Sangoma

Managed Network Security

By Sangoma

Managed Network Security

Sangoma's Managed Network Security is a flexible and scalable firewall and Unified Threat Management (UTM) solution designed to protect single and multi-location businesses from unwanted and malicious traffic coming into their environment. It is a fully managed service, offloading all security measures away from businesses to Sangoma's cloud network operations team, enabling them to focus on their core business needs.

UTM is a collection of functions that capture threats at various stages of infiltration. This suite of tools work to protect customers against attacks and losses from such things as spam, viruses, ransomware, botnets, etc.

Unified Threat Management Features:

Antispam

Detects unwanted and malicious emails with global spam filtering that uses sender IP reputation and spam signatures.

Web Filtering

We rate more than 250 million websites with 1.5 million new URL ratings weekly to block traffic to certain content types as desired.

Antivirus

Identifies and neutralizes hundreds of thousands of malware programs using patented techniques.

Botnet + Domain Reputation

IP and domain address reputation tools block tens of thousands of botnet command and control communication attempts daily.

App control + IPS Service

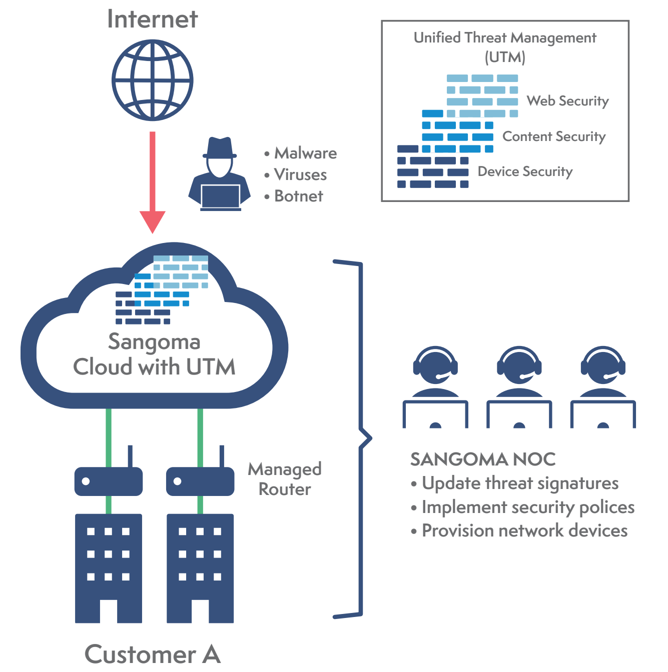
Blocks ~470,000 network intrusions with new Intrusion Prevention System (IPS)signatures deployed daily.

Deployment Methods

Managed Network Security deploys a managed router with firewall protection to each customer location and protects businesses inbound traffic in the following two options:

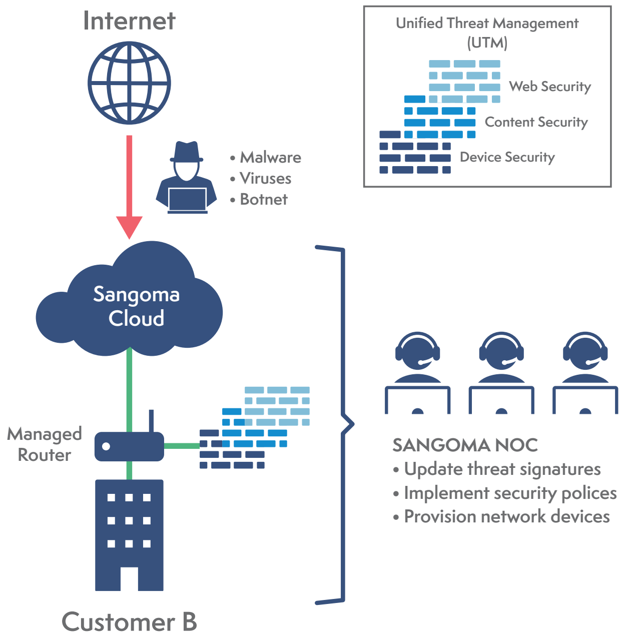
Cloud

Outbound internet traffic is sent to the Sangoma core network, processed by UTM remotely, and sent out to the public internet. Inbound traffic is similarly handled at Sangoma's core, before reaching the customer's environment.



On-Premise

Outbound traffic is processed locally, by UTM within the on-site router(s) and sent directly out to the internet, from the customer's local network. Inbound traffic is similarly handled, by UTM on-site, before entering the local environment. Traffic policies can be shared amongst locations, or unique by location.



**Customers using our Managed VPN or Managed SD-WAN solutions leverage their existing managed router to add a Managed Firewall license for operation.*

As a fully managed service, profiles and protection policies are established and managed by Sangoma experts, architected and overseen by our Chief Information Security Officer. Policies can be shared and distributed across the entire enterprise.

Secure Remote Workers with SSL VPN

For work-from-home or traveling workers, our SSL VPN secures remote access to the network. A software application is installed on each user device, which creates a VPN connection to the corporate network. Best of all, SSL VPN is included free-of-charge with our Managed Firewall service.

Powerful Add-ons

Multi-Factor Authentication

- Mobile application
- Authentication key for SSL VPN users

Standard & Advanced Active Directory / LDAP Authentication for Single Sign-on (SSO)

- LDAP integration for SSL VPN users
- Utilizes LDAP to eliminate additional username/password credentials

Sangoma

www.sangoma.com

100 Renfrew Drive, Suite 100, Markham ON L3R 9R6 Canada | +1 (256) 428-6000 or 1 (877) 344 4861 (toll free in N. America)

Every effort has been made to ensure the accuracy of this document. However, Sangoma reserves the right to make changes without notice.