N4EPMS
KEY FEATURES

N4EPMS
Fully Managed Endpoint Management Service

Modern computing is now comprised of multiple entry points into distributed networks and dispersed data stores. Managing those gateways and securing information on those diverse endpoints is a difficult and time-consuming necessity. With such varied threats constantly probing and testing security policies it is clear that a consistent and professional management service is vital to ensuring that data is safe and systems are clear of security threats.

Node4's Endpoint Management Service provides dedicated security experts who monitor, react and remediate your endpoint security issues. Hosted from Node4's Security Operations Centre, SOC, your endpoint infrastructure is in safe hands. Threats will alert the SOC who will take investigative action in order to contain any outbreak. Endpoints polices are applied based on device, department or user allowing you to have fine-grained control over who does what.

N4EPMS Standard provides a fully managed facility for all Windows, Mac and Mobile endpoints that connect to your network, preventing access to your network from unauthorized devices. Antivirus and antispyware through anti-phishing to web and email scanning, the service provides comprehensive protection and control over diverse endpoints connecting to your data services. Cloud based advanced heuristic analysis monitors and blocks malicious processes in real-time.

N4EPMS Advanced delivers protection techniques that Standard provides plus prevention of exploits and botnet infiltration as well as antispam filters to keep company email system free from junk email, all at the point of entry. Using fast yet light-touch agents is the key to impact free protection for all your endpoints. Switch on remote firewall shields in public Wi-Fi areas and prevent outside interference. Manage web access remotely to restrict specific website categories with blacklists and whitelists and protect virtualised environments remotely.

N4EPMS Encryption protects valuable endpoint data with local encryption and centralised key management. Full disk encryption using FIPS 140-2 validation as well as protecting removable USB sticks and other temporary media at file or full level. Instant encryption for files dropped into personalized encryption folders as well as full integration with email clients to transmit encrypted files to key holder recipients.

Utilising ESET's comprehensive and award winning technology N4EPMS provides the best tools wielded by the best security experts for an outstanding fully managed security service. Our cost effective solution provides OPEX flexibility for customers wishing to flex budget with their growth for the best outcomes for the minimum of spend. Let us be your security experts providing you with a secure endpoint environment which is fully monitored and managed.

KEY BENEFITS

COST EFFECTIVE
Benefit from industry security experts and technology by using an OPEX monthly rental solution to mitigate the risks from diverse endpoints.

SCALABILITY
A solution which scales with your business, add systems and features as a fully managed service.

SPEED
Fast to deploy with the ability to easily switch on features you need

RESILIENCE
Award winning technology and security expertise provides customers with confidence behind their security border.

COMPREHENSIVE
N4EPMS monitors and maintains endpoint organisational security policies with centralised management and reporting, across a diverse range of endpoints.

MANAGED SERVICE
Our monitored and managed service provides the Node4 Security Operations Centre (SOC) team response to incidents and offers customers regular reporting intelligence with monthly reports

For more information on Cloud services or other products and services we offer please call us on: 01743 244 933 or email us: info@pure-telecom.co.uk

Powered by NODE4

N4EPMS
KEY FEATURES

N4EPMS Standard

Antivirus & Antispyware
Eliminates all forms of threats, keeping your network protected online and off. ESET's cloud-powered reputation database increases scanning speed and minimises false-positives.

Host Intrusion Prevention System
Provides tamper protection and secures the system from unauthorised modification. You can customise the behaviour of the system, down to every last detail and detect even unknown threats based on suspicious behaviour.

Device Control
Block unauthorized media and devices, based on pre-set policies and parameters. Set access permissions (read/write, read, block) for individual media, devices, users and groups.

Auto-Scanning of Removable Media
Automatically scans USB, CD and DVD media for threats upon insertion to eliminate autorun and other removable risks. Choose from these scanning options; starts automatically/notify (prompt user)/do not scan.

N4EPMS Advanced

Web Control
Provide limits to website access by way of automatic cloud based classification.

Two-Way Firewall
Prevents unauthorized access to company network and protects company data from exposure. Remote administration provides a firewall rule merge wizard that makes aggregating firewall rules in the network easy.

Trusted Network Detection
Define trusted networks and protects all other connections with strict mode, making company laptops invisible in public wifi networks; hotels, airports and at conferences.

Client Antispam
Protects your business communications from spam and email borne threats. Set whitelist, blacklists and self-learning separately for each client or group. The antispam natively supports Microsoft Outlook and also POP3, IMAP, MAPI and HTTP protocols.

N4EPMS Encryption

Comprehensive
Complete disk encryption as well as specific file and folder security. Removable media protects data on CD, DVD and USB storage.

On The Fly
Text and clipboard encryption.

Compatible
Plug-In for Outlook email client provided email encryption for mail in transit.

Protect
Protects laptop computers against loss or theft.

Centralised Management

SOC
Our real-time web based dashboard gives you visibility of everyday network security issues providing clear information on threats and the ability to control endpoint issues, all from inside our secure SOC.

Policies
Apply custom or template policies for specific device or departmental requirements.

Reports
Customers can choose from pre-defined monthly reporting or specify custom reports.

Triggers
Node4 can define specific tasks to activate once triggers are set.

Tasks
Node4 can define various security related tasks for customers.

Cost Effective

OPEX Monthly
No expensive capital outlay, simple fixed monthly rental cost.

Scalable
Add systems and assets to your service as you grow.

Low Investment
Select initial services and add features when required.

Experts on Hand
Compliment your team by utilising our expert Security consultants as part of your security strategy.

Risk Mitigation

Visibility
Aggregated event data from disparate systems and devices provides a comprehensive overview, graded for risk and interpreted by our Security Service consultants for our customers.

Control
Providing security analytics to event data in real time for the early detection of targeted attacks and data breaches, and to collect, store, analyse and report on log data for incident response, forensics and regulatory compliance.

Regulatory Compliance

Reportable
Reports on alarms, estate assets, system availability, trends and performance.

Compliance
Reports are available to support specific compliance requirements such as PCI DSS 3.1, HIPAA, FISMA, ISO 27001 and SOX

Asset Control
Track alarms on assets for security events and vulnerabilities maintaining a valid inventory.