OpsRamp

[Whitepaper]

The OpsRamp Platform: **Security and Compliance**

Table of Contents

Introduction

OpsRamp is a comprehensive SaaS platform for IT operations management. We help modern IT teams control the chaos of hybrid IT operations with a digital operations command center. With OpsRamp, enterprise IT and digital operations teams can deliver hybrid visibility and control, transform insights into action and replace routine operational tasks with intelligent automation. This paper reviews the security and compliance standards of the OpsRamp platform.

Overview

OpsRamp is committed to maintaining the availability, integrity and confidentiality of customer data. We've implemented robust processes and standards to secure customer data across all our platform operations, using:

- Data Security
- Product Security
- Platform Security

Data Security

OpsRamp follows strict practices for customer data that we manage and store in the platform. We only capture and keep data that's needed for IT operations management functions on devices/applications that we manage. We encrypt all sensitive data and each customer's data is accessible only to authorized users of that tenant.

Data Capture

OpsRamp only collects data that helps us manage our customer's IT environment, including:

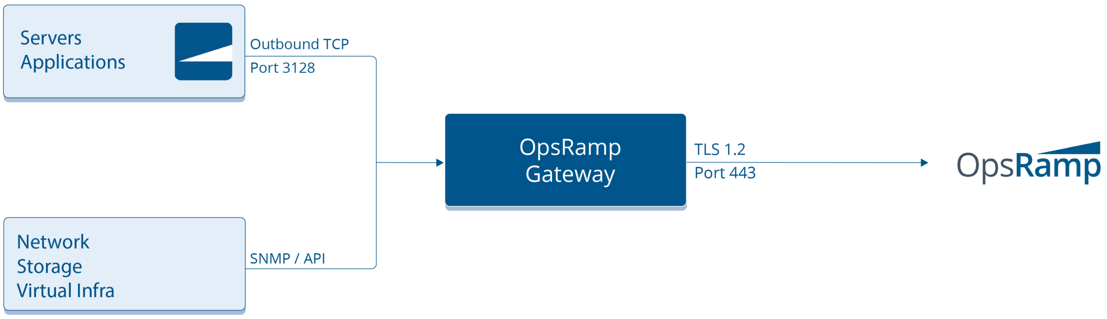
- **Performance Statistics.** We collect system-level information to monitor the availability and performance of managed devices.
- **Events and SNMP Traps.** We capture operating system events and SNMP traps to understand device health.
- **Device Metadata.** We fetch device configuration status for DNS names, models, operating systems and application configuration parameters.
- **Application Performance Statistics.** We track the performance of managed applications using relevant performance metrics.

Agent and Gateway Security

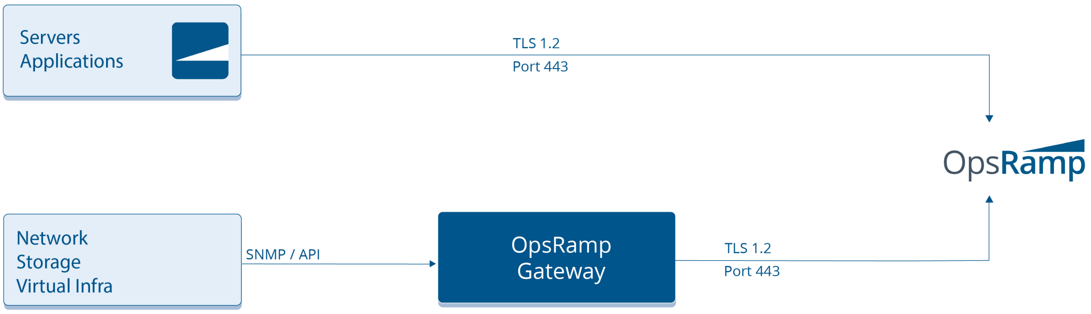
The OpsRamp Agent monitors and manages compute infrastructure across hybrid IT environments. The OpsRamp Gateway is a virtual appliance that monitors app services, network and storage infrastructure. The Gateway can also act as a proxy between an Agent and the OpsRamp cloud for secure communication.

Deployment Architectures

Option 1. Telemetry data for compute (servers and applications) and non-compute infrastructure (network, storage and virtual machines) is first sent to the OpsRamp Gateway.The Gateway then transmits this data to the OpsRamp cloud through secure channels.



Option 2. Telemetry data for compute infrastructure managed by Agents is directly sent to the OpsRamp cloud. Telemetry data for non-compute infrastructure is first sent to the OpsRamp Gateway, which in turn pushes it to the OpsRamp cloud.



Integrations

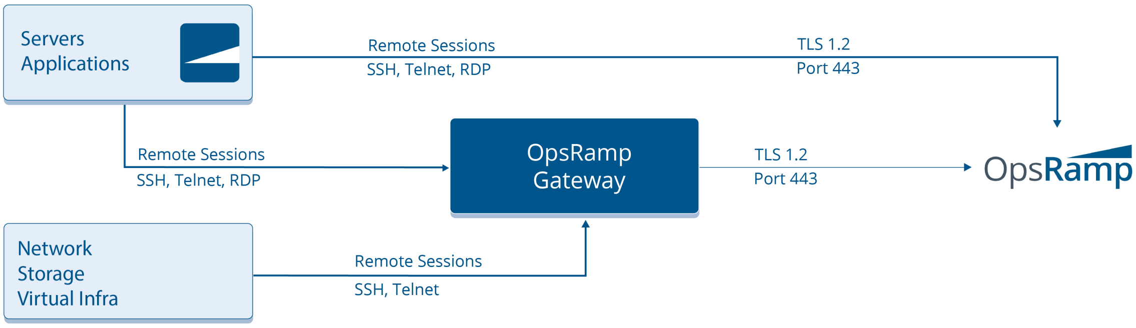
Our API framework lets you send alerts and tickets from your favorite IT monitoring and IT service management (ITSM) tools to OpsRamp. We support inbound and outbound connections across all integrations for true bi-directional communication:

Basic Authentication. OpsRamp supports basic authentication for outbound HTTP posts with user credentials.

OAuth/Webhook Authentication. OpsRamp supports OAuth 2.0/webhook authentication for inbound and outbound communications (data exchange) with third-party tools.

Remote Access and Control

Access distributed hybrid infrastructure in a secure manner with OpsRamp's remote consoles.Remote consoles let you securely log into hybrid infrastructure through a wide variety of protocols like Secure Shell (SSH), Remote Desktop Protocol (RDP), Telnet, Virtual Network Computing (VNC) and Remote Shell (RSH). OpsRamp records all actions carried out by an administrator on a device. You can use video playback recordings for audit trails, change and compliance management and training purposes.



Product Security

OpsRamp has broad security features for maintaining the privacy and security of customer data. We've designed the platform 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.

Audit Logs

We maintain logs of user activity and remote access across hybrid IT environments using the audit logs feature. Customers can generate ad-hoc or scheduled reports on user activity for identifying access-related risks.

Communication Security

OpsRamp uses Agents and Gateways to collect relevant metrics on the health and performance of hybrid IT infrastructure. The data collected by Agents and Gateways is then sent to the OpsRamp cloud for processing and delivering the right operational insights.

All communication to the OpsRamp cloud is Transport Layer Security (TLS) encrypted. We provide encryption for data in-flight and at-rest. TLS encryption ensures that all network communications are secure without any kind of eavesdropping and tampering.

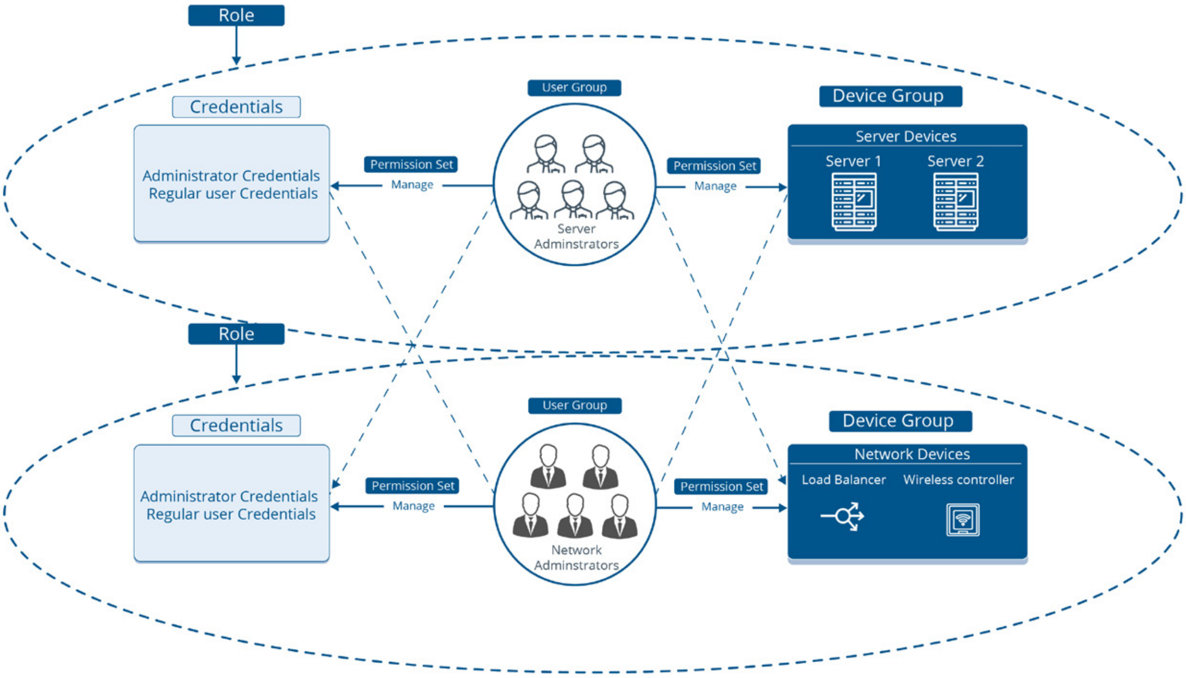
- All data transmitted (in-flight mode) between the OpsRamp Agent/Gateway and the OpsRamp cloud is encrypted using TLS 1.2.
- Any data-at-rest mode in the OpsRamp cloud is similarly encrypted using AES-256 for enhanced data protection.

Identity Management

OpsRamp offers different options to manage user identity, including built-in user management within OpsRamp, integrations with SAML and OAuth2 based authentication and third-party authentication services. OpsRamp 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 platform using fine-grained permissions built on role-based access controls (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. You can restrict the activities a user performs in OpsRamp based on roles, user groups, credentials, devices and device groups and permissions and permission sets.



Vulnerability Assessments

Our SaaS Operations teams conduct quarterly security audits to identify vulnerabilities and threats that can compromise platform 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 platform release.

Platform Security

OpsRamp leverages multiple layers of defense to provide a secure cloud platform to our customers. Our architecture, cloud operations, access and authentication and deployment architecture guarantee the highest levels of security and protection.

Platform Availability

We've built the OpsRamp platform for 99.90 % availability. The platform offers immediate and automatic failover when we lose connectivity to a primary datacenter. During an automatic failover, the platform routes traffic to the secondary datacenter using the BGP protocol for built-in disaster recovery, fault tolerance, redundancy for seamless operations.

Platform Architecture

The OpsRamp production environment is self-hosted across four different geographies so that we can better serve global customers. Each geographic instance is a Point of Delivery (PoD) with active/active architectures for better scalability and easier manageability.

Geography	Locations
North America	Ashburn, Sunnyvale and Rancho
Europe	London and Amsterdam
Japan	Tokyo
Canada	Canada Central - Toronto

* We don't replicate data across PoDs to comply with data sovereignty and protection norms for each geography.

Platform Certifications

OpsRamp ensures continuous protection of customer data through compliance with leading industry standards and regulations:

- 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.

The OpsRamp platform is hosted in Tier 1 datacenter providers (Equinix and Sungard) which hold the following certifications:

- ISO 27001. Our platform operations have legal, physical and technical controls formimplementing, maintaining and continually improving information security processes that are in accordance with ISO 27001 practices.
- SOC-1 Type I. OpsRamp's information security practices, procedures and operations meet the SOC 2 Type 1 standards for security, availability and confidentiality.

Conclusion

The OpsRamp platform is more than just a unified platform for managing enterprise hybrid IT environments. We've made strategic investments in people, policies, tools and infrastructure for the highest levels of platform security.

ABOUT OPSRAMP

OpsRamp enables IT to control the chaos of managing their hybrid IT operations and act as a service provider back to the business. Built in the cloud, the OpsRamp service-centric AIOps platform drives total visibility across hybrid infrastructures, offers complete multi-cloud infrastructure monitoring and management of business-critical services, and optimizes services through automation and integration with ITSM and DevOps tools.

TO LEARN MORE
OpsRamp.com // 1.855.847.8272