DSAAS
Deep Security As A Service

Node4 provides UK based, enterprise-grade, physical (IL3+ data centres) and cloud virtual hosting (N4Cloud), with dedicated private connections to Amazon Web Services (AWS), Google Cloud Platform and Microsoft Azure cloud platforms.

This infrastructure allows Node4 to provide Deep Security as a Service (DSaaS), as part of Node4's overall Security as a Service (SECaaS) infrastructure platform. Companies are able to utilise Node4's UK cloud infrastructure to manage their Deep Security™ system or can use Node4's managed service wrap as an OpEx expenditure. Many businesses are implementing the economic and operational benefits of hybrid cloud computing, and managing comprehensive security policies.

The ability for organisations to carry this out effectively with a single viewpoint across multiple cloud platforms is key to managing hybrid cloud security.

In the cloud, security is a shared responsibility. The cloud provider is responsible for the security of the physical and network infrastructure up to the hypervisor layer. It is up to you to protect what you put in the cloud such as the workloads; including operating systems, service configuration, applications, and data.

Powered by XGen™, Trend Micro™ DSaaS, is designed to augment cloud provider security with complete protection for cloud workloads. DSaaS provides a complete suite of security capabilities including intrusion detection and prevention, firewall, malware prevention with web reputation, predictive machine learning, sandbox analysis, integrity monitoring, log inspection, and multi-platform application control.

DSaaS gives you the proven protection of Deep Security™ without all the work. As a service deployment, we do the heavy lifting for you. We manage regular product and kernel updates, set up and maintain the security database, and administer the Deep Security™ manager.

Our cloud-based security offering enables quick setup, automates, and simplifies security operations for cloud instances.

Key Benefits

Managed Platform
Managed Platform from the Node4 Security Operations Centre (SOC), our security experts control and manage the infrastructure for your security policies.

Scalability
A solution that scales with your business. Add systems and features as a fully managed service.

Cost Effective
OPEX monthly rental solution to secure and enforce dispersed security policies.

Comprehensive
Powered by XGen™, Trend Micro™ DSaaS is designed to augment cloud provider security with complete protection for cloud workloads.

Visibility
DSaaS monitors and maintains centralised management and reporting, across a diverse range of virtual machines and operating systems to give granular control over systems and applications for you to manage.
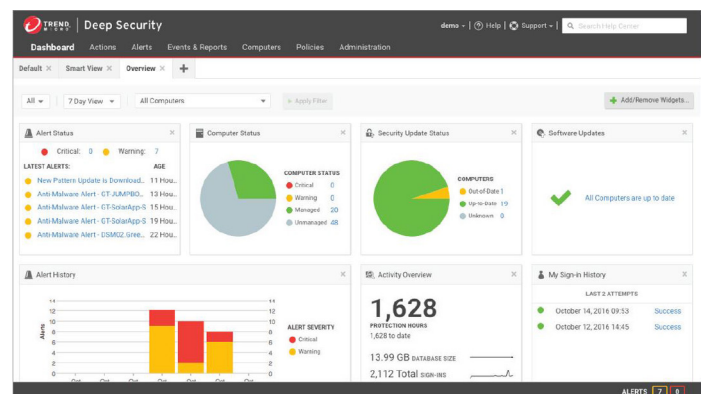
For more information on DSAAS services or other products and services we offer please call our Sales Team today on 0845 123 2222 or email us at info@node4.co.uk

Intrusion detection and prevention

Proactively protects against known and zero-day attacks by shielding known vulnerabilities

Examines all incoming and outgoing traffic for protocol deviations, policy violations, or content that signals an attack

Virtual patching helps compliance with major regulations like PCI DSS, HIPAA, etc.

Defends against SQL injection, cross-site scripting, and other web application vulnerabilities

Provides increased visibility into, or control over applications accessing the network

Malware Protection

Protects your workloads against malicious software with advanced techniques like predictive machine learning

Isolates malware to protect instances from sophisticated attacks, including ransomware

Provides detection of suspicious activity or unauthorized changes and the ability to quarantine and recover quickly with behavioural monitoring

Multi-platform application control

Increased visibility and protection for Windows and Linux servers

Gives administrators the ability to lock down servers so that no new applications can run without being whitelisted

Increases visibility into applications running on a given system and detects and blocks unauthorised software, such as malicious attacks like ransomware

Scans a server and determines what applications are currently on that machine

Increases operational control and stability, allowing administrators to determine if new applications can be added and safely run

Integrity Monitoring

Monitors and tracks system changes and reports malicious and unexpected changes in real time

Event tagging automatically replicates actions for similar events

Web reputation

Integrates with Trend Micro™ Smart Protection Network™ to prevent communication with known Command and Control servers

Decreases the attack surface by creating a firewall perimeter to block attacks

Limits communication to only the ports and protocols necessary

Centrally manages server firewall policy, including templates for common server types

Log inspection

Collects and analyses operating system and application logs for suspicious behaviour, security events, and administrative events

Assists compliance (PCI DSS) by identifying of important security events

Forwards events to SIEM system or centralized logging server for correlation, reporting, and archiving and integrates into N4Threat Detect (SIEM) services

Clear control at your fingertips

Enables policy-driven management and administration

Customisable dashboard enables users to see the health of their security environment at a glance

Customisable policy templates allow users to enable and disable security controls on the fly based on rules they assigned

Provides immediate notification of events or activities that may require immediate attention (Logging Alert)

Built for security in the cloud

Trend Micro™ DSaaS is optimized for leading cloud providers' infrastructures, including support of the most common operating systems

Powered by

Trend Micro
Deep Security™

Empowering business to do more