

## SECURITY AS A SERVICE

### Managed Security Services

Many businesses operate unaware of breaches and intrusions perpetrated inside their environment. It is only when the consequences of these breaches manifest, that subsequent investigation often reveals the extent to which these vulnerabilities have been exploited. Gaining information about threats and vulnerabilities inside and outside of your infrastructure, allows businesses to mitigate against the risks before they become today's data breaches and tomorrow's news item.

The inevitability of hacking means that businesses need to be pro-active and manage security beyond just firewall rules and malware detection. Comprehensive security management requires specific skills and techniques normally unavailable to most organisations. Implementing security systems can be prohibitive, the additional cost of managing and level of operation required to interpret these systems.

**N4NGFW** – Node4 Next Generation Firewall is our managed firewall service utilizing the best in Next Generation technology including Unified Threat Management (UTM), which covers Data Leak Prevention, Intruder Protection System, Intruder Detection System, DMZ and VPN management.

**N4Cloud Security** – comprehensive security for AWS, Azure and VMware cloud services which provides threat intelligence and multiple protective security techniques whilst maximising performance and operational efficacies from the cloud in public, private or hybrid environments.

**N4Threat Detect** – Node4's premier SIEM solution providing risk analysis and security intelligence across customer network estates. This OPEX service incorporates detailed Network Intrusion Detection System (NIDS) and Host Intrusion Detection System (HIDS), which examines packet behaviour and detects "bad actor" probing and reconnaissance. This allows for visibility of malware, rootkits and other rogue processes from user activity.

**N4MDM** – Mobile Device Management for deploying public, internal or bulk-purchased apps to devices automatically as well as managing device policies for restrictions, access control and notifications based on ownership (BYOD). Enables users to self-activate devices whilst providing companies control and management over access and security.

**N4EPMS** – EndPoint Management System allows the management and control over disparate endpoint devices, providing policy control on firewalls and web access as well as enforcing anti-virus and malware updates. Provides customers with centralised encryption management over file, folders, partitions and removable media on corporate endpoints.

**N4WAF** – Protection against DDoS and SQL Injection attacks on web sites as well as XSS and SSL attacks using invalid scripts. Customers with commercial web traffic need serious specific security for their POS web sites.

All services provides full monthly reporting is included to provide customers with intelligence of both internal and external threats, including top; alarms, attackers, attack strategies, destination ports, attacked hosts. This information can provide compliance for FISMA, HIPAA, ISO27001 and PCI 2.0 and 3.0 accreditation.

#### KEY BENEFITS

- ✓ **SCALABILITY**  
Services, which scale with your customers business, add systems and features as a managed service provider.
- ✓ **SPEED**  
Add customers easily and quickly providing a comprehensive service.
- ✓ **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](mailto:info@pure-telecom.co.uk)





# SECAAS

## KEY FEATURES

### Risk Mitigation

#### Visibility

Event data from disparate systems and devices provides a comprehensive overview, which is graded and interpreted by our Security Service consultants specific 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, analyze and report on log data for incident response, forensics and regulatory compliance.

#### Expert Consultation

Regular monthly face-to-face Security Service advisories provide critical analysis and guidance to the threats and vulnerabilities pertinent to your infrastructure.

### Regulatory Compliance

#### Reportable

Reports on alarms, estate assets, system availability, trends and performance as well as comprehensive overviews of logon failures to a host of systems.

#### Compliance

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

### 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.

### Systems Intelligence

#### OTX

Links to Alien Vault Open Threat Exchange (OTX) community (37,000 participants in 140 countries), for up-to-date threat intelligence.

#### ISO 27001 Information Security

Our ISO 27001 Security Certification ensures we meet stringent control requirements to manage information securely.

#### Asset Control

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

**Node4's Security as a Service (SECaaS): All solutions fully managed by our team of certified experts.**

