G-Cloud 15

Service Definition

Automated Pen Testing (PTaaS)

NG-IT

Lot 2a Infrastructure Software as a Service (iSaaS)

1. Introduction

Company Overview

NG-IT are the UK's leading provider of next generation Private Cloud, Hybrid Cloud and Cyber Security services. We make digital innovation a reality by delivering flexible, always available, highly agile IT services using innovative, next generation technology solutions.

As a multi award winning business, NG-IT is dedicated to meeting the demands of today's business environment. Instead of taking legacy ideas, systems, processes, and technologies, we deliver an exceptional experience around the understanding, design, deployment, and management of next generation data centric and cyber security solutions.

It is critical to stay head of attackers, and our solutions work to identify both new technologies and new and emerging threats. At NG-IT, we understand how important these steps are to ensure that your business is secure against old and new Cyber security threats. This way we can improve your security posture, reduce the risk to your business and keep you where you should be - ahead of the cyber attackers.

NG-IT have deployed over 400 private cloud, hybrid cloud or cyber security solutions including migrating more than 60,000 applications and 32,000 TBs of data. Our professional services capability allows us to provide a full end to end service for our customers, to ensure a seamless working relationship from the initial engagement to the delivery of the chosen solution.

We continually review and assess leading and emerging technology vendors, and our expertise lends us to consider the best options for our customers. We've invested heavily in our people to bring you the very best working relationship and technical consultancy there is to offer.

Social Value

In an increasingly digital and fast-paced world, our Social Value Strategy reflects a deep commitment to people, communities, and the planet. We believe that technology should not only drive innovation but also foster trust, inclusion, and long-term wellbeing. Our legacy is built on a human approach, listening, guiding, and delivering solutions that leave lasting confidence.

Our mission is to be a trusted advisor and supplier of hybrid cloud, security, and data protection services. Our vision is to help businesses prosper through innovative technology, and our values centre on a customer-first culture powered by quality people.

Kickstart Economic Growth

Commitment
We support inclusive economic growth by investing in SMEs and VCSEs, promoting fair pay, and enabling local innovation through ethical procurement.

Initiatives & SMART Objectives

- SME & VCSE Spend Growth: Audit current spend and increase by 15% over 3 years, aligned with local authority targets.
- Fair Payment Code: Ensure 100% of suppliers are paid within agreed terms by Q4 2026.
- Metrics & Monitoring:
- Regular audits
- Supplier satisfaction surveys
- Spend tracking via finance systems

Governance & Ownership

- Led by our Finance Department
- Reviewed annually

Make Britain a Clean Energy Superpower

Commitment

We reduce our environmental footprint and promote sustainable digital practices that support the UK's Net Zero ambitions.

Initiatives & SMART Objectives

- Carbon Reduction Plan: We are currently gathering baseline data on our operational emissions to inform a measurable reduction strategy. Our goal is to identify key areas for improvement and set a science-based emissions reduction target by the end of 2026, with a focus on energy-efficient infrastructure and remote-first working practices
- Net Zero Roadmap: We are currently in the process of gathering baseline data on our carbon emissions across Scope 1, 2, and relevant Scope 3 categories. This data will inform the development of a science-based Net Zero strategy. Our aim is to set a formal Net Zero target by the end of 2026, including plans for verified offsetting of any residual emissions.
- ISO14001 Certification: Maintain certification through annual audits and continuous improvement.

Metrics & Monitoring

- Carbon accounting via Scope 1–3 reporting tools
- Annual sustainability reports
- Internal audits and external verification

Governance & Ownership

- Led by our Operations Manager
- Reported to the Board

Break Down Barriers to Opportunity

Commitment
We foster inclusion through education, skills development, and fair employment practices, empowering underserved groups and future talent.

Initiatives & SMART Objectives

- Digital Skills Outreach: Deliver workshops annually in underserved regions via charity partnerships.
- Careers Advice Programme: Provide virtual careers advice and mentoring to students from diverse backgrounds.
- Volunteering Leave: Provide 2 paid days per employee annually, with 80% uptake by 2026.
- Gender Pay Gap Transparency: Publish annual reports, regardless of company size.

Metrics & Monitoring

- Diversity metrics tracked via HR
- Workshop attendance and feedback forms
- Careers advice session participation and feedback
- Volunteering uptake reports

Governance & Ownership

- Led by Finance and HR and Management
- Supported by Management

Build an NHS Fit for the Future

Commitment
We contribute to a healthier workforce and community through mental health support, wellbeing initiatives, and responsible leadership.

Initiatives & SMART Objectives

- Able Futures Promotion: Increase internal awareness and usage by 30% over 12 months.
- MHFA Training: Train 10% of staff as Mental Health First Aiders by 2026.
- Wellbeing Surveys: Maintain 90% response rate and use feedback to shape quarterly wellbeing actions.

Metrics & Monitoring

- Programme usage analytics
- Training completion rates
- Survey dashboards and action logs

Governance & Ownership

- Led by our Wellbeing Lead and HR Manager
- Reviewed quarterly by the Employee Engagement Committee

This strategy aligns with:

- PPN 06/20: Delivering social value in procurement
- PPN 02/23: Carbon reduction plans and Net Zero
- PPN 09/21: Modern slavery risk assessments
- PPN 03/23: SME-friendly procurement practices

We ensure proportionality to contract size and maintain flexibility to tailor initiatives to specific project needs.

Overview of the G-Cloud Service

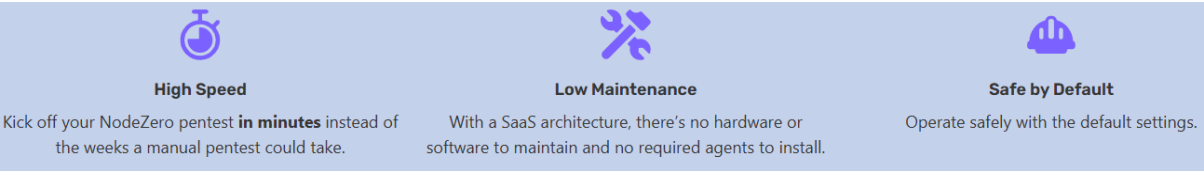
NG-IT take great care in selecting our service provider partners. We undertake a rigorous selection process that affords us the confidence to promote and justify Horizon3.ai as our key partner for delivering Automated Penetration Testing. Horizon3.ai provides essential insights and expertise across all types of environments and infrastructure, making them the ideal partner for our customers to engage and trust as the service provider for this proposed platform.

The Solution

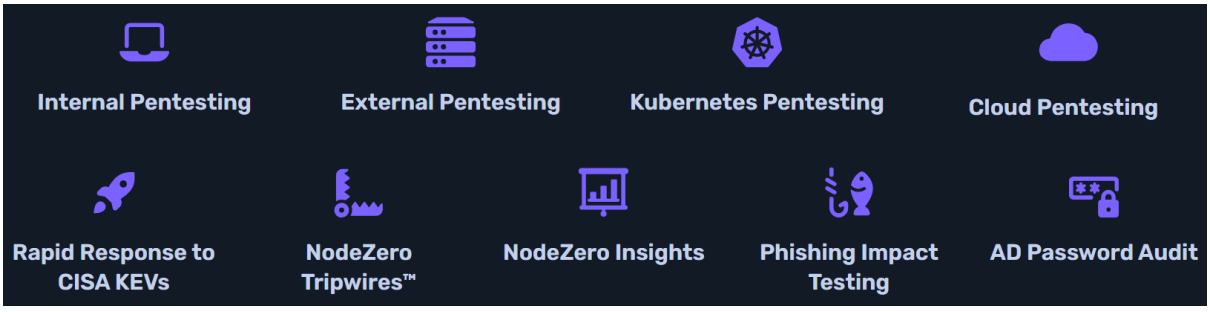
NG-IT have chosen to propose a suite of services from Horizon3.ai to address the challenges of delivering and maintaining adequate and effective protection from Horizon3.ai for your organisation, it's IT environment & critical data and the wider user community.

Automated Pen Testing

Horizon3.ai Automated Pen Testing is an AI-driven cybersecurity solution that performs continuous and comprehensive penetration testing. Delivered through their NodeZero platform, the Automated Pen Testing perform attack-like activities and will continuously assess your security posture by safely emulating real-world attacker tactics. Going beyond vulnerability scanning, it finds and prioritises security gaps across external/internal networks, cloud services, IDAM systems and IoT devices. This will help you identifying weaknesses across your organisation infrastructure before an attacker can and it is an efficient option to the traditional test that are time consuming and labour-intensive.

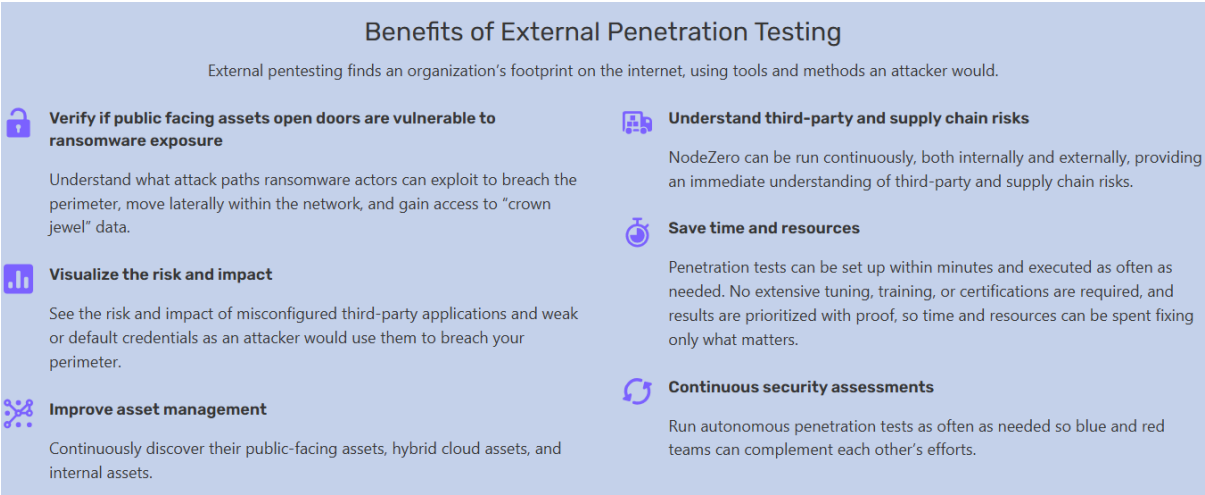


Test Types



Internal Pen testing – Simulates an attacker already inside the network, performing lateral movement, credential harvesting and privilege escalation. NodeZero runs on a Docker Host within your private network.

External Pen testing – Analyses public-facing assets to identify exploitable entry points and attack chains before attackers do. Discover your public-facing assets and run a pen test from the Horizon3.ai cloud.



Cloud and Hybrid testing – Extends to cloud resources and hybrid environments to uncover risk across complex modern estates. Run a pen test across your cloud and on-prem environments. NodeZero connects to both to identify and exploit hybrid attack paths.

AD Password Audit – Audit your users' active directory passwords and reveal weak, breached and re-used passwords.

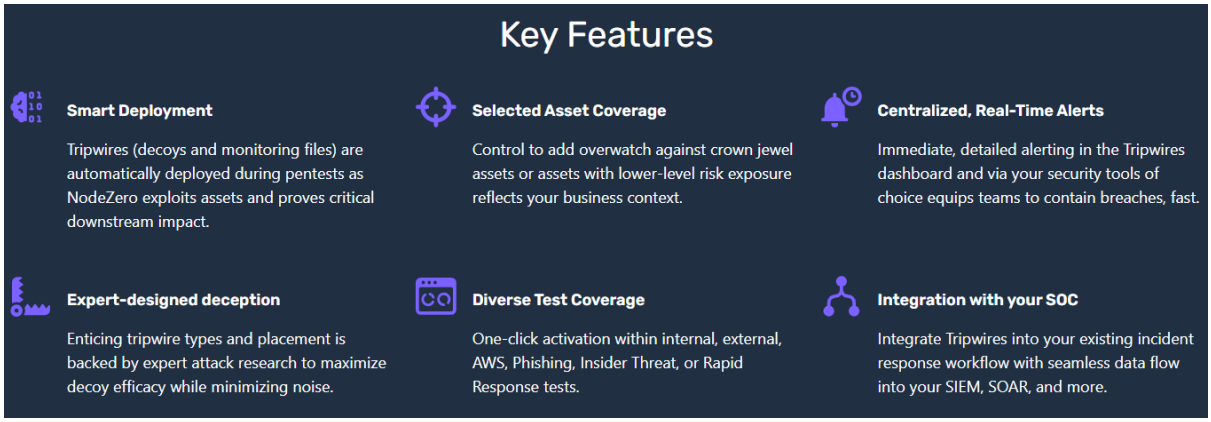
Phishing Impact testing – Discover what an attacker can do with phished credentials in your environment. NodeZero leverages phished credentials in order to validate user access and damage to the environment.

Rapid Response to CISA KEVs – Identify and act on emerging threats fast. NodeZero alerts you to zero-day and N-day risks in your environment and enables targeted testing and remediation before attacked can exploit them.

Kubernetes testing – NodeZero platform autonomously pen tests your Kubernetes clusters, continuously identifies risks, and exposes exploitable vulnerabilities like RBAC misconfigurations, container escapes, and secret exposures.

NodeZero Insights – Organization-wide visibility into your security posture so you can prioritize better, prove impact, and deliver strategic executive reports.

NodeZero Tripwires – Use the pen test findings to drop expert-designed decoys as it discovers critical risk. Tripwires alert in real time when they detect potentially malicious activity.



Service key benefits

Time and Cost Efficiency – 50x faster than a qualified human penetration tester. Automating tests reduce the time and resources needed compared with scheduling external manual pen test and allows frequent or continuous security validation.

Real-World Rick Focus - It finds and proves security problems that actually matter. By simulating actual attack paths instead of just scanning for known issues, the platform helps teams focus on risks that truly matter and would be most damaging if exploited.

Continuous Security Posture Improvement - proactively and continually testing help your security team to track improvements over time and reduce exposure before attackers.

Low training burden and clear results – NodeZero is designed to be intuitive for security teams of varying experience levels. Unlikely traditional penetration testing tools that require deep specialist skills, NodeZero automates attackers tactics and presents results in a readable and friendly format.

Quickly and effectively remediate proven exploits – Rather than flagging theoretical vulnerabilities, NodeZero executes real-world exploit techniques in a controlled manner. Because findings are tied to an actual exploitation path, remediation teams can act with confidence and resolve the most impactful issues first.

Confidence exploits are resolved – NodeZero workflow includes validation after remediation. Once a vulnerability has been fixed, the platform can be retested to confirm that the exploit no longer succeeds, providing confidence and assurance that fixes are not only implemented but effective.

Delivers precise alerts and warnings in areas of proven exposure – NodeOne produces alerts that are actionable, prioritised and contextualised, meaning that teams spend their time fixing things that matter, improving operational efficiency.

Curated penetration tests for Zero and N-day threats – This curation ensures simulated tests reflect the current threat landscape, not just legacy vulnerabilities. Security teams therefore gain visibility into exposures that traditional scanning and static assessments might miss entirely.

Proves the impacts of phished credentials not just likelihood – Standard risk assessments often estimate how probable a credential theft might be, but NodeZero goes further by demonstrating what an attacker could do with compromised credentials. This shifts discussions from abstract probability to real business impact and support stronger controls.

In summary, Horizon3.ai Automated Pen Testing is a continuous impactful and production safe offensive security platform that helps organisations find and fix exploitable risk rapidity and reliably than traditional approaches.

Associated Services

NG-IT can provide Professional Services to install and configure the proposed solution. Data migration services are available if required

2. Data Protection

Information Assurance

- Cyber Essentials Plus
- We are certified under the Cyber Plus scheme, demonstrating our commitment to protecting against common cyber threats across our remote working environment.
- ISO 9001 – Quality Management
- This certification ensures our virtual service delivery is consistent, customer-focused, and continuously improving.
- ISO 14001 – Environmental Management
- Reflects our commitment to sustainability through digital-first operations, reduced travel, and energy-efficient cloud-based tools
- Information Management Process:
- Secure Cloud Platforms: All internal and client communications are conducted via encrypted cloud-based systems with strict access controls.
- Remote Access Security: Employees use multi-factor authentication, VPNs, and endpoint protection to securely access company resources.
- Data Handling Policies: We comply with GDPR and the Data Protection Act 2018, ensuring lawful and transparent data processing.
- Incident Response: We maintain documented procedures for breach detection, escalation, and resolution, aligned with industry best practices.
- Supplier Vetting: All third-party vendors are assessed for compliance with security, ethical, and sustainability standards

Data Back-Up and Restoration

NG-IT Limited recognises that the efficient management of its data and records is necessary to support its core business functions, to comply with its legal, statutory, and regulatory obligations, to ensure the protection of personal information and to enable the effective operation and management of the organisation.

To guarantee that, we have a Data Backup Policy that applies to all staff within the Company with a purpose of safeguarding information belonging to us, any third parties and clients. We do not hold business critical data within a traditional on-premises network or managed data centre, all line of business application data and unstructured file data is located within cloud storage, owned and managed by the relevant application vendor the data is specific to.

This business systems technology model allows for continuous replication of data from production cloud platform to secondary storage or an alternative cloud platform, effectively providing always available, fully comprehensive, granular backup with quick restore capabilities.

Backup Model

- Full backups of all data are performed weekly. Full backups are retained for 3 months before being overwritten.
- Backups are stored in secure locations. A limited number of authorised personnel have
- Backup of data held within Database Systems have data backup routines which ensures database integrity is retained

NG-IT adopts the best security practices by defining security controls applicable to the entire organisation. Additional security measures identified through risk analysis, legal, regulatory, and/or contractual concerns, and/or specific standards -shall be addressed accordingly. Security controls and best practices are be considered and implemented as appropriate to the risk level

Business continuity statement/plan

Business continuity is not simply a matter of contingency, it is a core component of delivering consistent, reliable service in a competitive and fast-evolving industry. As an IT reseller/security and service provider operating with a fully remote workforce and reliant on only on cloud-based systems with no corporate network, NG-IT Ltd recognises the importance of being prepared for unforeseen disruptions, whether technical, operational, or external.

We have a Business Continuity Plan that outlines measures to ensure that our operations remain stable and responsive during periods of disruption. It defines the procedures, responsibilities, and safeguards that enable us to continue supporting our clients, maintain supplier relationships, and uphold our professional standards. The plan reflects our commitment to resilience and readiness, and will be reviewed regularly to ensure it remains aligned with our business needs and the expectations of those we serve

This Business Continuity Plan sets out the procedures and responsibilities required to ensure the continued operation of NG-IT Ltd in the event of a disruption. It applies to all employees and covers both the reselling of IT services, hardware and software distribution. The plan is designed to safeguard client relationships, maintain service delivery, and protect the company's reputation.

The key aims of this plan are to:

- Ensure continuity of service provision to clients.
- Minimise delays in hardware fulfilment and vendor coordination.
- Maintain secure and effective communication with customers and suppliers.
- Uphold contractual obligations and regulatory compliance.

The following functions are considered critical to the business and must be maintained during any disruption:

- Vendor liaison and procurement
- Order processing and fulfilment
- Customer support and issue resolution
- Financial operations including invoicing and payments
- Internal communication and collaboration

All our staff members have defined roles in the event of a disruption. The Managing Director is responsible for overseeing the implementation and maintenance of this plan. The Operations Manager and Finance Manager manages supplier relationships and hardware sourcing. The Technical Director and Cyber Lead ensure access to systems and data security. The Account Managers handles customer communications, and the Finance Officer ensures continuity of financial operations

All our business systems are cloud-based and configured for daily automated backups. Access is controlled via multi-factor authentication and role-based permissions. A centralised password manager is used across the organisation. Security audits are conducted quarterly to ensure compliance with data protection regulations and best practice.

Internal communications during a disruption will be conducted via internal messages and email, with SMS or telephone used for urgent alerts. External communications with clients and suppliers will be managed via email and telephone.

In the event of a disruption, recovery procedures will be activated immediately. Alternative suppliers may be engaged to maintain service continuity. Clients will be informed of any delays or changes to service provision. Staff availability will be managed through cross-training and flexible working arrangements. Any cybersecurity incidents will be addressed by isolating affected systems, restoring data from backups, and notifying relevant stakeholders.

This plan will be tested annually through structured exercises. Supplier performance and supply chain reliability will be reviewed in line with our ISO management system. Contact lists and standard operating procedures will be updated accordingly. Following any real disruption, a post-incident review will be conducted to identify areas for improvement.

Privacy by Design

We are committed to embedding privacy into every aspect of our service delivery. As an IT reseller, we do not process personal data directly through proprietary platforms, but we ensure that all technologies we recommend, resell, or support meet GDPR standards and respect user privacy from the outset.

- Privacy by Design: We assess privacy risks during the initial selection and onboarding of any suppliers. This includes reviewing data handling practices, encryption standards, and access controls before recommending solutions to clients.
- Supplier Vetting: All vendors we work with are evaluated for GDPR compliance, including their use of data processors, sub-processors, and data residency policies.
- Minimal Data Handling: We store minimal personal data (e.g., names and email addresses) solely for communication and support purposes. This data is handled securely, in line with GDPR principles, and is never used for profiling, marketing, or shared with third parties without consent.

3. Using the service

Ordering and Invoicing

To order services from our organisation, you can simply send an email to gcloud@ng-it.co.uk to discuss your requirements in more detail and initiate the process. We recommend including key information in your email such as your organisation name, a brief description of the services needed, preferred start date, expected outcomes, and any relevant procurement references. Once we have reviewed your request, we will assist you in completing the Order Form, which formalises the agreement under the framework and becomes the Call-off Contract. This includes support with service scope, pricing, and terms to ensure everything aligns with your expectations. Our fees are invoiced monthly in arrears, and payment terms are 30 days net from the date of invoice receipt.

Availability of Trial Service

A Automated Pen test thought NodeZero proof of value is a time limited engagement including internal pen tests, external/cloud/AD assessments, exploit-path discovery, prioritized fix actions, 1 Click Verify retesting, and executive/technical reporting. It excludes ongoing managed services, broad multi-tenant rollout and long-term licensing; scope is limited to agreed environments and features for evaluation.

Please contact gcloud@ng-it.co.uk for more details about the proof of value.

On-Boarding, Off-Boarding, Service Migration, Scope etc.

Once the Service Contract is signed and we have the confirmation of your order, the onboarding process begins, and a designated team is assigned within the Service Provider to coordinate all aspects of your contract and provide a smooth onboarding process. As the IT Reseller, NG-IT will assign a dedicated Service Delivery Coordinator, that will look after your contract and lease periodically with the Service Provider during the whole lifetime of your service. At this point, your dedicated Service Delivery Coordinator will make sure that the Service Provider will follow the steps outlined in their onboarding process.

Getting Started

As a starting point, you will receive a Welcome Email from the Service Provider. This servers as a formal starting point and you will be introduced to the team that will work with you during you are your pen test journey. You will get assistance from Horizon3.ai to start using NodeZero through a mix of structured documentation, guided onboarding, and live support.

During this phase, it is expected that the Service Provider walks through the initial scope of the service, get a mutual understanding of what is included and outline next steps and provide you with the Quickstart guide. The Quickstart guide walks new users step by step:

- Log in or register
- Check network prerequisites
- Set up a NodeZero host
- Run the first internal pen test to get immediate findings

Once you are signed on, Horizon3.ap will assign a Customer Success Manager to your account. The CSM will be responsible to runs onboarding calls, helps validate deployment plans (host placement, scope, deployment strategy), and ensures the account is correctly set up. To guarantee a seamless and smooth environment transition and data migration, the Service Provider will provide support and guidance as part of the Service onboarding. You will receive all the instructions to help you migrating and setting up your Service.

Please have in mind that this is not a static process and the steps and timeframes may vary according to the environment sizing and complexity. A detailed implementation plan can be provided to the buyer on request.

Off-boarding

You can download the results of their penetration tests at any time. At contract termination, customer data will be deleted within 30 days at the customer's request. Once your service ends and if you decide not to renew your contract, you will retain control over your data and have several options.

Throughout the contract and up to termination, customers can export pen test data directly from the NodeZero portal, typically in open formats such as CSV/ODF, with PDF available for reports and documentation. This allows them to take copies of all relevant results, evidence, and reports before any deletion occurs.

By default, when a contract expires, the tenant will typically move into an inactive / read only state: users can no longer run new tests, but historic results may remain viewable unless the customer chooses a stronger offboarding option.

Customers can instead ask Horizon3.ai to deactivate the tenant, which removes account specific data from the live portal but allows potential future restoration if they later renew. If a customer wants full removal, they can formally request GDPR style erasure. Horizon3.ai then runs a comprehensive process to scrub the company's data from systems in line with the DPA and GDPR commitments. In our G Cloud statement, we commit that, upon the customer's request at contract termination, customer data will be deleted within 30 days.

Training

As a reseller, we provide buyers with access to the service provider's comprehensive training and onboarding resources. These include online help documentation, knowledge bases, and guided assistance to support orientation with the new service. Introductory onboarding sessions are available to ensure buyers understand how to configure, monitor, and manage the NodeZero platform effectively. Where required, we facilitate access to the provider's customer success team for tailored onboarding support. Our role is to ensure buyers are connected to the appropriate resources and that any queries are escalated promptly to the service provider for resolution.

Service Provider will provide training around the Horizon3.ai systems and NodeZero portal, either via training materials or walk-throughs, to ensure that you have all necessary information to navigate through NodeZero with confidence. You will also have access to Webinars and Education Sessions, and an extensive learning content library available on the customer portal.

You will also count with 24x7 support team, that can be contact via chat, email or ticket and will be available not only to assist you with incidents and technical related issues but answering any questions you may have on how to use the Service Provider features.

Service Management

We take an integrated approach when it comes to the management of Services as we understand that an effective service delivery relies on a balanced integration of expert personnel, mature ITIL v4 aligned processes and technology. From a workforce perspective, our team possess both technical and behavioural competencies required. This includes not only the commercial knowledge of our products and solutions, but technical proficiency to build the service architecture, relying on a Team of experienced Solution Architects that holds the accreditations necessary to support the delivery of our Services.

In alignment with the technical team, we have a Service Delivery process in place that maps out the level of Service that is expected and provide operational consistency and governance throughout the delivery of the Service. This includes a Team of dedicated Coordinator that hold ITIL v4 Certification and is assigned to reinforce a customer-centred approach and guarantee that all aspects of your contract are being provided accurately. This process guidelines are outlined based on ITIL Framework, which set the basis for all the procedures followed to guarantee the delivery of IT Services that meet customer's needs.

This process counts with clear escalation paths, service level agreements and communication protocols to safeguard service continuity and accountability. We also count with a well-structured continuous improvement procedure, including post incident review with the customer and the Service Provider, and trend analysis that will help us to identify and tackle any systemic issue and enhance our client experience and satisfaction. These processes help us to set the standards of what we do as the IT Reseller but also direct what we expect from the Service Provider Partner.

Service Constraints

The Service Provider solution include outside factors that are outside their control including use of hosting providers. They also ingest data from 3rd party sources which could be delayed due to items outside of Horizon3.ai control and result in an inability to notify/detect threats for a given telemetry source. Their typical uptime SLO is at least 99.95%.

Rest assured that, as your IT Reseller, we will make sure that the Service Provider will notify you of any outages with a portion of its solution and provide a recovery time estimate.

Service Levels

Standard SLA commits to availability of 99.95% per calendar month. NodeZero support hours are 09:00 AM-09:00 PM EST, Mon to Friday.

Incident severity is tiered as below:

Critical (severity 1) - response within 1 business hour
Major (severity 2) - response within 4 business hours
Minor (severity 3) - response within 2 business days

As mentioned, NG-IT as your IT Reseller, throughout its Service Delivery Process and according to the ITIL v4 Framework guidelines, will make sure that the Service Levels will be followed by the Service Provider according to what has been agreed on the Service Agreement signed by all parties. As part of this, you will be able to count with a dedicated NG-IT Service Delivery Coordinator that will conduct period checks to all support tickets that you might have opened with the Service Provider and action on whatever is required to guarantee the effective delivery of the service.

Outage and Maintenance Management

Service Provider will monitor and manage the technology components required to deliver 24/7 Service. This includes upgrades, uptime/status monitoring, etc. As well as monitoring their own infrastructure we also monitor the feeds / agents / sensors etc. from our customers environments that are ingested into their environment. The Provider, to the extent possible, will notify the Customer about scheduled or emergency maintenance through the Provider's Account Management Application and portal. The Provider, to the extent possible, will notify the Customer about scheduled or emergency maintenance through the Provider's Account Management Application. The Provider will constantly update the Account Management Application information to advise the Customer when a maintenance is completed.

NodeZero reports outages to users primarily via a public status page. This is published at https://status.horizon3.ai. The status page is the authoritative source for: Current service status, ongoing incidents, scheduled maintenance, historical uptime availability information. The status page also lets users subscribe to outage and incident updates via email.

NG-IT as your IT Reseller, throughout its Service Delivery Process and according to the ITIL v4 Framework guidelines, will make sure that the Service Levels will be followed by the Service Provider according to what has been agreed on the Service Agreement signed by all parties. As part of this, you will be able to count with a dedicated NG-IT Service Delivery Coordinator that will conduct period checks to the Service Provider state and promptly address any outages and request ad-hoc service if applicable. Root Cause Analysis and Service Improvement Plans will also be requested whenever is appropriate.

Financial Recompense Model for not Meeting Service Levels

While us, as your IT Reseller and the Service Provider, aim to meet all proposed Service Levels, there may be occasions where performance falls short of circumstances outside of our direct control as outlined in the Service Constraints and Outage and Maintenance Management sessions of this document.

In case of a failure from Service Provider on achieving the agreed SLAs, as your IT Reseller we will focus on addressing the issue with Horizon3.ai and providing you with clear answers and, when applicable, formal root cause analysis. We will also work collaboratively to ensure that a Service Improvement

Plan is put in place and, if necessary, apply any change to prevent the failure from happening again in the future.

Standard SLA commits to availability of 99.95% per calendar month. If the availability falls below 99.95% in a month, customers may apply for a Service Credit within thirty days following the calendar month. To apply, Customer will provide a detailed description of the incident in a customer support case. This is the only remedy for our failure to meet the Cloud Service availability standard; credits are not available for amounts that exceed 100% of Customer's monthly Cloud Service fee. Once validated, Service Credit will be applied to Customer's next payment period.

We are confident that this approach helps us maintain a strong and transparent partnership with our clients and service partner, keeping the service reliable, issues visible and improvement actions transparent.

4. Provision of the service

Customer Responsibilities

To deliver the best service and guarantee efficiency on the Service implementation and consistent service delivery, we operate under a shared-responsibility model, where all parties contribute and work in partnership during the lifetime of your contract. As our client, for service delivery effectiveness, we kindly ask your collaboration on:

- Providing the most accurate information during all phases of the Service Delivery
- Promptly notifying us of any significant business and technical changes that may affect the Service performance
- Providing timey responses to the Service Provider queries, incident responses and approval requests
- Adhering to agreed change-management processes, including approvals, lead times and risk assessments
- Submitting requests using approved channels
- Participating in Services Reviews if applicable
- Honouring contractual payment terms

Customer is responsible and liable for all uses of the Services and Documentation resulting from any access whatsoever provided to Horizon3.ai by Customer, directly or indirectly. Without limiting the generality of the foregoing, Customer is responsible for all acts and omissions of Authorized Users, and any act or omission by an Authorized User that would constitute a breach of the Service Agreement if taken by Customer will be deemed a breach of the service Agreement by Customer. Customer shall make all Authorized Users aware of this Agreement's provisions that are applicable to such Authorized User's use of the Services and shall cause Authorized Users to comply with such provisions. Customer shall use reasonable efforts to secure its passwords and credentials and will promptly notify Horizon3.ai of unauthorized account use of which it becomes aware.

Customer is responsible for accurately defining the scope of the Services for both internal and external testing. Customer authorizes Horizon3.ai to conduct testing and provide support on its behalf, at Customer's request and direction and in accordance with the scope of the Services defined by

Customer. Customer's authorization for external penetration testing must comply with any applicable third-party terms and conditions.

Customer has responsibility for the protection and backup of data and equipment used with its IT systems and will respond as though a real security penetration has occurred if activity from the Services is detected in Customer's systems or systems monitoring Customer systems.

Detailed Service Terms and Conditions, including the Contractual Customer Responsibilities will be addressed in the Service Agreement.

Technical Requirements and Client-Side Requirements

To determine the details about the exact technical and client-side requirements to deliver the service, it is essential that we have a full understanding of your current environment, operational needs and challenges you may be facing. This initial assessment will help us to guarantee the correct application of the Automated Pen Test. Therefore, many of the technical requirements and client-side requirements will be discussed prior to an order being placed, but also during the onboarding and implementation stages, where all parties will work together to refine connectivity, security, access and workloads considerations. All requirements discussed prior to the order being placed shall be documented in the Order form and agreed between the parties. We consider that this approach ensures that the technical prerequisites are mapped out accurately and are aligned to the customer needs and expectations.

After-sales Account Management

As the IT Reseller, we are not only committed to offering the best solution but also to build strong relationships with our clients, working with you closely, not only during the initial phase of the project but also after the Service is delivered and implemented. This is pivotal to us, as a Company, to work with you on a full end to end service and make sure your expectations regarding the Service are meet during the whole lifetime of your service. Unlike some specialist integrators, we are not just about selling a product, we are more interested in providing the right solution and we are committed to our customer's satisfaction.

As part of your service, you will have a designated Account Manager that will work closely with you on period reviews of our environment and will guarantee that you are being offered the most suitable solution/ service. You will also count with a Service Delivery Team that will liaise with you and the Service Provider on a regular basis, addressing all aspects of your service delivery and serving as your advocate to all your related service matters.

Termination Process

The term of this agreement begins on the Effective Date and, unless terminated earlier pursuant to the service agreement's express provisions, will continue in effect for the period set forth on the applicable order form. Horizon3.ai may terminate the agreement, effective on written notice to Customer. Upon expiration or earlier termination of the agreement, Customer shall immediately discontinue use of the Horizon3.ai IP and, without limiting Customer's obligations set under the Service Agreement, Customer shall delete, destroy, or return all copies of the Horizon3.ai IP and certify in writing that the Service Provider IP has been deleted or destroyed. No expiration or termination will affect Customer's obligation to pay all Fees that may have become due before such expiration or termination. Notwithstanding any termination of the Agreement, those provisions which by their

nature are intended to survive termination, including but not limited to provisions regarding intellectual property rights, confidentiality, indemnification, limitation of liability, disclaimers of warranties, dispute resolution, and governing law, shall continue to remain in full force and effect after such termination.

Termination for Unpaid Overages. If Horizon3.ai determines, through its monitoring or audit rights under the service agreement, that Customer has exceeded the scope of the licensed use (including without limitation, the quantity of purchased licenses), Service Provider will notify Customer in writing of such excess use and the corresponding fees due at then-current list prices. If Customer fails to remit full payment of such fees within fourteen (14) days of receiving such notice, Service Provider may, in its sole discretion, (a) immediately suspend Customer's and its Authorized Users' access to the Services, and/or (b) terminate the service agreement upon written notice. Customer acknowledges that any such use beyond the licensed scope constitutes a material breach of this Agreement.

Detailed Service Terms and Conditions, including the Termination, will be addressed in the Service Agreement.

5. Our experience

Case Study

Case Study: Horizon3.ai NodeZero in a Higher Education Environment

Organisation Overview

A multi-campus university with a diverse and distributed IT estate sought a more efficient, scalable, and user-friendly way to identify and prioritise security vulnerabilities. With no dedicated penetration testing team and increasing pressure to demonstrate cyber-resilience, the university needed an automated solution capable of continuous assessment across networks, systems, and applications.

Challenge

The university faced several persistent issues:

- **Fragmented, distributed networks** across multiple campuses made visibility inconsistent and manual testing impractical.
- **Limited security staff** meant traditional penetration testing was infrequent, expensive, and slow.
- **Growing attack surface** from research systems, student devices, cloud services, and legacy infrastructure.
- **Difficulty prioritising vulnerabilities**, often overwhelmed by long lists of findings with unclear business impact.
- **Lack of actionable remediation guidance**, slowing down IT teams already stretched thin.

Solution: Deploying Horizon3.ai NodeZero

The university adopted **NodeZero**, Horizon3.ai's autonomous penetration testing platform, to provide continuous, on-demand security validation across its entire environment.

Key Capabilities Delivered

- **Autonomous vulnerability identification** across all campuses, without requiring specialist penetration testing expertise.
- **On-demand assessments**, enabling teams to run tests whenever changes were made or new threats emerged.
- **Full coverage of distributed networks**, with NodeZero safely pivoting across segments to map real attack paths.
- **Risk-based prioritisation**, highlighting the most critical, exploitable issues rather than overwhelming teams with noise.
- **Clear, step-by-step remediation instructions**, enabling generalist IT staff to quickly fix issues without external consultants.

Outcomes

After deploying NodeZero, the university achieved:

- **80% reduction in time spent identifying vulnerabilities**, thanks to automated discovery and exploitation.
- **Improved visibility across all campuses**, including previously unknown assets and misconfigurations.
- **Faster remediation cycles**, driven by prioritised findings and easy-to-follow fix guidance.
- **Greater confidence in security posture**, with the ability to validate controls and patch effectiveness on demand.
- **Reduced reliance on external penetration testers**, freeing budget for other strategic initiatives.

Conclusion

NodeZero enabled the university to transform its vulnerability management approach from reactive and resource-intensive to proactive, continuous, and highly efficient. By empowering non-specialist IT staff with autonomous testing and clear remediation guidance, the institution strengthened its cyber-resilience across all campuses while reducing operational burden.

Clients

Contact Details

For any questions regarding this offer, please send an email to ***gcloud@ng-it.co.uk*** and we will respond as quickly as possible to assist with your request.