of tools with a holistic security policy. We have a “single pass” architectural advantage where the traffic flow passes through all the security tools at once, and we can do all security-relevant actions on the traffic in a single “decrypt/inspect/re-encrypt” cycle.

Perhaps the most important aspect of having a fully integrated security stack is that it provides the ability to share and leverage information for critical activities like managed threat detection and response. Open Systems’ MDR is operating on full data flows rather than logs alone; however, logs can be incorporated into the analytics as needed. For example, Active Directory logs are integrated into the data lake used for threat analytics. Thus, Open Systems can see signs of threats in context, such as the use of lost or stolen credentials. (Verizon reports that over 80% of data breaches within the Hacking category involve brute force or the use of lost or stolen credentials.)[9] Being able to see threats in full context improves detection capabilities. Going back to the cyber kill chain model, earlier detection and mitigation leads to less damage and cost.

TECHNOLOGY

When it comes to technology, organizations that are seeking a total networking/security solution must consider how they will do Technology Evaluation, which involves continuously keeping an eye on the market for new technology trends; and managing the Hardware and Software Life Cycle, where solution components must be replaced and new components integrated into the system from time to time.

Technology Evaluation

How to handle the technology aspects of a solution can be especially onerous for organizations that, basically, hand over their existing network to an MSP/MSSP to manage. In this model, the customer organization still owns the on-premises equipment and is fully responsible for determining if they have the right solution pieces in place: the router, the firewall, advanced security solutions, the SD-WAN, etc. The organization itself must have either internal or external experts who continuously monitor industry trends, evaluate the technology, and swap out components when new technologies provide more advantages.

Consider a scenario that has been repeated numerous times as the SD-WAN industry matures and consolidates. Suppose an enterprise’s network uses an SD-WAN component from a vendor that has just been acquired by a larger technology company; for example, VeloCloud by VMware, or CloudGenix by Palo Alto Networks. Someone – most likely the end customer – needs to evaluate the new roadmap of that SD-WAN to determine if it’s still a good fit for that enterprise. What’s more, this same scenario can easily happen with the many other components of the solution.

Challenges of traditional MSP

- Internal/external industry expert to analyze trends and evaluate technology

Cost
$ $ ○

Complexity
● ● ●

Even if the MSP determines and provides all the technology of the solution, Gartner has cautionary advice for customers: “Avoid SASE offerings that are stitched together. A large vendor may have all the individual SASE elements from acquisitions or partnerships. However, closely evaluate the integration of the services and its ability to be orchestrated as a single experience from a single console and a single method for setting policy.”[10]

Theoretically, at least, technology evaluation should be a constant process to ensure that the network plus security solution is always optimized for a specific organization’s needs. The process can be cumbersome and costly, owing to the deep technology expertise that is required for the position.

Cost
$ ○ ○

Complexity
● ○ ○

Benefits of Open Systems SASE

- Continuous (re)evaluation of existing and new technology

Open Systems assumes this task for our customers. Our experts continually re-evaluate our technology stack and the underlying hardware. We consider it a responsibility and part of our service, at no additional cost to the customer, and it is part of the ROI of the Open Systems solution.

Hardware and Software Life Cycle

No hardware will run forever, and software will eventually be outdated. Hardware and software lifecycle tasks are part of every operations team and won’t decrease with the complexity and speed of today’s network and security technology.

Challenges of traditional MSP

- Regular review of software and hardware components and handling of EOL situations and risk
- Hardware monitoring and replacement

Cost
$ $ ○

Complexity
● ● ○

All hardware and all software products eventually reach a point where they need to be replaced – the end of life (EOL), so to speak. For hardware in particular, the components may wear out and need to be replaced even before the expected EOL. In an MSP situation, the end customer may be responsible for handling the EOL situations and the risk of making and testing the changes in their environment necessitated by replacement.

Cost
$ $ ○

Complexity
● ○ ○

Benefits of Open Systems SASE

- In-house/third-party software evaluation and replacement including integration into platform
- Proactive hardware replacements

Open Systems’ service model ensures proactive hardware replacement by monitoring devices for problems and anticipating failures and EOL situations. We conduct regular software evaluations on our in-house and third-party software components. When replacements are necessary, we provide full integration into the platform as part of our normal service offerings. This takes away the burden from the end customer to manage the hardware and software life cycle, which in turn provides an ROI advantage.

SETUP

Every customer organization must pass through several phases of setup to get their network and security up and running. These stages include Design, Configuration and Optimization, which are necessary to define what a customer needs; Project Management, which involves coordination of all the steps to get the network and security deployed, and then Deployment itself, which covers all aspects of installation.

Design, Configuration and Optimization

The benefit of a SASE solution usually depends on how it is designed, how well it fits to the organization and if the architecture is flexible enough to cover future requirements.

Challenges of traditional MSP

- One-to-one migrations of deprecated designs
- Rigid and “one fits all“ configuration
- Outdated and chaotic policies due to “fire and forget“ practices

Cost

$ $ ○

Complexity

● ● ●

Cost

$ ○ ○

Complexity

● ○ ○

Benefits of Open Systems SASE

- Best practice recommendations (network design, security policies)
- Flexible configuration options
- Long-term configuration optimization

These are attractive services for an MSP to provide to a new customer because they are often billed back at a high rate for the use of Professional Services experts. Nevertheless, the configurations often follow a “one size fits all” model rather than customizing a network configuration for each and every customer.

Open Systems assigns a technical account manager to every new customer setup. This manager investigates what architecture is currently in use, and what setup the customer has, and then makes a customized plan and an architecture according to industry best practices for network design and security policies. This plan is discussed with the customer at a technical level to determine how best to go from the old network to the new one. Open Systems takes ownership of this process, even if there are components that would be out of our scope. We find this is the best way to get long-term configuration optimization.

PROJECT MANAGEMENT

As network and security services interact with many other technologies and teams within an organization, a holistic project management approach, including as many interfaces as possible, is crucial.

Challenges of traditional MSP

- Coordination of provider activities only
- Ad-hoc reporting and no governance structures
- Additional charges

Cost

$ ◐ ○

Complexity

● ● ○

Cost

$ ○ ○

Complexity

● ● ○

Benefits of Open Systems SASE

- Coordination of all parties involved
- Establishment of governance and reporting included

Project management is another “for fee” consulting service provided by most MSPs, and it usually includes only those activities delivered by the provider. There may be no governance structure set up.

Open Systems provides project management as another service simply included in the overall contract. We work with all vendors that are parties to the solution and establish the means for governance of the network.

Deployment

Global enterprises need deployment options for all regions in the world, also difficult locations. A zero-touch installation process is required since it's too expensive and simply impossible to have technical personnel all over the world.

Challenges of traditional MSP

- Costly on-site visits to install on-prem devices
- Limited shipping countries/shipping is up to the customer

Cost

$ $ ◐

Complexity

● ● ◐

To deploy the network, MSPs often charge professional service fees to provide costly on-site visits to install devices on the premises. In some cases, they may not even be able to deliver equipment to certain countries.

Cost

$ $ ○

Complexity

● ● ○

Benefits of Open Systems SASE

- Easy-to-follow installation instructions (cloud or on-prem)
- Experienced logistics (over 180 countries)

In contrast, Open Systems is able to coordinate shipping logistics to more than 180 countries – even those in challenging locations. What's more, Open Systems has made its installation procedures so easy that, in most instances, no on-site visit of a technician is necessary. Following a zero-touch model, Open Systems pre-configures and labels everything and provides simple installation instructions. Someone in the customer office can simply plug in the device to connect to the cloud for further self-setup.

> "One of the benefits of Open Systems was the cost capabilities that they enabled us to realize. Open Systems allowed us to avoid a lot of upfront capital investment, which saved us a lot of cash out of pocket, but long-term, it also saves us and helps us realize a lot of the operational expense cost savings that SD-WAN in general promises, but a lot of companies aren't able to realize."

Chris Hall, VP of Global Information Technology at KEMET

OPERATIONS

Operations is the heart of caring for the network on a day-to-day basis. Operations includes the aspects of 24x7 Change and Incident Support, which is technical support for problems or issues; Patching and Upgrading, the process of keeping everything up to date; and Monitoring and Alerting, the process of watching for problems and threats as they emerge.

24x7 Change and Incident Support

With network and security being part of digital infrastructure services, incidents and changes need to be supported 24x7. Even more important than the availability of this support is a high-quality level which usually requires familiarity and experience with the technology and the environment.

Challenges of traditional MSP

- Included tickets are limited/pay per ticket and high fee for emergency changes
- Hard/lengthy to get through to the L3 support
- Not really 24x7 support (on-call only)

Cost

$ $ $

Complexity

● ● ●

Cost

$ ○ ○

Complexity

● ● ○

Benefits of Open Systems SASE

- Unlimited number of change/incident/request tickets including emergency requests
- Expert-level engineers only
- 24x7 follow-the-sun DevOps support

For many MSPs, the process of providing change and incident support – a help desk and ticketing system – is a lucrative service. The support contract often includes a limited number of tickets, and beyond that number there is a per-ticket fee to resolve problems or implement required changes. There can be a higher fee for emergency change requests. Initially, tickets are usually assigned to level-1 technicians who have the minimal skills to provide basic support and troubleshooting. It can be a challenge and take considerable time to get through to the level-3 (expert level) product and service support personnel. Because this is a "for fee" service from the MSP, it can be quite costly for the customer organization.

In contrast, change and incident support is an area where Open Systems really shines. We operate several network and security operations centers (NOC/SOC) with 24x7 staffing by all level-3 expert level engineers. All customers enjoy an unlimited number of change/incident/request tickets, including emergency requests, and it's all-inclusive, which provides significant ROI through cost avoidance. These centers include 24x7 DevOps support for customized needs. Account managers that are assigned to specific customers also provide direct support to their customers because they have intimate knowledge of that specific setup. Within Open Systems, everyone that codes our software and all service engineers also spend time working in operations – and this is unique in the industry.

Patching and Upgrading

All systems eventually require patches to fix problems as well as upgrades to provide new features and functions. The devil is in the details for these activities – the details being how often the patches are pushed out, how well they are tested before deployment, whether third parties are involved in providing any of the patch or upgrade components, and so on.

Challenges of traditional MSP

- Patching and upgrades need to be coordinated/executed by the customer
- Significant delay in covering all deployments with security patches

Cost

$ $ ○

Complexity

● ● ◐

Cost

$ ○ ○

Complexity

● ○ ○

Benefits of Open Systems SASE

- Standardized firmware version: regular patching and upgrading
- Rapid deployment of security patches

For an MSP that doesn't own the software stack, and who must rely on third-party vendors as part of the total solution, coordinating and executing the patching and upgrading process can be cumbersome, as the third parties are following their own schedules. Oftentimes, the coordination process is left up to the customer organization to do, and this in turn requires skilled resources to perform the changes. The process can be costly and time consuming.

Open Systems has regularly scheduled intervals – typically every second week – where we deploy patches. We do rapid deployment of security patches. Major upgrades happen annually, and smaller upgrades happen every quarter. Having patches and upgrades on a regular schedule allows us to keep everything secure and very up to date with new features and functionality. What's more, the regularity of the schedule and the defined processes help to keep cost and complexity to a minimum.

Monitoring and Alerting

Real-time and continuous monitoring and alerting on out-of-order activity is inevitable for being able to provide stable and reliable network and security services.

Challenges of traditional MSP

- Customers need to build their own monitoring and notification framework
- Alert flood with unspecific alerts that are completely decoupled from business

Cost

\$ \$ ○

Complexity

● ● ◐

It's critically important to monitor the network end to end, and to be alerted to security threats as well as issues on the network, such as a service outage. This can be an expensive operation, depending on the systems used for monitoring, correlating information, and consolidating and prioritizing alerts. Some MSPs may provide this service for an extra fee, or they may leave it up to the customer organization.

Cost

\$ ○ ○

Complexity

● ○ ○

Benefits of Open Systems SASE

- Monitoring and alerting comes with every feature
- Custom alerting through notification self-service

Open Systems ensures that every software component we develop internally includes embedded monitoring and alerting features. These embedded capabilities are known as "nurses" because they continuously monitor the health and performance of the software code. As of this writing, there are more than 280 "nurses" in operation to monitor our systems. Our customers can set preferences for automated alerting over any aspect of operations. Developing the monitoring and alerting capabilities alongside the code development, as well as automating the alerts, helps to reduce complexity and keep costs low.

ORGANIZATION

Committing to any networking and security provider is a strategic business decision that has long-term ramifications. It's critical to choose a partner wisely – a partner that has the technical expertise and the business acumen to get the customer organization where it needs to go, now and in the future. Thus, we look at two aspects of the provider organization, that being Expertise in knowing how to provide what the customer needs; and the ability to future-proof the Network Setup to provide customers with long-term agility.

Expertise

Complex solutions such as SASE technology and processes require high expertise and a lot of experience to be operated successfully. With a global shortage of cybersecurity experts numbering in the range of four million professionals[11], finding, hiring and holding onto people with the required expertise is a tough challenge today.

Challenges of traditional MSP

- Professional services billed on top
- External SMEs that don't know the customer setup
- Struggle to attract and retain experts

Cost

$ $ $

Complexity

● ● ●

The telco or MSP that is providing the communication links of the network and managing the SD-WAN and security aspects of the network is going to need significant expertise in all areas to support all the third-party components that are part of the solution. The provider may struggle to attract and retain experts and use external subject matter experts who don't know the customer's setup. Regardless of who is brought in to provide the expertise, the telco/MSP is going to invoice the customer for those professional services on top of the regular contract fees.

Cost

$ ○ ○

Complexity

● ○ ○

Benefits of Open Systems SASE

- Included professional services
- More than 70% of staff with an engineering degree
- Our experts are your experts

As for expertise and technical knowledge, more than 70% of the Open Systems staff has an engineering degree. We include the professional services of these experts in the cost of the contract fee. Our motto to the customer is, "Our experts are your experts" because they intimately know the customer's setup. After all, they are the ones who designed and installed the network and security.

Future-proof Setup/Agility

In these times, businesses must have the agility to change directions quickly. At the start of 2020, who could have predicted the need to suddenly have tens and hundreds of millions of people around the world working from home? Organizations that had secure remote and mobile access capabilities built into their networks didn't skip a beat when their employees went home to work for months at a time.

Challenges of traditional MSP

- Extensive investment in trend evaluation needed (internal/external)
- Missing long-term digital transformation view and strategy
- Managed service providers instead of partnering up

Cost

$ $ $

Complexity

● ● ●

Telcos and MSPs that merely manage their customers' networks are missing the opportunity to provide a long-term digital transformation view and strategy. This is something a true technology partner would provide, but MSPs are primarily caretakers of the existing network.

Cost

$ ○ ○

Complexity

● ○ ○

Benefits of Open Systems SASE

- Continuous trend and technology evaluation
- Strategic roadmap
- We're in this transformation together

Open Systems takes the stance of being that true technology partner, in order to help customers become more agile and prepare for the future. We do continuous evaluations of networking trends and technologies and incorporate leading features and functionality into our strategic roadmap. The ROI for customers is that they are better prepared for whatever digital transformations they need to take on.

Summary

Open Systems’ implementation of holistic SASE SD-WAN has significant cost and simplicity advantages over the types of “stitched together” network and security solutions that telcos and MSPs provide. These advantages yield a better return on investment over the life of a networking contract, but more importantly, the flexible architecture of the SASE SD-WAN provides an organization with business agility and future-proofs it against technology lock-in.

[1, 2] **Lawrence Orans, Joe Skorupa, Neil MacDonald, Gartner, Inc., “The Future of Network Security Is in the Cloud,”** August 30, 2019, ID G00441737

[3, 4] **Lawrence Orans, Joe Skorupa, Neil MacDonald, Gartner, Inc., “The Future of Network Security Is in the Cloud,”** August 30, 2019, ID G00441737

[5] **Gartner, Fact or Fiction: Does SD-WAN Really Save You Money?,** 10 February 2018

[6, 7] **Note: These are savings attributed to any SD-WAN, not just SD-WAN from Open Systems.**

[8] **Verizon, 2020 Data Breach Investigations Report**

[9] **Verizon, 2020 Data Breach Investigations Report**

[10] **Lawrence Orans, Joe Skorupa, Neil MacDonald, Gartner, Inc., “The Future of Network Security Is in the Cloud,”** August 30, 2019, ID G00441737

[11] **Infosecurity Magazine, Cybersecurity Skills Shortage Tops Four Million,** 7 November 2019