White Paper

HardenStance

New Managed Security Opportunities for Telcos

By Patrick Donegan, Principal Analyst, HardenStance

Sponsored by

NOKIA Symantec

July 2018

Executive Summary

- Demand for managed security services will grow, driven by increased cyber-security risk, greater complexity and the global shortage of cyber-security professionals.
- Telcos have key assets that position them well to capture market share.
- Financial risk aversion and lack of familiarity with the enterprise security model are the main barriers to telcos committing to leading in managed security services.
- An entry-level play managing security technology is unlikely to be very rewarding.
- Telcos should consider partnering with leaders in managed security services to share risk, assets and know-how, and grow their revenues and brand in this market.

Key trends in enterprise IT security

The trend is evolving away from enterprises spending capex on their own dedicated on-premises hardware.

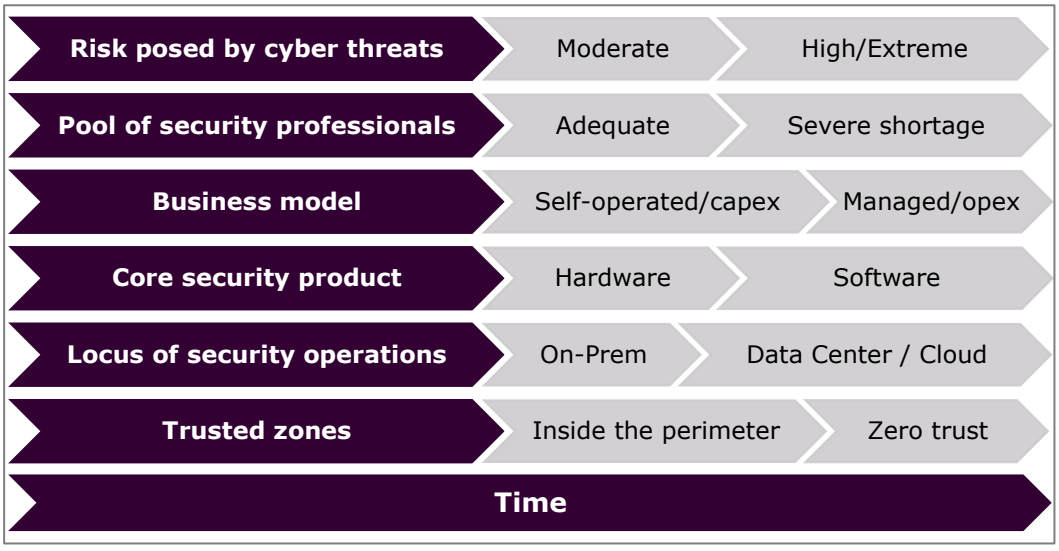
It's many years since best-in-class enterprise security centred around shipping a firewall product into a customer's premises. It's almost as long since the first telcos entered that market with a managed services wrapper around these boxes for those business customers that didn't want to operate them themselves.

As shown in **Figure 1,** dedicated boxes on-premises are increasingly a legacy approach now. The trend is evolving away from enterprises spending capex on their own dedicated on-premises hardware to consuming security software delivered from the cloud across their data centre, public cloud and on-prem environments.

The security 'perimeter' that firewalls were designed to protect has had permanent holes punched through it. This is due to the extension of enterprise infrastructure into the cloud and by the Bring Your Own Device (BYOD) phenomenon of employees and third-party partners accessing enterprise applications at home, in public and on premises.

Firewalls are now widely recognized as just one of the many security layers needed to enforce Confidentiality, Integrity and Availability (CIA) in information security. In what is now recognized as a compromised, 'zero-trust' environment, threat monitoring and Incident Response (IR) that were once confined to the very largest organizations handling the most sensitive data, are becoming increasingly commonplace. Management and their IT security teams are also having to build compliance to the General Data Protection Regulation (GDPR) into their IT security posture.

Figure 1: Trends in Enterprise Security



Source: HardenStance

As enterprises increasingly look for an opex rather than a capex-oriented model, the role of Managed Security Service Providers (MSSPs)* is evolving as well. It's no longer just about managing a customer's firewall device on their premises but about managing protection, detection and remediation services from a Security Operation's Centre (SOC) across a customer's assorted IT environments 24 hours a day, 365 days a year.

HardenStance expects that demand for managed security services will grow over the coming years, driven by three main factors and the inter-dependency between them:

- increased business risk posed by the growing sophistication of cyber threats;
- growing complexity of managing security across hybrid enterprise infrastructures;
- the global shortfall in qualified cyber-security professionals. This critical talent - including threat monitoring analysts – is expensive and very difficult to retain for all but the very largest enterprises and the very best among cyber-security companies.

Many leading MSSPs report that 60% or more of their sales are in the United States.

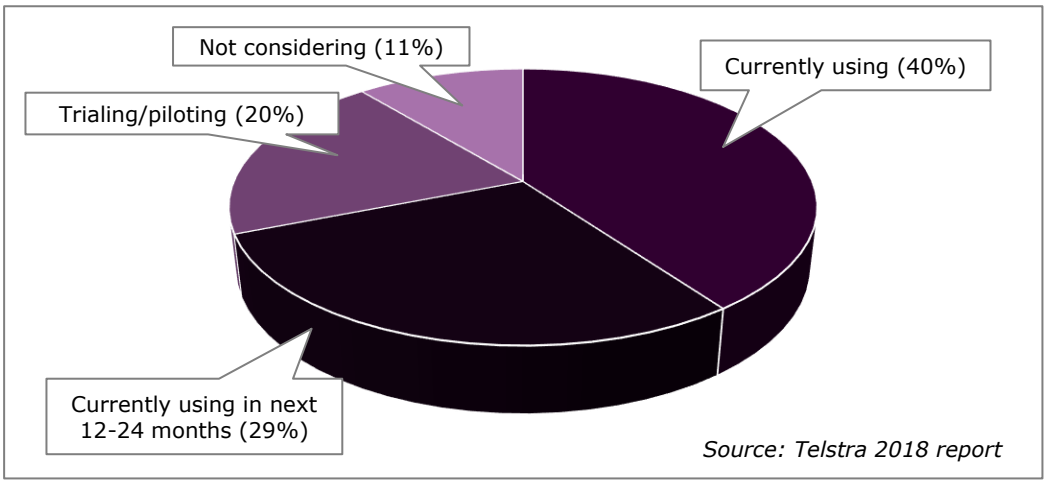
Recent credible surveys of IT decision-makers support this assertion that demand for managed security services will increase:

- A February 2018 Ponemon Institute survey reports that out of 1,100 IT practitioners in the U.S and EMEA, 68% already believe managed security services are important, very important or essential and that fully 80% take that view over the longer term.
- In **Figure 2** Telstra's 2018 Security Report states that while 40% of its global sample of 1,250 IT security decision-makers is already using managed security services, still more - 49% - are in trials or pilots or considering them in the next year or two.

Global trends in outsourcing to MSSPs are quite nuanced. Many leading MSSPs like IBM Security, Symantec, Secureworks, Verizon, BT, Trustwave (owned by Singtel) and CenturyLink, report that 60% or more of their sales are in the U.S.

Even though many Fortune 500 companies still manage most of their security themselves, they are still outsourcing sizable shares of their security spending to fill gaps in their in-house capabilities. Hence the largest MSSPs continue to report that these Fortune 500 customers account for the largest share of their sales, followed by government and public-sector organizations.

Figure 2: The Outlook for Adoption of Managed Security Services



*MSSPs shouldn't be confused with Managed Service Providers (MSPs) which tend to be smaller, locally or regionally based, companies that provide a variety of IT outsourcing services. Many MSPs provide some security services but aren't specialized in cyber-security. A subset of MSPs are competitive in the MSSP space, some by partnering larger MSSPs.

In addition to growing share with these established buyers, the largest new opportunities in managed security services in the coming years will be among key segments of the enterprise market that typically have not been major buyers until now.

Buyer segments with significant new growth potential are:

- Large national and regional corporates in EMEA and Asia.
- Medium and Small-Medium Enterprises (SMEs) worldwide, employing between five hundred and a thousand people.

These buyers have not spent much on managed security services until now, due in part to the largest MSSPs focusing on the Fortune 500s as well as pricing and ease of use challenges. Telcos are potentially well placed to help drive adoption because they have a reach into these customers at a national market level that a global MSSP lacks.

Telcos need to ask whether it's even credible to try growing enterprise ICT revenues without a strong cyber-security play.

The telco outlook on the MSSP market

The strong outlook for managed security services, combined with how the leading global MSSPs have left large market segments materially underserved, explains why security invariably comes up whenever telcos review their enterprise strategy. These days telcos looking to grow their enterprise ICT revenues need to ask whether it's even credible to pursue that without a strong supporting cyber-security play.

To date, only a small subset of the world's largest telcos have made substantial commitments to deliver globally competitive managed security services as part of a long-term commitment to enterprise security. The most recent annual security revenues of BT, Telefonica and Singtel are shown in **Figure 3**. Other recognized players include Orange, CenturyLink, AT&T, Verizon, Telstra and NTT Security. Recognizing that in an uncertain world, growth in demand for cyber-security services over the long term is as safe a business planning assumption as you're going to find, Vodafone, KPN and Deutsche Telekom have also committed to this market more recently.

HardenStance estimates that managed security services already account for between a quarter and a half of total security revenues in the case of most leading telcos that are active in the enterprise security market. There is a clear opportunity for these established players to grow that share in the coming years. Other telcos that want to commit to cyber-security should also be thinking about putting managed services at the heart of their strategy.

What telcos bring to the table – scale, reach and security efficacy

As well as traditional advantages like reach, scale in procurement, and generally trusted customer relationships, telcos will be able to exploit a new type of 'natural advantage' that's only just emerging in enterprise security.

Network Functions Virtualization (NFV), and 5G in particular, will drive telco networks in a direction that puts them in a stronger position to differentiate in enterprise security. This is because the telco network is effectively going to become meshed with the cloud.

Figure 3: Examples of the security revenues of leading telcos

Country	Operator	Annual security revenues	
		Local currency	US$
UK	BT	£ 500m	$660m
Spain	Telefonica	€ 430m	$500m
Singapore	Singtel	SGD 530m	$390m

Source: HardenStance, sourced from latest earnings reports

The cloud-native 5G network will be enabled to host enterprise applications. In light of enhanced cyber threats and regulatory requirements like GDPR, enterprises that want to create new digital experiences for customers leveraging 5G will expect tighter control of the infrastructure that these applications run on, including the security features. In providing enterprise services across their virtualized network infrastructure, telcos will be drawn deeper into securing those enterprise applications than in the past.

This plays out notably in the way NFV enables distribution of network functions to the edge of the telco network. Some edge use cases will require that a telco's Virtual Network Functions (VNFs) share the same hardware instance as the enterprise's own software instances, like analytics. These software instances of telcos and their enterprise customers will need security protections from one another.

Edge distribution also gives telcos a unique competitive advantage. Hosting some security services at the edge rather than according to a centralized model can enable higher security efficacy, lower costs, or both. Think of providing DDoS protection in real-time rather than just sampling traffic at intervals, for example. Telcos will have an advantage here in enterprise security relative to non-telco MSSPs.

Hosting some security services at the edge can enable higher security efficacy.

There are two types of approach to the market that telcos can take

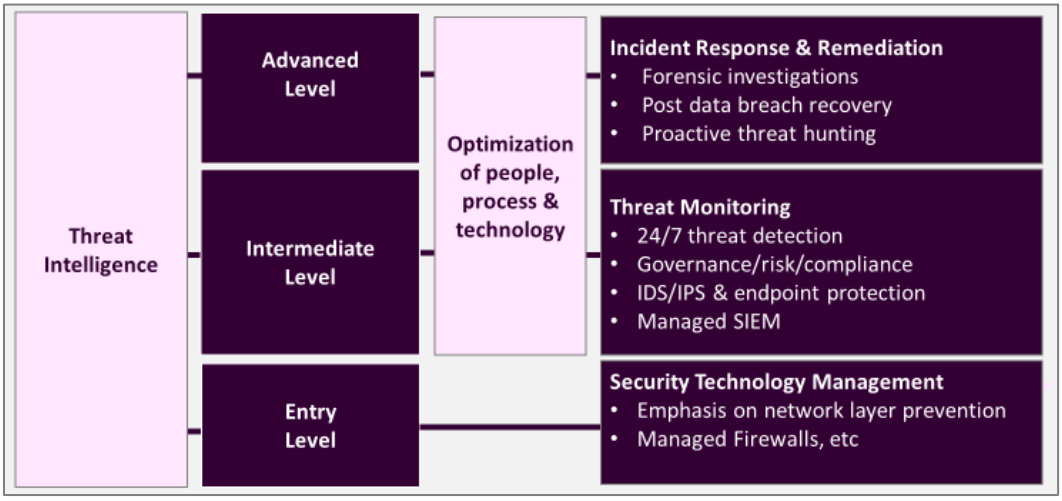
Telcos that wants to commit to the MSSP market must answer two key questions:

- Will they commit to intermediate and advanced segments or just to the entry level?
- Will they make a basic or a strategic commitment to the market?

Figure 4 provides a generic, simplified, depiction of the three tiers of an MSSP's services portfolio. Today's leading MSSPs – including the MSSP arms of most of the telcos listed on page 4 – are present in all three tiers. Threat intelligence underpins all three. It can be collected from multiple sources including the telco itself, curated, and tailored to different customer groups, including by industry vertical.

It's only with the addition of Intermediate and Advanced levels that an MSSP can help drive the very best IT security posture for an enterprise via the end-to-end optimization of people, process and technology. This is the greatest value that an MSSP can bring. It creates the best possible platform for monitoring for internal threats and understanding which external threat actors pose what specific threats to a customer's own unique infrastructure, whether on-premises or in the cloud. They can then tailor protection to meet those threats before, during and after an attack leveraging trained playbooks wherever possible.

Figure 4: Three tiers of managed security services



Source: HardenStance

Entry-level technology management corresponds most closely to a telco's core business model. This is why, over the years, some telcos have entered the MSSP market at this level and stayed there. Others have entered here, only to subsequently exit when they found the market yielded too little revenue or was too cut-throat. Until now, it's only the largest that have committed to investing up the value chain in intermediate and advanced threat monitoring, Incident Response (IR) and remediation layers.

Telco barriers to investing beyond the entry level

Making a strategic commitment to the managed security services market requires telco management being willing to navigate important internal barriers such as the following:

- **Lack of in-house expertise**. The global shortfall in cyber-security personnel is a barrier in itself. This extends to specific advanced areas like threat monitoring and digital forensics where it's very challenging to attract and retain top talent.

The modern telco is typically risk-averse. Sizable up-front capex in SOC resources tends not to sit well with many telco CFOs.

- **Adapting to greater ambiguity in the business model.** Compared with telecom and other ICT services, MSSP services operate on the basis of far less certainty. MSSPs must invest resources in investigations that sometimes don't yield conclusive results. They can't show with certainty that a vulnerability isn't hiding somewhere in a customer's infrastructure with potential to cause future damage. Telcos must adapt to this and focus on the right performance metrics.
- **Aversion to financial risk.** The modern telco is typically risk averse. Sizable up-front capex in SOC resources doesn't sit well with many telco CFOs. They also tend to expect fast time to revenue for any new service the company sells. The fact is that in intermediate and advanced MSSP services, the procurement cycle is longer. Enterprise customers need to spend some months familiarizing themselves with an MSSP's people and capabilities before placing an order – and that first order is often for just one or two services.
- **Lack of familiarity with customized service contracts.** Although their business models have evolved in recent years, the core of a telco's business model still consists of selling commodity services at scale. The ability to engage in a high level of customization for enterprise customers is a key requirement in most managed services and managed security services is no exception.

The next two chapters map out what the two different approaches – basic and strategic commitments - look like from a telco perspective. There is an element of correlation between this choice that telcos face and the choice they face as to whether to confine themselves to the entry level segment.

It might appear obvious that the greater a telco's commitment to intermediate and advanced services, the more strategic its commitment must be. There are nevertheless two important qualifiers to that proposition. The first is that investing initially in the entry level can serve just as a first step into the bigger managed security services market. Conversely, as will be shown, if the underlying operating model doesn't meet an enterprise customer's expectations of a strategic partnership, even the broadest portfolio of advanced MSSP services will still feel basic or tactical to customers.

The risk with a basic approach

The case for only targeting entry level services like managed firewall tends to go as follows. L1-L2 or L1-L3 technology management is what telcos do; it's what they're good at. Demand for cyber-security is growing across all business segments. Since so many 'boats' have risen with this 'tide' of demand until now, there's no reason why another one won't rise as well. Revenues from managed firewalls might not set a CFO's heart racing, but if there's additional revenue on the table, and since the time-to-revenue tends to be quite rapid, then so long as margins are acceptable what's not to like?

There are several flaws in this logic. For example:

- Robust cyber-security involves integrated optimization of technology, people and processes. Technology management only addresses one of these in isolation.
- If, as expected, enterprises increasingly demand higher value services, that will leave the market in managed-technology-only services subject to fiercer price competition. A race to the bottom for market share could easily follow.
- Due in part to the inherent limitations of any one product in a security architecture, the market in managed products like firewalls is vulnerable to high churn. Where a telco's brand gets caught up in a cycle of high churn, customer push-back can negatively affect that telco's reputation and Net Promoter Score (NPS).
- A rising tide may have lifted all boats. But if the market is evolving towards greater maturity, new players targeting just the low end may have missed their chance.

On its own, technology management is unlikely to yield positive results, especially when softer brand-impacting factors are properly factored in.

For most telcos, a focus on just the managed technology segment is unlikely to yield very positive results.

Common flaws in basic MSSP business models

Whether they focus on one or two services or a full suite of services, basic MSSP models that are run along tactical operating lines tend to be heavily sales-driven and call-centre focused. Common flaws in the way they are run include the following:

- **The wrong kind of automation is prioritized.** Pooled call centre automation is considered at least as important as security workflow automation. Rapid initial pick-up is core to the value proposition pushed to customers. Zero-touch, push-button re-directing of calls by operatives is central to the company's own cost containment. Customers usually engage a different operative each time, even when calling back with the same unresolved issue.
- **SOC analysts are incentivized according to metrics that correlate poorly to actual value as perceived by customers.** There tends to be a myopic focus on analysts hitting diagnostic micro-targets that meet minimum contractual obligations. If an analyst is completing more events or closing more tickets than a colleague, that alone is deemed to mean they are the higher performer of the two in these call centre environments.
- **Customer and employee churn rates are high.** The best cyber-security talent is motivated by a combination of financial reward and pride in a job well done. These environments may offer the former, but they don't satisfy the latter. SOC analysts are frustrated by inflexible and mis-aligned metric management. Customer escalations are also frequent. They feel they lack a trusted advisor for when they encounter major difficulties, even if granular contractual targets are largely met. Customers are easily tempted to change provider.
- **Revenue growth is heavily dependent on new customer acquisitions derived from high marketing spend and aggressive discounting.** Rates of renewal, upselling to existing customers, and customer referrals tend to be low.

There are doubtless a few markets where a telco can derive some value for a given period from this approach. On balance, however, most telcos are better off using an entry level play as an initial stepping stone or avoiding the MSSP market altogether.

Figure 5: How basic and strategic MSSP business models compare

Feature of an MSSP business model	Basic MSSP business model	Strategic MSSP business model
Segments targeted	Entry-level	Intermediate & advanced
Familiarity to telcos	Very familiar	Unfamiliar
Automation priority	Cost saving	Time to resolution
Management metrics	Response times	NPS & churn
Customer escalations	Frequent	Rare
Revenue potential	Low	Medium-high
Time to revenue	Short term	Medium term
Impact on NPS	None/negative	Positive
Customer/employee churn	High	Low

Source: HardenStance

Excellence in managed security services can be very powerful from both a customer retention and customer referral perspective.

The opportunity with a strategic commitment

Making a strategic commitment to managed security services is a fundamentally different proposition. Clearly, the revenue opportunity itself is very much larger. As an example, the world's largest MSSPs are each generating revenues of $500 million or more now. In addition, the potential to enhance a telco's core brand through excellence in managed security services is potentially very powerful from both a customer retention and customer referral perspective.

Here's a summary perspective on what a strategic, high-end MSSP operating model looks like and how it compares with a more basic model:

- **Employees are trusted with an important level of discretion, responsibility and ownership of the customer relationship.** Some cross-function SOC analysts are permanently assigned to the same customer groups or individual customers. This level of customer intimacy – for example, allocating analysts per industry vertical - improves the actual time taken to fix issues and improves customer intimacy.
- **Orchestration is prioritized alongside automation.** There is proper investment in intelligent workflow automation. Menial tasks and responses to known threats are automated. Wasteful steps taken by humans are eliminated rather than automated. Allocation of specific staff to specific customers for first line response co-exists with pooled resources. Machine learning and AI supports investigations into complex threats. The limitations of automaton in Incident Response are recognized because ambiguity can be better served by orchestration than automation.
- **Management focuses on the incentives that correlate most closely to customer satisfaction.** Employee performance is evaluated less against arbitrary metrics and more against the propensity of their customers to renew their contracts and grow spend as well as their willingness to refer the business to peers via their Net Promoter Score (NPS). An individual's contribution to teamwork in enhancing the efficacy of security orchestration is recognized, not just individual performance.
- **The business has more balanced sources of revenue growth.** Rather than being largely dependent on new customer acquisitions, revenue growth also relies on customer renewals, upselling, and customer referrals.

The case for partnering in the MSSP space

Some telcos do buy into the strategic rationale of making a substantial, long-term commitment to the managed security services space. However, they are held back by the barriers to investing in it for the reasons cited. For these companies, the obvious solution that presents itself is to go to market in partnership with a bigger player.

Larger, more security-focused partners can fill in the gap in expertise and familiarity with the managed security operating model. They bring a sizeable footprint of assets to the table which should substantially reduce the upfront investment that any telco needs to enter this market. And they bring the market power that can attract and retain top cyber-security talent which most smaller players – including most new entrant telcos – just can't. This is the path that will offer most telcos the highest chances of long-term success in this important market.

About the sponsors

The sponsors of this White Paper are Nokia and Symantec.

About Nokia

We create the technology to connect the world. Powered by the research and innovation of Nokia Bell Labs, we serve communications service providers, governments, large enterprises and consumers, with the industry's most complete, end-to-end portfolio of products, services and licensing.

From the enabling infrastructure for 5G and the Internet of Things, to emerging applications in digital health, we are shaping the future of technology to transform the human experience. Nokia's holistic managed security services approach targets security challenges across mobile, IP and fixed networks. Our global presence and wide security portfolio help address varied security issues with telco grade quality.

Nokia security services help prepare for cyber threats and comply with regulation and ensure secure adoption of cloud, big data and IoT technologies in the digital transformation era. Nokia's Managed Security Service and Security Risk Index provide a comprehensive backbone for telecom security encompassing all areas of security, including the assessment and protection of cross-technology networks operating in multivendor environments. Nokia offers Managed Security Services also as a white-label option for communications service providers to cater to their enterprise needs. nokia.com

About Symantec

Symantec Corporation (NASDAQ: SYMC), the world's leading cyber-security company, allows organizations, governments, and people to secure their most important data wherever it lives. Enterprises across the world rely on Symantec for integrated cyber defense against sophisticated attacks across endpoints, infrastructure, and cloud.

More than 50 million people and families rely on Symantec's Norton and LifeLock Digital Safety platform to help protect their personal information, devices, home networks, and identities at home and across their devices.

Through Symantec's Managed Security Services (MSS), companies receive 24x7x365 security monitoring and real-time security analytics, equipping them with the strategic insights needed to prioritize and respond to the most critical incidents and build strategies to protect the assets, reputations and viability of their organizations.

MSS is a comprehensive, advanced threat detection service that is built on a close partnership between our MSS analyst teams and each customer. Together, they build the security monitoring program that is tailored to each customer organization's security issues and business goals. Telcos already partner with Symantec. They utilize the

company's deep cyber-security services expertise, comprehensive monitoring and threat intelligence to enrich their own managed security services for their customer base. Symantec.com

About HardenStance

HardenStance is a leading independent industry analyst firm delivering trusted research, analysis and insight in IT and telecom security. HardenStance.com