

## **NOC, SOC and DC Management Solution**

Network Monitoring is an end-to-end IT performance management and monitoring suite for today's heterogeneous, hybrid and scaleout infrastructures. While specialized monitoring tools provide deep dive visibility into each tier. It is a general practitioner for your IT infrastructure – i.e., it provides the unified console from where administrators can detect and resolve a majority of IT issues. From a single pane of glass, IT administrators can monitor all aspects of their on-premises and cloud environments across servers, applications, virtualization, storage, containers, and more.

It enables to centrally manage all devices in your data centers. It allows you to connect to, collect data from, and configure your devices via SNMP, HTTPs, and other protocols for IP-based networks.

- Automatically collect real-time data from all your devices – down to the individual outlet level – through a single interface
- Set power and environmental thresholds on collected data and receive alerts so you'll be the first to know about potential issues before they become bigger problems
- Configure polling frequencies to your intervals that provide meaningful data while maintaining efficient network traffic
- Forward and filter traps to receive only the notifications that matter to you
- Analyze and trend collected data to uncover insights around your data center operations, including capacity forecasting
- Gain peace of mind about your data center security with door locks and card reader permissions that let authorized users in and keep intruders out

Tools are :

- a) EMS / NMS
- b) ITSM
- c) SLA Management Tool
- d) Asset management
- e) Email Gateway
- f) Remote Desktop
- g) Remote Management System
- h) IP Address Management System
- i) Dashboard
- j) OSS Suite
- k) Patch Management
- l) Traffic Analyzer

This Network Security Application provides complete server protection. Full application control enables micro segmentation, administrator privilege de escalation, patch mitigation, and protection against zero day threats in today's heterogeneous private/public cloud data centers.

Our Solution can:

- Protect and harden your heterogeneous virtual and physical server environments.
- Protect and harden critical applications running on legacy and end-of-life (EOL) platforms.
- Achieve visibility, harden, and protect environments.
- Effectively deliver security while migrating off EOL server platforms.
- Quickly respond to critical vulnerabilities and unauthorized application configuration changes.
- Secure your organization's critical server infrastructure against zero-day threats and new vulnerabilities.
- Execute and monitor application and instance-level security in your organization's AWS, Azure, and cloud deployments.
- Quickly provision application-centric security hardening for newly created physical and virtual workloads.
- Embed security provisioning and hardening into your organization's IT processes

Tools are:

- a) VAPT
- b) Security Information and Event Management
- c) Syslog
- d) Privilege Access Management
- e) Identity & Access management
- f) Network Access Controller
- g) Authorization, Authentication & Accounting
- h) Directory Services
- i) Forensic Simulator