

NGS | NEXT GENERATION SECURITY

SECURITY STORAGE RESELLER OF THE YEAR
2020 | 2021 | 2022 | 2023



**STORAGE
AWARDS**
THE STORRIES XVIII

WINNER



Do More. For Less. Better

The Next Generation of Security

At NGS, what we do is enshrined by 4 core principles; to Be Transformative by Driving Value, to put your Users First and give you a Better Response.

Be Transformative



Emerging technology brings business benefits, but also challenges in terms of complexity, alongside lack of skills & resources – plus risks if not deployed correctly. We help our customers to take advantage of these trends; whether through new entrants into an established technology, or completely new, disruptive technologies.

Drive Value



Breaches are constantly increasing, along with threats and attack vectors – yet budgets are not always keeping pace. Additionally, lots of solutions mean silos of information, or even gaps in IT security. Faced with this challenge, it's about delivering more for less, and so we work to help our customers drive value from their security solutions investment.

Users First



By helping security teams to understand, educate, and ultimately change the behaviour of their users, we can hugely impact the security posture of the business. Strong security and a good user experience are not mutually exclusive, and we look for ways to align the two.

Better Response



Too many cyber security solutions produce high volumes of alerts, in turn creating “noise” (or alert fatigue), making it harder to identify real threats. We look for ways to both reduce this noise, but more importantly, respond to and remediate threats quickly.

Our services have been recognised by these awards



We are certified by










Who are NGS?

Formed in 2018, NG Security (UK) Ltd are independent, vendor agnostic, next generation security 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 100 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 our clients' critical aspects. 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 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.

-  100+ years of industry experience
-  Security Reseller of the Year for the past 4 years
-  Recognised by the leading next generation security vendors
-  Technical Expertise
-  Client-driven
-  Consultative approach
-  Cyber Essentials and IASME accredited

The Cyber Security Market Today

In 2022, the global cyber security market was valued at \$153 billion. The market is projected to grow from \$172 billion in 2023, to over \$424 billion in 2030. As the cyber market has drastically grown, the associated threat landscape is rapidly evolving with it. Long gone are the days where the focus is on the firewall at the perimeter, and anti-virus on the endpoint. With the location now well beyond the security of the office, as remote working has become the norm for most businesses, cyber security is of high priority for all organisations.

The challenge today is no longer just detection and protection, but also recovery. Although new malware is being developed at a tremendous speed, it is essential to understand where the risk starts and finishes, to then build a response and remediation plan for when these attacks inevitably happen.

As malware and threat actors are evolving at a faster rate, protecting your organisation can no longer rely on products that use static signatures and traditional detection methods. Behavioural analytic, machine learning and AI are now at the forefront of cyber security technologies and can offer a greater level of protection and increased reaction time to security incidents.

With an every-changing work culture and threat landscape, staff are increasingly working from public and mobile networks. 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 must interact with on a daily basis is constantly on the rise, as is the number of passwords being reused. With the rise in phishing attacks and threat actors using social engineering from different vectors, password loss is one of the greatest risks to organisation's data. Complex password policies are no longer the answer as users must be able to still work efficiently, but in a secure manner. Privileged access management, identity management, multi-factor authentication and cloud access security brokers are now an essential for any organisation to ensure they not only protect user credentials but to enable staff to work without hindrance.

With GDPR now in full effect, the financial implications of a data breach become greater if cyber security is not at the forefront of board level conversations. For most organisations, maintaining pace with threats is simply not possible due to resource and financial constraints. Managing security products requires specialist skills and knowledge which can be challenging without dedicated security focused employees which can cost a business upwards of £80k per year. Cyber security service providers can help organisations improve their security posture whilst delivering efficiency and cost benefits.

Why NGS?


As recognised thought leaders within the IT industry, the leadership team at NGS brings over 100 years of experience of the ever-evolving cyber security landscape.

We do things differently to our industry peers. In a crowded marketplace, we choose to work with technology and solution providers who, like us, understand the numerous challenges our customers face.

At NGS, what we do is enshrined by four core principles; to be transformative, drive value, to put our users first and provide a better response. We strive to always do more, for less, better, by working with best-of-breed technology vendors who share our values and mission. We are aware of the issues and consequences that follow a poor security strategy and work to ensure minimal downtime through our extensive service offerings.

We have a rich history at NGS, with previous successes including winning Security Storage Reseller of the Year consecutively since 2019. Our extensive technical capabilities has led us to employ a fully managed SOC, GRC team and Senior Technical team, including 1 of 23 Juniper Global Ambassador experts.

The areas of security that we 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

Our Partners



Services

Initial Engagement

With any engagement for new solutions, the first step in the process is understanding. NGS will work with you to have a complete 360 perspective of your pain points and then collaborate to provide the best solution to overcome these and add value. We want you to make the right choice for your organisation and, as NGS are vendor agnostic, we will consult with you and provide options that we feel 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 with our service level agreements. All calls are logged and progress is 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 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 and dedicated team who believe in delivering bespoke, robust solutions to fit the exact needs of the business from assessment consultation and design, then to employment 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 integration, and you can rest assured that you are in good hands.

Advanced Foot-printing

The NGS Advanced Foot printing service takes a leaf out of the hacker's play book to help you stay ahead of the cyber criminals. 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 Health-check & Security Review

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

Phishing Simulation Service

The NGS Phishing Service educates your employees and raises their phishing awareness whilst enabling you to measure employee susceptibility to social engineering. Due to this, it is important to include phishing awareness in your employee security training. Awareness training is best achieved through explanation and demonstration, with phishing simulation achieving this by targeting your employees or specific functions. Highly credible email phishing campaigns are used with the aim of raising awareness of the risks and improving knowledge of how and when to act 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, mapping them against industry leading practices. 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 including steps recommended to re-mediate them.

Virtual CISO

From strategic board level advice, risk management and technical guidance and best practice, NGS offer a virtual CISO 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 choose. NGS offer 8x6, 24x7 support and Managed Security Services which can be tailored to your organisation's needs. For all of 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 by a username and a password.

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

Support Management

The NGS support and service desk runs to ITIL guidelines and performance is reviewed weekly with a major quarterly review to ensure service levels are maintained to the standards you expect. We use ITIL guidelines to align ourselves with the needs of your organisation, 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.

Our adoption of ITIL practices and strong experience in 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 immediately escalated to the highest level. Furthermore, NGS management frequently attend account management meetings so are 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, but also expensive and time consuming. Powered by an agnostic service, the NGS Managed Security Service goes beyond just a Managed SIEM solution, bringing together multiple essential security capabilities in a single service with everything you need for threat detection, incident response, and compliance management.

Basic defences, such as 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 essentials alongside highly skilled staff to successfully identify threats and system compromises.

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



Comprehensive Security Monitoring for Cloud & On Premises

Eliminate security blind spots with automated asset discovery and continuous, centralised 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 prioritisation, combined with built-in response orchestration and automation.



Simplified Compliance Management

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

The Service

Our service delivers superior security and compliance for your organisations 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 who 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 needed to understand the risk and demonstrate compliance
- Flexible reporting, from granular daily log analysis to quarterly threat reports, we tailor reporting to your 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, 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 merging threats and protect our customers:

THREAT	DISCOVERED	IOC's AVAILABLE TO CUSTOMER	TIME TO DETECTION IN USM
Wanna Cry	May 12, 2017	April 18, 2017	1 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 BEFORE
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

Incident Response

Our team comprises of industry veterans and Cyber Security experts, meaning every incident identified will have the right people analysing them. Depending on the integration into your organisation, our analysts will perform full incident triage and response. We 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 being 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 in line with the service purchased). By monitoring your infrastructure 24x7, we can ensure your organisation is secure and compliant with all regulatory requirements.

Our SOC

All technologies we use have been carefully selected to ensure we can not only deliver the best service and value to our customers, but also to ensure their ability to integrate into all of our tool sets. We can then orchestrate and automate our Incident Response processes by automating repeatable tasks and analysis which speeds up our response time. For example, a new strain of malware is discovered (such as WannaCry), within hours of the IOC's can be downloaded from the Threat Intelligence source, a scan of your organisation is triggered, with the IOC's then 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 every incident or event that may occur. The process describes the method used by NGS support team of how the incident is initially recorded, triaged, investigated, resolved and reviewed.



SECURITY STORAGE RESELLER OF THE YEAR
2020 | 2021 | 2022 | 2023



☎ 03333 111001 | ✉ sales@ngsuk.com | 🌐 ngsuk.com

Fountain House,
4 South Parade,
Leeds
LS1 5QX

2-7 Clerkenwell Green,
London,
EC1R 0DE