GoodNet Network Security Systems Ltd.
(778)819-8501
info@goodnet.io

GoodNet.io is a managed, easy-to-use, flexible and versatile *cyber-security service* that turns the Internet and all of your IT assets into a Good Net for your business. A comprehensive cyber-security plan includes protection, detection, and response to cyber events. Most companies and products focus heavily on protection. The **GoodNet.io** service equally emphasizes all three of these critical components of a strong cyber-security plan.

`

GoodNet.io Router

The **GoodNet.io** service uses a border router designed for comprehensive cyber-security incident protection, detection, and response. A border router connects an organization's internal networks and the Internet, and routes traffic between them.

The **GoodNet.io** border router performs the standard border router functions as well as:

- Deny- and allow-listing DHCP server to control devices that have access to your networks and subnets
- Deny- and allow-listing DNS server to control Internet domains that can be used on your networks and subnets
- Deny- and allow-listing IP firewall to control access between networks and to external services and geographic regions
- Deny- and allow-listing service firewall to control traffic types that can be used on your networks
- Deny- and allow-listing intranet access to create security zones within your networks
- Automatic deny-listing of external networks and hosts, or internal devices based on suspicious behaviour patterns
- Precise control of inbound, outbound, and intra-network traffic, including untrusted IoT, IIoT, and guest devices
- Site-to-site and user-to-site IPSec VPN server
- Access control through profiles that can apply to whole networks, subnets, user groups, and / or individual users
- Time and event based access control profile changes (e.g. different access control during non-office hours)
- Email, SMS, and phone alerting of real-time events
- Daily reports on network, server, and machine usage (highly customizable to meet corporate needs)
- Secure off-site logging of traffic patterns to support cyber-event detection and analysis
- Detailed and highly customizable envelope and full packet logging to support detection and response
- Complete off-site audit trail and log of all router configuration changes and state for enhanced intrusion detection and recovery
- Automatic syncing of configurations between different sites
- Automatic updates to software and patterns

GoodNet.io Machine Configuration Auditor

A comprehensive cyber-security plan requires tracking changes to machine configuration and state. The **GoodNet.io** service includes a software agent, installed on Windows Server and Desktop machinesthat autonomously collects configuration and state data and logs these reports into an off-site database. Differential analysis of the configuration reports enables detection of machines operating with higher risk of cyber-intrusion, early detection of intrusions, the extent of malware spread within a network, and highlights mitigation and response actions.

The **GoodNet.io** configuration agent collects the following:

- Local and domain accounts
- Windows and Office missing updates and update status
- Root certificate stores
- Installed applications and drivers
- Executing applications, libraries, shared code, loaded drivers, and installed services
- Installed Windows Tasks and Auto-run applications
- Anti-malware scan activity and results when using Microsoft Security Essentials or Windows Defender
- DNS and ARP Cache contents
- Visited networks and network types
- Windows security events
- Windows firewall status, rules, and events
- Installed hardware including machine type, CPU type, installed memory, network interfaces, hard drive size, and free space