N4Cloud Security

Comprehensive Cloud Security

Security of the cloud is very different from security in the cloud. Many companies utilising cloud services from many providers assume that comprehensive security is inherent and active within their cloud deployment. IaaS provides secure access with usernames and passwords, subject of course, to those credentials being secured. However, what about the operating systems, applications and traffic passing through your virtual data centre? What about security in the cloud, what is securing the applications and data?

Virtual machines are the most important endpoints to maintain data and system integrity, it is important they be provided with substantial and comprehensive protection specifically tailored to the cloud environment.

N4Cloud Security utilises technology to provide layered protection for four key areas of cloud; Anti-Malware layer combines anti-malware with behavioural monitoring and web reputation features ensuring servers and applications are secure from threats such as ransomware.

Intrusion Protection defends against network and application threats for network traffic, and helps mitigate against Denial of Service attacks, and detects reconnaissance scans.

Integrity Monitoring identifies suspicious changes to critical operating systems components and applications files, whilst application control locks down servers against unauthorised processes, all in real-time. Finally, Log Inspection provides auditable reporting for PCI or SANS compliance as well as correlate diverse warnings for analyse for suspicious behaviour.

Native integration with AWS, Azure, N4Cloud and private cloud allows for complete and comprehensive security across a hybrid cloud platform into a single fully managed SOC controlled by Node4's security experts.

Key Benefits

✔	**Fully Managed Service** Managed from the Node4 Security Operations Centre (SOC), our security experts control and manage your security policies.
✔	**Scalability** A solution that scales with your business, add systems, more mobiles and features as a fully managed service.
✔	**Cost Effective** OPEX monthly rental solution to secure and enforce dispersed security policies.
✔	**Comprehensive** Comprehensive Security technology combined with Node4 security expertise provides customers with confidence behind their extended security border.
✔	**Visibility** N4Cloud Security monitors and maintains centralised management and reporting, across a diverse range of virtual machine and diverse operating systems to give granular control over systems and applications.

For more information on N4Cloud Security or other products and services we offer please call our Sales Team today on 0845 123 2222 or email us at info@node4.co.uk

N4Cloud Security
Key Features

Hybrid Cloud Security

Comprehensive security for Amazon (AWS), Google Cloud, Azure & N4Cloud.

Providing elastic security for dynamic workloads.

Embracing micro-services with containers including Docker containers.

Diverse support for many platforms and technologies including; Windows, RHEL, CentOS, SUSE, Ubuntu, Cloud Linux, Amazon, Hyper-V, vSphere, NSX, Azure, HP-UX, AIX, Oracle Linux, Solaris and Debian.

Anti-malware

Proactive signature based file scanning in real-time.

Document exploit protection defends data against modifications such as the bulk encryption of ransomware attacks.

Registry scanning for malicious drops.

Optional copying of original data against modification so any encrypted files through ransomware are instantly recoverable.

Anti-exploit functionality prevents DLL injection methods from malicious software using Data Execution Prevention (DEP), heap spray and Structured Exception Handling Overwrite Protection (SEHOP) technologies.

Endpoint correlation identifies malware that has “wrapped” and dropped subsequent threats by analysing the “crime chain”.

Intrusion Prevention

Controlling incoming network traffic and actively preventing intrusions, dropping malformed packets and analysing frames to RFC specifications.

Comprehensive patch management for operating systems and applications.

Analysis on cross-site scripting and SQL injection.

Lateral firewall technology including Tap and Inline modes for testing and subsequent implementation, protects and isolates VMs from cross contamination of malicious code.
Deep packet (Stateful) inspection.

Virtual patching offering protection from vulnerabilities as soon as they are released.

Integrity Monitoring

Recommendation scans offer insights into rules and policies on applications and system security.

Application control and behavioural management.

Identify suspicious changes to critical operating systems and application files on servers, in real-time.

Log Inspection

Auditable reports for PCI 10.6 & SANS compliance.

Suspicious behaviour detection.

Correlate events across diverse operating systems and applications.

Cost Effective

OPEX Security - Monthly per VM per month
No expensive capital outlay, simple fixed monthly rental cost.

Add systems and assets to your service as you grow.
Compliment your team by utilising our expert Security consultants as part of your security strategy.

Regular reporting on VM estate provides comprehensive analysis on security status.

Regulatory Compliance

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

Reports are available to support specific compliance requirements such as PCI 10.6, DSS 3.1, HIPAA, FISMA, ISO 27001, & GDPR.

Millennium Way, Pride Park, Derby. DE24 8HZ
T: 0845123 2222 **E:** info@node4.co.uk **www.node4.co.uk**