FORTINET

WHITE PAPER

Empowering the MSSP

Part 3: Monetizing Fortinet's Ecosystem in a Multi-Tenant Cloud Service

Introduction

As discussed in part 1 of our ‘Empowering the MSSP’ series, the Managed Security Services (MSS) market is enjoying rapid growth. A large proportion of this future growth will come from cloud-based delivery, which is expected to grow to 69% of the MSS market over the next five years.

For MSSPs, cloud-based security service delivery has quickly become the preferred model due to the ability to accommodate large numbers of customers and drive down customer costs while still maintaining efficiencies in datacenter infrastructure and administration. The benefits of cloud delivery are, of course, not without challenges, so identifying the most suitable approach for providing a successful service takes a significant investment in time, research and planning.

In this document we will look at different scenarios for cloud-based delivery and some of the major considerations MSSPs must take into account in order to deliver successful and profitable cloud security services. From a threat perspective we will consider the fundamentals of perimeter security services such as Firewall, Next Generation Firewall (NGFW), and Unified Threat Management (UTM). We will also study examples of a typical service definition matrix and potential return on investment from a FortiGate platform.

Service Considerations

Aligning Service Protection to Service Criticality

One of the most important elements of a successful multi-tenant security service is to understand how to offer the most appropriate level of service to each customer segment. Not all customers will consume the same set of services and not all services require the same level of protection. So to maintain a successful managed security business it is essential to segment customers and the core services they consume, then align them with the most appropriate security offering.

For example, a single site customer that utilizes hosted virtual server for file storage or backup is unlikely to need a fully managed UTM service with mission critical SLAs. Similarly a customer that purchases a multi-site MPLS private network with central Internet breakout would consider a firewall-only service to be insufficient. Having a 'one-size fits all' approach to service delivery could at best confuse customers and at worst completely lose them. There is a clear need to have a flexible but robust solution that enables security services to be customized to suit individual requirements and delivered from a single, scalable, and easy to manage platform.

The security services offered to the customer should complement the other core services that make up the provider's portfolio. This isn't limited to typical network security services such as those centered around the network firewall either. Mission critical public facing infrastructure such as web applications and hosting, domain name services, and communications services like video conferencing and Voice over IP (VoIP) can all be vulnerable to attack, potentially leaving the provider and the customer exposed. The question all service providers should ask themselves is "Do I offer the most appropriate level of protection across all of my available services?" If the answer is "No" then there is an opportunity to do so. Trying to apply all levels of protection to all services and all customers will ensure any business case will fail, as it is simply not necessary.

However, identifying those customers that generate a significant percentage of their annual revenue from a web application will increase the likelihood of uncovering a captive audience for advanced security services such as DDoS mitigation and Web Application security.

Drivers for Cloud-Based MSS

■ **Legacy firewall migration:**
Compared to a sprawl of individual firewalls, located either on customer sites, in their data center, or a mix of both, cloud delivery provides a more economical security estate that is easier to manage, while still offering more scalability and services.

■ **New service infrastructure:**
Demonstrating the value of a solution that combines consolidated licensing with a feature rich set of 'sellable' services will make it easier for the MSSP to visualize the profit opportunity that a Fortinet cloud based service offers.

■ **Advanced Services:**
As MSSPs maximize their "traditional" firewall-based services, they are actively looking to incorporate other features such as Next Generation Firewall (NGFW), or Advanced Threat Protection (ATP) into their service offering. MSSPs could also be looking to offer other protection for mission critical business processes, such as breach detection and distributed denial of service (DDoS) attack mitigation services.

Evaluating The Current Customer Base

The best MSSPs will focus closely on their customers' needs and understand that this is the key to success. Having an in-depth understanding of the customer base will enable it to be segmented and create the ability to position an appropriate, competitive security service. Following on from our discussion earlier regarding aligning services and security, if the provider doesn't have a clear idea of how the customer views IT, it will prove difficult to capitalize on the whole customer base. Take for example the difference between those customers driven by value and those by cost.

Customers driven by cost will always struggle to see the benefit of a dedicated service that provides the best available SLAs, proactive monitoring, reporting, and delegated administration, because the added value increases the cost. They will typically select a service that appears to offer the most for the lowest possible price, will look to commit to short-term contracts (typically 12 months), and have no concern about changing providers. To acquire these customers and keep them at renewal time, a provider needs to offer an entry-level package that can easily be provisioned and maintained at the lowest possible price per customer, with other options such as reporting and management coming as an optional chargeable extra if and when customers want them.

Conversely, customers driven by value will want certain levels of stability, security, and response time, and will be more likely to justify the premium in cost. However, their expectations of the level of service will be a lot greater and they will only be driven to another provider if the service is unacceptable, rather than as a result of cost. Factors such as a dedicated virtual or physical environment, higher allocation of throughput, a fully enabled set of security services, regular and bespoke reporting, and levels of delegated administration will all be part of their consideration.

Other considerations will include any government or industrial compliance regulations customers are subject to, as these will prohibit certain types of cloud-based delivery or require a greater level of investment in the cloud platform itself. If the MSSP can demonstrate they meet certain compliance criteria it will make it easier to acquire the more sensitive government or financial institutions.

Finally, it is advantageous to strike a balance between volume and bespoke delivery. If the MSSP can be flexible enough to accommodate the nuances of a new customer while still conforming to a level of standardization it will be possible to achieve scale and address a larger section of the target market, which will deliver the best possible ROI for the security service. Too much accommodation of bespoke customer requirements will impede the provider's ability to scale and address the wider customer base, whereas too much focus on volume will mean some of the more valuable customers will be missed through inflexibility.

To summarize, success is largely dependent on two things:

- Clear categorization and segmentation of customers aligned to a relevant and competitive set of service packages
- Investment in a single security platform that can be easily tailored to meet the needs of the different groups of customer.

Challenges of Hosted Security Services

■ **Scalability, Performance, and Minimal Footprint:**
It is essential to be able to scale into tens, hundreds and even thousands of customers without necessarily increasing the footprint of datacenter hardware. Fortinet's multi-tenant technology and ASIC architecture delivers unmatched performance in the slimmest form factor.

■ **Ease of Provisioning and Management:**
Centralized management, integration with existing management portals, and the ability to automate certain processes is a key requirement of multi-tenant environments. Fortinet's central management platform and associated APIs enable MSSPs to simplify provisioning and ongoing management.

■ **High Total Cost of Ownership:**
Typically multi-tenant security platforms are expensive. Add this to the cost of a sprawling hardware estate and management, and it can impact greatly on the overall service cost with a detrimental impact on the provider's competitiveness.

■ **Ease of Leveraging Additional Security Services:**
For MSSPs with an established firewall estate, the need to integrate additional security services is the next objective. The challenge comes when the incumbent firewall platform does not offer this functionality. With FortiGate technology, the performance degradation associated with running multiple security functions on the same platform is minimized.

Perimeter Security Services

Planning Considerations

Building a centralized platform to deliver scalable multi-tenant security services invariably involves doing so before realizing a return on the initial investment, which can be a risk, especially if there is no proven history of selling these types of services. Failing to take the time to analyze the return on investment (RoI) will ensure one of two things; either the project will never get as far as being signed off or, if it is, the organization will struggle to maximize any potential profits through lack of a 'go to market' strategy and planning. Fortinet platforms benefit from a simplified license model, which makes it very transparent when trying to understand the capital and operating costs associated with delivering a service. Also, being able to leverage feature-rich platforms such as the FortiGate, with no per-user licensing, makes it easier to deliver customized services to each customer segment.

Here are several key exercises that should be considered throughout the planning stage:

Analyzing The Current Firewall Estate (if applicable)

As briefly discussed in part one, the most traditional delivery model is customer premise equipment (CPE) or dedicated customer hardware in the MSSP core network. If an estate of existing firewalls has already been amassed the first thing to consider is its cost of ownership versus performance. Typically these appliances will have been purchased ad-hoc on an individual customer basis. Considered in isolation they may be meeting today's requirement. However, depending on their age and capability, it could be more cost effective to migrate them to a new platform to reduce TCO. Fortinet's price versus performance advantage enables providers to realize the significant technical and commercial benefits associated with this type of migration. For estates hosted by the provider, power consumption and peripheral utility costs should also be a consideration.

Profiling The Customer Base

As discussed earlier, customer knowledge is one of the keys to success. Understanding those that are driven by cost and those that are driven by value is essential.

Identifying a Customer Acquisition Rate

The rate of successful customer adoption is almost certainly the biggest factor that affects how quickly a provider will achieve RoI and CAPEX payback. An unrealistic or uninformed idea of how quickly customers can be acquired will give a distorted view of RoI, so be sure to be conservative rather than over-optimistic. If there is an existing estate from which customers can be migrated from physical to virtual (P2V), identify when the warranty expires on the appliances for those customers and offset current OPEX budget against the CAPEX to pay for the central platform. (For those customers that are not suitable for P2V migration, it may still be possible to reduce TCO by migrating them to a newer dedicated physical appliance)

Dissecting The Resources of a FortiGate

Due to its proprietary virtualization technology it is possible to dissect the FortiGate's overall capabilities together with its complete set of underlying security and network services into many isolated environments. The ability to do this with fully customized UTM (or sub-sets of services such as NGFW or ATP) is unique to Fortinet. However, with potentially hundreds of virtual environments, careful planning is required to identify what the mean allocation

of resource should be to each customer based on the suggested total num ber throughout the initial lifecycle (normally 3-5 years). Managing this exercise properly will reduce the risk of oversubscription to the service and ensure that platform's resources aren't consumed before the return is maximized.

Capacity planning thresholds may also need to be factored in to limit the amount of resource that is considered in this planning stage. From a service stability perspective it's not always desirable to plan up to the platform's finite capability.

Equation for dissecting resources in a **1: 1 VDOM/Customer ratio:**

$$\frac{\text{Total throughput} \times \text{Capacity planning (\%)}}{\text{Total number of customers}}$$

Equation for dissecting resources in a **1: n VDOM/Customer ratio:**

$$\frac{\text{Total throughput} \times \text{Capacity planning (\%)}}{\text{Total VDOMs / Total number of customers}}$$

Forecasting a 3-Year Cost Base

One of the most prohibiting factors of building out a centralized service is a lack of transparency into all the applicable costs of hardware, subscriptions, support, warranty, and other licensing. Having a clear view of costs incurred for all of these elements, based on the growth of the service, is key when it comes to justifying the project. Due to Fortinet's simplified license model and the inclusion of various default functions and services it makes it very easy to demonstrate overall lifecycle costs.

Identifying a Competitive Tiered Service Sell Price

One of the most difficult parts of this whole process is identifying what would constitute a competitive price for each level of service in the market, while still maintaining a healthy profit line for the business. There are two sides to consider when deciding on the pricing strategy – value for the customer and cost to the provider. Costs to be considered other than technology should include people, operations, billing, and utilities to name just a few. Visibility of the hard costs associated with the technology is a good starting point. Technology vendors should be able to provide a transparent view of costs throughout a service lifecycle and any that cannot do so should cause concern. Also, consider what existing skills are already available within the business for supporting the service. Are recruitment and training of new staff required?

In terms of value, how much does the service give the customer, what problems does it address, and what security protection does it provide? Once these factors have been considered it is easier to make informed decisions about a pricing strategy. For example, it may be decided to have aggressive pricing for the more commoditized lower tiers of service and premium pricing for well differentiated services. Promotional pricing may also be employed to encourage new customer acquisition. Whatever the strategy, pricing should be research driven, standardized, and reviewed regularly. It should never be decided ad-hoc at an individual sales level, as this will create inconsistencies in the market and create a high risk for the profitability of the business.

Recurring Revenues

As we have discussed some of the customers driven by cost will look to review suppliers as frequently as every 12 months to obtain the best cost. Value driven customers will be happy to stay providing the level of service meets their expectations. Recurring revenues are pivotal to the growth of MSSPs. With visibility of revenues 2-3 years in advance it makes it much easier to plan and make informed decisions on future investment to fuel growth. It is also conducive to customer 'stickiness', making it easier to sell other services. To gain visibility of what the underlying costs will be for years two and three a provider should look to incentivize customers to commit to longer-term contracts.

Using Fortinet MSSP Calculator

Whilst all of the points above are key to any planning stage, some of them are quite difficult and time consuming to complete effectively. The Fortinet MSSP Calculator is a RoI calculation tool that aims to take a lot of the pain out of completing these exercises and quickly give a summarized view of the commercial viability of any cloud-based project. Although there are always factors and costs individual to the provider that are outside of Fortinet's control, the cost and capability of the platform delivering the service plays a significant part in its success or failure. The greater the level of transparency from the vendor, the easier it is for the provider to make informed decisions on how to deliver the service.

The tool enables an MSSP to build a Fortinet solution and then dissect its throughput into (up to) three tiers of

service. Based on a customer adoption rate for each tier it then identifies what the average throughput allocation per customer should be, based on total forecasted customers in a three-year lifecycle. Once the relevant license costs have been selected and an annual sell price per customer proposed, it will dynamically calculate the approximate profit and loss for each year. To take advantage of the Fortinet MSSP Calculator please consult with your Fortinet representative.

Service Definitions

As discussed earlier, the need to have a flexible approach to service delivery is essential, due to the fact that a MSSP's customer base very rarely consists of one single type of customer or the same requirement for security. It is Fortinet's proprietary virtual domain (VDOM) technology that allows provisioning of independent customer environments for true multi-tenant shared services.

Dedicated Virtual Domains (VDOMs)

The traditional approach for MSSP cloud delivery would be to assign one VDOM to every customer, giving them their own environment that can be controlled and managed by both the provider and customer, if necessary. This is an ideal scenario for larger customers who require isolation, shared administration, dedicated ports, and provisioning of a bespoke set of policies and profiles. However, this comes at a cost, as each VDOM needs to be licensed and so this approach should be reserved for services aimed at mid to upper tier customers. Incorporating this cost into lower tiers, where customers are more price sensitive, could make the offerings uncompetitive. A different delivery model is typically used for lower tiers of service.

Shared VDOMs

Smaller businesses are often amenable to more standardized security offerings as they typically have less stringent compliance regulations than larger enterprise customers. One of the biggest challenges for MSSPs is how to address the SMB market with cloud security services that are palatable and appropriate for SMB budgets. Fortinet offers MSSPs a solution by allowing them to provision multiple customers into a single VDOM. Every Fortinet appliance has advanced routing capability enabling providers to route customer traffic using virtual LANs (VLANs) and virtual routing and forwarding (VRF). Segmenting customer traffic via VLANs allows providers to service multiple customers while reducing the cost per customer and taking advantage of better economies of scale.

Despite the clear benefits in certain scenarios, particular aspects need to be considered when planning the shared VDOM model such as session tables, shared administration, IP address management, and resource allocation. Although traffic is securely separated by a VLAN, customers in a shared VDOM will share a firewall session table.

Allowing customers to administer the service is much more complex with a shared VDOM as FortiManager allocates delegated administration privileges on a per VDOM basis. It is possible, but only with the use of Application Programing Interfaces (APIs) and Software Development Kits (SDKs), otherwise the provider would need to manage change requests. However, customers requiring this level of service would typically be prepared to pay for dedicated VDOMs and any associated management portal service costs.

IP address provisioning would need clear processes for documentation and management to ensure duplicate IPs are not assigned to different customers in the same VDOM. In addition, resource allocation to the shared VDOM must be limited to ensure it cannot consume the resources of any premium service paying customers. Finally, careful planning is required with regards to the usage requirements of each customer within the shared VDOM, to reduce the risk of any bottlenecks.

Example of a Service Definition Matrix

Below is as an example of how a MSSP may wish to model its services to suit different customer segments. Any security service definition matrix must be true to the customer base it is intending to serve as well as the existing connectivity or compute services available.

	Tier 1	Tier 2	Tier 3
Virtual Domain	Dedicated	Dedicated	Shared
Firewall	•	•	•
DMZ	•	•	
SSL VPN	•	•	
URL Filtering	•	•	
Anti Malware	•		
Intrusion Prevention	•		
Application Control	•		
Traffic Shaping	•		
Wireless Controller	•		
Wireless APs	Optional	Optional	
2FA Controller	•	•	
2FA Tokens	Optional	Optional	
Throughput Allocation	High/Dedicated	Medium/Dedicated	Low & shared
Cost	High	Medium	Low
€ per month	€€€	€€	€
SLA	Proactive monitorting	Reactive 4 hr	Reactive daily
MSSP Management	Fully managed	Part managed	Limited
Delegated Management	• (restricted)	• (restricted)	
Standard Reporting	•	•	
Bespoke Reporting	•		

Additional Revenue Streams

Default Controller Functions

A successful managed security services practice should unlock as many different revenue streams as possible and utilizing the default functionality in the FortiGate is one of the simplest ways to start. Every FortiGate appliance running the full version of FortiOS is a controller for Fortinet's wireless access points (FortiAP) and two-factor authentication tokens (FortiToken), providing the ability to seamlessly integrate the management and security of wireless networks and remote users respectively.

This default controller functionality should be included in the description of all services delivered with dedicated VDOMs. Whilst this function may never be used, and is also dependent on whether the provider's management capability extends to the local area network (LAN), it clearly demonstrates the capability of the FortiGate platform

Similarly, for services including VPN connectivity, an optional service to consider is 2 factor authentication as a dynamic layer to add to the traditional username and static password. Adding this extended layer of security is as simple as purchasing a perpetual license for the FortiToken, so it as an easy way to add incremental sales from new and existing customers.

As discussed earlier, extending the management boundary offered by the provider will make it much easier for a customer to take on more services, making them 'stickier'. If these additional services and revenue streams can be delivered from a single platform it makes it quicker and easier to provision and manage, ultimately reducing the total cost per customer and improving the profitability of the security service.

Management & Reporting

Management and reporting for central FortiGate platforms is delivered by FortiManager and FortiAnalyser, which should both serve to reduce administration overheads for the provider while offering revenue streams from new and existing customers. By including basic management and reporting functions as standard, and offering bespoke or more time consuming services as chargeable extras or only making them available on upper tiers of service, will encourage customers to pay extra for premium services.

A popular scenario for a delegated administration and reporting portal is the delivery of security services to wholesale channel partners. While a smaller partner would benefit from the size and scale offered by a MSSP, it is still common for them to wish to retain an element of control in order to add value to the end customer. The FortiGate platform combined with FortiPrivateCloud is unique in its ability to enable this shared administration of a completely isolated environment. The added benefit for the smaller partner is the ability to leverage this platform with little or no capital outlay (depending on the MSSPs pricing model).

Case reference – Talk Straight Ltd

Established in 2007, Talk Straight Ltd is one of Fortinet's fastest growing MSSP partners, leading the way in cloud-based security. Fortinet has always been Talk Straight's security platform of choice and while the original security model was to deploy customer premise equipment, in recent years it became apparent that a more efficient security model was required in order to cope with the company's exponential growth. In 2012 Talk Straight started a process to migrate all customer premise equipment to a fully resilient hosted cluster of carrier class FortiGates, enabling them to provision customer firewalls significantly quicker than the traditional on premise model.

The flexibility of the platform also enables Talk Straight to offer multiple levels of service, its Gold, Silver, and Bronze security packages. These packages are seamlessly aligned with a variety of connectivity services and correctly positioned to different customer segments.

The unmatched price versus performance and functionality value that Fortinet offers ensures Talk Straight's security proposition is always very competitively priced, which fuels the acquisition of new customers and the retention of existing ones by delivering outstanding service at the best price.

> *"As a MSSP, security services form a significant part of our growth strategy and our strong partnership with Fortinet along with their continued innovation in multi-tenant security platforms enables us to differentiate and maintain a competitive edge. We can provision completely isolated and independent virtual environments in minutes rather than days, significantly reducing our time to service new customers."*
>
> *David Tindall, Managing Director, Talk Straight Ltd*

Talk Straight's differentiation in the internet services market continues to attract the attention of industry leaders, which is proven by the company winning the award for "Best Business Use of Cloud" at the 2014 ISPA (Internet Service Providers Association) annual awards, the UK's most respected internet industry awards. A key factor in winning this award was Talk Straight's innovative model for delivering cloud security.

ROI with FortiGate

3-Year Profitability Example

As already discussed, Fortinet's simplified and transparent license model makes it much easier to assess the commercial viability of a potential managed security service. This analysis is made even easier with the use of the FortiCalculator tool, which reduces the time taken to gain insights into CAPEX and OPEX costs, potential levels of service, and profitability to minutes rather than hours or even days.

For this example we will use a high availability cluster of FortiGate 1500D's applying two tiers of service. We will also assume that 35% of customers adopt the premium tier one service and an active/passive configuration taking the output only from the primary unit in the cluster.

Fig. 1 - Solution overview & customer acquisition rates

Solution Overview	
Hardware	2 x FortiGate 1500D
Support	24 x 7 next Business Day
Security	Fully licensed (NGFW, Web Filtering, Advanced Threat)
Virtual	74 (over 3 years)
FortiManager	Virtual pltaform base license, cover for up to 80 VDOMs, 24 x 7 support
FortiAnanlyzer	Virtual pltaform base license, cover for up to 26Gb logs p/day, 24 x 7 support
Capacity	Overall solution capability capped at 85%
Configuration	Active/Passive

Tiers of Service	
Tier 1	Comprehensive 50Meg security; fully managed, Unified Threat Management, dedicated virtual domain, customer portal read access and reporting visibility
Customers (Year 1)	15
Customers (Year 2)	20
Customers (Year 3)	24
Total	59

Tier 2	Enhanced 7Meg Security; Fully managed, Firewall and Anti-Malware, Shared Virtual Domain (5 customers per domain), no customer portal
Customers (Year 1)	25
Customers (Year 2)	35
Customers (Year 3)	50
Total	110

The capacity-planning threshold provides the ability to take a more conservative view of resources, rather than always working to the top line throughput figure, and the starting point can be reduced depending on the MSSPs attitude to risk. This threshold can be as low as required or not reduced at all, however the average is typically between 75% and 90% utilization.

For the purpose of the calculations, overall resources are then divided accordingly between each tier. In this example tier one is allocated 80% of the resources and tier two the remaining 20%. With an expected adoption of 59 customers on tier one the resources are averaged out across each customer, which provides an average figure of 50Meg proxy mode anti-virus per customer. Sharing the remaining 20% of resources across all 110 tier two customers results in an average of 7 Meg proxy mode anti-virus throughput. While anti-virus in proxy mode significantly reduces the throughput capability, it has a far greater rate of malware detection due to the increased level of inspection. This is also typically one of the most resource intensive functions available on the platform, which provides a useful figure when planning to enable multiple security services.

As these figures are based on an average across all customers, it is plausible for this level of security service to be aligned to a slightly larger connectivity package, because not all traffic will be enforced with all types of security and not all customers will be at 100% utilization all of the time. This, again, is another way of trying to remain conservative at the planning stage. Once a customer adoption rate has been forecasted and an approximate level of service identified it is much easier to not only calculate the cost per customer over the lifecycle, but to also decide on a competitive and profitable sell price.

This example suggests an MSSP service sell price of €750 per month (€9,000 per year) for the tier 1 package and €150 per month (€1,800 per year) for the entry-level tier 2 package. The total cost per customer over the three years equates to €4,299 and €604 for tier one and two customers respectively.

Assumptions and considerations

Although this analysis aims to be as realistic and accurate as possible it can't be done without making certain assumptions. Here is a list of things to consider during this stage of any project:

The FortiCalculator assumes all new customer adoption to be apparent on the first day of each year, which is unlikely to be the case in a real world scenario. This will slightly overstate the profit figure produced as well as understate the projected loss. For true forecasts, customer adoption should be phased throughout the year.

The analysis also assumes that each new customer remains on the service for the remainder of the project lifecycle, paying the stated annual price per year. In reality this may not be the case, especially for customers on the more commoditized tiers, who may only commit to a 12-month contract and move to another provider after only one year.

Total cost per customer is not phased in line with how long each customer is present on the service. This cost is calculated by dividing the total CAPEX and OPEX costs between the total numbers of customers throughout the project lifecycle.

The FortiCalculator aims to provide a guide only and every project should always be subject to the chosen hardware being tested to replicate a real world environment. This should ideally be part of a documented test plan with clearly defined success criteria. Actual performance is dependent on many factors, such as types of traffic and the mix of security functions enabled, as well as the number of users.

Other elements to consider for a truer profitability forecast are the provider's other internal expenditure. These elements vary but can include costs such as technical support functions, staff training and education, billing, sales and marketing, as well as branding and collateral.

The return can be seen in the table below, which shows a potential payback period of around 12 months for the initial capital outlay.

Fig 2 - Commercial overview and levels of service

By Year			
	Year 1	Year 2	Year 3
Total costs	145,291	77,617	94,143
Profit & Loss*	34,709	345,389	625,857

Explanation of costs
Year 1 - Costs include Hardware, Support, Security updates (FortiGuard), FortiManager, FortiAnalyzer licensing and VDOM licensing
Year 2 - Costs include Support, Security updates (FortiGuard), FortiManager, FortiAnalyzer licensing and additional VDOM licensing
Year 3 - Costs include Support, Security updates (FortiGuard), FortiManager, FortiAnalyzer licensing and additional VDOM licensing

Fig 3 - 3-Year view of ROI

Summary

Fortinet's comprehensive eco-system eases the process for delivering complex managed security services. With custom built ASIC accelerated hardware architectures for scalability and performance, simplified licensing, and feature rich functionality that delivers true value for money, establishing the commercial viability of starting a new security service is made significantly more transparent and easier to justify.

The key to any successful multi-tenant service is taking the time to research the target market or customer profiles together with alignment to existing services. Positioning a security service to secure a particular application or network segment for a specific customer within a relevant budget will ensure a greater level of success than trying to work to a one-size-fits-all approach.

Success also comes from maintaining a clear view of exactly what challenges the MSSP is looking to address, not only for themselves but also for their customers. Fortinet offers multiple delivery models across its technologies such as shared, dedicated, physical, or virtual, so MSSPs can select the most appropriate model or even a mix of models.

Standardize on the chosen models and implement processes that automate or simplify management but remain agile enough to suit the customers' demands. This will ensure the correct operational efficiencies in order to scale and the flexibility to win bespoke, premium paying customers. Integrate Fortinet's management and reporting platforms and leverage the comprehensive intelligence and correlation across multiple security services through the power of the FortiGuard Labs.

Finally utilize Fortinet specialist MSSP resources and analysis tools such as the FortiCalculator to gain an insight into not only the capabilities of the Fortinet platform, but also the potential profitability of delivering it as a service.

www.fortinet.com

GLOBAL HEADQUARTERS
Fortinet Inc.
899 Kifer Road
Sunnyvale, CA 94086
United States
Tel: +1.408.235.7700
www.fortinet.com/sales

EMEA SALES OFFICE
120 rue Albert Caquot
06560, Sophia Antipolis,
France
Tel: +33.4.8987.0510

APAC SALES OFFICE
300 Beach Road 20-01
The Concourse
Singapore 199555
Tel: +65.6513.3730

LATIN AMERICA SALES OFFICE
Prol. Paseo de la Reforma 115 Int. 702
Col. Lomas de Santa Fe,
C.P. 01219
Del. Alvaro Obregón
México D.F.
Tel: 011-52-(55) 5524-8480