Network Security

Network Security components keep your network safe.

Cognosec Services

Features

Network Security refers to the security components which reside at the network layer of the business. The network layer connects the individual computers servers, applications and data storage areas together. Many attacks and interception attempts take place at this level, so it is a critical area to protect. The rapid adoption rate of cloud services and smart apps is becoming increasingly complex to manage, for both businesses and individuals in their own capacity. We provide a full service offering for any size of business from 25 users to 80,000 users, ranging from consulting, gap analysis, architecture & design, implementation and management of:

- Host-based Intrusion Prevention Services HIPS) – For Servers
- Perimeter facing and Internal facing Firewalls
- Web Application Firewall Services
- Network Access Control (NAC)
- Network Intrusion Prevention (NIPS) Services

Description

Network Security components keep your network safe and include some or all of the following, depending on your requirements:

Firewalls (FW) – These are network devices that operate like border controls – only allowing the traffic you want to pass in and out of your company.

Web Application Firewalls (WAF) – These are similar to firewalls but designed to protect public websites. They only allow specific web traffic through in either direction to protect sensitive or confidential information often held in databases linked behind the website. WAFs are Essential for eCommerce businesses, who need public facing websites that facilitate payments.

Network Intrusion Prevention Services (NIPS) – protects against malicious hidden processes and hacking using devices on the network. These devices process large volumes of traffic and generate many lines of log data, which have to be managed properly to deliver proper value.

Network Access Control (NAC) – This technology prevents unauthorized (or “Rogue”) devices from joining your network. When a device does not meet your security policies or standards it should not be able to access your network.

Network Data Loss/Leakage Prevention (NDLP) – is a technology which utilizes policies on a computer that helps prevent sensitive data from being transmitted to the wrong people, both inside and outside the company.

Distributed Denial of Service (DDoS) Services –DDoS attacks have evolved into complex and overwhelming security challenges. The attacks target the transport and network layers of a communication system and flood network interfaces with traffic, causing inability to respond to legitimate traffic. This

impacts your ability to conduct business using the network or internet, causing financial loss.

By choosing the correct managed cybersecurity services provider, all technologies can be deployed, configured and managed from a central console, but have to be properly tuned and managed to deliver ROI to the End User.

All reporting, remediation and escalation activities coordinated centrally.

Sweden
Cognosec Nordic AB
Birger Jarlsgatan 12
114 34 Stockholm
Sweden
Tel +46 (0)8 400 170 00
sales.se@cognosec.com

UK & Ireland
Cognosec Limited
3rd Floor
The News Building
3 London Bridge Street
London SE1 9SG
UK
Tel +44 (0)20 3870 1539
sales.uk@cognosec.com

Germany
Cognosec GmbH
An der Welle 4
60322 Frankfurt
Germany
Tel +49 (0)69 7593 8490
sales.de@cognosec.com

Austria
Cognosec GmbH
Castellezgasse 16/2
1020 Vienna
Austria
Tel +43 (0)1 212 2020
sales.at@cognosec.com

UAE
Cognosec DMCC
2202 Indigo Icon Tower
Cluster F
Jumeirah Lakes Towers, Dubai
UAE
Tel +971 (0)4 451 1552
sales.dxb@cognosec.com