Cybersecurity Service Packages - The New Opportunity

For many organisations, cybersecurity has just got too complicated and difficult to manage completely in-house. As the global threat landscape has continued to become more complex, this was perhaps inevitable. But when you add in other factors of our times, such as the move to home-working, the move to cloud, the move to IoT, cybersecurity skills shortages and the need for 24/7 security operations, then you have overwhelming pressure for fundamental change. To deal with escalating technical complexity as well as the human creativity of attackers, security products on their own are not enough - expert managed and professional services are now needed, by qualified security engineers.

For many, the only practical way ahead is to outsource part or the whole of the security function, and in particular the functionality of a 24/7 security operations centre (SOC).

Distribution of Packaged Services

This situation creates an exciting opportunity for a completely new business in validating, packaging and distributing a complete family of cybersecurity services, via a network of resellers and MSPs (managed service providers). The task is not only technical, and legal, but is also commercial in the sense of achieving scale by reaching out via existing reseller relationships to many hundreds of thousands of end-user organisations. This is the domain and expertise of a distributor, which can now find whole new areas of added value to offer its resellers. Not only can a distributor such as Titan Data Solutions supply this whole new business line, with comprehensive reseller contracts and technical support, but it can also offer a family of services from different vendors which complement each other - for example, incident response to wrap around MDR (managed detection and response), or penetration testing from one supplier to test the MDR from another supplier.

An Efficient Business Model for Resellers

In this new world of packaged cybersecurity services, the reseller no longer needs to invest in expensive in-house technical support – the distributor can provide any necessary presales technical support and the SOC provides the service to the end-customer, which the SOC supports entirely itself. The sales training for the service packages is straightforward, so the business can start immediately. By selling standardised third-party expertise and services, instead of products, the cybersecurity business model is transformed into a much more attractive proposition for resellers. Even non-cybersecurity resellers, such as storage and archive resellers, are now seeing that this may now be the time to catch the wave and add cybersecurity into their existing portfolio.

Added Value for MSPs

While resellers can benefit from selling service packages and then standing back from the technical aspects of supplying them, on the other hand MSPs can benefit from a second contractual model in distribution whereby the services are provided to them and they in turn provide them to their end-customers, as part of an overall service offering. In both cases the reseller invoices the customer and manages the customer relationship, but the arrangements for provision of the services are entirely different. The distributor of

packaged cybersecurity services should provide a reseller contract that covers both types of commercial scenario.

Delivering Winning Cybersecurity Strategies – Critical Asset Protection
Armed with cybersecurity service packages, resellers and MSPs can provide innovative cybersecurity strategies that offer greater security benefit for less cost, versus earlier strategies. In addition to the managed services approach itself, which is based on SaaS (software as a service), there is the opportunity to reduce costs in a new way by focussing maximum defensive attention on the most critical assets within the network.

For example, the security budget may not be large enough to cover MDR (managed detection and response) services on all the servers, but a subset of those servers may be defined which will be covered. An MDR service such as the one provided by Alert Logic, and distributed by Titan Data Solutions, makes this a much more effective solution than it may already even seem: since this is a service-based solution to the real customer problem, the SOC will ingest logs from network devices and also scan network traffic, in addition to taking log information from agents on the covered servers. The resultant 24/7 monitoring and response service is not constrained by any "product" definition – it is tuned to the reality of the customer situation, to deliver maximum security value, while existing as a standardised package. The charging basis in this case is determined simply by the number of server nodes covered, and each node includes the ability to ingest a particular volume of log data every day from other devices such as firewalls. Building up in this way, highly cost-effective cybersecurity strategies can be implemented, delivering substantial cost savings versus alternative approaches. Resellers can use the distributor's technical staff to make these arguments and demonstrate the security benefits. The reseller can go on to win large contracts as a result which will grow over time and bring future renewal revenue.

Of course, attackers may attempt to penetrate the weakest point of a network such as a laptop, and then move laterally to attack critical assets. To counter this, complete MDR coverage of all endpoints would be possible, but the high cost of detailed human attention in any monitoring service across the whole estate is likely to be difficult to justify. Alert Logic's MDR service is designed specifically to support a critical asset protection strategy. It monitors network traffic of the server among other things and can pick up the signs of an infected laptop or user account, even if it is not directly monitoring the laptop. Moreover, for example, compromised user accounts can also be detected and suspicious activity on centralised user management servers can be picked up. On top of this, Alert Logic provides an extended endpoint protection program that can run on laptops and other endpoints, alongside antivirus, to substantially elevate the preventative security capability there, along with vulnerability scanning and asset discovery.

Developing this kind of services-based strategy, which enables a new level of targeted threat monitoring of critical assets as well as uprated general endpoint security, is especially important when endpoints such as laptops and other connected devices are under increased risk of compromise. This may be the case now, for example, as a result of the mass move to home working, or when IoT (internet of things) devices are being added into a network.

Simplifying Cybersecurity for the Cloud

The popular migration to cloud-based architectures raises new and complex cybersecurity challenges. Cybersecurity managed service packages, delivered via distribution, can deliver cost savings and also greatly simplify the approach to these areas - which include network threat detection, security monitoring, log analysis, vulnerability scanning, web application firewall and application-level attack monitoring.

For example, the SaaS-based MDR (managed detection and response) service from Alert Logic, as distributed through Titan Data Solutions, can be implemented with immediate value on Microsoft Azure, as well as AWS and Google Cloud Platform, based on its out-of-the-box ruleset which has been tried and tested on a customer base numbering over 4,000 end-customers and which is continuously updated by the in-house threat intelligence teams. The managed service approach removes the need for the end-customer themselves to set up alert scenarios, maintain threat intelligence, carry out initial triage of events, provide 24/7 human monitoring of data, and produce actionable recommendations in response to an alert. While large enterprise end-customers may still want to do this themselves, for example using Microsoft's Azure Sentinel as a cloud-native SIEM, for very many customers the cybersecurity managed service package will be a practical and highly cost-effective solution. Even large customers may decide ultimately to use an MDR service package, such as Alert Logic, perhaps in order to focus their in-house resources on incident investigation in conjunction with the service provider.

The Alert Logic package is designed, as a managed service, to address the end-user's spectrum of cloud-based requirements and it does so in a way that a set of products could not match. For example, in addition to collecting logs and network traffic from the protected environments, the service uses vulnerability scanners and cloud APIs to build up an asset topology complete with vulnerabilities and misconfigurations, and it carries out UBAD (user behaviour anomaly detection) on Microsoft 365, Azure AD and other authentication platforms. The result is a complete solution, comprising cutting-edge, up-to-date knowledge as well as the SaaS-based software tools and their day-to-day operation.

Professional Service Packages

While MDR-based strategies for critical asset protection are important considerations for very many companies with 25 or more servers in their network, certain other types of cybersecurity packaged professional services can also be attractive for organisations of all sizes which need to increase their level of security.

For example, the CREST-accredited, UK-based SOC DigitalXRAID provides a range of cybersecurity professional services via Titan Data Solutions as distributor. These bundled services are standardised and are easy for resellers to present to end-customers. Starting from "pass-first-time" Cyber Essentials Plus certification and vulnerability scanning, further services can be added including penetration testing of infrastructure and web applications, and phishing simulation and training. These service packages provide a phased approach to increasing the end-customer's level of cybersecurity, and to becoming a much harder target for attackers.

Conclusion

There is a new opportunity arising from the emerging meeting point between, from one side, the worsening threat landscape, the uptake of cloud, risks arising from the move to home working, risks arising from the move to IoT, constrained corporate budgets and skills shortages; and on the other side, the latest state of technology and the SaaS-based cybersecurity service packages that it now enables. Cybersecurity strategy proposals based on managed service packages and critical asset protection will carry significant competitive advantages over alternative approaches, both for cloud and on-premises implementations. In order to bring these new service packages to the end-customer at scale and at affordable prices, a new kind of value-added distribution is required. The distributor Titan Data Solutions has assembled a family of cybersecurity service packages from leading vendors including Alert Logic and DigitalXRAID, together with a sales, legal and technical support framework to enable its wide network of resellers and MSPs to take those service packages to market efficiently and at scale.

Keith Maskell
Head of Cybersecurity
Titan Data Solutions Ltd
October 2020