Empowering business to do more

Schedule document

N4EPMS

PUBLIC

Node4 limited

01/06/2024

Schedule document

N4EPMS

This Schedule contains additional terms, service description and service level agreement applicable to the N4 End Point Management Service and should be viewed with associated Order Form, Node4's General Terms and Conditions.

1. Service description

N4EPMS provides a managed suite of security controls for endpoint devices, monitored by Node4 SOC. The different service features of N4EPMS are described below.

Information discovered by the service will be critical to the security integrity of the client. It is important that the information from the service is escalated to the appropriate areas within the client's organisation that mitigating actions can be taken by the Clients IT department.

2. Definitions

"Fees" means fees as described in this Schedule and where relevant set out in the Order Form, and shall be payable by the Client in accordance with Clause 6 of Node4's Standard Terms and Conditions;

"Exploit" A method to use a Vulnerability to gain unauthorised access to functions, data, or privileges with malicious intent. An exploit can include a script, virus, Trojan, or a worm. The exploit is mainly defined by the way it replicates and spreads. An attack is the use of an Exploit.

- A script refers to a document with steps to manually find and exploit vulnerabilities. A script is replicated by publishing it.
- A virus refers to malicious software attached to a medium (e.g., files, removable media, and documents). A virus replicates using this medium.
- A Trojan refers to malicious software embedded in applications. The Trojan will not replicate itself; it spreads with the application.
- A worm refers to a self-contained program (or set of programs) that spreads copies to other computers. A worm can spread through network connections and e-mails in a matter of hours.

"HIPS" means Host Intrusion Prevention System providing tamper protection and secures the system registry, processes and applications from unauthorised modification.

"Incident" means an unplanned interruption to a service or a reduction in service quality

"Installation Fees" means fees payable by the Client for the installation of Firewall Services as provided in the Order Form;

"Non-Service Affecting Incident" means a Incident or condition which is not a Service Affecting Incident.

"Professional Service Fees" means the professional service fees detailed on the Order Form or otherwise agreed in writing between the Parties in accordance with Clause 4 below;

"Service Desk" means the single point of entry for all Service Tickets and Service Requests which can be accessed over the phone, by email or via our portal.

"Service Request" means a request for a change for information

"Service Ticket" means the tickets which are raised in relation to Incident or Service Request

"SOC" means Security Operations Centre.

"Threat" A (suspected) use of an Exploit, or the (suspected) presence of a Vulnerability in the configuration, platform, of application code. A Threat can be an infection by a worm or virus, or it can be a targeted attack. Exploits can also combine into Blended Threats, exploiting multiple security weaknesses or defects

"Threat Signature" Code used to recognise a Threat by its pattern. A Threat Signature may contain algorithms to detect dynamically changed malicious behaviour, combat obfuscation, or impersonation.

"Vulnerability" A weakness or defect that can be exploited to gain access to data, functions, or privileges violating the intended authorisation. Vulnerabilities can range from defects in application or system software (e.g. bugs), in the user administration (e.g. non-protected user accounts), in the configuration (e.g. unintended network or file access), in the policy and rule set definition (e.g. unrestricted open ports or exposed IP-addresses), etc. The combination of all vulnerabilities of a given system or infrastructure is the exposure.

3. Specific terms

The following terms and conditions shall apply when Node4 provides N4EPMS Services to the Client.

3.1 Termination of service

Upon the termination or cessation of the service, the Client is obligated to remove all N4EPMS licences from devices and infrastructure within 1 month of the end of service date.

3.2 Client indemnity

N4EPMS involves the use of network scanning and testing technology that has inherent risks, including, but not limited to, the loss, disruption, or performance degradation of a Client's or a third party's business processes, telecommunications, computer products, utilities, or data (the "Scanning and Penetration Tests Risks"). The Client authorises Node4 to perform the network scanning and assumes all risk for adverse consequences resulting from or associated with such component of N4EPMS. Node4 shall take reasonable steps to mitigate these Scanning Risks; however, the Client understands that these Scanning Risks are inherent in the provision of certain computer security services and the use of certain computer security products and cannot be eliminated.

The Client shall indemnify and defend Node4 for all costs and expenses related to a third party's claim of loss, damages and liabilities (including legal expenses and the expenses of other professionals) incurred by Node4, resulting directly or indirectly from any claim attributable to or arising out of Node4's use of network scanning technology (each, a "Scanning Claim"), including, without limitation, the use by Node4 of network scanning technology to analyse assets that are not controlled directly by the Client, including, without limitation, servers hosted by third parties. This obligation of the Client in connection with a Scanning Claim shall not apply if Node4's gross negligence or wilful misconduct gave rise to such Scanning Claim.

4. Warranty

Node4 does not warrant that N4EPMS will detect and prevent all possible threats and vulnerabilities or that such service will render the Client's network and systems invulnerable to all security breaches and vulnerabilities.

The Client hereby assumes the sole responsibility for the accuracy of the IP addresses and domains provided to Node4. Clients will be liable for all costs and expenses from any third party claims of loss, damage (including reasonable attorneys' fees) and liability of any kind that may be incurred as a result of Client's breach of the foregoing warranty.

5. Fees

Installation and reoccurring Fees will commence when the implementation of such Product or Service is completed by Node4 and such Product or Service is available for use by the Client, Fees could include the following:

5.1 Fees payable by the Client

Fees may comprise any or all of the following Fees including an Installation Fees and a Monthly Service Fees.

5.2 Set-up fees

Any applicable set-up fees for the implementation of the support service shall be detailed on the Order Form.

5.3 Service fees

Service Fees are paid either monthly or annually in advance based on the support provided and any other related service and are identified on the Order Form.

Service fees are applied as and when the service is made available.

5.4 Additional professional services

A full range of Professional Services are available to the Client in addition to what is provided as part of the support contract. The Professional Service Fees include but are not limited to:-

- Installation and configuration
- Remote services
- Management

The Professional Services are subject to the price list below. Specific rates for large or repeat orders can be agreed on a case by case basis in writing.

All incremental expenses incurred during these Professional Services will be passed directly to the Client. Provisioning costs such as cabling will be discussed and agreed with the Client in the Order Form.

Additional tasks undertaken at the request of the Client by Node4 personnel, will be charged at rates agreed between the parties in advance.

6. Service provision

6.1 Service features

N4EMPS Standard

- Antivirus & Antispyware
- Host Intrusion Prevention System
- Device Control
- Auto-Scanning of Removable Media

N4EPMS Advanced

- Web Control
- Two-Way Firewall
- Trusted Network Detection
- Client Antispam

N4EPMS Encryption

- Windows BitLocker
- DESLock+

6.2 Implementation

Prior to commencement of N4EPMS, Node4 will schedule a Deployment meeting to introduce the N4EPMS service delivery team, identify the appropriate contacts for Client, and discuss the scope of the N4EPMS service and its business impacts. The details of this will be held as the Clients' scoping document.

6.3 Centralised management

Node4 SOC will manage administration tasks and MACs for the Client. Client requests for highly secure actions, such as password resets, will be processed once authorisation is established by a call back to a known authorised person and contact telephone number.

6.4 Management reports

The reports functionality allows you to access detailed information about the devices, users, and applications in your N4EPMS solution. Details of access will be sent to nominated users. (See section 5.7 Self Service Portal)

6.5 Device enrolment

The enrolment process may differ slightly depending on the device platform. Node4 SOC will provide assistance via standard ticketing process. Device models are restricted to Apple Mac OS X and Windows.

6.6 Policies

You can think of policies as the settings and rules that help you enforce corporate rules and procedures. They contain the settings, configurations, and restrictions that you want to enforce on devices. Each device type can have device specific profiles. Default built-in policies are provided, but additional restrictions may be requested by the Client.

6.7 Self service portal

Client access to the self-service portal will be restricted to the Help Desk role. The Help Desk role provides the tools necessary for most Level 1 IT Help Desk functions. The primary tool available in this role is the ability to see and respond to device info with remote actions. However, this role also contains report viewing and device searching abilities

6.8 Exclusions

Node4 does not provide onsite installation, architectural and policy design services under N4EPMS service. N4EPMS service also does not include policy and configuration reviews, initial setup or maintenance of configuration on Subordinate Devices or migrations from management stations located on the Client's premises to management stations hosted the SMC or from third-party owned management stations to management stations either located on the Client's premises or hosted in the SMC. All of these excluded services, however, can be conducted by Node4 under a separate agreement.

7. Incident management

This section refers to Incident and management pertaining exclusively to the service portal for the N4EPMS service and does not include any Client systems or Client infrastructure.

7.1 Incident handling

Incident are handled as outlined in the Incident management schedule Document.

7.2 Hours of support

The following table details the different Support Hours relating to the support hours defined on the Order Form.

Support Hours	
Bronze	Standard business hours support 9am to 5.30pm week days, excluding bank and national holidays
Silver	Support hours between 7am and 7pm weekdays, excluding bank and national holidays
Silver Plus	Priority 1 and 2 - Support hours between 7am and 7pm 7-days a week, including bank and national holidays, excluding Christmas day, Boxing day and new year's day Priority 3,4 and Service Request - Support hours between 7am and 7pm weekdays, excluding bank and national holidays
Gold	Priority 1 and 2 - Support hours 24/7 Priority 3,4 and Service Request - Support hours between 7am and 7pm weekdays, excluding bank and national holidays

7.3 Incident priority

Each new Incident will be assigned a priority level by the Service Desk based on the following definitions. These levels allow us to prioritise resources and escalate where appropriate.

Priority	Description
1 - Critical	A major Incident resulting in total loss of service.
2 - High	A major Incident resulting in a severe service degradation or loss of service to a significant percentage of users.
3 - Medium	A minor Incident resulting in a limited or degraded service or a single end user unable to work.
4 - Low	General, single user with degraded service, non-service affecting support.
5 - Service Request	Request for a change to an existing service or system, a request for information or simple questionnaire to be completed.

7.4 Incident duration

All Incident recorded by the Network Management System will be reconciled against the corresponding Service Ticket raised by the Service Desk. The exact Incident duration will be calculated as the elapsed time between the Service Ticket being opened and the time Service is restored.

7.5 Time to repair

Node4 aims to respond, update and resolve requests in relation to the N4EPMA services within the following times (In not specified on the Order Form then Gold is included for N4EPMA services):

Priority	P1	P2	P3	P4	Service Request
Response / Acknowledgement	30 Mins	1 Hour	2 Hours	4 Hours	12 Hours
Commencement	1 Hour	2 Hours	4 Hours	N/A	N/A
Frequency of Updates	1 Hour	2 Hours	12 hours if Resolve / Target to Fix exceeded		
Resolve / Target to Fix	4 Hours	8 Hours	12 Hours	36 Hours	60 Hours

Resolution times in the table above do not apply where there is a Client Responsible Incident, a Third

Party Attributable Incidents or events outside Node4's reasonable control, any incidents including these aspects will be excluded from reporting provided.

All priority 1 & 2 Incidents should be raised via the Service Desk by a phone call. Should a priority 1 or 2 incident be raised via the portal or e-mail, the Client is required to follow this up with a corresponding phone call to enable work to commence immediately on the issue.

* Acknowledgement refers to an automated service which generates a response and alerts engineers of a service failure; or where there is dialogue between the client and the engineer.

Where Incident resolution involves third parties, or hardware replacement, then this is subject to the support contracts in place with those parties.

*** Service Requests will be completed as per the table. This does not include Service Requests outside of the support contract, or Service Request implemented outside normal business hours these will be dealt with as chargeable projects.

7.6 Maintenance window

Where Node4 plans to perform essential works on the portal, Node4 will endeavour to perform such works during low traffic periods and will endeavour to give the Client at least five (5) days prior notice. In the event of an emergency or Service affecting Incident such notice may be less than 24 hours.

8. Service credits

Service credits are not available for N4EPMS Services.