Data Sheet

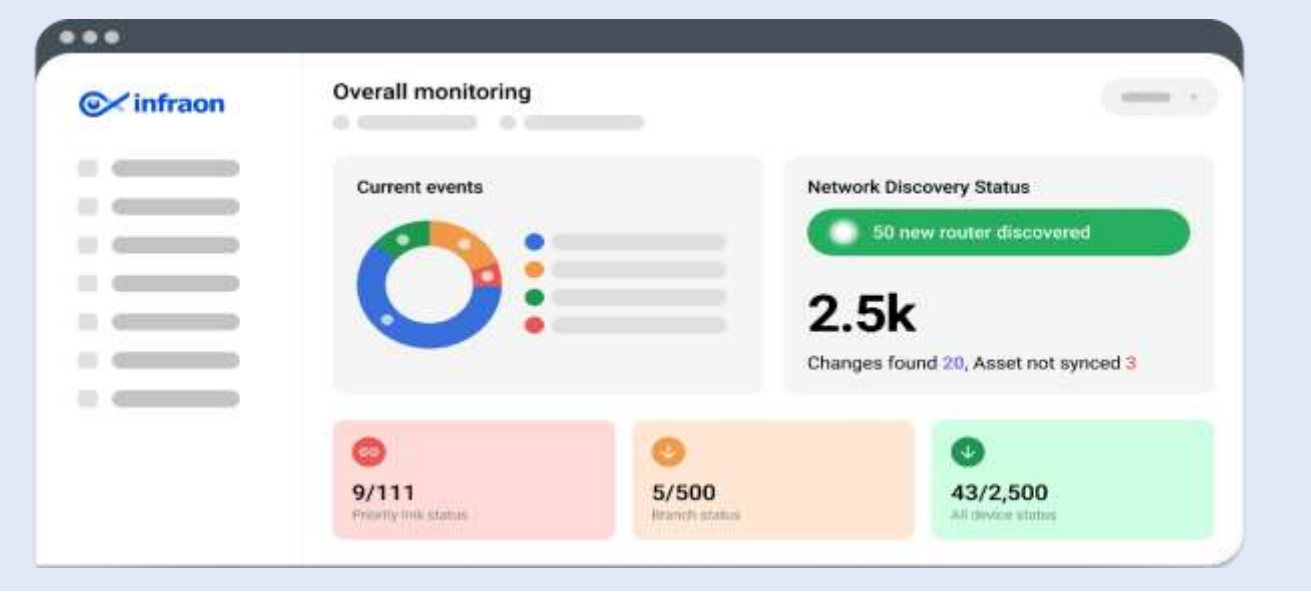
Infraon IMS

A complete Unified Infrastructure Monitoring Suite for IT, Networking, Cloud, App, & IoT Devices

Overview

Infraon IMS provides a complete Network monitoring & Management System (FCAPS), including IT Infrastructure Monitoring (Network, Server, Storage, Cloud, VMs, CCTV, Wireless, UPS, etc.), Network Configuration & Change Management, Traffic Flow Analysis with QoS Monitoring, Reporting & Dashboards with integration capabilities, Syslog Monitoring or Log Management, SDWAN Performance Monitoring, HelpDesk ITSM Tool, Zero Trust Network Access, and Link Monitoring with SLA Calculation.

The solution is scalable to monitor & manage over 5000 devices. Infraon is ISO 270001 certified for its internal processes and is capable of running on a Linux platform with an open-source database as the backend. It is available as Commercial-Off-The-Shelf (COTS) offering..



Key Highlights

- Flexible data retention policy
- Vendor agnostic tool,
- Multi-tenant,
- No additional supporting software cost,
- Flexible licensing model etc.
- Integrated platform with AIOPs-based automation & analytics which offers:
    - Capacity Planning,
    - Alarm Suppression,
    - Anomaly Detection,
    - Prediction Alarms,
    - Business Services and more.

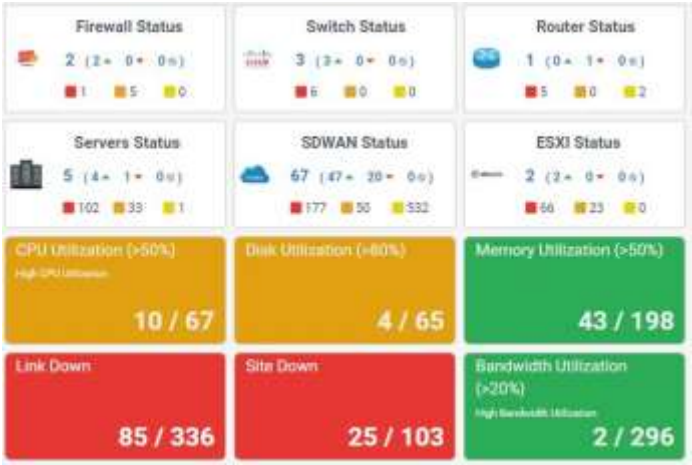
Infraon IMS is flexible in storing the polled data based on the customer's retention period and can discover both 1Pv4 and 1Pv6 devices for monitoring. It is a unified system that monitors the health and performance of network devices, servers, applications, databases and any IT device.

It can create specific views/ dashboards for any device, including Network devices, firewalls, servers, applications, IP Cameras, Wi-Fi, VSATs, UPS etc.

It is entirely multi-tenant, wherein every module and system can be assigned to a specific set of users or a group of users. The system is capable of retrieving and showing fault, performance, inventory and SLA data in a single dynamic view.

It has the capability to add any additional information about the nodes via custom fields, creating Node Tags for device grouping and resource/ interface tagging for element grouping. Apart from Node Tags, the system also has the option to perform device grouping based on default fields.

Key Feature Sets



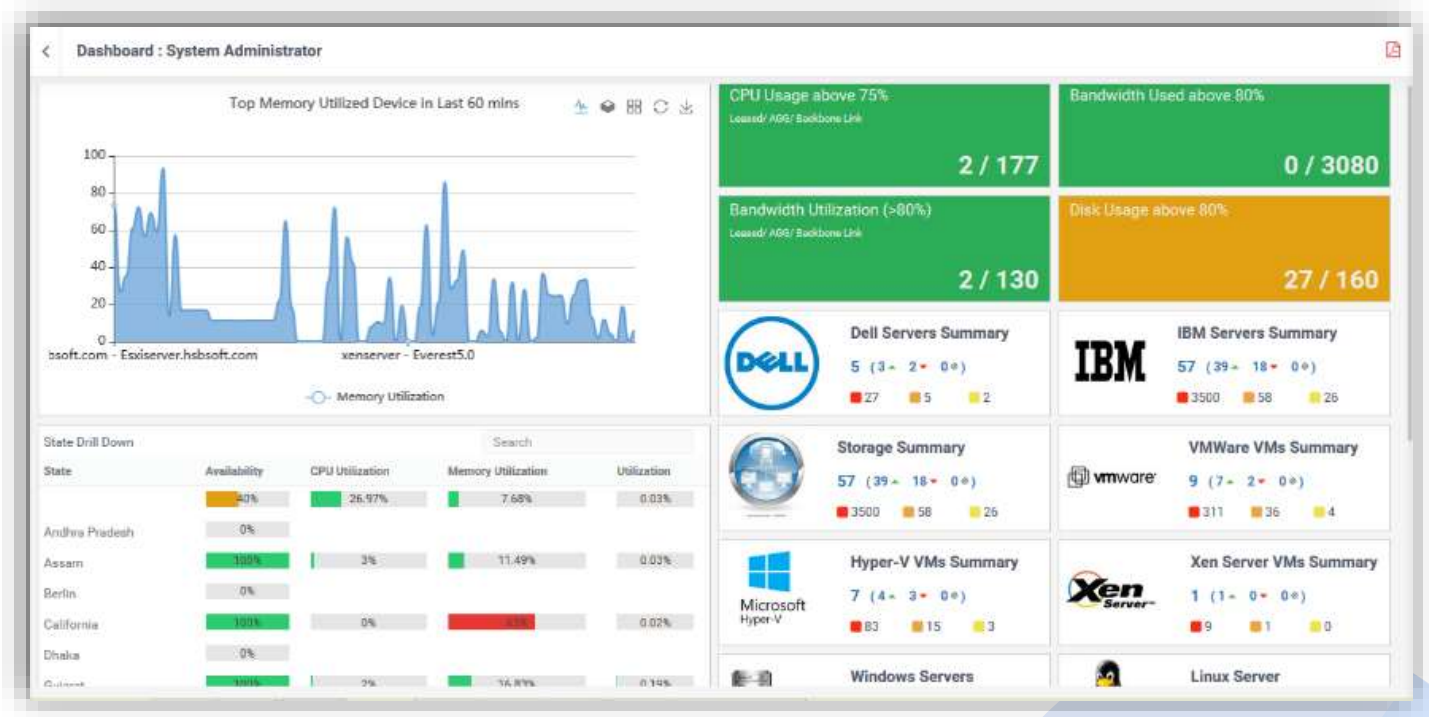
- It provides a mechanism to create multiple thresholds for each parameter which is being monitored. All fault, performance, views, and reports are configurable till the node, component or parameter level.
- The system supports a granular level of control across the system, with an option to export the views into PDF, Word, Excel, HTML and other formats depending on the user's needs, allowing each user account to have a specific type of toolbar according to the administrator's requirement.
- Each account can see/manage the list of equipment for which they are authorized.
- It provides a portal account for the end customers with restricted views limited to their specific infrastructure.
- Infraon IMS can be implemented in DMZ and non-DMZ zones with adequate security with segregation of admin users and portal users via separate logins and authentications.
- Infraon IMS can be integrated with 3rd party authentication applications like RADIUS, TACACS, TACACS-2, Active Directory, LDAP, and PIM, with an option for session-based approvals.
- It offers role-based access control, and the administrator can create custom roles and assign module level privileges.
- Provides powerful connectivity to other data sources or 3rd party applications for data import and export using REST APIs.
- It provides REST APIs to integrate with IT Infrastructure Management, Configuration Management, Network Management, and CRM tools to automate Events to Tickets. It also has an integrated ITSM module, certified by PinkVerify for ITIL v3 on at least 13 ITIL processes.
- Offers powerful Service Management features like Incident Logging, Viewing, Assignment, Escalation, Reporting, SLA Management etc., in the Service Manager tool GUI.
- The integration is bi-directional, with an optional bi-directional integrated Network Configuration and Change Management tool to use Infraon NCCM features with an additional license. The integration allows assets and topology to sync from the NMS module to the NCCM features to enable Root-Cause-Analysis of faults.

Discovery

- Discovery is automated and continuous.
- The tool offers CSV-based discovery for bulk discovery and allows adding custom fields to support customer-specific data to upload during discovery.
- Enables fetching topology via SNMP for ARP tables from routers, MAC tables from Layer 2 Switches, CISCO Discovery Protocol, Link Layer Discovery Protocol, Foundry Discovery Protocol or Synoptics Network Management Protocol.
- Offers the option to manually add any additional Topology in the network.
- Possesses the option to add Topology via GUI or tabular and enables downloading of topology connections. Discovery works intelligently by identifying the device in the network by the given IP range and categorizing it into network devices and servers with vendor and model details.
- It automatically learns devices that support SNMP, HTTP, Ping, SMTP, POP3, WMI, JMX, SOAP, REST API, PDC, SSH and Telnet, along with any required protocol to communicate to the devices. It discovers both the Primary and Secondary lines of each branch connected to DC and monitors the connectivity with the link IP address for fault and performance.

SLA

- The solution stops SLA calculation for every node in case of known downtimes.
- There is a one-click alarm masking capability in the system.
- The SLA calculation is made with the consideration of both the Primary and Secondary links together (for ISP Links) instead of individual links.
- The downtime calculation is measured when both the links are down for internal reporting and link based for ISP reporting.
- The tool provides a flexible configuration in the UI based on user needs.
- The SLA module is a template-based configuration where each branch measurement will be different for internal and ISP reporting.
- Users can configure multiple templates for their different needs and assign the related branches to a template.
- For branch connectivity with Primary and Secondary links, the system provides the flexibility for grouping multiple resources as a single service and allows the SLA computation against the service instead of individual resource/ component level SLA measurement.

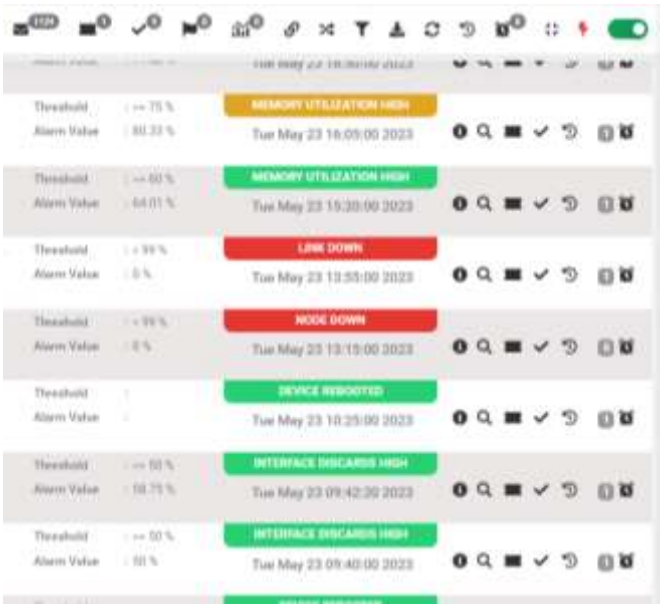


Fault Management

- Infraon IMS detects & highlights faults (abnormal situations) occurring anywhere within the network and provides Filtering, De-duplication, Holding, Suppression and Correlation capability to let the user focus on the critical event that affects the business and business processes.
- Provides multi-level (preferably six-level) Severity definition, can handle events automatically and inform the designated person as per operational requirement.
- Also supports separate Rule Engine-based alarms apart from the generic threshold.
- Infraon IMS has the capability to configure Device Group based, Node Based, Resource/ Interface based, and Aggregation link based.
- On selection of Nodes/Resources/Aggregation links, it has the flexibility to filter based on fields available in node information.
- Offers the option to configure rules and repeat counters
- Rules can apply the configuration on top of performance value or based on configured threshold alarms.
- Rules offer the option to configure the breach based on minimum, maximum and average values.
- Offers the option to select the custom alarm and clear alarm messages for individual configured rules.
- Offers the option to send severity levels like error, warning and information.
- Possesses notifications support based on configured rules.
- Provides alarm suppression withholds time, and aids in the prevention of flooding.
- Provides alarm suppression capabilities so that any duplicated events can be tracked to provide just a single event notification.
- Sends alerts via E-mail, SMS, Execute Batch file, SNMP Trap, XML notification, Pop-up window and Audio alerts too.
- Captures the SNMP traps from network devices and converts them to link down alarms automatically.
- Supports high-level status view with drill down support up to interface level.

Threshold

- Infraon IMS supports global thresholds and has the option to define individual resource/interface statistics level thresholds, with built-in algorithms to start monitoring with zero threshold configuration(s).
- It has self-learning algorithms to perform auto-baselining and automatically calculate the thresholds of components or nodes.
- It supports configurable parameters like frequency, data duration, resolution duration, sigma-based polarity value, and reset points and is available for algorithm fine-tuning.
- All thresholds within the tool have a set point, reset point, polarity, set point message and reset point message for ease of use.
- Offers an Anomalies Detection feature and can stop alarm flooding using dynamic thresholds.



Performance Management

- Infraon IMS monitors traffic from all the interfaces of the network device.
- It provides traffic utilization based on the individual interface level, nodes level or based on the group by location, branch, departments etc., as an Average, Minimum and Maximum bandwidth, utilization, throughput or any custom monitoring parameters.
- The tool has the provision to change the polling interval to any frequency depending on the priority till the individual component/resource level like each interface might have a different polling interval in the same device based on the criticality and importance of the customer.
- The tool has the provision to change the polling interval to any frequency depending on the priority till the individual component/resource level like each interface might have a different polling interval in the same device based on the criticality and importance of the customer.
- Infraon IMS monitors SDWAN device performance parameters like Latency, Packet Loss, Jitter, BFD Sessions, Control Status, CPU Utilization, Memory Utilization etc.

Polling

- Infraon IMS has the capability to configure business, non business hours or custom time polling.
- These configurations are available for every device and every component in the device.
- It has the provision to disable and enable the polling of specific types of devices and the capability to configure the maintenance period for any device.
- When a device is in a maintenance period, there is no polling done, and the SLA clock on the device can be stopped.

Notification

- Infraon IMS provides a notification mechanism that allows the administrator to define what notification channel is to be used at different times.
- Offers the option to trigger multiple notifications to alert multiple persons and actions.
- Possesses an escalation and acknowledgement function to ensure alternative personnel will be alerted when there is a critical situation and an acknowledgement mechanism for generated alerts. The escalation is available for any number of hierarchical sequences.

Diagnostics

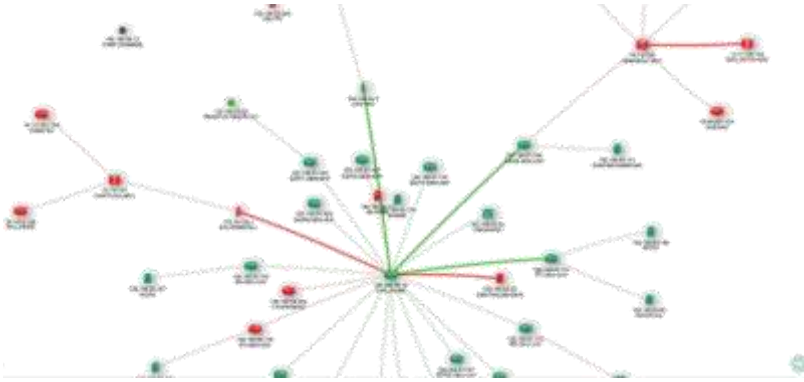
- Infraon IMS significantly reduces unwanted, non-business critical alert floods that are symptomatic of many systems management tools.
- It Identifies the root cause of any IT problem and filters out irrelevant information.
- It supports the instant diagnosis of the node status through Ping, Telnet and SNMP walk and supports real-time report generation for checking the continuous reachability of a target device.
- It can create a user-level repository of all the issues being faced. Users have the right to add data to this repository, and the system automatically retrieves back the same information.
- It offers an option to highlight the top processes consuming server for high utilization of CPU/Memory and can trigger a high alarm with a single mouse click.

Reporting

- Infraon IMS provides standard reports that display the current status of nodes and interfaces.
- Reports can be viewed on a daily graph (5-minute average), weekly graph (1-hour average), monthly graph (1-hour average), and yearly graph (1-day average).
- Offers online and offline reports that allow the user to view their device usage. Reports can be exported in HTML, PDF, Excel, and CSV formats.
- It automatically generates daily reports with a summary of the network. Custom reports can be sent by email at a pre-defined schedule to any recipient or saved into any specific folder or drive.
- It allows end-users to browse all reports using all popular web browsers. There is an option to get the required report during business and non-business hours for detailed analysis of single or multiple statistical splits based on the operations.
- It also provides a correlation report between all major network devices to determine if there is any degradation in these devices

Topology

- Displays the status of the connections based on the dependent connections and the utilization of the links by displaying connections with different widths.
- Navigates to the node page or interface page on click of the respective node or link.
- The filter topology view is based on a device group, node tag, vendor, model, IP address, hostname etc.
- The tool displays the distance between devices in Topology Maps, especially for branch gateway devices.
- It has algorithmic auto-arrangement capabilities and can use standard algorithms like forceAltas2base, repulsion or Barnes-Hut to ensure the map views are non-cluttered and arranged to the best non-overlapping method.
- It uses an SVG Map view with a drill-down option and can include any country's views: world > country > region > state > city, and the Country/Region/State/City colour can be changed based on the device status - red for all node down and orange for one or more node down and green for all node up.



Topology

The tool automatically learns IP Networks and their segments, LANs, hosts, switches, routers, firewalls etc., to establish the connections.

The different types of topology representations include:

1. Display physical connections of the different devices being monitored in the system
2. Display flat maps of the entire network or networks in a single view
3. Display customer maps based on user configurations
4. Display maps based on geo locations

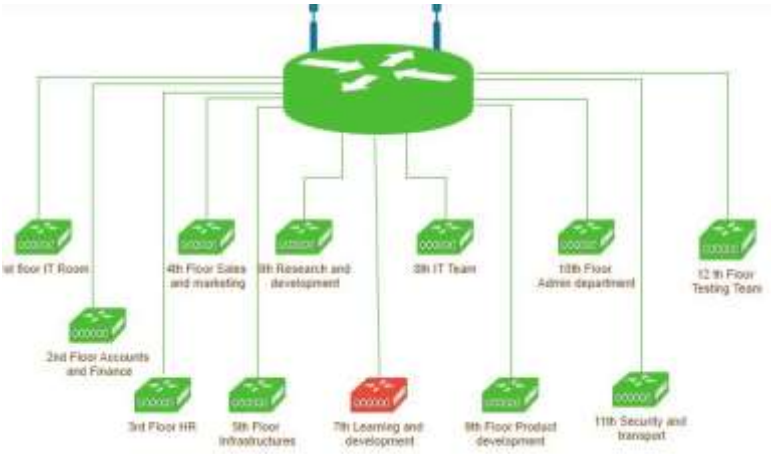
Infraon IMS searches for a specific device or resources in view of the map to the specific background for each level of the network and uploads appropriate changed icons of devices/ background of the network layers.

Flow

- The solution monitors network traffic by capturing flow data from network devices, including Cisco NetFlow v5 or v9, Juniper J-Flow, IPFIX, sFlow, and NetStream data and also sampled NetFlow data.
- The tool is capable of alternatively capturing flow data via packet capture.
- It identifies which users, applications, protocols, countries, AS numbers, top routers, and top interfaces are consuming the most bandwidth.
- It stores ALL flows without any rollups or loss for the retention period - for security and audit purposes.
- It highlights the IP addresses of the top bandwidth consumers on the network and finds out unwanted bandwidth usage.
- It associates traffic coming from different sources to application names and receives flows from non SNMP-enabled devices like VMware vSwitch.
- It monitors Class-Based Quality of Service (CBQoS) to find out if traffic prioritization policies are effective and if business-critical applications have network traffic priority.
- The tool supports CBQoS Nested policies and monitors Type of Service (ToS), Differentiated Services Codepoint (DSCP), Per-Hop Behavior (PHB), BGP AS, and NEXT HOP.
- The tool provides flow analysis with 1-minute granularity and is able to monitor up to 5 million flows per second and employs advanced optimization methods.
- It provides real-time flow and traffic analysis with 5-second granularity and sends alerts when traffic to known malicious domains is encountered.
- It can investigate if a security incident caused a breach and provides a way to list all Internal hosts that are impacted by a security incident. It helps locate infected computers in case of a virus outbreak and to recognize DOS attacks.

Network Diagram Builder

- Infraon IMS provisions drawing & mapping user-specific network diagrams.
- It has an integrated Web-based feature to build Network Diagrams.
- The builder is a Visio-like system with pre-loaded shapes and icons.
- It supports Drag & Drop based Network Diagram building and can dynamically upload images; it has customizable objects to support multiple vendors, with the capability to export maps in an XML format and upload to any other system.
- Any graph or network diagram configured has functions to associate every component in the diagram to an existing node or resource.
- Additionally, the system allows associating any parameter monitored to the specific element in the diagram.
- All network diagrams are user-controlled and viewable to only specific users. The tool defines primary & backup line connections.



Self-Monitoring Capability

- Infraon health check covering resource & process availability and load
- Tracks Infraon license usage
- Thread Status view to monitor Infraon internal threads

Panel View

- Panel view looks like the device's front panel.
- It automatically detects the device model and displays the right panel without additional configuration.
- The Panel shows all the monitored interfaces with status
- It also shows Fan status with a live fan icon and LED status for power

Virtualization

- The tool supports VM, Hypervisor and Cluster monitoring from different vendors like VMWare, Citrix, Nutanix, Linux etc.
- The tool licensing is based only on Physical Hosts and does not charge separately for individual guest VMs running on VM Hosts.

Application

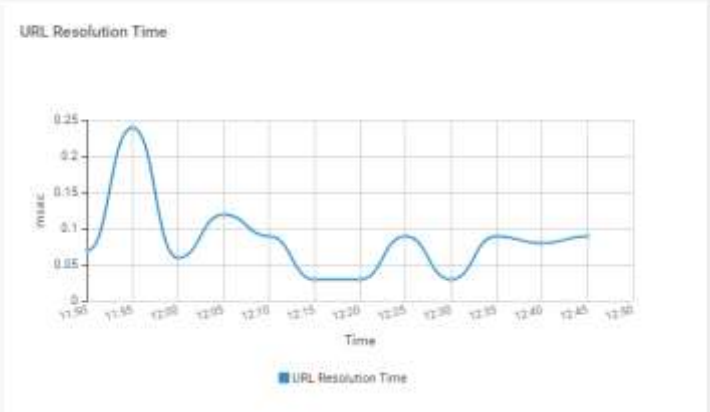
- IMS has the capability to monitor industry standard web servers like tIS IN Tomcat IS Web server statistics.
- It monitors HTTP service, HTTPS service, FTP server statistics, POP/SMTP services, ICMP services or any customer-specific port-based systems.
- It monitors various critical Relational Database Management. The tool (RDBMS) parameters such as database tables/table spaces, logs etc.

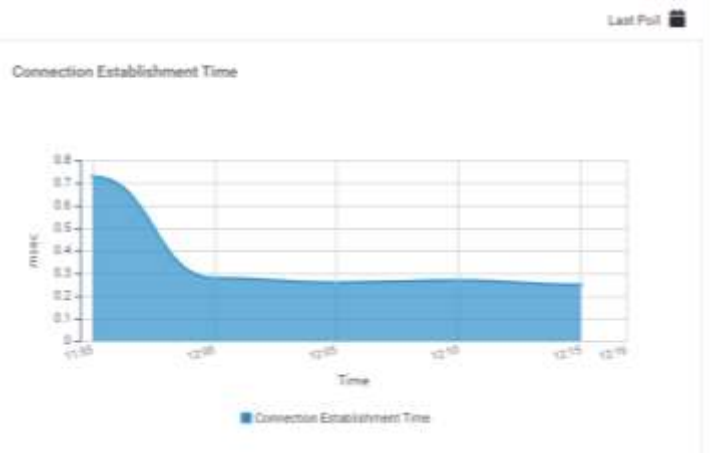
Syslog

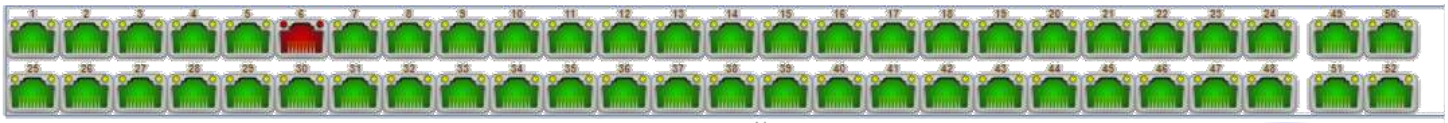
- The tool collects and stores system logs from target devices, including firewalls, routers, switches, WLC, servers, applications & databases.
- It has multiple filtering options for incoming system logs based on target device, log_ID, severity, level, message, OS type, application/database, etc. and an option to export specific Syslog messages to users via email / SMS.

Integration

- IMS offers integration capabilities with provisions on each module level. Any fault details are sent to third-party CRM, Customer Portal, UNMS or even EMS if needed using the Trap, XML, and even direct
- It provides XML, Corba, REST API, and SOAP-based systems to communicate with external software, and it is a completely integrated network management system to monitor and manage networks, servers, applications, WIFI, CCTV, VSAT, etc., from a single platform with end-to-end visibility of all the services in your network.







Panel View

Infraon Suite Product Integrations

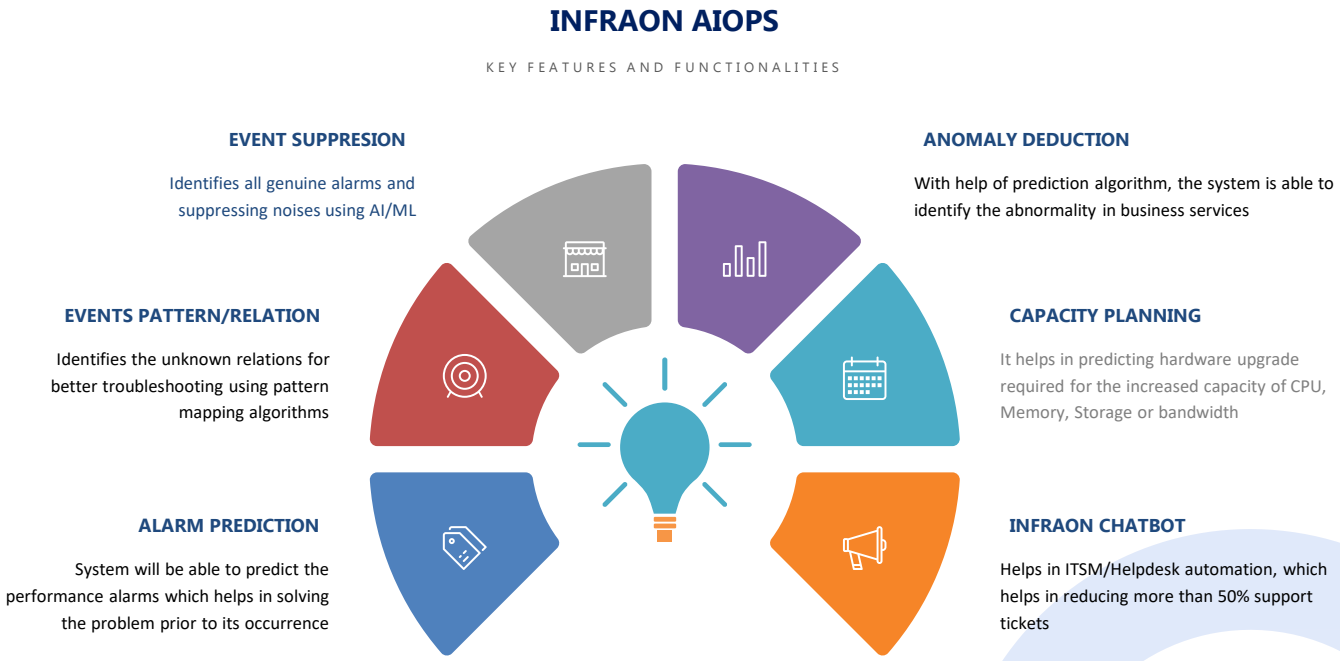
Infraon IMS, when integrated with other products from the Infraon Suite, forms a powerful offering that can address an array of ITOps challenges in a unified approach. You get a one suite-that-caters to all product. We have listed the key integration features of three other Infraon Suite products below.

QoS

- The tool allows QoS monitoring of WAN links across multiple technologies like Cisco IPSLA, Juniper RPM, Huawei NQA etc., across multiple protocols like HTTP, TCP, FTP, DNS etc.
- QoS parameters include link response time, link-level latency, link-level packet loss, link-level jitter, Round Trip-Time etc.
- It monitors Class-Based Quality of Service (CBQoS) to determine if traffic prioritization policies are effective and if business-critical applications have network traffic priority. It supports CBQoS Nested policies.

Deployment

- Infraon IMS covers geographically distributed networks through multi-level scalable distributed deployment architecture and can add new pollers at no extra cost for both scale-out and scale-up.
- Agentless deployments using standard protocols.
- Secure data transfer between remote and central servers.
- Local HA and DC/DR deployment models are supported.
- Supports database backup and restore of the deployment set-up data.



InfraonIMS Supported Devices

Network Technologies

- Wi-Fi | IP/MPLS | Metro Ethernet | DWDM | GPON | SDH | VoIP | ASON | FTTH | VSAT | RF | IOT

Network Devices

- Cisco | Juniper | Huawei | 3Com | HP | D-Link | Edge Core | ZTE | Checkpoint | Mikrotik | Brocade | Avaya | Foundry | Alcatel Routers | Network Printers | Power Backup devices | Broadcom | BDCom | Cyberoam | Palo Alto and any SNMP supported devices

Optical Network

- ECI | Nokia -ALU | Tejas | ZTE | Huawei | Calix

Servers

- Windows | Unix | Linux | Solaris | IBM AIX | Ubuntu | RedHat | CentOS | SuSE | Debian

Hypervisors

- VMWare ESXi | vCenter | XenServer | Nutanix

Applications

- .Net | IIS | MS Exchange | Tomcat | MSSQL | MySQL | Oracle | PostgreSQL

Protocols

- SNMP v1,v2,V3 | WMI | SSH | CORBA | XML | REST API |HTTP | TCP/UDP | Syslog | NetFlow v5,v9 | sFlow | LLDP | VoIP | CDP | ARP | BGP | FTP | TFTP | Telnet | TMF 814 | TL1 | Serial | IPv4/v6

Services

- DNS | IMAP2 | NTP | SMTP | JBoss | HTTP | HTTPS | POP | NNTP | SNMP | FTP | NFS | Radius | SSH | Oracle | Syslog | ICMP

Device Types

- Server | Routers | Switches | Firewall | Load Balancer | SAN | Cluster | Access Controller | Access Point | Satellite Phones | UPS | DMR Handsets | Power Rectifiers | Smart Server Racks | SMPS | SDH | DWDN | CWDM | ASON | OTN | PTN | OLT/ONT | MOT GPON

Key Monitored Performance Statistics

Network Availability | Application Availability | Resource Availability | Database Availability | Network Utilization | Network Throughput | Error Traffic | Overflow traffic | CPU Utilization | Disk Utilization | Memory Utilization | DB Status | DB Table Space | Connection Count | Aborted Clients | Aborted Connections | Job Run Count | Job Failure Count | Link Uptime | Buffer Overflow | Cache Utilization | Device Port Utilization | Latency | Packet Loss | Jitter | Ping Response Time | Web Response Time | DNS Response Time | Email Response Time | FTP Response Time

And many more…

Licensing

Infraon IMS has a simple device-based licensing model wherein the cost of monitoring a single router, switch, firewall or server is the same. The base pack includes fault & performance monitoring of devices bundled with topology mapping, reports, dashboards and notifications. Users also have the option to purchase certain addon modules for additional features, including Network Device Configuration Management, Application & Database Monitoring, Syslog Monitoring, Service Desk, etc.

Module Name	Base Package	Add-on Package
Topology Discovery	✓	
WMI, SNMP, SSH Monitoring	✓	
Performance Scan	✓	
Alarms & Notifications	✓	
Reports & Dashboards	✓	
Live & Static Maps	✓	
Business Specific Views	✓	
Network Diagram	✓	
SLA Management	✓	
Basic Inventory Management	✓	
Syslog Monitoring		✓
Database Monitoring		✓
Virtualization Monitoring		✓
QoS Monitoring		✓
Configuration Management		✓
Traffic-flow Monitoring		✓
Wi-Fi Monitoring		✓
CCTV Monitoring		✓

Minimum System Requirements (For VM as well as Physical Server)	
CPU	Quad Core 2 GHz
RAM	8 GB
Hard Drive	100 GB
OS	Oracle Linux 8.6 or above (64-bit)
Please contact our Pre-Sales team to get the exact specifications for your POC/Deployment	

About EverestIMS Technologies

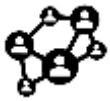
EverestIMS Technologies Pvt. Ltd. (Everest) is a leading software company – offering IOTM, AIOps and Telecom OSS solutions. Backed with rich market experience in the I&O, AI, IoT, and digital transformation space, Everest has widespread global footprints through its focused product portfolio. We specialize in providing integrated IT solutions, IT operations, and IT infrastructure to empower corporations, enterprises, and telecoms to deliver future-ready services to end-users. Our goal is to ensure that they adapt and stay competitive in evolving digital landscapes.

Navigate here for more details about us: www.everestims.com

300+
Enterprise Customers

1M+
Interfaces Monitored

5M+
Assets Monitored



100+
Vendors Supported

Reach Us

Phone
+91 80 4656 7100

email
sales@everestims.com

Web
www.everestims.com

Address

Sree Gururaya Mansion, SN 1,
No 759, 8th Main Rd, South
Wing, KSRTC Layout 3rd phase, J.
P. Nagar, Bengaluru, 560 078.
Karnataka, India