OpsRamp

a Hewlett Packard Enterprise company

SOLUTION OVERVIEW

GET TO KNOW THE WORLD'S LEADING AVAILABILITY SOLUTION.

CONTENTS

Now it's easy to consolidate all your operational activities into one place, handle the speed, scope and scale of modern IT, and drive productivity and business value.

- Consolidate your monitoring of application availability across a hybrid landscape with OpsRamp, a Hewlett Packard Enterprise company. OpsRamp offers hybrid monitoring for workloads across multi-cloud, cloud native, on-prem, private data centers, and more.
- Reduce mean-time-to-detect and resolve with AIOps-enabled event management that controls incident volume and Improves the efficiency of workflows across DevOps, ITops, and ITSM teams.
- Maintain complex infrastructure health and availability with smart process automation of routine maintenance, alert triage, and more.

Modern, hybrid, digital business needs a new solution to help control the chaos of increasingly complex infrastructure management and application availability. That's the power of OpsRamp.

This guide will serve as the technical overview of the solution. Read more for a deeper understanding of how OpsRamp can drive value for your organization.

1 / KEY FEATURES AT A GLANCE

1.1 / Core Solution Features

- SaaS-Based
- Multi-Tenant-Ready
- Role Based Access Control
- Single Sign-On
- Multi-Factor Authentication
- Custom Branding

1.2 / Discovery and Monitoring

- Hybrid Infrastructure Discovery
  - On-Prem Physical Servers, Network, Storage
  - Virtualization Environment
  - Private Cloud
  - Converged and Hyperconverged environment
  - Public Cloud [IaaS, PaaS, FaaS, and CaaS]
  - Cloud native applications – containerized environments
  - Synthetic Transaction Monitoring
  - Prometheus metric ingestion into OpsRamp
- Hybrid Infrastructure Asset Visibility & Status
- Service Maps
- Monitoring Automation
- Monitoring Hybrid Infrastructure for availability and performance metrics

1.3 / Event and Incident Management

- Event Management
  - Integration with 3rd party event data source
  - De-duplication and severity flapping
  - Event Correlation based on AI/ML
  - Event Correlation based on time and event attributes
  - Event Suppression based on AI/ML [Seasonal based Events], and attribute based
- Service Desk
  - Incident Management
  - Problem Management
  - Change Management
  - Service Request
  - Time Bound Management
  - Tasks

1.4 / Remediation and Automation

- Process Definition [Workflow Automation]
- Run Book Automation [PowerShell, Python and Shell]
  - Ad-hoc Execution
  - Schedule Scripts
  - Annotation based script execution [post diagnostic information to alerts]
- Remote Console Access [RDP, SSH, Telnet]
- Remote Session Recording
- Patch Management for Windows and Linux
- Network Configuration Backup [Running and Startup Configurations]

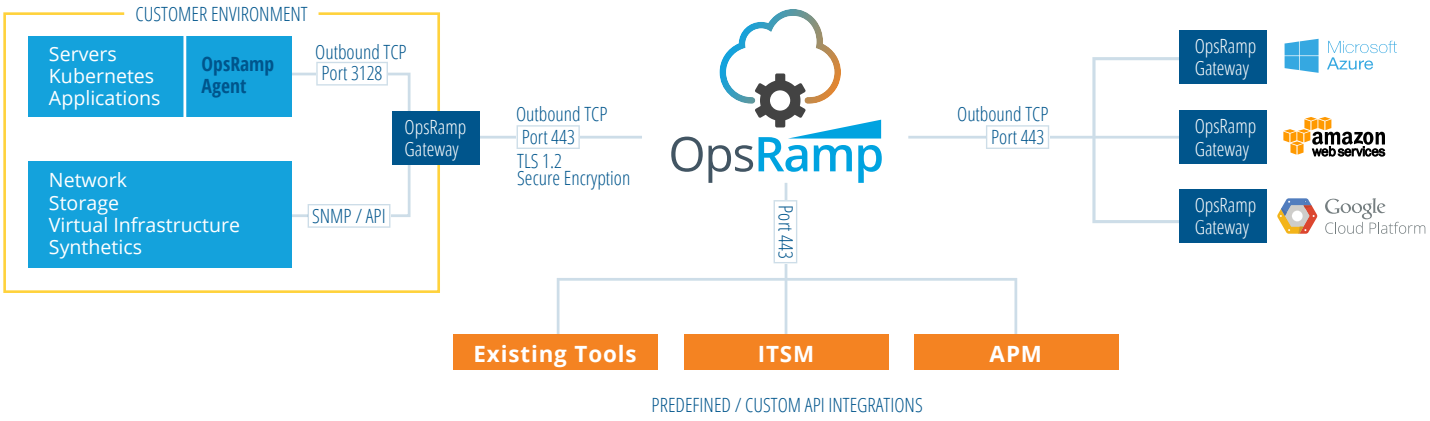
1.5 / Digital Operations Command Center

- Operations Reports – standard and custom reporting
- Integrations – OOB Plug-and-Play Adapters for 3rd Party ITOM & ITSM Solutions
- Open Integration Framework [Email, SNMP Trap, Webhook, and API]
- Extensive API
- Manager of Manager [MoM]
- Global Command Center [Dashboards]

2 / OpsRamp Hybrid Infrastructure and Monitoring

OS Monitoring (Windows & Linux) Application OEM Metrics	Event (Windows) Monitoring	SNMP Monitoring & Traps	Custom Monitoring (iSeries)
Log File Monitoring	Availability Monitoring	OpsRamp Agent and Gateway Heart-beat Monitoring	Agentless Monitoirng
Service / Process Monitoring	Disk Forecast Monitoring	Syslog Monitoring	Application Monitoring (DB, Web Servers, Middleware)
Network Monitoring	IaaS, PaaS, FaaS, CaaS Monitoring	Storage Monitoirng	Synthetics Monitoring
Sythetics Transaction Monitoring	Virtualization Monitoring	Hardware Monitoring	Netflow and UC Monitoring

The OpsRamp Discovery Engine finds IT assets across on-premise, private cloud, virtualized and public cloud, network, storage and synthetics based on IPs or IP Range. Then, the available devices can be added to OpsRamp.



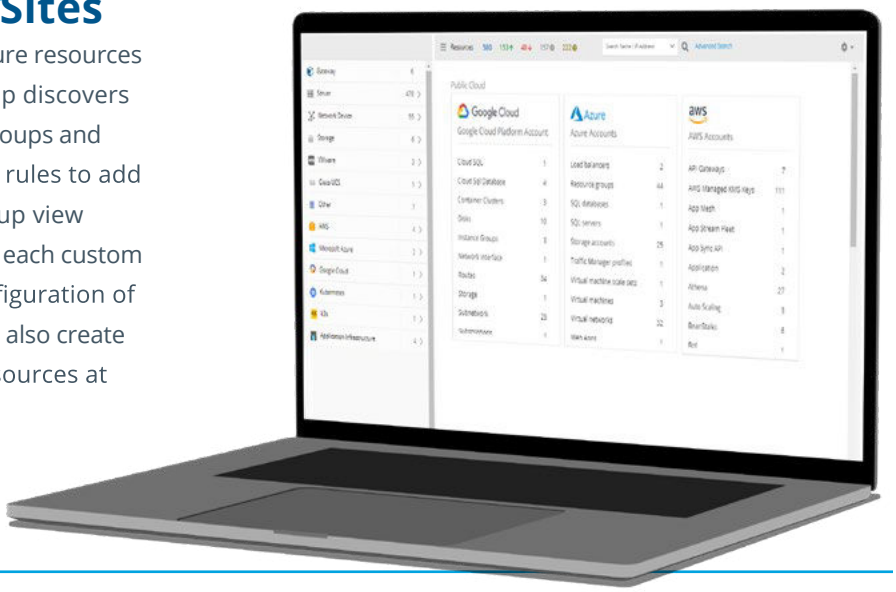
Policy-based discovery supports scheduling of discovery and the adding of new devices to a managed device list. Custom attributes can also be used to move the discovered devices to pre-defined groups automatically, based on Device Type, Business Services, Location, Customer, Datacenters, and Cloud provider.

- Discovery will collect the complete inventory of the discovered devices and the inventory data can be used to create dashboards and reports.
- An email notification can be sent to pre-configured users on new device discovery.
- For servers [Windows and Linux] the OpsRamp agent can be installed during the discovery through various channels including Automation Engines, Scripts and Deployment tools.

OpsRamp
a Hewlett Packard Enterprise company

2.1 / Resource Grouping / Sites

Custom groups help categorize hybrid infrastructure resources based on business requirements. Once OpsRamp discovers hybrid resources, IT teams can create custom groups and manually add resources to these groups or define rules to add resources to a custom group. The Resource Group view displays information on the resources available in each custom group. Creating custom groups enables the configuration of multiple resources simultaneously. IT teams can also create different custom groups and directly associate resources at any level.



2.2 / Service and Topology Maps

Service maps help IT teams model business-critical services and the underlying application and infrastructure stack supporting these enterprise services. Service maps help pinpoint proximate root cause for IT service degradation, deliver real-time visibility on the health of IT services, and identify the key performance indicators/health indicators for each part of the service.

Topology maps deliver dynamic network insights and real-time dependencies for enterprise application and infrastructure layers. IT teams can dynamically create a topology map of applications and network elements and their dependencies, and then use discovered topology to define service maps that model logical IT services.

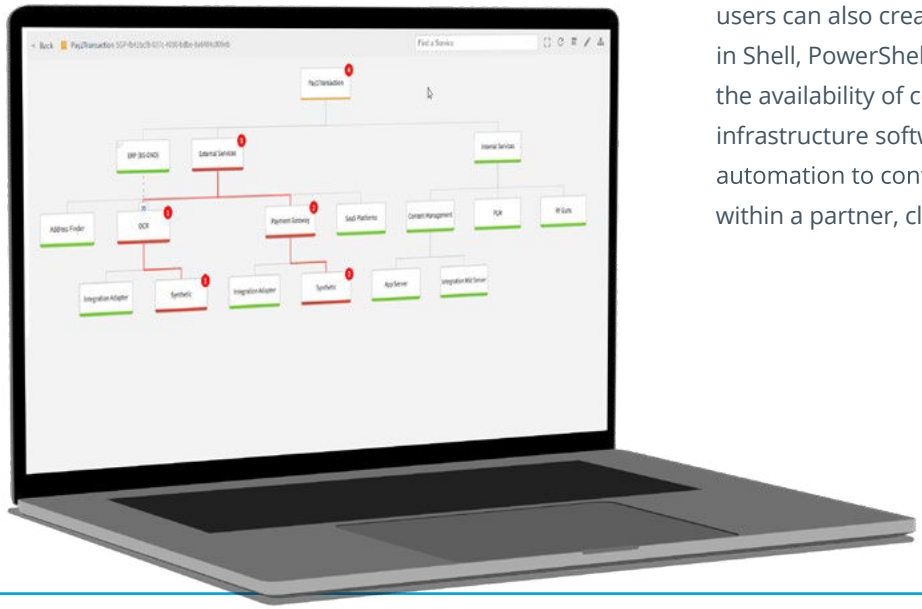
Service maps can easily handle IT services that span several applications and infrastructure resources across traditional on-prem, virtualized, cloud, and container environments. Service maps can monitor the health of an IT service (if all the resources are available in OpsRamp) even if third-party monitoring tools, original equipment manufacturers, or service providers manage some of the actual components of the service.

Resources can be dynamically assigned or reallocated to a given service using policies defined through filter criteria. The presence or absence of specific values associated with a resource name can automatically determine the inclusion or exclusion of a resource in a specific service map. Other options include identifying exact strings or identifying values using regular expressions.

OpsRamp
a Hewlett Packard Enterprise company

2.3 / Hybrid Infrastructure Monitoring

OpsRamp supplies hundreds of out-of-the-box monitoring policies across infrastructure solution, cloud providers, and application workloads. IT operations teams can customize monitoring policies to meet business needs or resource criticality requirements.



OpsRamp's hybrid infrastructure monitoring policies let enterprises manage mission-critical workloads with flexible polling frequencies (as low as one minute), warning and critical thresholds, alerts for threshold status violation, knowledge base article assignment to threshold violation condition, and pausing of resource polling in maintenance mode. OpsRamp users can also create custom monitors using scripts written in Shell, PowerShell, and Python. Custom monitors handle the availability of commercial software, custom apps, and infrastructure software. OpsRamp also delivers monitoring automation to configure policies for a specific set of resources within a partner, client, or line of business.

2.4 / Application Synthetic Transaction Monitoring

As part of hybrid infrastructure monitoring, application-level synthetic transaction monitoring is included as part of the solution. OpsRamp monitors HTTP(S) endpoints and other network end point which include – TCP, UDP, SSL, DNS, SMTP, FTP, with our wide spread of public synthetic pollers. The OpsRamp component "Gateway" can be provisioned as private poller for monitoring intranet-based URL's and synthetic transactions.

3 / Intelligent Event Management Powered by AIOps

The OpsRamp event management engine powered by AIOps consolidates both native and third-party events from legacy and next-generation workloads to extract the signal from the noise by reducing the overall volume of events and ensuring faster resolution by automatically routing incidents to right teams.

OpsRamp AIOps groups relevant alerts into incident tickets which are then routed to subject matter experts for rapid resolution. Digital operations teams will always be first to know about IT outages with automated event correlation, contextual awareness, and actionable insights. OpsRamp can also push alerts to popular ITSM tools like ServiceNow, BMC Remedy, Cherwell, Ivanti, and more.

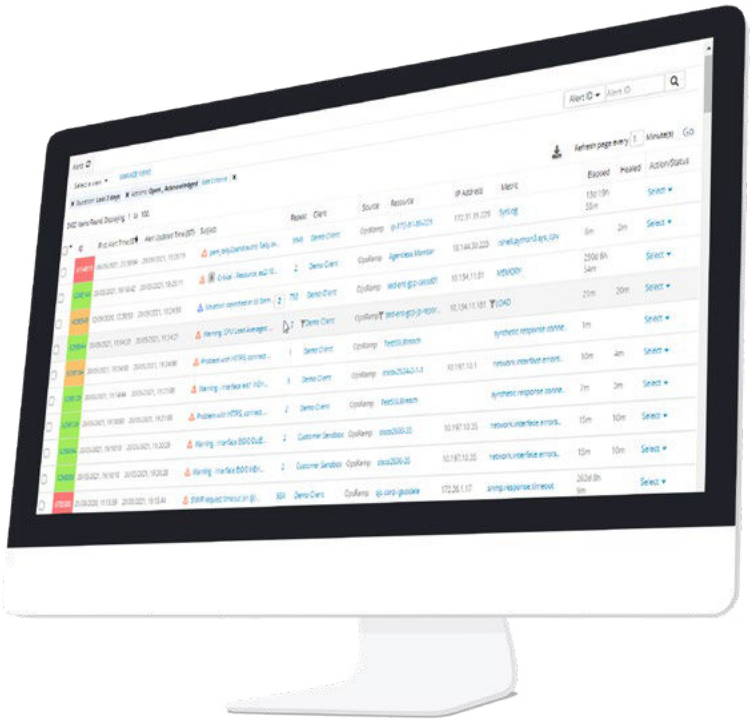
To build trust and confidence in analytical approaches for IT performance management, Observed Mode helps IT teams understand the potential for event volume reduction by simulating alert inferencing in shadow mode. Observed Mode lets IT pros preview the efficacy of AIOps alert inference models before they enable AIOps in production environments. Observed Mode lets IT teams not only examine algorithmic recommendations for alert correlation but also optimize the AIOps engine to suit operational needs.

Here's how OpsRamp can eliminate up to 95% of the human time spent on IT event management with AIOps:

- Gain Control: Identify and minimize service disruptions and IT outages for digital services across hybrid and multi-cloud infrastructure with machine learning techniques.
- Suppress Noise: Eliminate noise across endless event floods by compressing raw alerts into context-infused events.
- Prioritize Issues: Understand the business impact of an IT issue, using service maps for pinpointing interdependencies between IT services and underlying infrastructure.
- Faster Problem Resolution: Drive quicker mean-time-to-acknowledgement with smart notifications based on first-responder communication preferences.

3.1 / 3rd Party Alert Ingestions: APM and Log Management Solutions

The OpsRamp intelligent event management engine can receive events from third-party IT management tools, analyze and enrich these events using machine learning algorithms and dynamic topology, and send context-rich alerts and incidents. OpsRamp offers both ready-to-use and custom integrate using SNMP Trap, APIs, webhooks, and email to deliver an integrated notifications ecosystem that can include IT monitoring, IT service management, information security, and DevOps tools.



While OpsRamp can ingest, process, and analyze events from third-party tools, it can also automatically create new managed resources (if that resource does not already exist in OpsRamp) for alerts ingested from other monitoring tools. Automatic resource creation ensures rapid root cause(s) analysis for third-party resources with relevant context. Application owners can also tag external resources to service maps so that they can drill-down and troubleshoot the supporting hybrid infrastructure for the associated business-critical service.

3.2 / Inferences from AI/ML-based Event Correlation

OpsRamp AIOps drives higher productivity by helping enterprises manage a much larger volume of IT events without investing in additional staff or context switching between different tools. AIOps delivers proactive and predictive insights for operational optimization using three inference models to manage events across your hybrid IT stack:

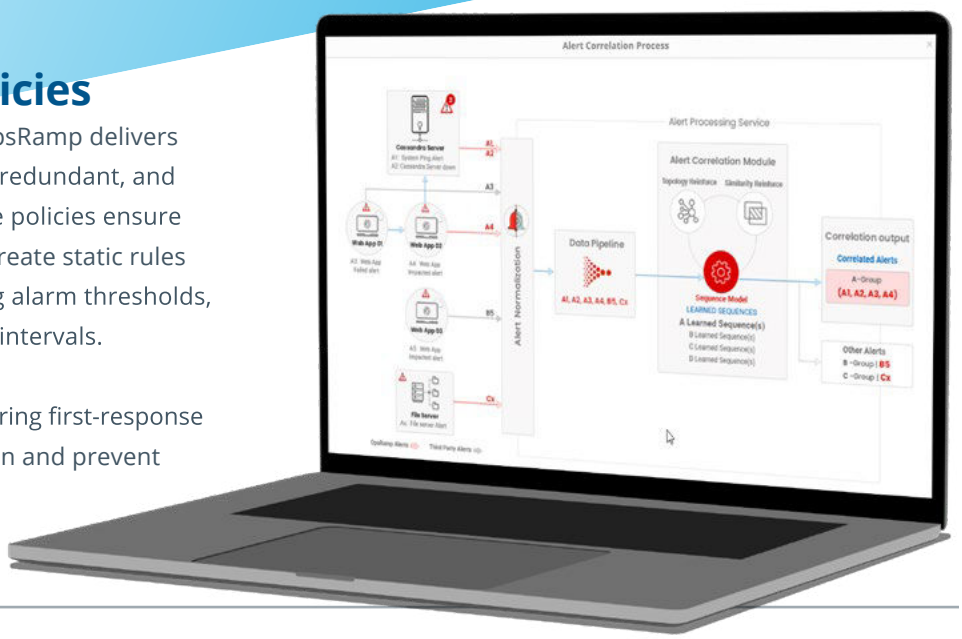
- Clustering-based Event Correlation: OpsRamp identifies and correlates alerts that share similar alert properties or event attributes such as subject, alert metric, alert source, host name, IP address and resource type. AIOps helps cut down on large volumes of false alerts and quickly act with the right alert prioritization.

- Co-Occurrence-based Event Correlation: Co-occurrence groups alerts based on the historical patterns of specific alert sequences. AIOps applies machine learning algorithms to learn existing alert sequences and reduce alert fatigue with pattern recognition and detection. Topology and any existing pattern model can be induced to achieve more accuracy while building machine learning models.

3.3 / First-Response Policies

Auto-alert suppression management in OpsRamp delivers first response actions to reduce seasonal, redundant, and noisy alerts. Learning-based first-response policies ensure that IT operations teams no longer must create static rules for a target set of resources by configuring alarm thresholds, defining filter criteria, and specifying time intervals.

OpsRamp provides two options for configuring first-response policies to ensure proactive event detection and prevent event overload:



3.3.1 / Time-Based Suppression

(Suppress seasonal and periodic alerts)

Machine learning policies understand overall event behavior and suppress IT events that happen seasonally during a specific interval of time. Seasonal alerts typically occur due to recurring IT operational processes like auto-scaling events from public cloud services or a high number of transactions during peak business hours.

3.3.2 / Attribute-Based Suppression

(Suppress alerts that match specific characteristics)

Battle-hardened IT teams have a holistic understanding of their production environments and can quickly judge whether an alert is critical or not during a time-sensitive incident. Digital operations teams can train OpsRamp's machine learning algorithms to detect these unique operational patterns by uploading CSV files that define required attributes that need to be suppressed. Learning-based auto-suppression recognizes alerts originating from operating procedures using matching criteria and ensures IT teams do not waste any time on redundant alerts.

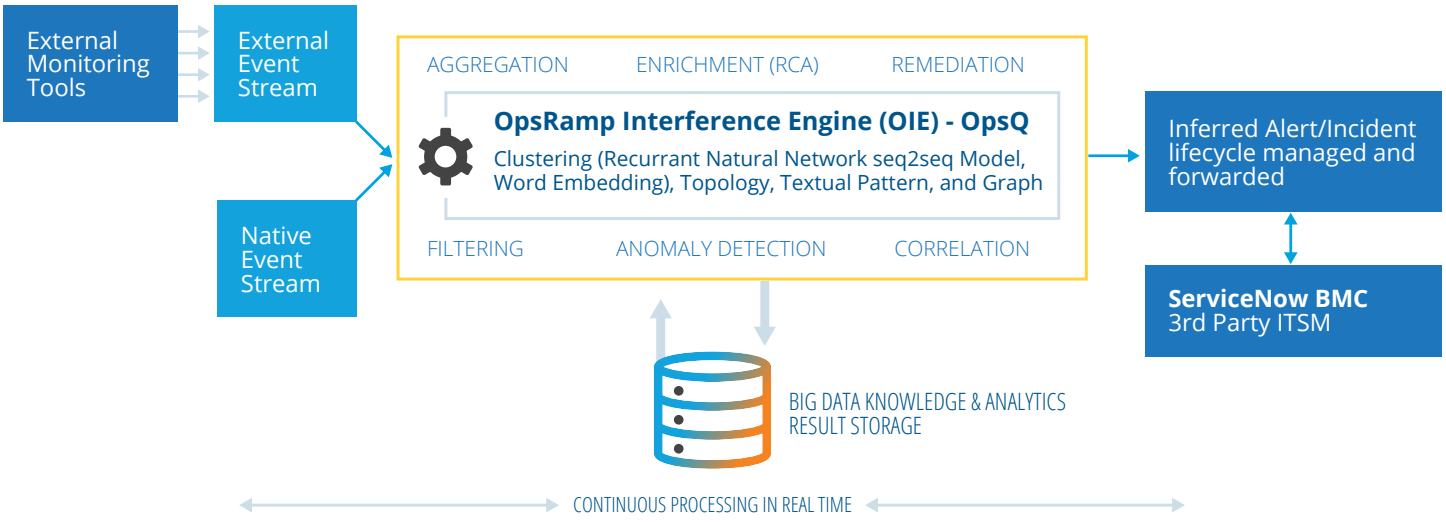
OpsRamp
a Hewlett Packard Enterprise company

3.4 / Alert Escalation Management

OpsRamp can escalate specific correlated and actionable alerts to notifications (email, SMS and voice) and auto-incident based on the requirement. Once an incident is created in OpsRamp, alert escalation policies deliver timely action on outstanding alerts by ensuring that critical alerts move up the chain of command using on-call schedules and escalation matrices. Alert escalation policies provide automated response actions for incoming alerts and help IT teams manage alerts to defined service levels. OpsRamp's alert escalation policies deliver context-rich incidents to on-call teams, automate incident routing, and integrate incident status with external ticketing tools so that they can:

- Be the First to Know with Alert Notifications Engine: During critical outages, application owners, IT infrastructure, and DevOps teams work together to quickly restore affected services. Using shift rosters, OpsRamp's alerts notification engine dispatches alerts to on-call staff with the right expertise to troubleshoot and repair impacted IT services.

- Reduce Mean-Time-To-Resolution with Auto-Incident Creation and Routing: With OpsRamp's auto-incident capabilities, IT teams no longer must manually create and route incidents anymore. OpsRamp's machine learning-powered escalation policies can proactively learn from existing incident data to assign incident priority based on business impact, urgency, category, sub-category, priority, and assignee groups.

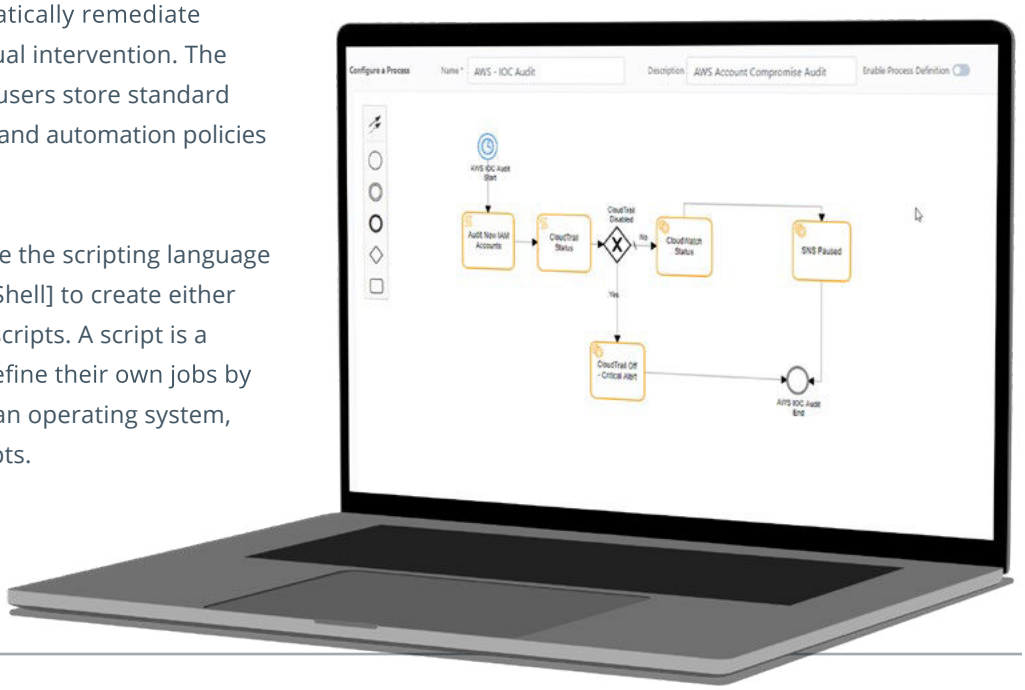


OpsRamp
a Hewlett Packard Enterprise company

4.1 / OpsRamp Process Definition

Process Definition is used to automatically remediate operational issues without any manual intervention. The process automation framework lets users store standard operating procedures, remediations, and automation policies in a single location.

Technology operations teams can use the scripting language of their choice [PowerShell, Python, Shell] to create either self-heal scripts or task automation scripts. A script is a user-defined job and IT teams can define their own jobs by writing code to be executed against an operating system, database, and other application scripts.



4.1.1 / On-Demand Runbook Automations

IT teams can identify a common set of operations on a single resource and then extend it to hundreds of resources in their datacenter or public cloud. Runbooks streamline service delivery and speed resolution times for digital operations management.

4.1.2 / Schedule-Driven Runbooks

Enterprises can automate routine maintenance tasks at predictable schedules for a resource or group of resources. TechOps teams can track the results of their process automation with a complete log of audit trails or receive an email with the result of the script.

4.1.3 / Event-Driven Runbook Automations

OpsRamp policies can respond to critical alerts with predefined remediation of problems as they occur. IT teams can address business requirements rapidly with the ability to trigger real-time workflows in response to events.

4.1.4 / Alert Enrichment

With OpsRamp Process Definition framework, native and 3rd party ingested events can be enriched to change severity, alter subject and descriptions

4.1.5 / Agentless Run Book Automation

OpsRamp can integrate with Ansible automation, to initiate playbooks based on event on servers, network, storage, cloud services (via API) and as well execute the scenarios in regular intervals.

4.2 / Patch Management

Enabling patch management in your organization can help you fix and avoid the chance of any vulnerabilities in the future. OpsRamp supports patch management for two types of environments: Windows and Linux. OpsRamp delivers protection from missed OS patches and handles vulnerabilities for a safe and available infrastructure through:

- Patch Visibility: OpsRamp makes it simple to manage all patching activities by running patch scans, configuring patches, creating whitelists, and offering global and site level visibility for users.
- Manageability: OpsRamp makes it easy to manage patch approvals and monitoring with custom jobs for both standard and third-party patches.
- Reports: Use OpsRamp reports outlining the patch metrics along with the ability to schedule the report in the preferred format for recurring/specific time & period.

4.3 / Remote Console Sessions

Remote console access helps subject matter experts access an impacted resource from OpsRamp UI via various channels: RDP, SSH and Telnet, and resolve issues in a secure manner. Actions taken on the target resource are recorded for audit trails, training, and change control.

Key Features:

- OpsRamp supports Secure Remote access to managed resources.
- Remote Desktop Protocol (RDP), Secure Shell (SSH) with Public Key and credentials, Telnet, File Transfer are Supported.
- Remote Access sessions are recorded and available in OpsRamp for playback

Benefits of Recorded sessions:

- Compliance and Audit
- Act as Training medium for frontline teams on troubleshoot and resolution by SME/Technical teams
- Document or build Knowledge Base

4.4 / Network Configuration Management

Network Configuration Management always maintains desired configurations by taking a backup of startup and running configuration for network resources. This makes it easier to recover from any resource failures or identify any configuration changes that happen on a resource. IT teams can also dynamically receive alerts whenever resource configuration changes.

5 / OpsRamp Core Features Overview

The OpsRamp platform enables organizations to manage their hybrid infrastructure from a unified portal with multiple features embedded into it for ease of users to authenticate, authorize, visualize dashboards and more based on their roles.

5.1 / Multi-Tenancy:

With our multi-tenancy architecture, organizations managing multiple clients or having multiple business units within an organization can practice / implement this feature to understand each tenant's (individual client or business unit) availability and performance across the hybrid infrastructure supporting their business needs.

5.2 / User Management:

OpsRamp provides an extensive user management module to provide access to the solution:

- Partner User: A user who can access the solution at parent level who has access to all tenant's infrastructure or few of them. Using our Roles Based Access Control module we can restrict the level of access to be provided to an individual or a group of users.
- Client User: A user who can access the solution at tenant level (a single client or a single business unit). Using our Role Based Access Control module we can restrict the level of access to be provided to an individual or a group of users.
- Business User: These users are preferably non-IT users who can use OpsRamp portal to raise concerns or request for services within the organization or through 3rd party organizations.

5.3 / Role Based Access Control:

Our RBAC model is the central nervous system of the solution through which all actions (view, create, edit, manage and administration) are controlled and applied to individual users or group of users. This enables your organization to audit and maintain compliance.

5.4 / Single Sign On:

Today organizations have multiple solutions / tools implemented and it becomes difficult to remember credentials across them all. With our single-sign-on feature based on SAML 2.0 technology, we make it easy. Here are our SSO plugins available, or we can integrate with any SAML 2,0 based SSO solutions.

5.4.1 / Multi Factor Authentication:

Security is an important aspect to view and access information. Two - factor authentication enables organization to secure the user login with an additional layer of security using following technologies:

- FIDO
- TOTP
- YubiKey
- Duo Security
- Authenticator

5.5 / Custom Branding:

It's easy to customize OpsRamp with a logo, favicon and a URL title.

5.6 / Rosters:

24*7 customer support maintains service-level agreements with the teams to troubleshoot and address business critical alerts and outages. OpsRamp Rosters enable organization to create their 24*7 rosters shift schedule within the platform, and notifies the correct people in right shift about the critical and outage scenarios.

5.7 / Batch Data Export:

Organizations can incorporate OpsRamp-generated data [Metrics, Alerts, Incidents, and Inventory data] into their BI tools. Snapshot and Incremental export of data for each tenant can be pushed to the customer owned Amazon AWS S3 bucket and Microsoft Azure Blob Storage in JSON format. Additionally, on-demand and recurring export schedules can be used to export data. Organizations can drive capacity management with our inbuilt dashboard and widgets, as well by publishing data to 3rd party BI system.

5.8 / Data Retention:

A summary of OpsRamp data retention follows below. For extended data retention, our "Batch Data export" feature can be utilized to stream data into customer's BI engine as explained in above section.

Data Type	Criteria	Retention
Resources	Inactive resources	90 days
Partners	Inactive partners	90 days
Clients	Inactive clients	90 days
Tickets	Closed tickets	12 months
Tickets	Open tickets	As long as the ticket is open.
Metrics	Metrics collected from managed environment.	12 months
Alerts	Suppressed and closed	90 days
Alerts	Open alerts	As long as the alert is open.
Graphs	Graphs with no data.	15 days
Reports	Recurring reports	Last 5 generated reports.
Reports	One-time reports	90 days
Jobs Scripts, and Patch activity	Jobs results	90 days
Jobs Scripts, and Patch activity	Custom script	90 days
Patches	Missing patches, once detected but not re-detected for 180 consecutive days or longer.	90 days
Secure Console Recordings	Rolling history of console recording for each resource.	90 days
Patches	Missing patches, once detected but not re-detected for 180 consecutive days or longer.	
Secure Console Recordings	Rolling history of console recording for each resource.	

5.9 / API Capability:

OpsRamp's extensive API capability, enables organizations to consume data from cloud, as well push configurations related to OpsRamp across the modules - "Hybrid Infrastructure Discovery and Monitoring", "Event and Incident Management", and "Automation and Remediation".

5.10 / Dashboards and Reporting:

OpsRamp provides interactive dashboards and operations reporting module in-built into the solution. Performance Dashboards allow several metrics to be grouped together in the dashboard so that those relevant for a specific application or component can be viewed quickly and easily, often without the need to consult a SME. Dashboards and Widgets are highly customizable from the OpsRamp UI.

Reports permit you to view status and summary information about enterprise resources and operations. You can configure a report to run on-demand or on a recurring schedule from a predefined template and as well create custom reports.

6 / OpsRamp SaaS Solution Security

Our architecture, cloud operations, access and authentication and deployment architecture guarantee the highest levels of security and protection.

- Platform Security: OpsRamp has broad security features for maintaining the privacy and security of customer data. We have designed the solution with security-first principles that integrate safety and reliability into day-to-day operations. We carry out quarterly due diligence audits for evaluating compliance with security policies through internal teams and third-party auditors.

- Identity Management: OpsRamp offers different options to manage user identity, including built-in user management, integrations with SAML and OAuth2 based authentication and third-party authentication services. The platform supports various SAML-based single sign-on solutions including Active Directory Federation Services, Okta, Centrify and One Login. You can also enable multi-factor authentication access to the OpsRamp platform with services like FIDO, TOTP, YubiKey, Duo Security and Google Authenticator.

- User Management: We grant user access to the OpsRamp solution using font-grained permissions built onrole-based access control (RBAC). Customers can create multiple roles and assign roles to users based on their responsibilities. RBAC lets you control the way your users' access, view and manage data.

- Vulnerability Assessments: Our SaaS Operations teams conduct quarterly security audits to identify vulnerabilities and threats that can compromise solution security. As part of each audit, we assess existing processes, assess security infrastructure, and build the right controls. Critical issues identified during audits are immediately fixed. High and medium severity issues which require code changes are prioritized for the next immediate solution release.

- Solution Health: OpsRamp publishes the health of the SaaS solution via our portal, and users can subscribe to updates. The updates include solution major upgrades and maintenance activity. The OpsRamp Gateway and Agent are monitored for heartbeat and alert when there are issues identified. Agents and Gateways has the capability to re-establish the connection to OpsRamp cloud on regular intervals to self-heal post issues are addressed.

7 / OpsRamp Compliance Standards

OpsRamp ensures continuous protection of customer data through compliance with leading industry standards and regulations. OpsRamp SaaS platform is hosted with public cloud – GCP, Azure, AWS and Colocation data centers – Equnix, Sungard and we adhere to their security standards.

- SOC 2 Type II. OpsRamp's data management and operational control practices are SOC 2 Type II certified. We have robust internal controls and rigorous processes in place to protect the confidentiality of customer data.

- GDPR. Our platform instances hosted in Europe (London and Amsterdam) are compliant with GDPR regulations. Protecting personal privacy and security in line with applicable data protection laws is a commitment we take seriously at OpsRamp.

- ISO 27001. Our platform operations have legal, physical and technical controls for implementing, maintaining and continually improving information security processes that are in accordance with ISO 27001 practices.

- SOC-2 Type I. OpsRamp's information security practices, procedures and operations meet the SOC 2 Type I standards for security, availability, and confidentiality.