Managed Cyber Security Service by Nasstar

Service Definition Document: G-Cloud 15

Contents

1 About Nasstar 4
2 Service Summary: Managed Security Service by Nasstar 6
3 Service Overview 7
3.1 Nasstar Managed Security Service 7
3.2 Endpoint Security Sensor Management 7
3.3 Nasstar Security Advisor 7
3.4 Network Security Sensor Management 8
3.5 Vulnerability Management 8
3.6 Cyber Safety & Phishing Awareness Training 9
4 Why Choose Nasstar Managed Security Service? 10

1 About Nasstar

At Nasstar, our people are ultimately here to do one thing: help organisations navigate complex change with confidence. Simple. Or at least it should be.

Technology is complex and always evolving and keeping up can feel like a full-time job. Our goal is to help you embrace transformative technology to help you deliver more, better, and faster.
We're a partnership, collaborating with you and providing the expertise to tackle today's challenges and identify tomorrow's opportunities. It's a journey, and we're your navigator. Let's get started.

- Our team of experts, pioneers, innovators, forward-thinkers and problem-solvers are here to make your goals a reality, through the power of technology.
- Our bread and butter, our jam, our superpower. However, you want to say it, we're good at it. 25+ years pioneering breakthrough solutions is why organisations continue to trust us.
- Nasstar's people are paramount in all we do, which is why our 780+ strong team aspire to build long-term relationships with customers, not short-term flings.
- Our in-depth sector knowledge gives us insight into our clients' world, meaning we're always on the same wavelength.
- We believe in collaboration at every step – both with our clients, and our technology partners. We partner with the very best, including Microsoft, AWS, Cisco and Fortinet, to deliver the very best.

A Network that Connects and Protects

Networks do a lot more than just connect devices. They keep your team productive and your business moving. But without strong network security, they can quickly become your greatest liability. We help organisations like yours build secure networks that connect and protect. Whether it's rolling out SASE, working with Zero Trust frameworks, or just simplifying a complicated setup, we've got the tools and experience to help.

We understand that as your business grows, so does your digital footprint, and with it, the potential for risk. But you don't have to tackle this alone.

With partner support from Cisco and Fortinet, and a team that genuinely cares about your success, we'll help you create a network security strategy that lets you move forward with confidence.

- Let's replace complexity with clarity by securing legacy systems, modernising your infrastructure, and exploring frameworks like SASE and Zero Trust.
- You're managing a lot: legacy systems, evolving threats, new ways of working. We understand how overwhelming that can be, and we're here to lighten the load. From protecting your systems to empowering your people, we're with you every step of the way.
- Cyber threats aren't what they used to be, so your network shouldn't be either. That's why we'll help you embrace modern security frameworks like SASE and Zero Trust. They'll give you visibility and control across your entire digital landscape, so you can scale with confidence.

- We work across public and private sectors to build IT foundations that are secure, modern, and built to last. Whether you're juggling remote teams, legacy systems, or scaling fast, we've got you covered.
- The future of networking is AI-enabled, automated, and intelligent. Together, we'll build a secure, responsive network that gives you time back, reduces stress, and keeps your business running strong.

Why Nasstar?

Nasstar brings over 25 years of innovation to the table, delivering next-generation services and solutions that keep organisations ahead of the curve. Our deep in-house expertise spans Technical Leads, Project Managers, Account Managers, and a broad team of specialists—all dedicated to providing the guidance and support our customers need. Backed by a market-leading portfolio and partnerships with industry leaders such as Fortinet, Cisco & Microsoft, we ensure our customers benefit from cutting-edge technology and trusted best-in-class solutions.

Quality and compliance sit at the heart of everything we do. Nasstar is accredited to ISO 27001, 20000, 14001, and 9001 standards and is PCI-DSS certified, demonstrating our commitment to delivering secure, compliant, and reliable services. As a trusted HSCN (NHS Digital) and Crown Commercial Services approved partner, we proudly support public sector organisations with assurance and confidence. Our next-generation managed services provide 24/7 proactive monitoring, systems automation, and AI-driven capabilities, ensuring resilient, future-ready operations for every customer.

2 Service Summary: Managed Security Service by Nasstar

Empowering Your Business with our Managed Cyber Security Service

Nasstar's Managed Cyber Security Service provides a managed 24x7x365 cyber security capability that addresses the challenge of securing platforms, infrastructure and data against the threat of modern cybercriminals.

The Service is built using market leading technologies and provides a solution that easily and natively integrates to protect Customer infrastructure and devices. The goal is to provide the necessary security without the excessive costs and efforts associated with integrating point security solutions, and centralised signal processing and management to improve the overall security posture.

Managed Security Service

Nasstar's team of dedicated Security Analysts from the UK-based Security Operations Centre (SOC) monitors the Customer environment 24/7, using the latest security technologies, including machine learning and AI to deliver rapid threat detection and security incident management.

Overlaying the monitoring activities with Nasstar's Security Advisor extends Nasstar's day-to-day Managed Cyber Security Services to provide an ongoing monthly security review and assessment. Leveraging Nasstar's industry and technology expertise, it provides a detailed assessment of the Customer's security posture and threat landscape – providing insights into key events and anomalous behaviour, with commentary covering best practise and recommendations to mature the existing security posture.

Why Nasstar?

With Nasstar, you gain a trusted partner delivering a tailored, scalable managed cyber security service which includes incident response - so you can focus on driving your business forward.

3 Service Overview

3.1 Nasstar Managed Security Service

Nasstar's Managed Cyber Security service provides 24x7 enterprise-class security monitoring, and management capabilities for both cloud-native and hybrid platforms.
This service is delivered by Nasstar's dedicated assurance teams. It is provided by Nasstar's level 2 and level 3 support teams along with the Operations Centre. It is designed to augment an existing IT service delivery capability either provided by Nasstar's End-User Service Desk service, or by a customer designated service desk (that provides level 1 support to end-users) and integrates with their internal processes and workflows.

3.2 Endpoint Security Sensor Management

The service component delivers management of EDR agents that are hosted on Customer corporate endpoint devices (laptops, desktop, and servers). The agent continuously monitors activity on the devices, to identify suspicious or threatening behaviour in real-time. Information is recorded and analysed for internal or external attacks. EDR can identify specific behaviours to alert organisations to potential threats before the attackers can cause harm.

Key Benefits:

The configuration and ongoing management of Endpoint Detection and Response agents on the customer's endpoints (laptops or desktops).

Where relevant, the following activities are performed by Nasstar:

- Deploy the agent
- Check agent health
- Ensure signature definitions are up to date
- Check agent version is an approved version
- Isolate infected device upon threat detection

3.3 Nasstar Security Advisor

The Security Advisor at Nasstar will be the Customer's point of contact for any queries and question about the Security Managed Service. They will arrange regular security meetings to review the monthly security report and agree actions to address any recommendations or improvements to the current security posture. Any critical vulnerabilities will be logged within the Customer's ServiceNow™ Risk Register.

Key Benefits:

The Nasstar Security Advisor delivers quantitative and qualitative feedback on the Cyber Security service via regular review meetings. Where relevant, the following activities are performed by Nasstar:

- Monthly cyber security service meeting to discuss the cyber security service report
- Monthly cyber security service report produced that includes:
    - Review monthly executive report and recommendations.
    - Review in-scope devices for the vulnerability managed Service.
    - Alarms, events trends over the past month within the environment.
    - High level incident reporting for the previous month.
    - Notification of any Critical Vulnerabilities reported over the previous month.
    - Review of current network security posture

3.4 Network Security Sensor Management

Network sensors are a combination of existing customer firewall devices and standalone collector devices that are configured to send network activity logs to the Nasstar SIEM solution for event correlation.

- Configure customer firewalls to export logs to the Nasstar SIEM solution.
- Deploy, configure and maintain collectors to allow event logs to be exported to the Nasstar SIEM solution.

The configuration and management of network sensors to monitor internal corporate network traffic or third-party firewalls for known threats and Indicators of Compromise (IoC).

Where relevant, the following activities are performed by Nasstar:

- Install collectors into the customer network
- Configure collectors for log export
- Maintain collector's software/firmware version in line with Nasstar policy
- Configure customer firewalls for log export to Nasstar SIEM solution

3.5 Vulnerability Management

Nasstar's vulnerability management solution continuously monitors Customer networks and end-user devices for known vulnerabilities – alerting when new vulnerabilities emerge anywhere in the world, or if there's a device in the technology estate that could be susceptible.

- Reporting of vulnerabilities
- Implementation of patches
- Installation of agents

Automated scanning of infrastructure to understand vulnerabilities as queried against the centralised vulnerability database.

Where relevant, the following activities are performed by Nasstar:

- Install agents where appropriate onto Nasstar managed customer endpoints and/or servers
- Where a vulnerability is identified, Nasstar will raise the remediation request to the appropriate resolver group.

3.6 Cyber Safety & Phishing Awareness Training

Nasstar's managed Cyber Safety and Phishing Service provides regular, easy-to-consume, bite-sized security awareness training combined with simulated phishing attacks to test ongoing awareness and compliance. Results and progress are discussed in a monthly meeting with the Nasstar Security Advisor.

This service component delivers a web-based training portal for customers to consume security awareness content, role-specific or persona-based cyber security support, and data-driven human risk reporting.

Where relevant, the following activities are performed by Nasstar:

- Setup of customer dedicated training portal
- Provision of access credentials for the online portal
- Reports detailing training progress (delivered via Nasstar Security Advisor)

4 Why Choose Nasstar Managed Security Service?

With Nasstar, you gain peace of mind, predictable performance, and a partner committed to keeping your business protected and connected.

- 24/7 proactive service
- Simplified security operations
- Detection **and response**
- Enhanced security
- Enhanced business continuity

The Nasstar manged Cyber security service gives you:

- **Security Expertise:** As a manged service customer, you have 24/7 access to our team of highly experienced security specialists. They will be on hand to answer questions and will continually monitor your IT environment for known and unknown threats and suspicious or malicious behaviour.
- **Near real time threat response:** Using Nasstar's SOC and SIEM, our security analysts are able to identify and isolate threats as they happen – within 15 minutes – ensuring that you don't lose precious time in either mitigating or remediating the threat
- **Reporting:** You will be given access to our online reporting portal, from which you will be able to view the technical details of every incident flagged. We will also provide a monthly summary report which highlights all events, alarms, and incidents which occurred within your environment, including remediation actions taken.