



*Your Next Generation Security Trusted Advisor*

# WHO ARE NGS?

Formed in 2018, NG Security (UK) Ltd are independent, vendor agnostic, next generation security trusted advisors, providing all-encompassing solutions from the perimeter to the endpoint.

The Directors, previously at the helm of the Security Reseller of the Year 2013, bring with them over 60 years of IT security industry experience. Using their broad experience of the Security market combined with the vast knowledge and ability of the wider team, NGS give an unrivalled delivery capability that will help your business develop a strategic architectural blueprint, a business case and a clear roadmap. We translate ideas into actions, delivering significant and measurable value with every element of work undertaken. Unlike many, we're not offering point solutions but providing total security solutions.

NGS are recognised as thought leaders in the Next Generation Security marketplace and constantly research the threat landscape and how to protect their clients critical assets. Partnering with the best technology vendors enables NGS to provide exceptional customer satisfaction.

The delivery of projects and adopting new strategies can often be a multi-year program, involving organisational and cultural change, process re-engineering & numerous technology components. NGS will deliver options to ensure the most informed decisions are made, offering consultation and pre-sales services, then supply, install and support services, providing everything from concept to completion.

- 60+ years of industry experience
- Rebirth of the Security Reseller of the Year and fastest growing Checkpoint Partner 2013
- Recognised by the leading next generation security vendors
- Technical expertise
- Customer focussed
- Consultative approach
- Cyber Essentials and IASME accredited



IASME Consortium®



**Phil Dick**

Managing Director



**Jonathan Lassman**

Managing Director



**Dilan Hindocha**

Director



**Rob Jeffery**

Technical Director

# THE CYBER SECURITY MARKET TODAY

In 2004 the global cyber security market was worth \$3.5 billion. In 2017 it was worth over \$120billion, and as the cyber market has grown, the associated threat landscape is rapidly evolving with it. Long are the days where the focus was on the firewall at the perimeter and anti-virus on the endpoint. With the location now well beyond the security of the office as more and more users are working remotely, cyber security is on the list of the most important threats to business.

The challenge today is no longer just detection and protection, but also recovery. Although new malware is being developed at tremendous speeds that needs to be detected and remediated before it becomes a problem, the real initial necessity is to understand where the risk starts and finishes and then to build a response and remediation plan to an attack because that attack will happen.

Protecting your organisation can no longer rely on products that use static signatures and traditional detection methods, malware and threat actors are evolving at a faster and faster rate. The technologies you use to protect your organisation need to evolve as well. Behavioural analytics, machine learning and AI are now at the forefront of protection technologies and can offer a far greater level of protection and increased reaction times to security incidents.

With an evolving working culture comes an evolving threat landscape. Staff need to be more and more agile and mobile, and are working from public and mobile networks more and more. The traditional hard shell model is no longer suitable to protect your business and the ability to secure the corporate network from outside this perimeter is paramount.

The number of systems users have to interact with on a daily basis is constantly on the rise. Users are increasingly re-using passwords more and more, and with the rise in phishing attacks and threat attackers using social engineering from different vectors, password loss is increasingly becoming one of the greatest risks to organisations data. Complex password policies are no longer the answer as users need to be able to still work efficiently but, in a secure manner. Privileged access management, Identity management, multifactor authentication and cloud application security brokers are now a must for any organisation to ensure they not only protect user credential but, enable staff to work without hinderance.

With the GDPR now in effect the financial implications of a data breach becoming ever greater cyber security is not at the forefront of most board level conversations. However, securing an organisation now needs to evolve as rapidly as the threats do. For most organisations maintaining pace with threats is simply not possible due to staff requirements and financial constraints. Managing security products requires specialist skills and knowledge, these dedicated security focussed employees are not always financially viable within some organisations. On average an IT security specialist can cost a business upwards of 80k per year. Specialist cyber security service providers can help organisations not only dramatically improve their security posture but also deliver cost and efficiency benefits.

## WHY NGS?

In a market where leading security vendors have multiple partners, we have returned to the arena with open arms for our partners, and customers old and new.

Despite being worth around 30 times more than it was, they say that the market today is almost back to where it was in 2004. There's a few leading partners and then a layer of boutique security focussed specialists who are built on a team that have the experience, at both partner and vendor level, but with the understanding of the ever evolving challenges that the customer faces. We have always believed that we do this role in reverse, deciding what to sell in a marketplace that is becoming more and more crowded.

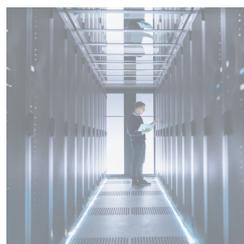
NGS focus on a few key messages; doing more for less, consolidating solutions where possible, driving change and awareness of the right use of technology, and to ensure that our customers have the fastest recovery time from a breach or attack. Of course, we can help reduce time to detection with an aim to prevent, however we are realists and we understand that the threats are evolving. Minimal downtime will be essential to every business and we understand that different levels of security maturity will form an appropriate roadmap plan with the customer.

We're trusted advisors, and we constantly strive to bring the best next-generation technology to the market.

We've been here before, and with previous successes as the Specialist Security Reseller of the Year in 2013 & 2014 and the Fastest Growing Check Point Partner 2013, both prior to the sale to Capita, NGS bring with them over 60 years experience in the cyber security space. NGS solve problems for customers, and we understand that the added value begins from the first discovery meeting and continues throughout the service and sales cycle and beyond.

The areas of security that we can offer:

- Perimeter Security - cloud and on-premise
- Web, Email and Endpoint Security
- Cloud Access Security Broker (CASB)
- Secure Messaging and Collaboration
- Privileged Access Management, Network Access Control and Identity Management
- Phishing, Simulation Training and awareness
- Breach Detection, Insider Threat, and SIEM



# PARTNERS



# SERVICES

## Initial Engagement

With any engagement for new solutions the first step in the process is understanding. NGS will engage with you to have a complete understanding of your pain points and then work to provide the best solution to overcome these and add value. We want you to make the right choice for you and as NGS are vendor agnostic, we will consult with you and provide options that we feel will offer you the best solution to meet your requirements.

## Support

NGS understand that effective and responsive technical support is essential to our customers ongoing business operations. NGS offers telephone and email support during office hours as standard with 24/7 support also available. We pride ourselves on being able to respond quickly and being able to work through problems with our customers and partners. 1st and 2nd line support will be available to all NGS customers and where necessary will be escalated with our vendor partners in accordance to our service level agreements. All calls are logged, and progress monitored to ensure that each call is resolved and results in a successful outcome.

## Co-Managed & Fully Managed Services

In addition to the standard support services that NGS offer, we can also provide both co-managed and fully managed support services. These options can take away the headache out of managing complex security solutions allowing you to eliminate in-house administration and reallocate IT resources to projects better aligned to your business initiatives.

## Professional Services & Consultancy

With our professional services we provide a complete end-to-end service to smoothly and efficiently deliver a total security solution. NGS are supported by an experienced, passionate & dedicated team who believe in delivering bespoke, robust solutions to fit the exact needs of the business from assessment, consultation and design, then to deployment and knowledge transfer.

To ensure the transition from old to new is seamless and pain free, NGS also look at the supporting infrastructure and make recommendations if required, so you get the best out of your solution. Our professional services team have experience in all types of deployments from small software implementations to complex multi-vendor integrations, and you can rest assured that you are in good hands.

# SERVICES

## Advanced Footprinting

The NGS Advanced Footprinting service takes a leaf out of the hacker's play book to help you stay ahead of the cybercriminals. We use the same methods as would-be attackers to build a complete picture of your Internet attack surface to help you bolster your defences. With a full list of the networks, infrastructure and applications associated with your business, as well as the hard-to-find details that opportunistic hackers typically target, you'll be able to strengthen your security posture proactively before an attacker strikes.

## Firewall Healthcheck & Security Review

The NGS Firewall Health Check and Security Review is an in-depth assessment of the security and performance of your firewall or next generation firewall. We review the health of your appliances and system performance metrics, their configuration and the security of the running rule set. On completion of the review, we provide you with a written report setting out our findings and recommendations in order of priority.

## Phishing Simulation Service

The NGS Phishing Simulation Service helps educate your employees and raise their phishing awareness and enables you to measure employee susceptibility to social engineering. It is therefore important to include phishing awareness in your employee security training. Awareness training is best achieved through explanation and demonstration and phishing simulation helps achieve this by targeting your employees or specific functions, with highly credible email phishing campaigns with the aim of raising awareness of the risks and improving knowledge of what to do when a suspicious email arrives.

## Security Resilience & Readiness Check

The NGS Security Resilience & Readiness Check is a detailed assessment of your full security posture, covering policy, processes and technology platforms. Our consultants review the critical areas of your security architecture and practices and then map them against industry leading practice. From this we create a maturity score of your security posture, identify risks and areas for remediation and provide you with guidance around the high priority issues identified and the steps recommended to remediate them.

## Virtual CISO & IT Security Manager

From strategic board level advice, risk management and technical guidance and best practice, NGS can offer a virtual CISO and IT Security Manager to provide you with expert security services at any level. vCISO removes both the cost implications and the challenge of finding the right person by making available industry recognised and certified consultants, who can be called into action to cover the security needs of any organisation.

# SUPPORT SERVICES

## Standard Support

The NGS Support team can be available 24 hours a day, 365 days a year for any critical support issues you have, depending on the level of support you decide to choose. NGS offer 8x6, 24x7 support and Managed Security Services which can be tailored to your organisations needs.

For all our support offerings, your IT practitioners will be able to open cases with the Security Operations Centre (SOC) by email, telephone or via the NGS online support portal. The portal will also provide access for you to review any case (open or closed) and view updates as the case progresses. Statistics from the NGS health monitoring service will also be available. Access to your account in the support portal will be secured by SSL transport and authenticated using a username and password.

NGS operate a UK based SOC staffed by full time support engineers, available to answer queries and resolve any issues that may arise, and our active training and certification program will ensure that the skills of all our staff supporting you are improved and kept up to date. Where required issues that are identified as requiring vendor input are escalated at the earliest opportunity.

## Support Management

The NGS support and service desk is run to ITIL guidelines and performance is reviewed weekly with a major review quarterly, to ensure service levels are maintained to the standards you expect. We will use ITIL guidelines to align ourselves with the needs of your organisation and to support its core processes and use it as a tool to help you facilitate change, transformation and growth as we support your security infrastructure.

The key benefits of our adoption of ITIL practices is that our experience within the industry allows us to:

- Support business outcomes
- Enable business change
- Optimise your experience
- Manage risk in line with your organisations needs
- Give you value for money
- Continually improve

Our technical support engineers have direct access to Account Managers, Professional Services Consultants, Head of Support and the NGS Technical Director, where they will be able to discuss any matter at any time. Any serious issues during the service will be escalated quickly and to the highest level. Furthermore, NGS management frequently attend account management meetings so they will be readily contactable if you wish to provide direct feedback.

# NGS MANAGED SECURITY SERVICE

Trying to build and maintain an in-house security team with the necessary skills and tools to be effective is not only difficult, it's expensive and time consuming. Powered by Alien Vault the NGS Managed Security Service goes beyond just a managed SIEM solution and brings together multiple essential security capabilities in a single service, giving you everything you need for threat detection, incident response, and compliance management

Basic defenses like firewalls and anti-virus are no longer enough to combat increasingly sophisticated threats and changing attack methods. More advanced technologies, including SIEM and IDS, along with real-time threat intelligence have become must-haves alongside highly skilled staff to successfully identify threats and system compromises.

The NGS Managed Security Service delivers true visibility into your infrastructure and work pro-actively to not only identify threats when they enter your organisation but, to prevent known and unknown threats by identifying vulnerable systems.



## Comprehensive Security Monitoring for Cloud & On-Premises

Eliminate security blind spots with automated asset discovery and continuous, centralized monitoring of cloud, on-premises, and hybrid environments.



## Protection Against Emerging Threats

Stay ahead of emerging threats with the most up-to-date, global threat intelligence delivered continuously and automatically to the USM platform.



## Accelerated Detection & Response

Stop attacks sooner with early threat detection, classification, and prioritization, combined with built-in response orchestration and automation.



## Simplified Compliance Management

Ease compliant efforts with continuous monitoring, centralised log collection, secure log storage, and audit-ready reports.

# NGS MANAGED SECURITY SERVICE

## The Service

Our service delivers superior security and compliance for your organisation without the need to install, configure and manage individual products.

- Managed SIEM built in partnership with an industry leading vendor
- Monitored and managed by Cyber Security experts
- 24x7 or 10x5 event monitoring to provide constant security vigilance for your organisation
- Access to highly trained Cyber Security Experts act as an extension of your own team
- Customer Portal that provides full visibility of your security and compliance posture, giving you the intelligence and analytics you need to understand the risks and demonstrate compliance
- Flexible reporting, from granular daily log analysis to quarterly threat reports, we tailor reporting to you needs
- Fully integrates with Cloud services and applications including, AWS, Azure GSuite and Office 365

## Advanced Threat Detection

By combining multiple detection technologies into a single platform when coupled with your internal log sources and our Threat Intelligence feeds, we can quickly identify and protect your organisation from new and emerging advanced threats.

The following table demonstrates how quickly we can respond to emerging threats and protect our customers.

THREAT	DISCOVERED	IOC's AVAILABLE TO CUSTOMER	TIME TO DETECTION IN USM
WannaCry	May 12, 2017	April 18, 2017	One Month BEFORE
Samba CVE-2017-7494	May 25, 2017	May 25, 2017	Same Day
Intel AMT Vulnerability CVE-2017-5689	May 06, 2017	May 09, 2017	3 Days
Wordpress Content Injection	February 01, 2017	January 26, 2017	6 Days BEFORE
Adobe 0-day (CVE-2015-0311)	January 22, 2015	November 16, 2014	3 Months BEFORE

# NGS MANAGED SECURITY SERVICE

## Incident Response

Our team comprises of industry veterans and Cyber Security experts. This means that every incident identified will have true experts analysing them, depending on the integration into your organisation, our analysts will perform full incident triage and response. We will then either notify the relevant contacts within your organisation with a step by step remediation plan or will perform full remediation in line with your change control process.

## Continuous Security & Compliance Monitoring

Regardless of the service level you opt for, you can be safe in the knowledge that your infrastructure is been monitored 24 hours a day, 7 days a week. (all service tiers include 24x7 monitoring however on 10x5 service tiers IR will only be performed inline with the service purchased). By monitoring your infrastructure 24x7 we can ensure your organisation is secure and compliant with any regulatory requirements you must meet.

## Our SOC

All of the technologies we use have been carefully selected to ensure we can not only deliver the best service and value to our customers but, for their ability to integrate into all of our other tool sets. By doing this we can orchestrate and automate our Incident Response processes, critically by automating repeatable tasks and analysis this reduces our response times. Depending on the criticality and type of the incident in some cases the entire IR process can be automated. E.g. A new strain of malware is discovered (such as Wannacry), within hours the IOC's can be downloaded from the Threat Intelligence source, a scan of your organisation is triggered and the IOC's pushed out to the HIDS clients and IDS sensors.

## Service Level Agreement

The SLA and Managed Service contract offerings will be there to meet your specific organisations requirements. All NGS response and escalation timescales are modified based on the criticality of the situation. Criticality is based on the effect (or potential effect) the issue could have to your normal and enhanced operations rather than a purely technical assessment.

## Incident Management Process

NGS have a documented Incident Management process that is used for each and every incident or event. The process describes the method and procedure used by the NGS support team, of how the incident is initially recorded, triaged, investigated, resolved and reviewed.

