Remote Infrastructure Management

About us

- Maple Cloud Technologies is a Cert-In empanelled information security company, we rank in top 50 Information Security Companies in India.
- We are having presence in Delhi NCR and Mumbai where we are helping our customers meet their required business.
- Our team with more than 2-decade experience in providing consulting services to meet customer business requirements
- MCT is a young and vibrant Information Security company in diversified areas catering to more than 100 businesses.
- When everything is connected, security plays a big role in running the business smoothly.
- That's why MCT delivers solutions that protect every side of cybersecurity for all business sizes: Small, Medium and Large. We provide the services to protect the most critical information, systems and operations. We help to organize a safer place.

MCT Remote Infrastructure Management

The practice of remote infrastructure management (RIM) is becoming more and more common for organizations of all sizes in a wide variety of industries. This increase in popularity is because of how RIM can add value to IT systems, reduce costs, increase efficiencies, and improve service availability. In general, it includes remote monitoring, network monitoring and management, security services, database administration, and desktop and server administration.

SOC

- Continuous Proactive Monitoring
- Alert Ranking and Management
- Threat Response
- Recovery and Remediation
- Log Management
- Root Cause Investigation
- Compliance Management

NOC

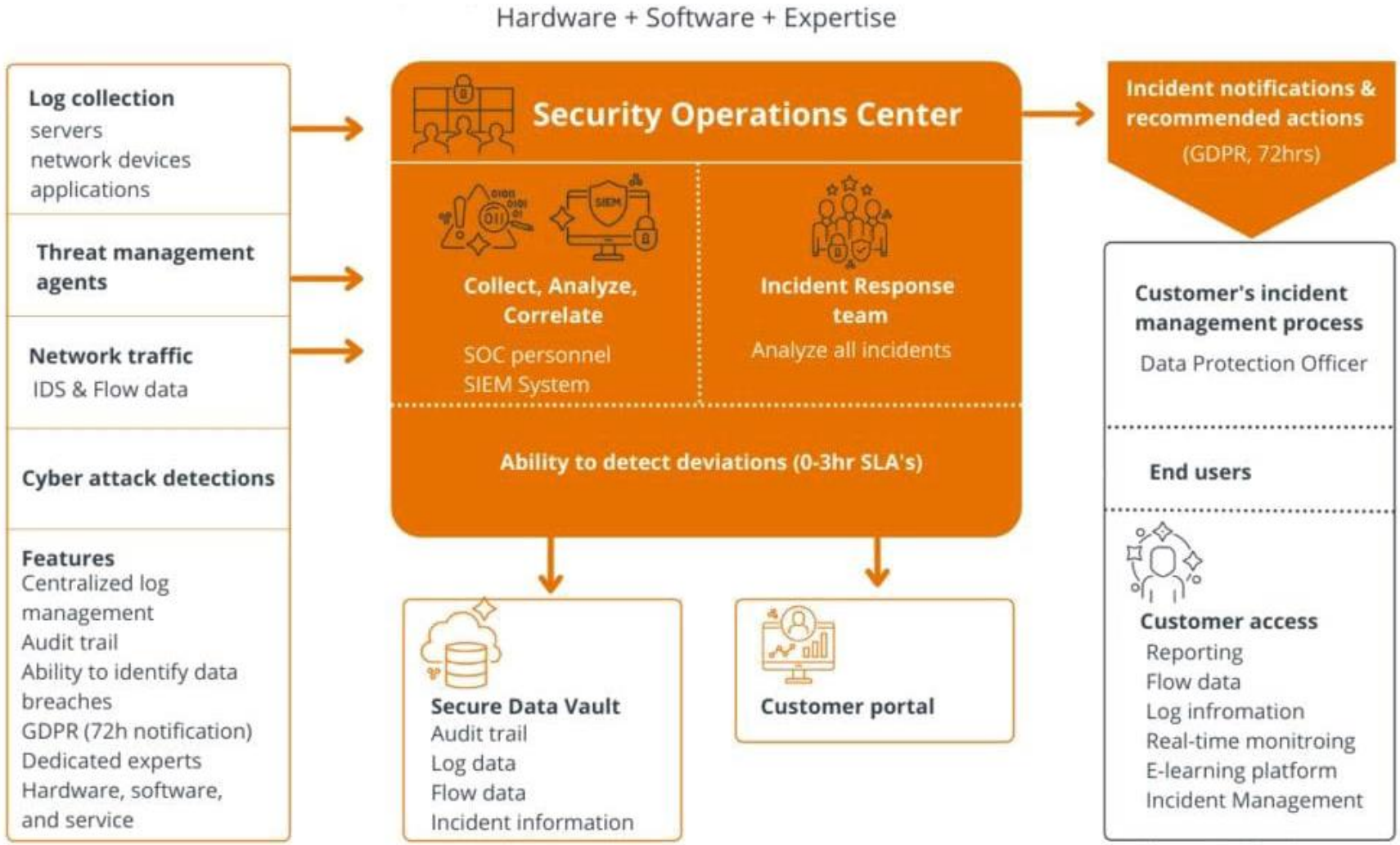
- Firewalls
- Network devices
- Servers
- Wireless systems
- Internet of things devices
- Virtual machines (VMs)
- Databases
- Software and Services (internal and external)

Service Desk

- Ticket Management
- SLA Management
- Task, Problem, Asset, Release, Contract, and Change Management
- Knowledge Base and Customer Service Portal
- Service Catalogue
- Dashboards
- Automation
- Analytics

MCT shall be setting up a 24x7 RIM and provide the required security services for a period of one year.
The resources (People, Process and Technology) required to run and manage the RIM shall be deployed from the MCT side to manage, monitor, analyze, mitigate and report incidents as they occur along with 24*7 offsite monitoring

Security Operation Centre As A Service



SIEM

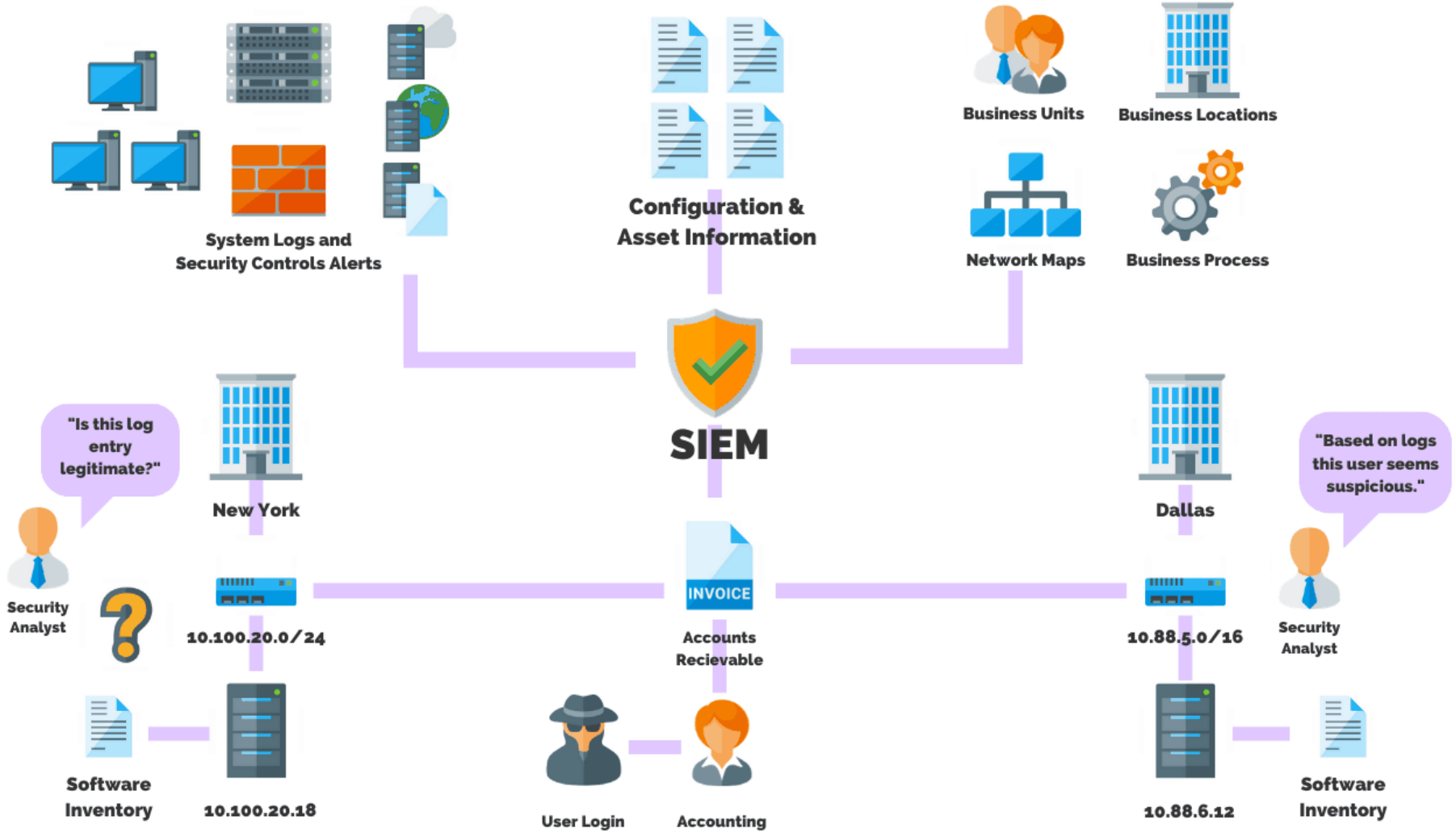
SOCs need **S**ecurity **I**nformation and **E**vent **M**anagement (**SIEM**) solutions that offer:

- The capability to ingest data from IT operations management and UEBA tools for quick incident detection.
- Real-time analytical dashboards for quicker incident detection.
- Automatic workflow management comprising predefined workflow actions.
- Built-in ticketing systems and/or the ability to communicate to the information technology infrastructure library (ITIL)
- tools to ensure accountability in incident resolution.

SIEM tools enable IT teams to:

- Use event log management to consolidate data from several sources
- Attain organization-wide visibility in real time
- Correlate security events collected from logs using if-then rules to effectively add actionable intelligence to data
- Use automatic event notifications that can be managed via dashboards

SIEM Flow


System Logs and
Security Controls Alerts
Configuration &
Asset Information
Business Units
Business Locations
Network Maps
Business Process
SIEM
"Is this log entry legitimate?"
Security Analyst
New York
10.100.20.0/24
Software Inventory
10.100.20.18
INVOICE
Accounts Recievable
User Login
Accounting
Dallas
10.88.5.0/16
10.88.6.12
"Based on logs this user seems suspicious."
Security Analyst
Software Inventory

SOAR

SOAR (**S**ecurity **O**rchestration, **A**utomation, and **R**esponse) refers to a collection of software solutions and tools that allow organizations to streamline security operations in three key areas: threat and vulnerability management, incident response, and security operations automation.

- **Security orchestration** is a process that puts alerts from disparate security and network tools into an actionable context with a procedure in place to handle the alert manually and/or automatically.
- **Security automation** reduces the need for humans to deal with repetitive tasks and alerts that can be resolved automatically.
- **Incident response** is a set of processes and technologies used to plan and implement the steps needed to address an incident

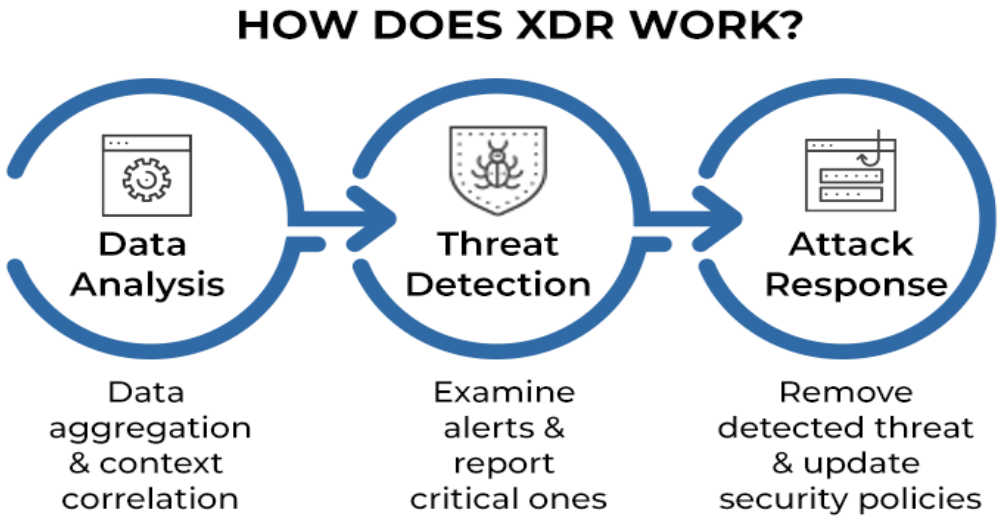
Benefits of Using SOAR in your security operations

- Faster response time
- Optimized threat intelligence
- Reduced manual operations & standardized processes
- Streamlined operations
- Reduced cyberattack impact
- Easy technology & tools integration
- Lowered costs
- Automated reporting & metrics capabilities
- Standardized communication during incident response

XDR

XDR solutions bring a proactive approach to threat detection and response. It delivers visibility across all data, including endpoint, network, and cloud data, while applying analytics and automation to address today's increasingly sophisticated threats. With XDR, cybersecurity teams can:

- Identify hidden, stealthy and sophisticated threats proactively and quickly
- Track threats across any source or location within the organization
- Increase the productivity of the people operating the technology
- Get more out of their security investments
- Conclude investigations more efficiently



IDAM

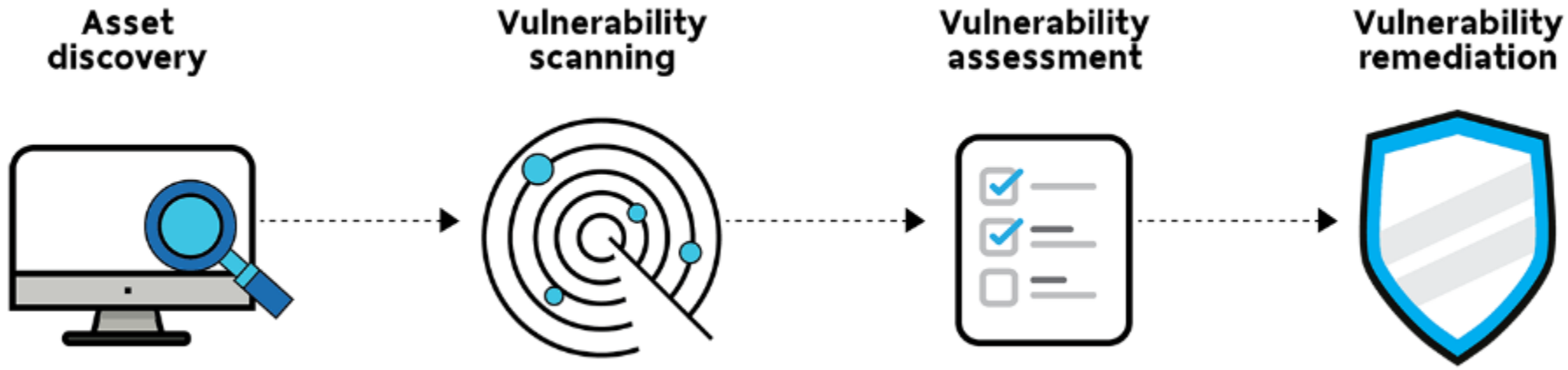
Identity and Access Management (IDAM) is the process of managing digital identities within an organization, including restricting or allowing access to certain data. Through identity and access management, every person in an organization is granted a certain level of access to company data.

MCT VA Tool

Transform security capabilities to effectively outmanoeuvre today’s threat actors and enable operations to provide resilience against future compromise.

- Evaluate existing security posture
- Evolve cyber risk management strategy
- Prepare for breach impact
- Apply up-to-date threat intelligence

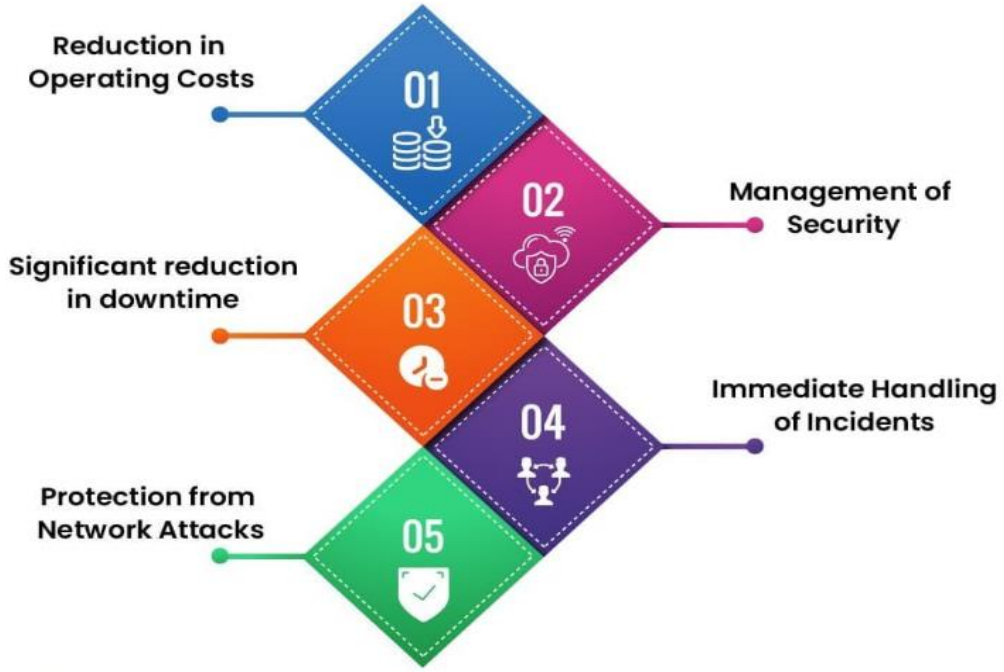
Evaluate your cyber risk exposure for effective decision-making and risk mitigation by identifying risks most relevant to your organization and understanding the potential harm they pose to your business.



NOC

A **NOC**, or **N**etwork **O**perations **C**entre, is a centralized facility where IT support technicians control, monitor, and maintain customer connections. The overall goal of a NOC is to keep the network going smoothly and without interruptions.
The **NOC** Services provide data security for network quality 24 hours a day, seven days a week, to assist, avoid downtime and ensure uninterrupted services.

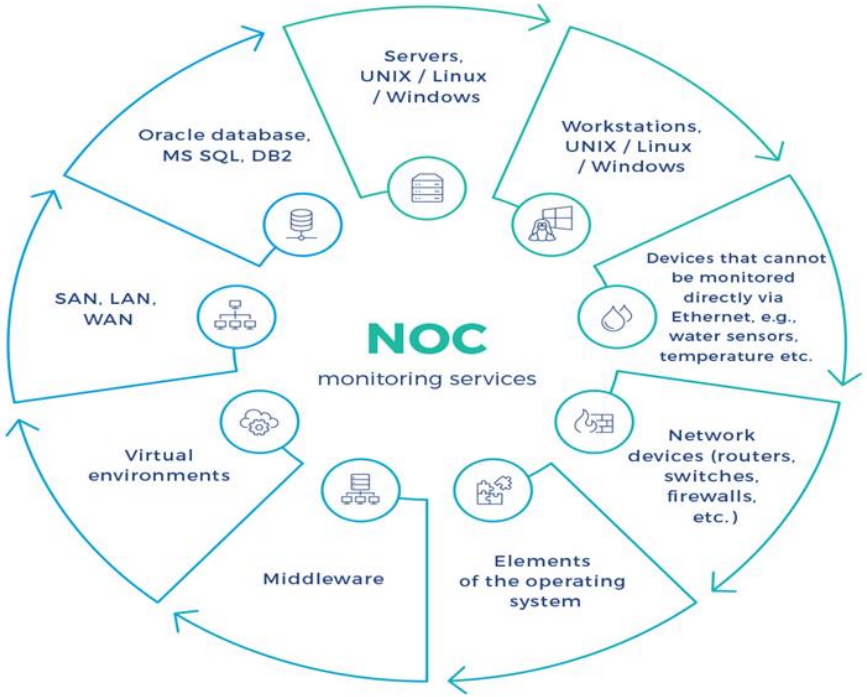
MCT NOC Solution can help you with



NOC Security

A **N**etwork **O**perations **C**entre **(NOC)**team delivers technical support. Key responsibilities include

- Endpoint monitoring and management
- Incident identification, classification, and resolution
- Software installation and management
- Email management
- Backup and storage management
- Patch management
- Threat analysis
- IT performance reporting



Proposed Solution Component

Centralized IT infrastructure management offers greater coordination and ease of maintenance and helps make IT an enabler of innovation. Benefits include cost savings, improved availability, reduced risk, and increased productivity, flexibility, and efficiency. Outsourcing RIM processes to remote infrastructure management providers lets enterprises concentrate on core business and meet growing business requirements without inflating the IT budget.

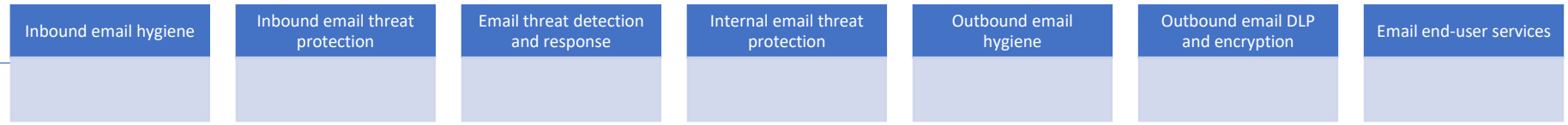
Element Management System (EMS)

The EMS is a critical part of the telecommunications management solution. One reason is that the EMS is the only exposed network element within the TMN and acts as the mediator of the information. It also controls the network elements within a network management system
Element Management System (EMS) manages specific types of one or more network elements within a telecommunication management network (TMN). In most cases, it is the job of the EMS within a network element to manage functions and capabilities

Components of EMS

Secure Email Gateway

A type of email server that protects an organization's or users' internal email servers. This server acts as a gateway through which every incoming and outgoing email passes. A Secure Email Gateway (SEG) is a device or software used for email monitoring that is being sent and received. Email gateway protection is designed to prevent unwanted emails and deliver good email



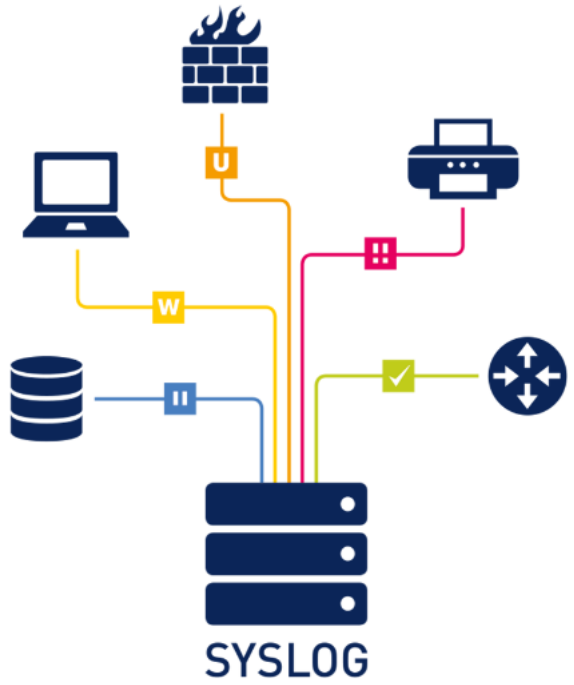
MCT **SEG** Components

Sys Log Solution

MCT Sys Log centrally stores the syslog messages and SNMP traps from various network devices. With centralized storage, you can easily search, filter, and view Syslog messages. The Syslog server typically contains the following components:

Syslog Listener: It gathers the event data to allow the collector to start receiving messages over the network.

Database: Syslog collector generates a large volume of data. The server shall have large database for fast read/write operations.



IPAM

IPAM (IP Address Management) is the administration of DNS and DHCP, which are the network services that assign and resolve IP addresses to machines in a TCP/IP network. Simply put, IPAM is a means of planning, tracking, and managing the Internet Protocol address space used in a network.

- Address Space Management
- Virtual Address Space Management
- Multi-Server Management and Monitoring
- Network Audit
- Role-based access control

MCT IPAM Components

Key Deliverables from MCT

- Alerts & Incident volume
- Significant Incidents
- SLA performance
- Event throughput
- Summary of sources onboarded along with their frequency of update (real time vs batch)
- Number of new rules added with associated playbook
- Risks, issues & dependencies to be included to ensure service quality remains optimized
- False positives and effectiveness of tuning actions to reduce them
- Average time taken to triage & escalate events to incidents, split by priority & category
- Recommendations based on MCT's experience.
- Quarterly Security Updates on KPIs and KRIs for each BU

Key Performance Indicators (KPIs)

KPI/Service Level Agreement Factor	Qualitative Consideration
Incident reports completed and submitted on time	Quality rating of reporting, supervisory review and satisfactory resolution of reporting defects
Response time or Time Service Factor (TSF)	Percent meeting combined dispatch & response target time with satisfactory resolution of initiating event
Corrective action plans (percent compliance)	Analysis of plans by type and location to connect the dots, isolate root causes and ensure systemic mitigation of issues.
Service quality	Often calculated on staff appearance, courtesy, helpfulness factors.
Service level improvements submitted & adopted	Improvement that measurably contributes to increased productivity, eliminates hours of required service or improves risk outcomes within acceptable time frame.
Number of customer requests for support	Number processed with satisfactory vs. unsatisfactory resolution as defined by the customer.
Key process cycle time	Percent achieved vs. missed with proven steps to eliminate defects.

SLA & Response Time

Below are the expected Service level Agreements (SLA) for 24x7 SOC Service. For all the respective services the MCT Shall maintain 99.5% uptime. MCT Shall consider the requirements and propose the number of onsite FTEs to maintain the SLAs.

Severity Level	Initial Response Time to incoming alerts	Time to Escalation to Ingram Micro team, after triage & investigation
Critical	Up to 30 mins	30 mins
High	Up to 1 hour	4 hours
Medium	Up to 4 hours	1 Business Day
Low	Up to 1 day	Summary of Security Alerts via daily reports.

Delivery Model

MCT believes in providing quality services to our customer all the time. We deployed required skilled professional to provide the best service in the industry, we are proposing following delivery model to meet customer business objective:

People	Skills	Model	Remarks
Service Desk	0-2 Years of experience in managing the Service Desk.	Dedicated/ Remote	Service Desk executive shall be working MCT Help Desk where customer will log a ticket on the same. Service desk executive shall be first point of customer from MCT side.
L1	0-2 Years of experience in the relevant technology	Dedicated/Remote	L1 resource shall be working on the incident which is assigned to them and will provide the satisfactory response to customer. Assign the ticket to L2 resource if ticket is not resolved as per the KPI section.
L2	3-5 Years of Experience on the relevant technology	Shared/Remote	Shall be working on the incidents/tickets which is assigned to them by the L1 Engineer, Involved in change and configuration management.
L3	6-10 Years	Shared/Remote	Working on the incidents which is assigned by L2 engineer. Taking care of Problem Management Taking care of Change Management
Project Manager	5-10 Years of Experience in Project Management	Shared/Remote	Project Manager will be the single point of contact from MCT
Process	ITIL Process		MCT Shall be following ITIL Process framework to deliver the services, following process shall be under MCT Incident Management, Problem Management Change Management

Resource Mapping

MCT believes in providing quality services to our customer all the time. We deployed required skilled professional to provide the best service in the industry, we are proposing following delivery model to meet customer business objective:

Sl. No.	Resource Type	Support Coverage	Period of Support
1	PM – Project Manager	Server Monitoring; Link Monitoring; Firewall Monitoring; End User Calls; Any activity related to server and firewalls; change management request; Anti-virus implementation & Support; SQL Database & Server Configuration/Troubleshooting	General Shift ; Remote/On-Site (as per requirement); Project Manager shall be single point of contact between customer and technical team.
2	L2 – Security + Network		General Shift or any other shift as per requirement Change Management Configuration Management Patch Management Configuration Management Escalation Management
3	L2 – Server		
4	L1 - Network + Security		3 Shifts Ticket Resolution & Problem Management Housekeeping of devices Periodic Health Check Configuration/Customization Support Threat Feed Integration Backup & Credential Management Gap Assessment for in scope devices Quarterly Improvement Plan
5	L1 – Server		
6	L2 – VA & PT	Vulnerability Assessment	General Shift; Perform vulnerability scanning; Perform Penetration testing; Implement Threat intelligence; Perform Security drill test
7	L2 – PT	Penetration Test	

MCTDMS

MapleCloud Technologies Document Management System is the ideal solution for businesses seeking to optimize their document management processes, enhance productivity, and ensure data security and compliance. With its advanced features, intuitive interface, and seamless integration capabilities, MapleCloud Technologies DMS empowers organizations to thrive in the digital landscape. By adopting MapleCloud Technologies DMS, businesses can streamline operations, save costs, promote sustainability, and foster collaboration. Thank you for your attention, and we are excited to address any questions you may have about MapleCloud Technologies DMS.

Document Management System (DMS) by MapleCloud Technologies. Businesses must find a simplified and safe management solution for the massive amount of papers and information they must deal with in this digital age.

The MapleCloud Technologies DMS provides a robust and user-friendly platform for effectively recording, organizing, and accessing documents.

Let's examine the main characteristics, advantages, recommended methods for installation, and special features of MapleCloud Technologies DMS.

KEY COMPONENTS OF DMS

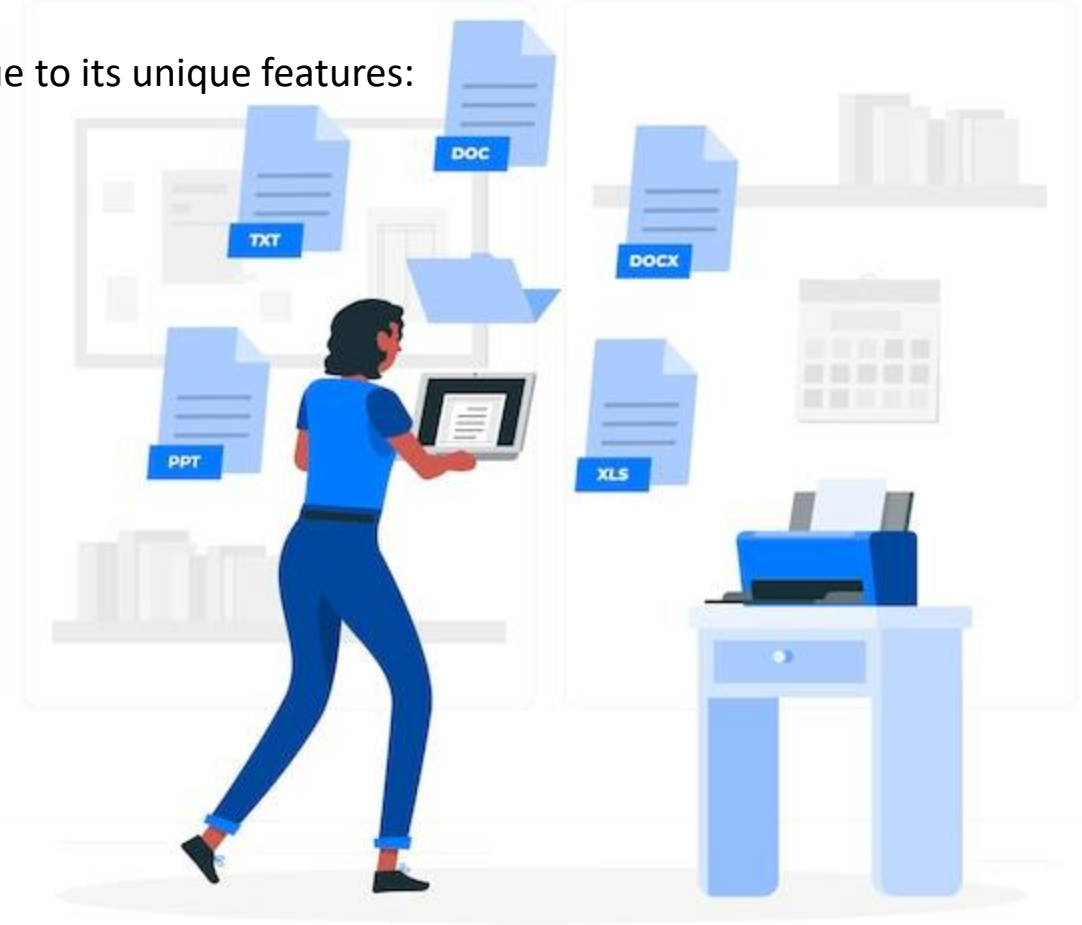
MapleCloud Technologies DMS is a cutting-edge software solution designed to enhance document management processes for businesses of all sizes. It leverages advanced technology to offer a wide range of features that simplify document handling and foster collaboration. Let's take a closer look at the key components of MapleCloud Technologies DMS:

- **Document Capture:** MapleCloud Technologies DMS allows seamless document capture through various channels, including scanning, electronic forms, email integration, and direct uploads.
- **Centralized Storage and Organization:** All documents are securely stored in a centralized repository, organized into customizable folders and subfolders. The system employs metadata tagging for effortless categorization and quick retrieval.
- **Version Control:** MapleCloud Technologies DMS maintains a comprehensive version history of documents, enabling users to track changes, view revisions, and revert to previous versions if needed.
- **Security and Access Control:** Security is a top priority for MapleCloud Technologies DMS. It employs robust access control measures, encryption protocols, and audit trails to ensure documents are accessible only to authorized personnel.
- **Intelligent Search and Retrieval:** The DMS features an intelligent search function, allowing users to quickly locate documents using keywords, metadata, or content-based searches, significantly reducing time spent on document retrieval.
- **Workflow Automation:** MapleCloud Technologies DMS streamlines business processes with customizable workflow automation. It enables automatic document routing, approvals, and notifications, optimizing productivity and minimizing manual tasks.
- **Real-time Collaboration:** Users can collaborate in real-time on documents, making edits, leaving comments, and engaging in discussions, promoting efficient teamwork and decision-making.
- **Seamless Integration:** The DMS seamlessly integrates with other business applications and systems, including CRM, ERP, and cloud storage platforms, ensuring smooth data exchange and an interconnected workflow.

FEATURES OF MCTDMS

MapleCloud Technologies DMS stands out from the competition due to its unique features:

- **Advanced AI-Powered Search:** The DMS incorporates cutting-edge AI technology for smart and context-aware document searches, making it easier to find relevant information.
- **Intuitive Mobile App:** MapleCloud Technologies DMS offers a user-friendly mobile app, enabling access to documents on-the-go, promoting flexibility, and enhancing productivity.
- **Customizable Workflows:** The DMS provides highly customizable workflow automation, tailored to fit specific business processes, resulting in seamless and efficient operations.
- **Scalability:** MapleCloud Technologies DMS is designed to scale effortlessly as the organization grows, accommodating increased document volumes and user demands.



MCTNMS

MCT NMS, an network management platform designed to monitor and manage complex networks efficiently. MCTNMS has evolved into a mature and reliable solution for network monitoring and management.

MCTNMS is a powerful, feature-rich network management system that provides end-to-end monitoring and management of network devices, servers, applications, and services. MCTNMS collects and reports on a variety of data from a computer network, including routers, switches, firewalls, load balancers and even endpoints like servers and workstations.

The collected data is filtered and analyzed to identify a variety a network problems. The network problems can be of device failures, link outages, interface errors, packet loss, application response time, configuration changes, etc. The functions of a network monitoring and management system can be broken down into several categories, each of which performs a specific function.

INTRODUCTION

Event collection and processing

Event collection relies on Simple Network Management Protocol (SNMP) traps and syslog to collect network event data. Event processing is used to identify critical events, reducing the volume of alerts that network administrators must use to identify the root cause of the problems.

Network change and configuration management

Network change and configuration management (NCCM) archives network device configurations and can be used to automate configuration updates. Configurations may be retrieved and updated using any the command-line interface (CLI),

Configuration analysis identifies day-to-day changes and audit compliance exceptions where configurations don't match network design policies.

Telemetry

Devices and monitoring systems may employ network telemetry to push network performance data to a network monitoring system. Some network monitoring systems and related network devices use representational state transfer interfaces to collect data using these same data formats.

INTRODUCTION

IP address management

IP address management tracks IP address use and controls the allocation of addresses to network devices.

Topology mapping

The topology and mapping function of MCTNMS collects device connection data to create physical and logical topology maps that form the foundation of basic troubleshooting. SNMP polling used to collect data on routing neighbors (Layer 3), switching neighbors (Layer 2), address translation tables (Layer 2 to Layer 3 mapping) and neighbor discovery protocols, like Link Layer Discovery Protocol.

Digital experience monitoring

Digital experience monitoring employs active testing tools, such as ping, traceroute and synthetic monitoring, to test that the network is working as intended. Combining application performance monitoring with network monitoring enables IT organizations to diagnose whether an application problem is due to the network or some other factor, including external networks.

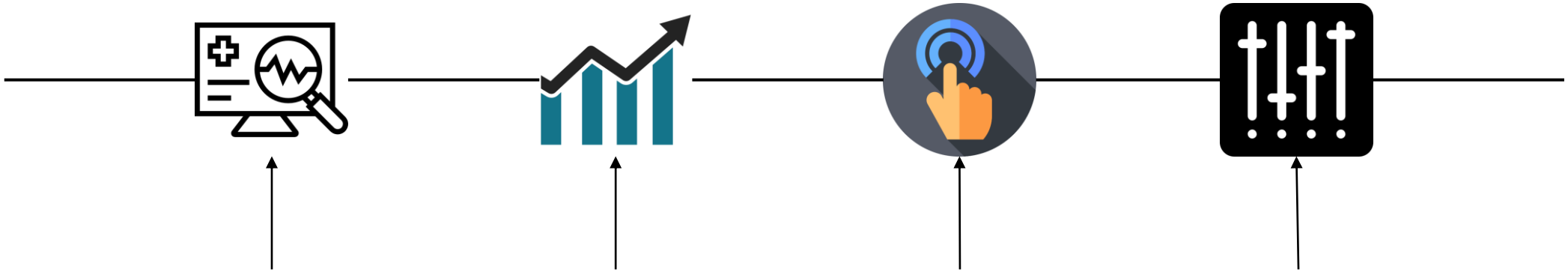
INTRODUCTION

Security and automation

MCTNMS architecture focuses on security and automation throughout the modules in Network Monitoring and Management. Security continues to be an important element of a smoothly running network, and automation is used to guarantee consistent implementation of network policies.

Combining data from multiple sources enables a secure network monitoring system to identify failures quickly and to report on performance problems before they negatively affect applications that use the network.

Network Analysis



Identifying the equipment that has to be watched

Choosing the frequency of the polling

Determining the appropriate protocols

Setting up useful thresholds

MCTNMS KEY FEATURES

Network Monitoring:

MCTNMS continuously monitors the health and availability of network devices and services. It supports various protocols such as SNMP, ICMP, HTTP, and more.

Fault Management:

The system detects network faults, generates meaningful alarms, and notifies the appropriate stakeholders, allowing for quick identification and resolution of issues.

Performance Measurement:

MCTNMS collects performance data, including response times, bandwidth utilization, and CPU/memory usage, to analyze trends and optimize resource allocation.

Provisioning and Configuration Management:

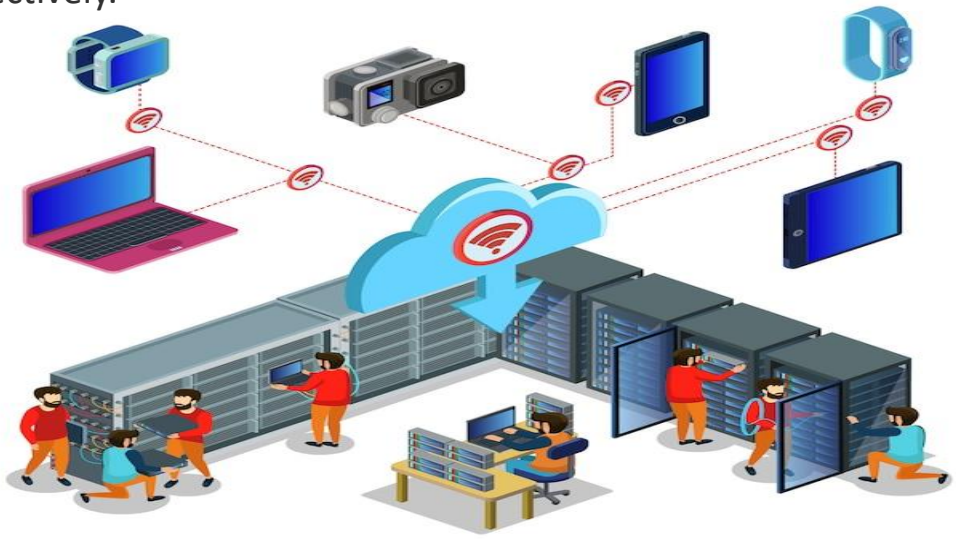
It automates the provisioning of new devices and simplifies the management of device configurations centrally. Users have the option of manual/automated addition of devices/nodes into MCTNMS for monitoring.

Notification and Escalation:

Administrators can set up flexible notification policies, ensuring that the right personnel are alerted promptly in the event of critical incidents.

Reports and Dashboards:

MCTNMS offers a range of customizable reports and interactive dashboards to visualize network performance and health data effectively.



MCT-AUTHENTICATOR

MCT-Authenticator is a high-performance, scalable, and extensible RADIUS server that provides centralized authentication and authorization for network access. It supports a wide range of authentication methods, including EAP-TLS, PEAP, MS-CHAP, and PAP.

FEATURES:

Authentication: MCTAuthenticator provides centralized authentication for network access. It supports a wide range of authentication methods, including EAP-TLS, PEAP, MS-CHAP, and PAP.

Authorization: MCTAuthenticator provides centralized authorization for network access. It supports a wide range of authorization methods, including VLAN assignment, restrictions, and limitations.

Accounting: MCTAuthenticator provides centralized accounting for network access. It logs the network activity, including session start and stop times, data usage, and connection quality.

Extensibility: MCTAuthenticator is highly extensible and supports a wide range of third-party modules, including LDAP, SQL, and Kerberos to work as a backend.

High Performance: MCTAuthenticator is designed for high performance and can handle large numbers of authentication and accounting requests. Scalability: MCTAuthenticator is scalable and can be deployed in distributed environments to handle large numbers of authentication and accounting requests.

Security: MCTAuthenticator provides robust security features, including support for TLS encryption. Compatibility: MCTAuthenticator is compatible with a wide range of network access devices, including switches, routers, and wireless access points authenticating through Radius protocol

Benefits

Centralized Authentication: MCTAuthenticator provides centralized authentication for network access, simplifying network security management.

Centralized Authorization: MCTAuthenticator provides centralized authorization for network access, enabling network administrators to enforce network usage policies.

Centralized Accounting: MCTAuthenticator provides centralized accounting for network access, enabling network administrators to monitor the activity of users.

Compatibility: FreeRADIUS is compatible with a wide range of network access devices, enabling organizations to leverage existing network infrastructure

CONTACT US

THANKS!

DO YOU HAVE ANY QUESTIONS?

fly@maplecloudtechnologies.com
+918178803636
www.maplecloudtechnologies.com