NetEnrich Security Document

Secure Remote Infrastructure Management

Document History				
Version	**Date**	**Version Description**	**Action Taken**	**Remarks**
V1.0	Oct 02, 2016	First Version of the Policy	First Draft	Full Release
V2.0	Jan 30, 2017	Access Security controls updated		
V3.0	Mar 15, 2018	Access Security controls updated		
V4.0	Oct 10, 2019	Access Security controls updated		
V5.0	Feb 19, 2019	Section 5.2.7 and 5.2.9 updated	Updated minimum password characters & two more network measures added	Full Release
V5.1	May 28, 2020	Section 4.0 updated	LogMein tool usage details updated	Full Release

Disclaimer
This documentation might include technical or process inaccuracies or typographical errors and is subject to correction and other revision without notice. NetEnrich, Inc. GIVES YOU THE CUSTOMER THIS DOCUMENTATION "AS IS." EXPRESS OR IMPLIED WARRANTIES OF ANY KIND ARE NOT PROVIDED, INCLUDING BUT NOT LIMITED TO THE IMPLIED WARRANTIES OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE. Some states or jurisdictions do not allow disclaimer of express or implied warranties in certain transactions; therefore, this statement may not apply to you.

Table of Contents

1. Introduction

As a business partner to clients, NetEnrich works with IT teams to provide critical services for IT operations and IT infrastructure management. NetEnrich complements in-house or partner IT teams to provide services. We combine industrialized elastic services with an automation platform and analytics to deliver a new world approach to IT operations. We mitigate risks with IT operations, drive innovation, and enable IT teams to become a service provider to the business. We also enable IT teams to unlock the potential of new world technologies such as cloud, virtualization, and mobility.

NetEnrich has enabled IT teams in enterprises to become a service provider to their business while achieving significant cost savings in IT operations, apart from delivering numerous other benefits to our clients. They run IT better with greater control and peace of mind as they are first-to-know about key outages. Our clients grow their business with confidence as we free their skilled resources from doing routine fire-fighting or performing L1 and L2 tasks, to focus on strategic initiatives for the business. We enable their IT to offer SLAs, service catalogs, chargebacks, business value dashboards, and business process mapping.

All this is made possible by our NetEnrich Enterprise Command Center and Intelligent Business Operations framework that together drive fundamental improvement in IT operations.

NetEnrich takes network security, data integrity and the maintainance of rigid process standards very seriously to ensure that business users receive the most secure experience from their IT infrastructure services. This is why NetEnrich has invested in International Organization for Standardization (ISO) certification and institutionalized Information Technology Infrastructure Library (ITIL) standardized processes to measure, review and continually improve the internal security, operating policies and procedures performed on behalf of our clients.

This document provides the internal security framework, certifications, policies and procedures adopted by NetEnrich.

2. Company Profile

NetEnrich partners with CSPs, MSPs, VARs, large SPs, ISVs, and distributors across the globe to provide remote, industrialized IT Operations Services for IT infrastructure. NetEnrich is a strategic partner with Microsoft on Azure, and has a comprehensive range of packaged solutions for cloud -- Azure, AWS, Google Cloud, and Openstack. NetEnrich enables CSPs to rapidly scale their business and increase recurring revenues. Its industrialized and remote IT operations services for cloud, DC, and cyber-security, are powered by automation and an advanced, next-gen platform, to monitor and manage IT infrastructure and operations across on-premise to cloud. NetEnrich is headquartered in the Silicon Valley, California, USA and has over 10+ distributors, 100+ partners, more than 1,000 end-clients, and six offices across the world. It has over 500+ employees with competency in various advanced technologies and processes. For more details, visit (**www.netenrich.com)**.

2.1. Locations

Corporate Headquarters:

Company	NetEnrich Inc.
Address	2590 N. First Street, Suite 300 San Jose
State, Country & Code	California, 95131 USA.

	SAN JOSE	DALLAS	HYDERABAD	BHIMAVARAM
FUNCTIONS	• Customer Management • Consulting & Professional Service • Temporary service backup function • Architects & Management • Onshore Support (On demand)	• Customer Management • Consulting • Onshore Support (On demand)	• Customer Management • Incident & Problem Management • Diverse Technology Support • Strong CoE Competencies	• Event Management • SOP-driven Services • 24X7 Operations • Automation

3. About NetEnrich

NetEnrich comes with a strong background in infrastructure managed services experience bundled with automation as a key driver for delivering these services. We bring ITOM (IT Operations Management) tools from OpsRamp (a NetEnrich technology partner) to make the implementation and manageability of our services easy and faster for our partners and end-clients. OpsRamp along with NetEnrich's automation capabilities, play a major role in minimizing the time to market of our services.

NetEnrich partners with OpsRamp to complement their industry leading Enterprise Command Center orchestration platform that includes IT operations lifecycle management capabilities for hybrid cloud environments.

4. Tools used

NetEnrich will use the following tools to deliver various technology services and techniques to protect the security of systems, networks, and data:

- **OpsRamp** for IT Operations management
- **LogMeIn** for remote help and support (remote access) into client devices.
- **QualysGuard** to run security assessments
- **Prognosis** for managing unified communication devices.

4.1. OpsRamp

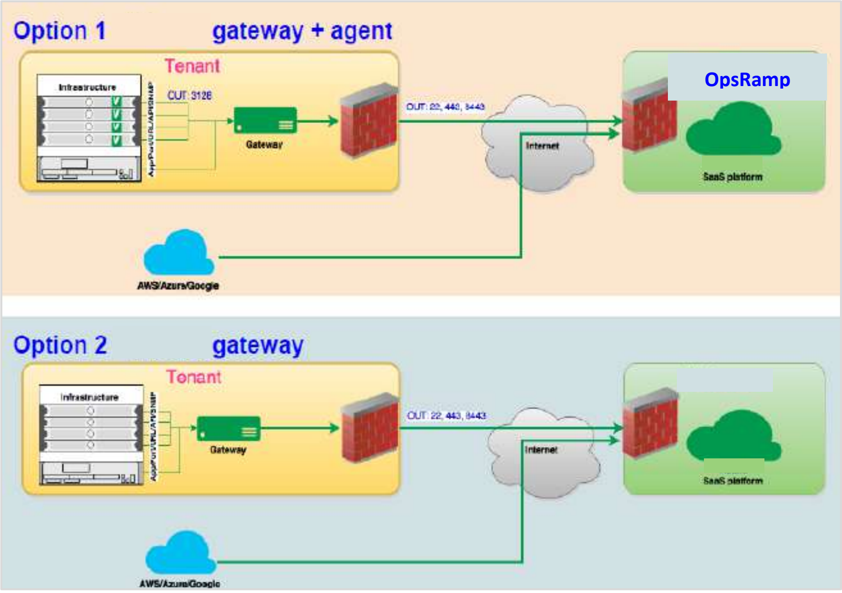
OpsRampIT, Inc. is a privately held company with headquarters in San Jose, CA and has operations across the US, Japan & India. OpsRamp serves both traditional Service Providers and Enterprise IT organizations who want to transform into service providers for their business.

4.1.1. OpsRamp Gateway Architecture

The OpsRamp Gateway (OR) has a web-based administrative user interface and management system for basic configuration. The services gateway has limited interfaces exposed within the client environments, so that OR is not accessible by unauthorized users. Only NetEnrich professionals can access via OR’s proprietary interfaces to system configurations. Simple plug-and-play and network configuration interfaces are prebuilt into OR to help deployment of OR. The OR firmware, is subjected to our standard scans for detecting any open channels and vulnerabilities before being released. New firmware and security updates are pushed out to all the gateways on a regular basis.

- Hardened Linux Appliance runs in the customer application environment
- Connects to the OpsRamp Cloud using SSH2, Transport Layer Security (TLS) protocols
- OpsRamp Gateway needs be configured to connect to OpsRamp Cloud (Primary DC, Secondary DC) using firewall rules
- Tunnel to OpsRamp Cloud is always initiated by gateway (it cannot be initiated from OpsRamp Cloud)
- Collects performance data from source systems/applications (Port/App/API/SNMP/URL Monitoring and so on) over the internal network
- OpsRamp Gateway sits in the customer’s private environment and doesn't need a public IP address
- Acts as a proxy for agents to connect to OpsRamp Cloud.

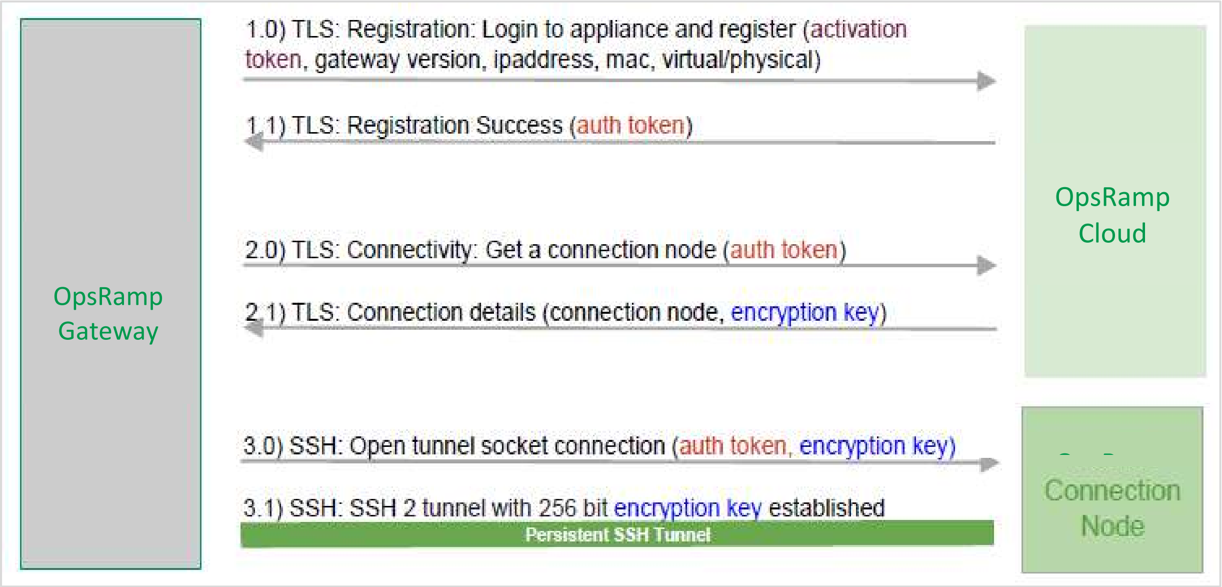
Requires outbound ports from gateway	22, 443 and 8443
Requires inbound ports to gateway	None



OpsRamp

4.1.2. Gateway Handshake

- Install OpsRamp gateway appliance in the customer's private network
- Generate a unique single use activation token (uuid) for the customer in OpsRamp Cloud
- Register the gateway using the activation token generated by OpsRamp Cloud
- The gateway fetches connection details, encryption key (on every connect) and establishes persistent SSH tunnel with the OpsRamp connection node (this step is repeated on tunnel disconnect).


OpsRamp Gateway
1.0) TLS: Registration: Login to appliance and register (activation token, gateway version, ipaddress, mac, virtual/physical)
1.1) TLS: Registration Success (auth token)
2.0) TLS: Connectivity: Get a connection node (auth token)
2.1) TLS: Connection details (connection node, encryption key)
3.0) SSH: Open tunnel socket connection (auth token, encryption key)
3.1) SSH: SSH 2 tunnel with 256 bit encryption key established
Persistent SSH Tunnel
OpsRamp Cloud
Connection Node

OpsRamp Agent

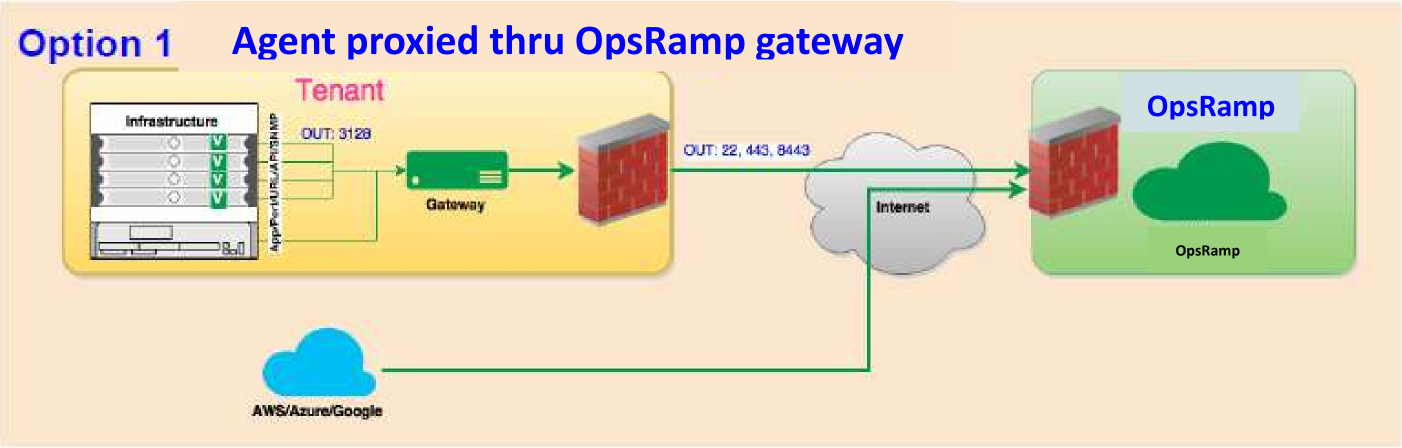
- An Agent is an executable application that runs on managed Windows and Linux devices
- An Agent manages devices such as servers, desktop and laptops
- OpsRamp agent runs on the linux/windows servers for monitoring and managing the applications running in the server
- Collects hardware information, operating system information and performance data from deployed servers
- Can be configured to directly connect to OpsRamp Cloud OR proxied thru gateway
- Communication between agent and OpsRamp Cloud is secured with oauth2 keys.

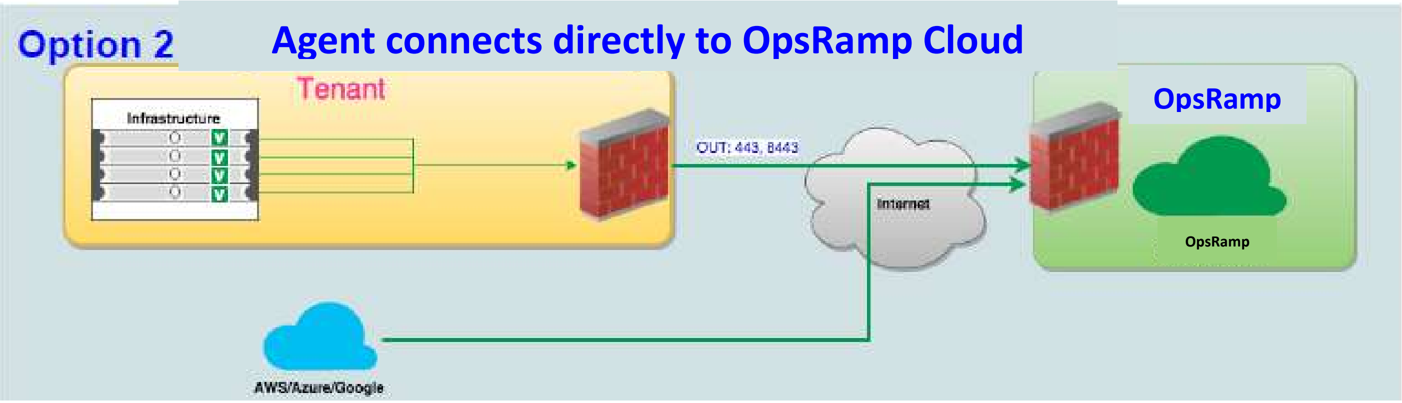
Requires outbound ports from server to OpsRamp cloud (Direct connect)	443 and 8443
Requires outbound ports from server to gateway - internal (Proxied thru gateway)	3128
Requires inbound ports to server	None

4.1.3. OpsRamp Agent Prerequisites

- Linux agent requires "sudo" permissions

- Windows agent requires “administrator” permissions.





OpsRamp Master Agent

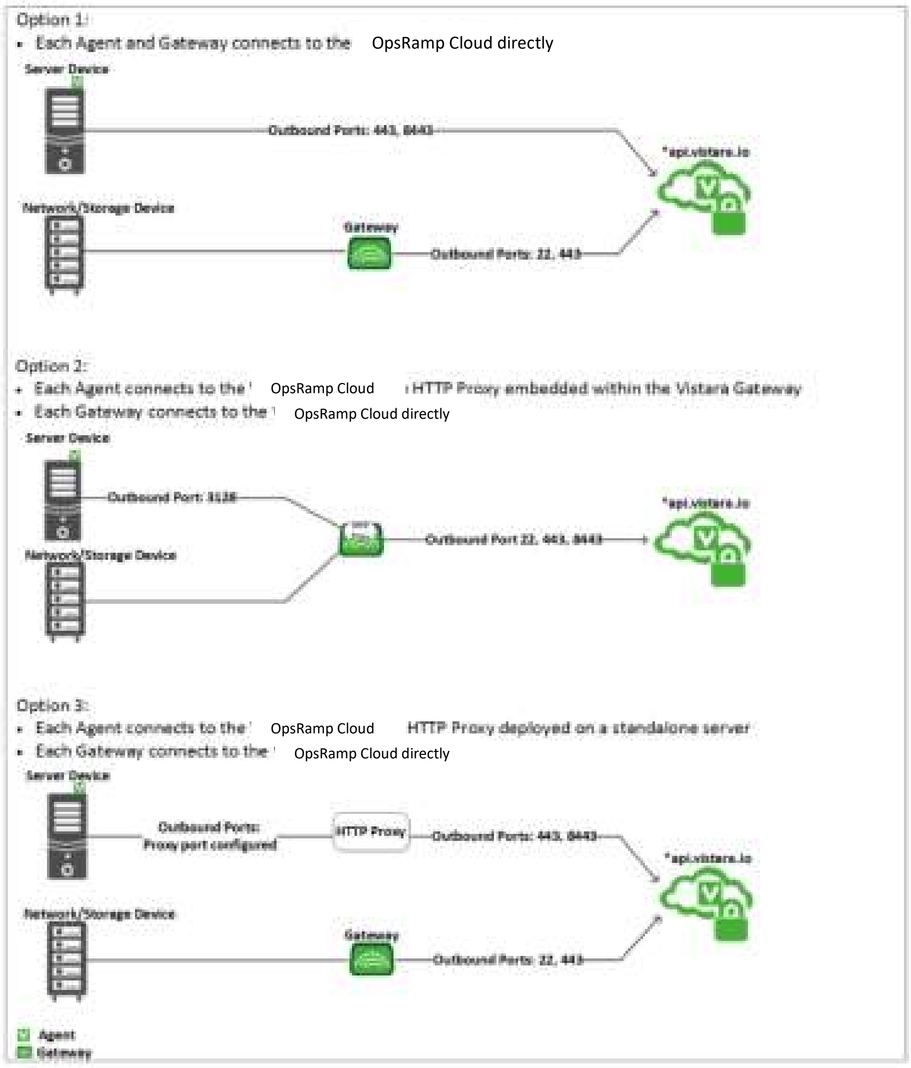
- A master Agent supports additional monitoring. It functions as a Simple Network Management Protocol (SNMP) trap listener within the environment, and also performs scheduled Ping, URL, and Domain Name System (DNS) monitoring
- Any existing Agent can be configured as Master Agent
- A client can have multiple master Agents within the network

OpsRamp Gateway

A Gateway is a virtual machine that manages devices such as:

- Servers
- Switches
- Routers
- Firewalls
- Storage
- Virtual Environment.

Agent and Connectivity options



Option 1:

- Each Agent and Gateway connects to the OpsRamp Cloud directly

Option 2:

- Each Agent connects to the ' OpsRamp Cloud ı HTTP Proxy embedded within the Vistara Gateway
- Each Gateway connects to the ' OpsRamp Cloud directly

Option 3:

- Each Agent connects to the ' OpsRamp Cloud HTTP Proxy deployed on a standalone server
- Each Gateway connects to the ' OpsRamp Cloud directly

Agent and Gateway connectivity to OpsRamp

When to deploy Agent and Gateway

Scenario	Required deployment
Manage servers only	• Agent is required on each managed server. • There are three options to configure Agents to connect the OpsRamp Cloud. See Agent and Gateway connectivity options.
Manage network and storage devices	• Gateways are required to manage network and storage devices. • Each Gateway must connect directly to the OpsRamp Cloud. See Agent and Gateway connectivity options.
Manage servers, network and storage devices	• Agent and Gateway are both required. • There are three options to configure Agents and Gateways to connect to the OpsRamp Cloud. See Agent and Gateway connectivity options.

4.1.4. Gateway Security

- Gateway password stored with SHA-512
- encryption in/etc/password with a 16 character salt
- Single mode login is disabled (To prevent unauthorized access or prevent users entering single user mode)
- Allows only 2 new sessions for every 60 seconds
- After 5 wrong passwords, account gets locked for 3 minutes
- Inbound firewall rules on gateway (TCP)
  - 21 (ftp for UCM manager)
  - 22 (ssh)
  - 3128 (proxy port for agent connectivity)
  - 5480 (admin portal)
- Inbound firewall rules on gateway (UDP)
  - 67 (dhcp based gateway ip address)
  - 69 (tftp for UCM manager)
  - 161 (snmp)
  - 162 (snmp trap)
  - 514 (remote syslog)
- Can be configured to connect to only OpsRamp Cloud (Primary DC, Secondary DC) using the firewall.

4.2. LogMeIn

LogMeIn remote access products use a proprietary remote desktop protocol that is transmitted via Secure Sockets Layer (SSL). An SSL certificate is created for each remote desktop and is used to cryptographically secure communications between the remote desktop and the accessing computer.

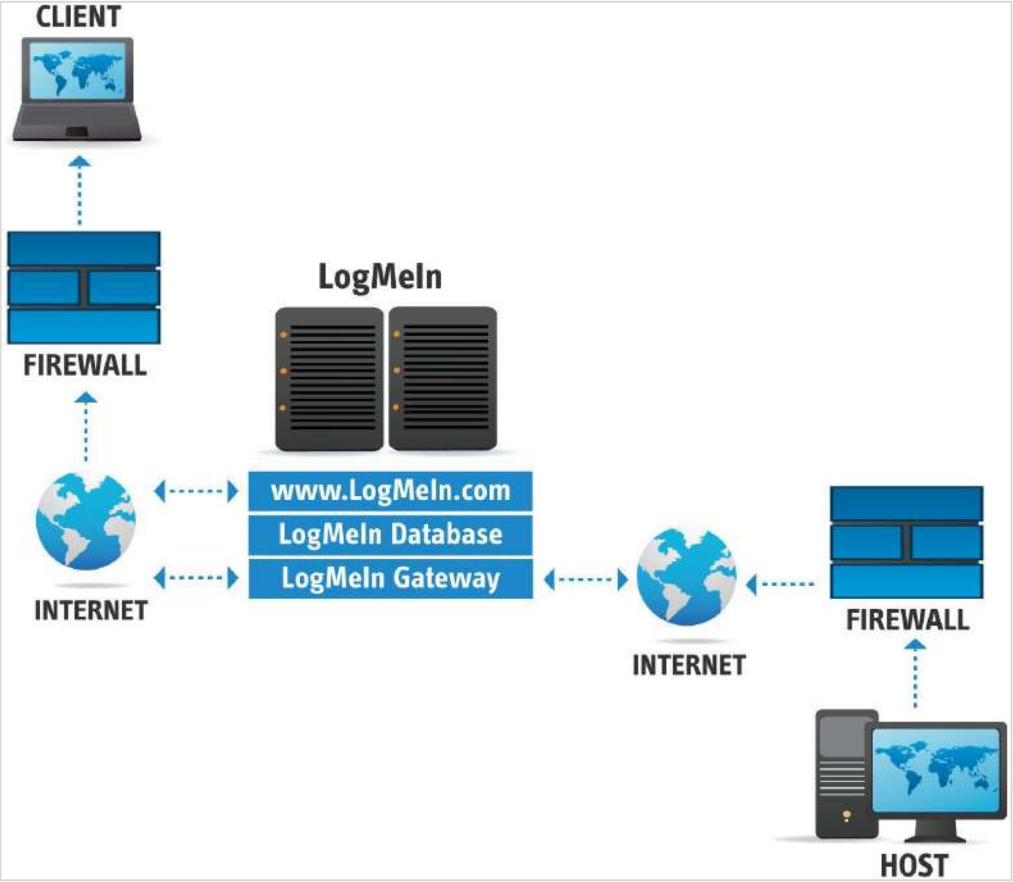
Users access remote desktops using either the LogMeIn Ignition stand-alone application or a web portal. The web portal requires either an ActiveX plugin for Internet Explorer, or an extension for Firefox (the LogMeIn plug-in for Firefox), or an extension for Safari (the LogMeIn plug-in for Safari), or a plugin for Google Chrome. Failing that it falls back to requiring Java in order to run a Java program, and failing that it falls back to "a screen-shot-based HTML remote control". The web portal also provides status information for the remote computers and, optionally, remote computer management functions.

The service connects the remote desktop and the local computer using SSL over Transmission Control Protocol (TCP) or UDP (User Datagram Protocol) and utilizes Network Address Translator (NAT) traversal techniques to achieve peer-to-peer connectivity when available.

4.2.1. LogMeIn Architecture

Before explaining the exact security mechanisms employed by LogMeIn, it is necessary to give a quick introduction to the solution architecture.

There are three key components to any remote access session. The roles of the client and the host should be straightforward – the third component is the LogMeIn gateway.



The LogMeIn host in the above figure maintains a constant SSL-secured connection with one of the LogMeIn gateway servers in one of our physically secure datacenters. This link is initiated by the host and firewalls treat it as an outgoing connection, like secure web browsing traffic.

The client browser establishes a connection to LogMeIn and authenticates itself. Based on the client's identity, it is authorized to exchange data with one or more hosts (the hosts belonging to the user's account).The gateway then forwards the subsequent encrypted traffic between the client and the host. It is worth noting that the client will also need to authenticate itself to the host – the gateway mediates the traffic between the two entities, but it does not require that the host implicitly trust the client. Once the host has verified the client's identity and authorized the client to access the computer the actual remote access session begins.

The benefit of using the gateway, instead of establishing a direct link between the client and the host, is that either the client or host (or both) can be firewalled. The LogMeIn gateway ensures that users do not need to configure firewalls.

4.2.2. LogMeIn Security Mechanisms

When users think of Internet data security, they are usually concerned about data encryption – to the point where security is measured in the length of the encryption key used. However, encryption and decryption, while being very important, are fairly trivial tasks compared to the other challenges faced by designers of secure systems. As you will see, data encryption is just one of the main goals set forth by the designers of LogMeIn.

4.2.3. Authentication of the Gateway to the Client

First and foremost, when a user connects to a LogMeIn installation via a gateway – the “server” – they need to be 100% positive that the computer they are about to exchange data with is really the one to which they intended to connect.

Suppose that an attacker poses as the server towards the user, and it poses as the user towards the server. The attacker, in this case, can sit between the two parties while reading, or possibly modifying, the data in transit. This is known as a “Man in the Middle”, or MITM attack and is especially hard to protect against.

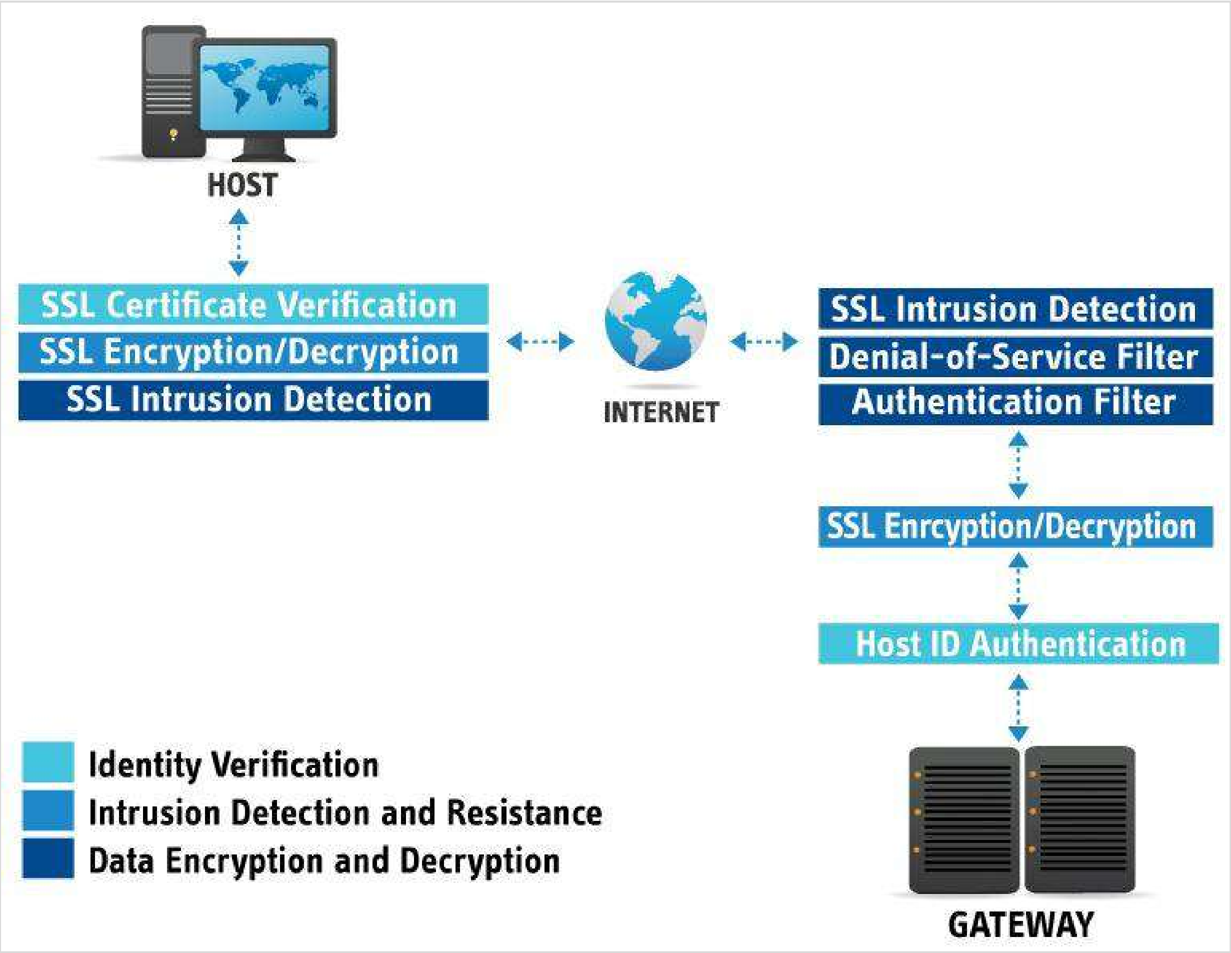
LogMeIn utilizes SSL/TLS certificates to verify server identities and thus protect against MITM attacks. When a connection is made, the server’s certificate is verified. If the certificate was not issued by a certifying authority the user has chosen to trust, a warning will be presented. If the certificate was issued by a trusted certifying authority, but the hostname in the URL does not match the hostname included in the certificate, a different warning will be presented.

If the server passes these verifications, then the user’s browser generates a “Pre-Master Secret” or PMS, encrypts it with the server’s public key contained within its certificate, and sends it to the server. As ensured by the use of public key cryptography, only the server that holds the corresponding private key can decrypt the PMS. The PMS is then used to derive the Master Secret by both the user and the server, which, in turn, will be used to derive initialization vectors and session keys for the duration of the secure session.

In short, the above process ensures that the user is establishing the connection with the server, and not with a third entity. Should an MITM attack be attempted, either one of the security warnings will be triggered or the PMS will be unknown to the MITM, effectively rendering the attack impossible.

4.2.4. Authentication of the Host to the Gateway

The gateway verifies the host’s identity when it accepts an incoming connection using a long unique identifier string. This string is a shared secret between the two entities and is issued by the gateway when the host is installed. This unique identifier is only communicated over an SSL-secured channel, and only after the host has verified the gateway’s identity. The below figure illustrates how the host and the gateway authenticate each other before a host is made accessible to the client.



4.2.5. LogMeIn Data Encryption

The SSL/TLS standard defines a wide choice of cipher suites such as RC4 and 3DES, and some implementations offer more advanced suites that include AES as well. RC4 operates on 128 bit keys, 3DES uses 168 bit keys. AES can utilize 128 or 256 bit keys. The client and the host agree on the strongest cipher possible. This is done by the client sending the host a list of ciphers it is willing to use, and the host choosing the one it prefers from this list.

The SSL/TLS standard does not define how the host should choose the final cipher. In LogMeIn, the host simply selects the strongest available cipher suite that the client has offered.

This method allows both the client and the host to decline the use of specific data encryption algorithms without the need of updating both components, should an algorithm be deemed as broken or insecure by research.

4.2.6. LogMeIn Intrusion Detection

LogMeIn provides two layers to detect intrusion attempts: SSL/TLS and LogMeIn Intrusion Filters.

SSL/TLS

The first layer of intrusion detection is provided by SSL/TLS to ensure that the data has not changed in transit. This is achieved by the following techniques:

- **Record Sequence Numbering**: Record Sequence Numbering means that SSL/TLS records are numbered by the sender and the order is checked by the receiver. This ensures that an attacker cannot remove or insert arbitrary records into the data stream.
- **Message Authentication Codes**: Message Authentication Codes (MACs) are appended to every SSL/TLS record. This is derived from the session key (known only to the two communicating parties) and the data contained within the record. If MAC verification fails it is assumed that the data was modified in transit.
- **Cipher Block Chaining**: The cipher suites preferred by LogMeIn also utilize Cipher Block Chaining (CBC mode); meaning that every SSL/TLS record will depend on the contents of the previous record. In this mode, the input to the cipher is not only the current plaintext record, but the previous one as well. This again ensures that packets cannot be inserted or removed from the data stream.

LogMeIn Intrusion Filters

The second layer is provided by LogMeIn itself, and comprises of three intrusion filters.

IP Address Filter

When LogMeIn receives a connection request from a client, it first checks its list of trusted and untrusted IP addresses and possibly denies the connection. An administrator can set up a list of IP addresses within LogMeIn that are either allowed or denied to establish a connection to the selected host (for example, designate the internal network and another administrator’s home IP address as allowed).

Denial of Service Filter

A Denial of Service Filter rejects connections if the IP address request it is coming from has made an excessive number of requests without authentication within the observation time window. This is done to protect against someone overloading the host computer by, for example, automatically and very quickly requesting the login page over and over again.

Authentication Filter

If the user made an excessive number of failed login attempts, the Authentication Filter rejects the connection. The Authentication Filter is in place to prevent a potential intruder from guessing an account name and password.

How to set filters on a LogMeIn host

1. Access the host preferences from either the host or the client:

   a. If you are at the host, open LogMeIn and follow this path:

   Options > Preferences > Security

b. If you are at the client, connect to the host Main Menu and follow this path:

Preferences > Security

2. Under **Intrusion Control**, click **Edit Profiles** to begin creating a filter profile.

4.2.7. Data Forwarding

The gateway provides end-to-end encryption by forwarding encrypted data between the host and the client. If you are familiar with how SSL works, this might sound impossible; after all, the assumption is that since the client is confident that it is communicating with the gateway it is only the gateway that can decrypt the data sent by the client. This is a valid point, but LogMeIn made a few important changes to how SSL sessions are handled between the host and the gateway.

The first part of the SSL negotiation is performed between the gateway and the client. The gateway then passes the exchange on to the host, which re-negotiates the SSL session and agrees on a new session key with the client, thereby providing true end-to-end encryption.

When the traffic is relayed through the gateway, the client (browser) establishes an SSL session with the gateway using the gateway's certificate. The gateway transfers this SSL session's state (including the pre-master secret) to the host. After agreeing on a new session key, the host uses this session state to handle the rest of the SSL session directly with the client. As far as the client is concerned, the session is secured using the gateway's SSL certificate, but it is actually talking directly with the host, without the need for the gateway to decrypt and re-encrypt traffic.

A MITM attack is rendered impossible since both the host and the client verify the gateway’s certificate and the client uses its RSA public key to encrypt information that is used to derive the SSL/TLS Pre-Master Secret.

4.3. QualysGuard

Qualys, Inc. is a provider of cloud security, compliance and related services for small and medium-sized businesses and large corporations based in Redwood Shores, California.

Founded in 1999, Qualys was the first company to deliver vulnerability management solutions as applications through the web using a "software as a service" (SaaS) model, and as of 2013 Gartner Group for the fifth time gave Qualys a "Strong Positive" rating for these services. It has added cloud-based compliance and web application security offerings.

4.3.1. QualysGuard

Network requirements/configuration

Bandwidth	Minimum recommended bandwidth connection of 1.5 megabits per second (Mbps) to the Qualys Cloud Platform.
Outbound HTTPS Access	The local network must be configured to allow outbound HTTPS (port 443) access to the Internet, so that the Scanner Appliance can communicate with the Qualys Cloud Platform.
Appliance Access to Qualys Cloud Platform	The Scanner Appliance must be able to reach a certain infrastructure located at the Qualys Cloud Platform where your Qualys account is located. Tip - Log into your account and go to **Help > About** to see the Qualys Cloud Platform URLs.
Appliance Access to Target Host IPs	The IP addresses for the hosts to be scanned must be accessible to the Scanner Appliance. The Appliance must be able to resolve external DNS for the hostnames to be scanned.

LAN Interface is Default	The LAN interface services both scanning traffic and management traffic to the Qualys Cloud Platform, unless split network configuration is defined for the Appliance.
Virtual local area network (VLAN) Support	VLAN configuration options: 1) If you have connected the LAN interface to a 802.1q trunked port and need your Scanner Appliance to use VLAN tags on the LAN default network, enter the VLAN tag number using the Appliance console. 2) For any Appliance, you can choose option 1) and also configure more VLANs (to be used for scanning) using the Qualys user interface.
Dynamic Host Configuration Protocol (DHCP) or Static IP	By default the Scanner Appliance is pre-configured with DHCP. If configured with a static IP address, be sure you have the IP address, netmask, default gateway, primary DNS and Windows Internet Naming Service (WINS) server (if appropriate).
Proxy Support	The Scanner Appliance includes Proxy support with or without authentication - Basic or NTLM. The Proxy server must be assigned a static IP address and must allow transparent SSL tunneling. Proxy-level termination (as implemented in SSL bridging, for example) is not supported.
WINS Support	If your network is running WINS, the Scanner Appliance needs to use it for host name resolution during scanning. For an Appliance configured with DHCP, please be sure your WINS server IPs (primary and secondary) are added to your DHCP subnet configuration using “option netbios-name-servers WINS1, WINS2;”. For an Appliance with a static IP address, the WINS servers are defined with the static IP settings using the Appliance console.

4.4. Prognosis

IR is the corporate brand name of Integrated Research Limited (ASX: IRI), a leading global provider of proactive performance management software for critical IT infrastructure, payments and communications ecosystems.

More than 1,000 organizations in over 60 countries—including some of the world’s largest banks, airlines and telecommunications companies rely on IR Prognosis to provide business critical insights and ensure continuity. Critical systems deliver high availability and performance for millions of their customers across the globe.

Every second millions of critical systems and networks keep the world ticking. And every second, thousands of teams work tirelessly to maintain order but the threat of a problem is never far away.

To summarize (Prognosis 11):

- All communication between Prognosis servers are encrypted (i.e. between Monitoring & Managing servers)
- Have the option of being FIPS compliant (Federal Information Processing Standards (FIPS 140-2)
- All password credentials are encrypted & stored (AES256 encryption)
- Web Server is Internet Information Services (IIS)-based & runs on a secure https connection
- Can limit access to servers & web interface via Active Directory (AD).

5. Service Delivery Framework

All NetEnrich service management processes are ITIL-based and documented. ITIL represents the industry's most recognized best practices and IT processes. In addition, NetEnrich processes have been carefully developed and tailored over time, based on our experience of managing hundreds of business customers and thousands of devices to ensure the integrity and security of the customer's data and entire infrastructure.

NetEnrich services are delivered remotely from a secure OpsRamp Gateway (OR) deployed in the customer's network. OR provides a central point within the customer's IT Infrastructure or data center for the collection of monitoring data and management of servers, application and network infrastructure.

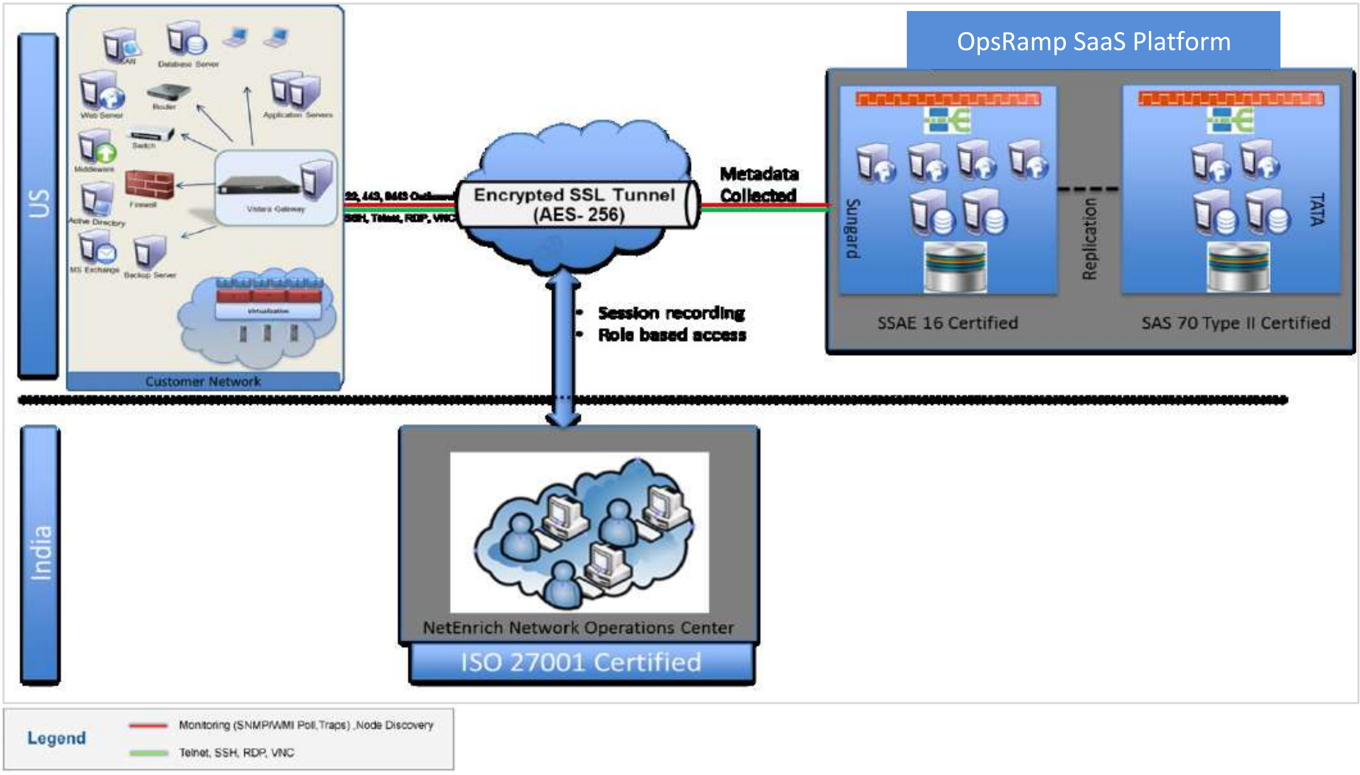
NetEnrich developed its technology arm and spun it off as 'OpsRamp IT' (www.OpsRamp.com) in January 2014. NetEnrich now partners with OpsRamp to serve 1000+ customers and 100+ service providers.

5.1. Proactive Notification & Incident Management

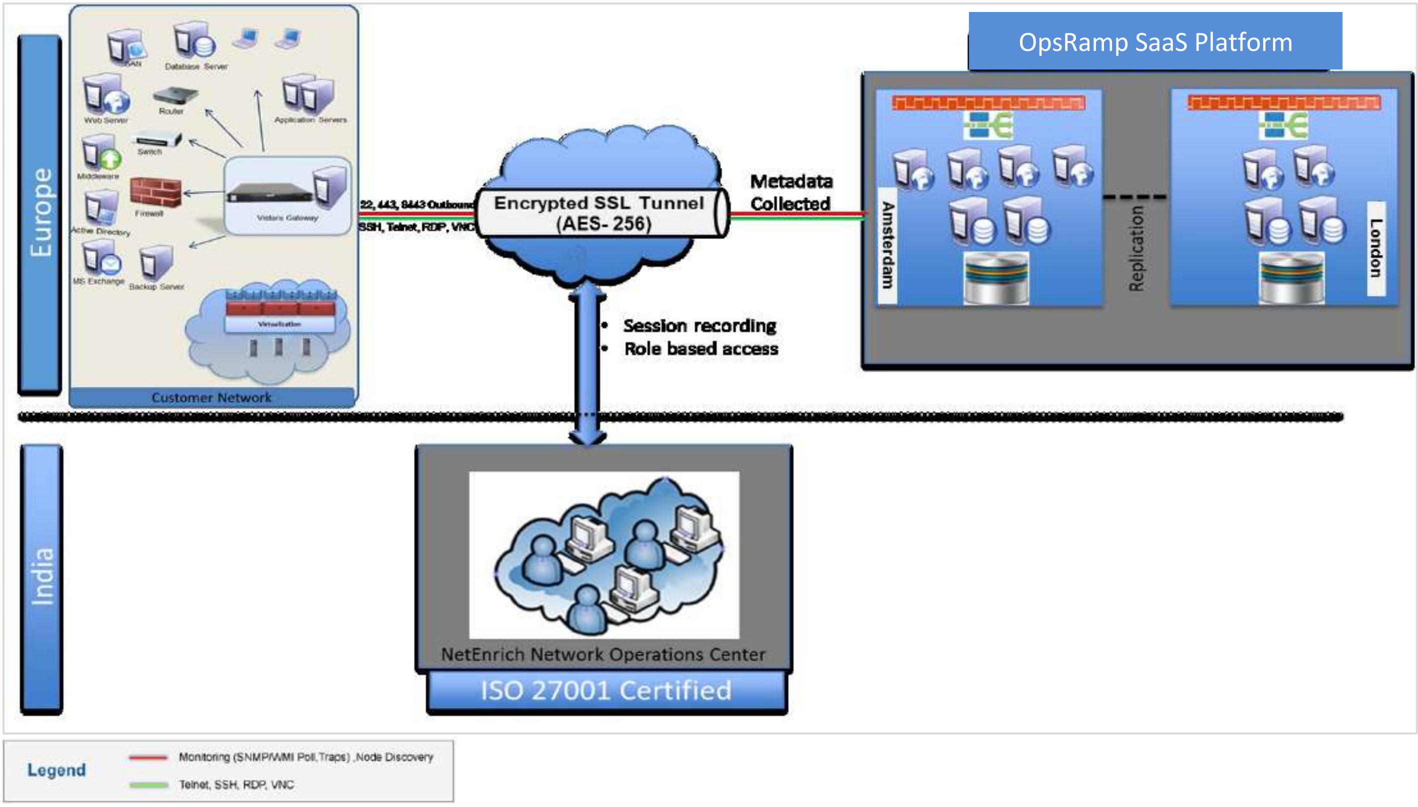
NetEnrich leverages an incident management system that has been highly customized with significant investments for SLA measurements, efficiency, incident handling, and problem & change management requirements. An array of additional tools have been developed by NetEnrich to manage the tickets and SLAs, which are critical when multiple customer sites across geographies need to be managed by a single shared group of NOC engineers.

NetEnrich provides secure web access to customers and partners to access our incident management system, allowing the VAR/customer to create, view, query and review incident records using a secured HTTPS connection. Tickets can be opened/created by user, email, and through operator managed system alert. This system also tracks and registers the date and time of all activities and updates through the life of the ticket for tracking purposes.

The below illustration depicts the OpsRamp Architecture for US.



The below illustration depicts the OpsRamp Architecture for Europe:



5.2. OpsRamp Cloud

OpsRamp collects and stores only data necessary to perform IT operations management functions on devices/applications that it manages. The below table summarizes the type of data OpsRamp collects.

Type of Data	Data Collected	Data Storage and Security
Performance Statistics	System level information necessary to monitor the performance and health of managed devices: · CPU and Memory utilization · OS Events · Hardware Events	Device performance statistics are stored only in the cloud. The Agent and Gateway collect and transmit this data to the OpsRamp Cloud
Events and SNMP Traps	Operating System events and traps generated by SNMP agents.	The Vistara Gateway and Agent processes events and traps locally and send resultant alerts to the OpsRamp Cloud secure channel. Raw event data is not stored in the Cloud.
Device Configuration and Device Metadata	System level information necessary to asses device configuration status: · DNS Names · Make/Model · OS and Application Configuration Parameters	OpsRamp Gateway and Agent sent configuration data to the OpsRamp Cloud secure channel.
Application Performance Statistics	Application information necessary to monitor the performance and health of managed applications	Application performance statistics are stored only in the cloud. The Agent and Gateway collect and transmit this data to the OpsRamp Cloud

5.2.1. Data Management

- Data Classification:
  - OpsRamp collects and stores only data necessary to perform IT operations management functions on devices that it manages
  - Data that OpsRamp collects is limited to device performance metrics, performance and failure events, and configuration information.
- Data Isolation:
  - OpsRamp implements strict multi-tenancy controls to ensure data access is strictly isolated between customers.
- Data Encryption (in-flight):
  - All data transmitted between the OpsRamp Agent/Gateway and the OpsRamp Cloud is encrypted with SSL and TLS/SSH (for gateway).
- Data Encryption (at-rest):
  - Device credentials stored in the OpsRamp cloud is encrypted using 1024-bit RSA encryption.
- Authentication:
  - OpsRamp Cloud offers SAML and OAuth2 based authentication
  - OpsRamp additionally supports 3rdparty authentication services such as OneLogin, Okta and ADFS
  - OpsRamp Cloud offers two-factor authentication.
- User Access Management:
  - OpsRamp has extensive role-based access controls
  - OpsRamp access controls are granular to the managed device, user, and feature.
- API:
  - OpsRamp provides REST APIs for integration with OpsRamp cloud
  - OpsRamp REST APIs are backed by OAuth2 based authentication.
- Regulatory and Compliance Requirements:
  - OpsRamp does NOT collect any Personal Identity Information (PII)
  - OpsRamp is hosted in co-location facilities provided by two U.S-based and two Europe-based datacenter providers. Each provider has their own security certifications – including Statement on Auditing Standards (SAS) and Standards for Attestation Engagements (SSAE).

5.2.2. Data Security

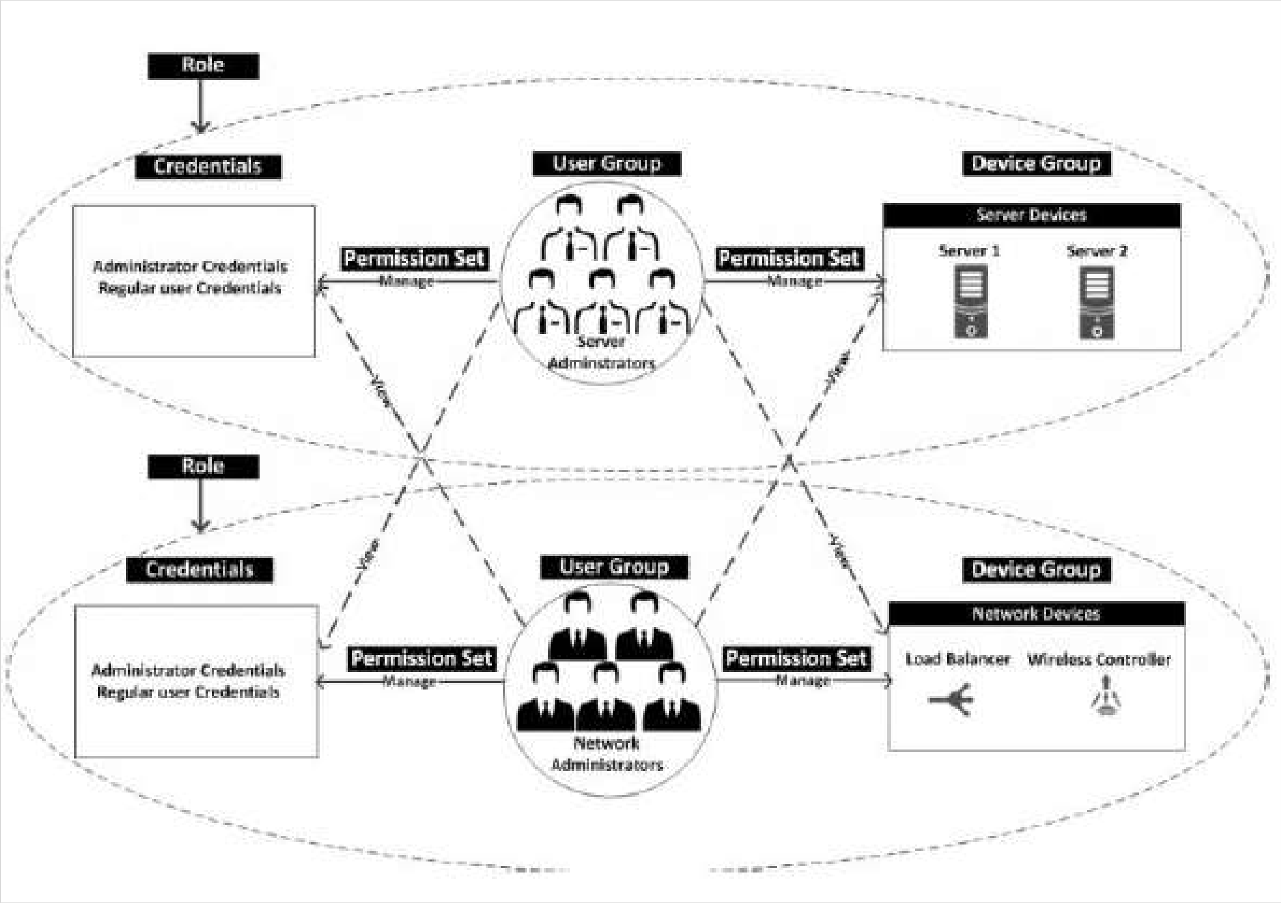
- All Sensitive data is encrypted
- Customer data (inventory, metrics, alerts and tickets) is logically partitioned and stored under tenant
- Customer data is accessible only by authorized users of tenant
- Role-based Access Control
  - OpsRamp supports comprehensive role based access controls. Users' access to devices and actions within OpsRamp is controlled by fine-grained permissions. Permissions are assigned based on users' roles.
- Identity Management for OpsRamp cloud
  - OpsRamp provides multiple options to manage user identity
  - Built-in user management system within OpsRamp
  - Integration with Microsoft Active Directory
  - Integration with single sign-on service OneLogin via SAML 2.0.
- Authentication and Passwords

- OpsRamp cloud follows standard practices for passwords:
  - Define rules of password strengths
  - CAPTCHA code based validation
  - Automated lockout after multiple unsuccessful login attempts
  - Two-factor authentication using yubico YubiKey.

5.2.3. Application Access Details

OpsRamp Role-Based Access Controls support fine-grained access controls on who can do what, based on:

- User and User Group
- Device and Device Group
- Specific Features
- Device Credentials.



5.2.4. Data Retention

- On contract expiry OpsRamp will inactivate the "tenant" in the OpsRamp platform
- Inactivate tenant instance inventory, metrics and alerts data will be available in passive state in the OpsRamp platform
- Monitoring, alerting and other management functionality will not be possible
- Based on mutual agreement between OpsRamp and the tenant, OpsRamp will delete all tenant information from OpsRamp cloud
- However, due to the 90 day data archival retention policy, deleted tenant data will be available in archival repository for 90 days.

5.2.5. Communication between various client sites

The basic principle of OR is to ensure all data transfer and management control communications between the customer's IT staff and NetEnrich. The communication is secured via 256-bit encryption over SSL/TLS. This level of encryption makes it impossible for any hacker or intruder to decrypt any of the communications in the NetEnrich network, even if they gain unlawful access. This is an essential automation component driving NetEnrich's IT as a Service delivery model.

Hosts and network devices are accessible only to authorized personnel and NetEnrich limits the type of access available to individual users via role based controls.

NetEnrich supports industry-standards based authentication that may be further supplemented with digital certificates for even stronger authentication. It also provides strong username and password control for individual accounts. All transmission of passwords over the network, and their storage in the NetEnrich system, is protected by layers of encryption. Additionally, digital certificates are used to authenticate third-party applications that integrate with NetEnrich.

All communication between the various customer sites and NetEnrich services are based on HTTP protocols and firewalled Internet protocols. The architecture also supports capabilities for teams to augment the security of the management solution by overlaying more third-party security and authentication layers, if needed. NetEnrich' s authentication module provides Application Program Interface (APIs) and integrates with other third-party authentication and directory servers such as LDAP, Active Directory, RADIUS, and TACACS Server. In larger environments where such authentication and directory services are the norm, teams can continue to use these mechanisms through integration.

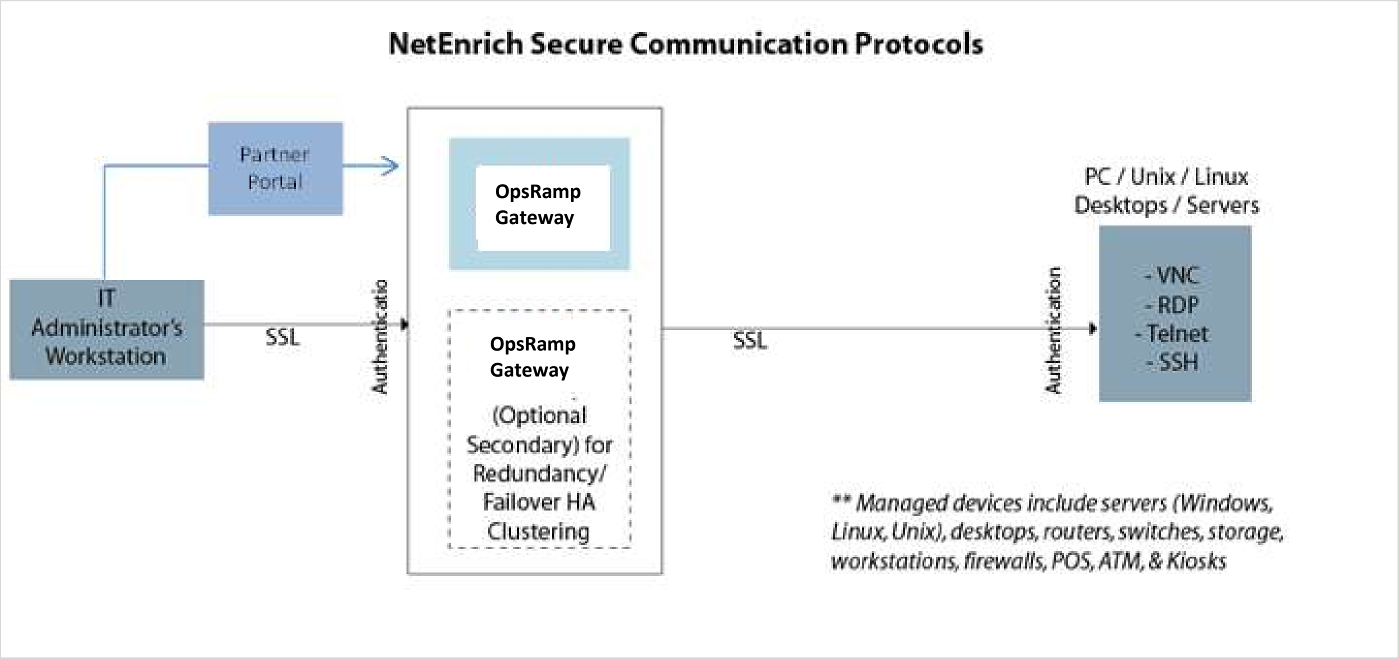
5.2.6. OR: No Trade-off between Security and Effectiveness

In general, to enforce a security framework for control and management of remote sites, management systems should provide the following:

- Authenticate users and provide role based access control (RBAC) to users – support Authorization
- Encrypt communications of all management traffic
- Provide session logs, audit trails, and reporting of all activity
- Detect and alert in real-time any physical changes to IT in remote sites, such as disconnection of ports
- Reduce risk of accidental damage to equipment in remote sites by enabling a lights-out environment
- Monitor environmental changes in remote sites such as temperature, humidity, smoke, vibration, or intrusion.

5.2.7. Control & Management Security Framework

NetEnrich provides a multi-tiered security model to enable an organization to effectively secure the management of its IT infrastructure. Hosts and network devices are accessible only to authorized personnel and NetEnrich limits this type of access available to individual users. NetEnrich supports industry standards based authentication that may be further supplemented with digital certificates for even stronger authentication. It provides strong username and password control for individual accounts. All passwords are a minimum of twelve characters long, and require a combination of letters, numbers and special characters. All transmission of passwords over the network, and their storage in the NetEnrich system is protected by layers of encryption (256-bit SSL and triple Data encryption standard (DES)). Additionally digital certificates are used to authenticate 3rd party applications that integrate with NetEnrich.


NetEnrich Secure Communication Protocols
Partner Portal
IT Administrator's Workstation
SSL
Authenticatio
OpsRamp Gateway
OpsRamp Gateway
(Optional Secondary) for Redundancy/ Failover HA Clustering
SSL
Authentication
PC / Unix / Linux Desktops / Servers
- VNC
- RDP
- Telnet
- SSH
** Managed devices include servers (Windows, Linux, Unix), desktops, routers, switches, storage, workstations, firewalls, POS, ATM, & Kiosks

5.2.8. Robust, Secure, and Scalable Architectural Platform

NetEnrich provides a robust, secure, and scalable solution for infrastructure management. This sub-section provides an overview of the security measures and methodology that NetEnrich employs in the architecture and deployment of its OR technologies.

Methodology

NetEnrich follows the industry standard of “defence-in-depth” using a combination of different technologies and practices to ensure security of the VPM platform itself. Technologies in use include:

- Encrypted communications using SSL and TLS
- Host-based firewalls
- Hardened embedded operating system (OS)
- Kernel-level mandatory access controls (MAC)
- Java sandbox
- Strong authentication (i.e. RADIUS, TACACS, two-factor authentication).

Additionally, practices in use include:

- Privilege separation
- Secure deployment architecture recommendations
- Least privilege
- Minimal access
- Rigorous coding standards
- Regular code reviews and audits.

5.2.9. Security Measures

Operating System

The OpsRamp Gateway uses a minimal embedded operating system that has been hardened using well-understood OS hardening techniques, including, but not limited to:

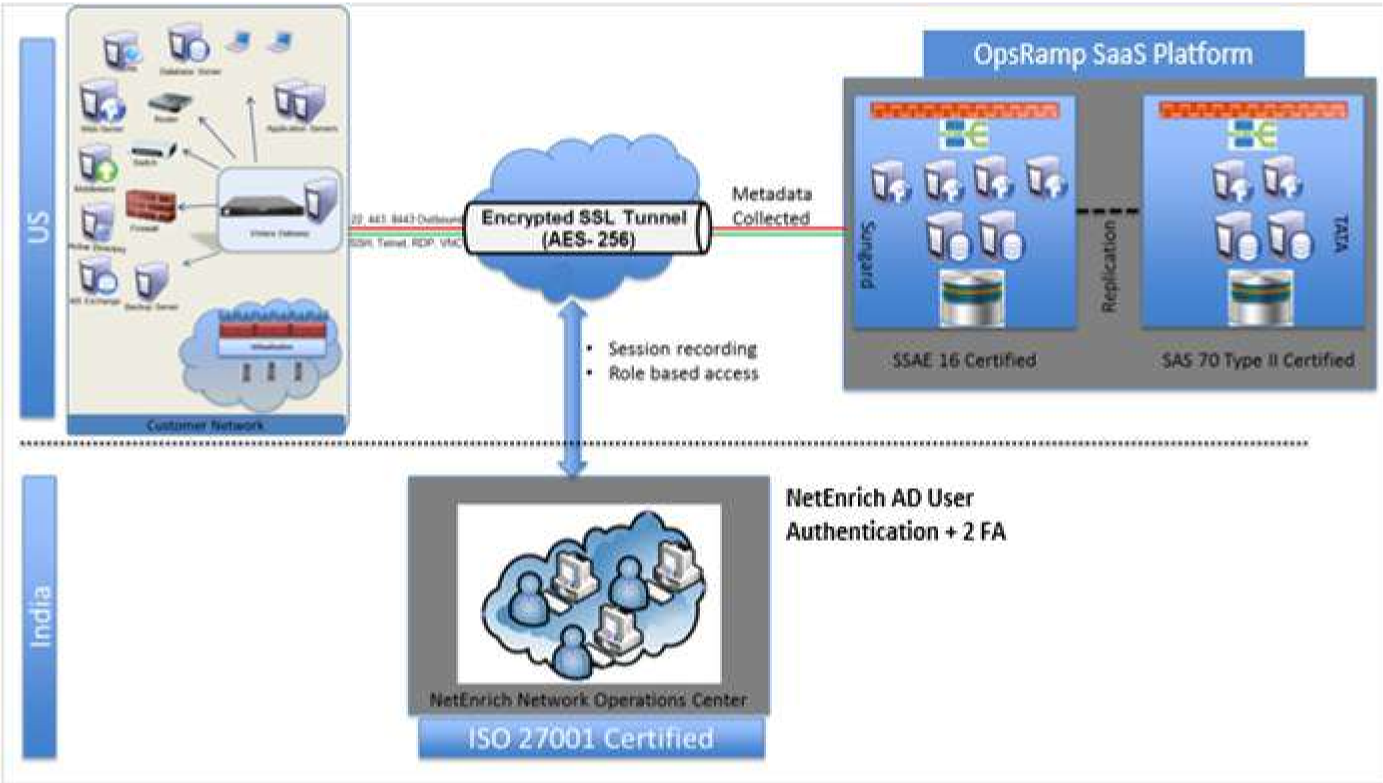
- Minimal software installation
- All unnecessary services turned off
- Latest patches and updates
- All unnecessary users and groups removed

An additional layer of assurance is provided by use of the security feature called AppArmor which is turned on for key software packages, and the firewall is extended to common services used by the operating system.

Network Measures

The NetEnrich solution takes a number of network-based security measures to provide assurance regardless of the organization’s deployment strategy, including:

- Only encrypted protocols like SSL and TLS are used for communications
- Ability to use standard identity management & authentication servers (e.g. RADIUS, TACACS, LDAP, Integrity)
- No remote access except via web browser or local serial console.
- Access to OpsRamp (US and EU) is integrated with NetEnrich ADFS for SSO Authentication.
- Access to OpsRamp (US and EU) is only allowed from Secured environment, like NE Delivery sites.



Application Measures

In developing its OR solution, NetEnrich strives to follow rigorous processes such as secure coding practices, regular code reviews and code audits. In the future, the NetEnrich product will be certified under Common Criteria or a similar certification.

5.2.10. Device Monitoring

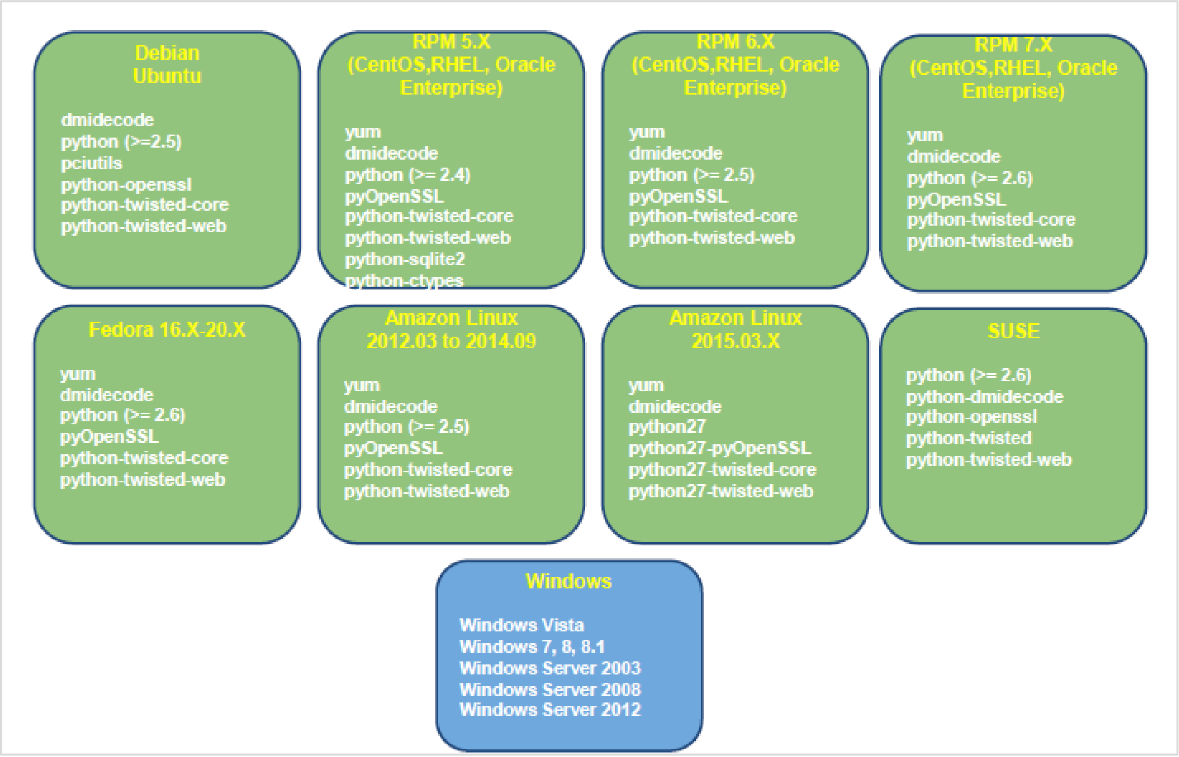
The OpsRamp Gateway is designed to monitor widely-used servers, applications and network infrastructure via SNMP, Windows Management Instrumentation (WMI), and Intelligent Platform Management Interface (IPMI) protocols. OpsRamp Gateway monitoring can be set to different time intervals (for example for every 1 minute, 15 minutes) depending on IT requirements. All metadata collected from the IT infrastructure is stored in Secured data centres in the United States. NetEnrich will not collect any data other than monitoring information.

5.2.11. Session Recordings and Audit Controls

Each time a NetEnrich engineer connects to a customer environment, a recording is created that captures the entire session and can be played back later by the customer for audit purposes. These recordings can be easily audited and reviewed by the client, the NetEnrich Network Operating Centre team or by the solution provider and detailed reports can be generated.

5.2.12. Data and Configurations on OR

All configurations of the OR are pushed from the NetEnrich cloud using the 256 bit encrypted channel created by OR. These configurations are not available to the end users because they don't have any access to OR. Sensitive data is either mangled or encrypted, depending on the sensitivity level of the data. For example, passphrases used for collecting monitoring data are encrypted on OR. The data collected by OR is relatively short-lived and doesn't get stored for extended periods of time. Once the collected data is synchronized with NetEnrich cloud components, the data on OR is purged as per standard policies.



Debian
Ubuntu

dmidecode
python (>=2.5)
pciutils
python-openssl
python-twisted-core
python-twisted-web

RPM 5.X
(CentOS,RHEL, Oracle Enterprise)

yum
dmidecode
python (>= 2.4)
pyOpenSSL
python-twisted-core
python-twisted-web
python-sqlite2
python-ctypes

RPM 6.X
(CentOS,RHEL, Oracle Enterprise)

yum
dmidecode
python (>= 2.5)
pyOpenSSL
python-twisted-core
python-twisted-web

RPM 7.X
(CentOS,RHEL, Oracle Enterprise)

yum
dmidecode
python (>= 2.6)
pyOpenSSL
python-twisted-core
python-twisted-web

Fedora 16.X-20.X

yum
dmidecode
python (>= 2.6)
pyOpenSSL
python-twisted-core
python-twisted-web

Amazon Linux
2012.03 to 2014.09

yum
dmidecode
python (>= 2.5)
pyOpenSSL
python-twisted-core
python-twisted-web

Amazon Linux
2015.03.X

yum
dmidecode
python27
python27-pyOpenSSL
python27-twisted-core
python27-twisted-web

SUSE

python (>= 2.6)
python-dmidecode
python-openssl
python-twisted
python-twisted-web

Windows

Windows Vista
Windows 7, 8, 8.1
Windows Server 2003
Windows Server 2008
Windows Server 2012

5.3. About NetEnrich Cloud

NetEnrich's Infrastructure is delivered from two data centers based in the US, at San Jose, CA, and Phoenix, AZ. Each of these facilities are engineered with fully redundant internet connectivity, power and HVAC to avoid any single points of failure, and are staffed 24 x 7 by highly trained technical support staff.

Security Features

Multiple physical layers of security including:

- 24/7/365 on-site security guards
- Full perimeter and interior surveillance cameras
- Impact resistant walls and windows
- Biometrics
- Electronic keycard readers
- Man-trap
- On-site Security Officers are responsible for access control, key control, camera surveillance monitoring and recording; regularly scheduled walking patrols; and asset protection of the facility.

Power Delivery Architecture

- End-to-End power delivery is provided with no single point of failure. All components are designed to a minimum of N+2 (need plus 2) redundancy and to a maximum of 2N (2 times need) redundancy
- 35-kVA feed from utility company. Pre-negotiated 1 hour advanced notice for any scheduled rolling power outages (brownouts)
- 14,000 sq ft. battery room, a total of 36 UPS; each UPS operates in hot-synch parallel
- Each Colocation/Hosting room is equipped with redundant and diverse PDU's
- Backup generator complex: 8 x 2 megawatt Caterpillar power plants fed by 50,000 gallon on-site fuel storage system
- Refuel-on-the-fly commitments allow indefinite self-power generation and delivery in the event of long term utility power loss.

Fire Suppression

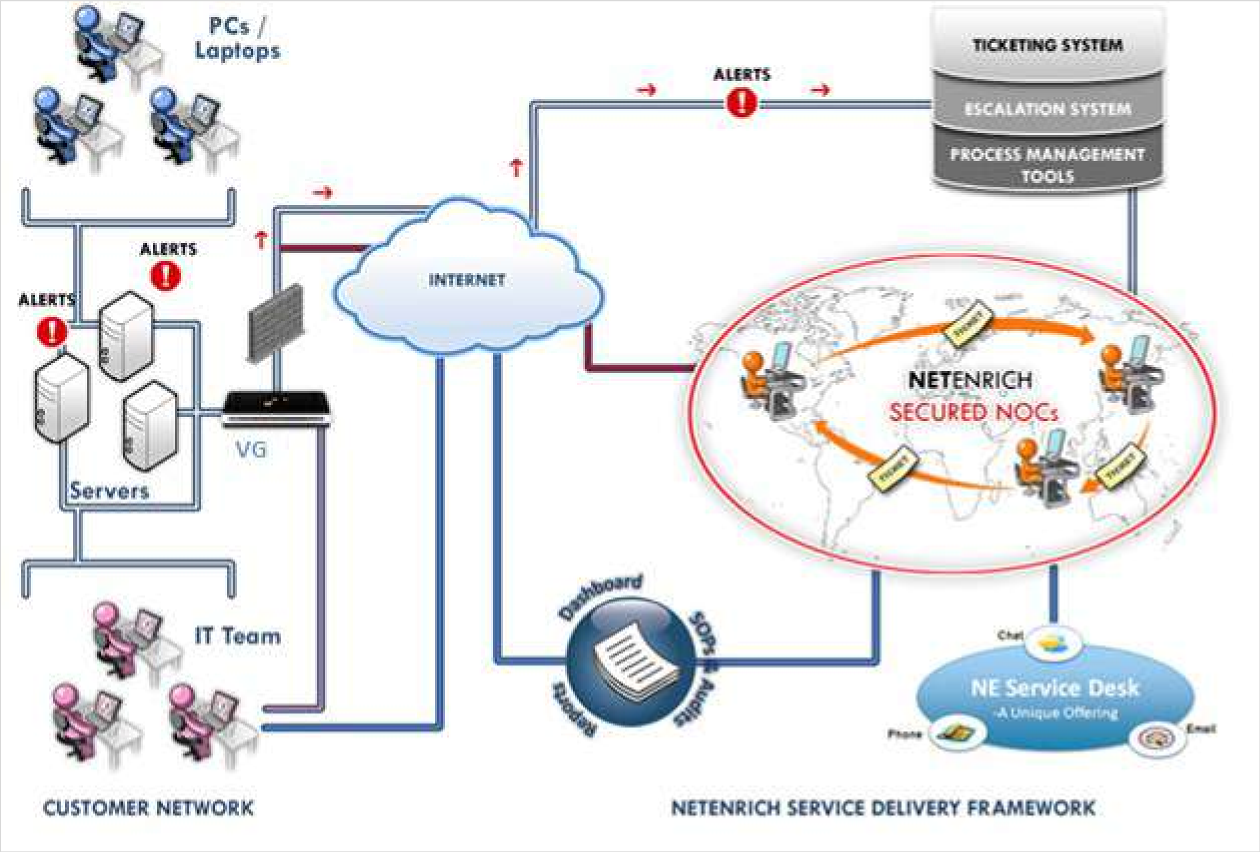
- Double pre-action dry pipe system with a two tiered activation system to prevent false positives
- FM-200 gas-based fire suppression system
- Laser based VESDA (Very Early Smoke Detection) air sampling devices to enhance our ability to respond to a situation and control it before a fire spreads.

Environmental Systems

- Air-cooled HVAC units in each room (N+1)
- DataTrax Foreseer system monitors all environmentals 24/7/365
- Onsite and remote facilities engineering teams available 24/7/365

Data Center Network

- Facilities are served through redundant fiber feeds to the Internet via diverse Tier 1 carriers
- They have 10G+ connectivity each
- Network infrastructure is monitored 24/7
- The IP network infrastructure utilizes state-of-the-art Cisco/Juniper/Foundry and other enterprise class solutions
- Servers are all connected on 1G/10G backbone



5.3.1. Cloud Portal Communications

All data transfer and communication from the customer's infrastructure to the Partner Portal happens over secured 128/256-bit encrypted connections. Limited services are run on port 80 that give generic information about the services we offer (for example websites, blogs and so on) - all others use SSL/TLS encryption.

5.3.2. Data Security

All data collected from ORs are stored in the backend database tier that is isolated from public facing web tier. Only authorized applications can access data from the database. This offers a better level of isolation for the data. All the sensitive information is encrypted within the database.

5.3.3. System Security

All servers run from standard OS images that are tested for their security vulnerabilities. In addition, local firewalls on the servers allow only permitted traffic. IPS scanners are deployed through the network. Syslog's are analyzed on an on-going basis for any kind of malicious activities.

5.3.4. Access to NetEnrich Cloud

Access to NetEnrich cloud is controlled using our own services gateway technology with two-factor authentication , each access is recorded and activity is archived for review. Users of the gateway are grouped into roles and role-based access control is given to servers. This approach helps limit the users that can access any given server. To improve security further, there are roles defined with limited duration access to the server, provisioned only in case of essential access needs. Standard password aging and password locking processes are in place for all user accounts.

5.4. NetEnrich Operations Portal

NetEnrich Operations portal (rebranded as 'OpsRamp') is a secured web portal that offers complete service delivery visibility of Managed Devices, Asset Inventory, Alerts (monitoring), tickets and related metrics and maintenance activities. The portal also presents device-level monitoring statistics (availability, performance) for analysis and trending.

The NetEnrich services team uses this portal to monitor, manage, and run health checks on managed devices. VARs logging in to the portal will see a consolidated view, including the Service Dashboard. When a client user logs in, only client-specific information is displayed.

6. Physical and Environmental Security

Physical access is restricted to the “secured areas” such as NOC, local server rooms and information sensitive areas. All “secured areas” are separated by effective security perimeters with access controlled entry/exit points.

6.1. Physical Security Perimeter

Manned reception areas and other means to restrict physical site/building access to authorized personnel only, and to positively authenticate visitors by suitable means of identification (such as photographic identity cards).

Access to secure areas are restricted to authorized persons who have been positively authenticated by biometric authentication, a photographic identity card, physical bag check and, where appropriate, knowledge of a password or Personal Identification Number (PIN). Access to secure areas are continuously logged and reviewed by management according to the risk of unauthorized access protocols.

Third-party personnel and other visitors are granted restricted access to secure areas only if required (example for maintenance and support purposes), authorized by management, and are supervised by a respective function member.

Closed Circuit Cameras are installed at all secure areas and are monitored 24/7 by experienced security personnel. Physical checking is performed by the security personnel whenever anyone enters the NetEnrich facility to restrict entering with classified restricted devices (example Storage Media).

6.2. Working in Secure Areas

Physical protection and guidelines are designed and applied to the personnel working in the secured areas:

- All storage equipment on computers installed in secured areas is disabled and not accessible. For example Universal Serial Bus (USB) stick, CD/DVD ROMs, flash drives etc. All the workstations within our NOCs are diskless and all external communication ports (except the Ethernet port) are disabled. All communications over the network are SSL encrypted.
- Photographic, video, audio or any other recording equipment (such as iPods/MP3 players and camera phones) are forbidden from designated secure areas.
- Printing and scanning equipment are restricted to enter the secure areas. Desktop computers are disabled for any physical printing.

7. Certifications

7.1. NetEnrich is ISO 27001 Certified

Given the depth, international standardization and auditability of ISO 27001, NetEnrich management made a decision to be audited and certified. Operational focus, documentation and training on standard policy and procedures enabled NetEnrich to become ISO 27001 certified in 2018. NetEnrich continues to improve its operational procedures and training with on-staff Six Sigma black belts and will maintain its certification with third-party ISO 27001 audits on an annual basis.

NetEnrich is committed to meeting the highest standards for information security, regulatory compliance and business continuity. ISO 27001 certification is a strong standard of baseline operation that every IT department should require of external vendors. By requiring ISO 27001, IT departments know they have chosen an external vendor who is focused on providing secure, compliant, and reliable IT services 24/7/365.

7.1.1. What is ISO 27001?

ISO 27001 is an Information Security Management System (ISMS) standard published by the International Organization for Standardization (ISO) and the International Electrotechnical Commission (IEC). The complete, correct nomenclature is: *ISO/IEC 27001:2013 - Information technology - Security techniques - Information security management systems - Requirements* (ISMS). The objective of the standard is to provide a model for establishing, implementing, operating, monitoring, reviewing, maintaining, and improving an Information Security Management System.

ISO 27001 standard requires that an organization to continually:

- Examine systematically the organization's information security risks, taking into account the threats, vulnerabilities and impacts;
- Designs and implements a coherent and comprehensive suite of information security controls and/or other forms of risk treatment (such as risk avoidance or risk transfer) to address those risks that it deems unacceptable; and
- Adopts an overarching management process to ensure that the information security controls continue to meet the organization's information security needs on an on-going basis.

To provide a better understanding of the operational coverage of the ISO 27001 standard, below is a breakdown of the 10 basic control areas for organizations:

- **Security policy** - This provides management direction and support for information security organization of assets and resources to help you manage information security within the organization
- **Asset classification and control** - To help you identify your assets and appropriately protect them
- **Personnel security** - To reduce the risks of human error, theft, fraud or misuse of facilities
- **Physical and environmental security** - To prevent unauthorized access, damage and interference to business premises and information
- **Communications and operations management** - To ensure the correct and secure operation of information processing facilities
- **Access control** - To strictly control access to information
- **Systems development and maintenance** - To ensure that security is at the forefront in the building and maintenance of information systems
- **Business continuity management** - To minimize interruptions to business activities and to protect critical business processes from the effects of major failures or disasters
- **Compliance** - Recognition of and adherence to criminal and civil law, statutory, regulatory or contractual obligations, and any security requirement minimizes legal risks and costs.

8. General Questionnaire

Standard	Response	Comments
Location of offshore team? (City/Country)	Hyderabad, India Bhimavaram, India	
Company size and setup? (Number)	800+	
What is the service you will be providing? (Name)	Remote Monitoring and Management	Remote monitoring and management of servers and network devices.
InfoSec Program		
Date of first certification? (Date)	1/23/2009	
Date of most recent recertification? (Date)	Sep. 2018	
Does your P&P follow the ISO17799/27001 guidelines? (Y/N)	Y	Documented in NetEnrich internal ISMS document. Reviewed and approved by third-party ISO 27001 auditor.
Does the organization have controls for enforcing P&P? (Y/N)	Y	Documented in NetEnrich internal ISMS document. Reviewed and approved by third-party ISO 27001 auditor.
Do you have documented policies and procedures? (Y/N)	Y	Documented in NetEnrich internal ISMS document.
Do you have Security Awareness Training? If yes then how often? (Y/N)	Y	Internal ISMS training is published for every employee. New employees are trained during induction.
Do you have a governance framework for monitoring and enforcing policies and procedures? (Y/N)	Y	
Do you have a documented DR plan and is it tested periodically? (Y/N)	Y	NetEnrich Disaster Recovery plan is fully documented and tested. Potential business interruptions are mitigated by redundancies in power and network access and staff training.
Do you have a governance framework? (Y/N)	Y	Internal ISMS document
Does any data goes out of US Data centres for US customers	N	Only metadata such as alert and performance matrix are stored and no other data is collected
Does any data goes out of European Data centres for European customers	N	Only metadata such as alert and performance matrix are stored and no other data is collected
Physical Security		
Do you have a badge or biometric access to ODC? (Y/N)	Y	Biometric with anti-pass back enabled on all ODC
Do you use locks for workstations? (Y/N)	N	
Is portable media allowed in or out of ODC? (Y/N)	N	Any removal of portable media or print material must have permission of IS coordinator and must be logged for exit and entry into NOC.
Is any media (including paper) moved in/out of ODC monitored facility? (Y/N)	N	Any removal of portable media or print material must have permission of IS coordinator and must be logged for exit and entry into NOC.
Do you have security guards? (Y/N)	Y	24 x 7 Security Guards on entire premises
Do you have CCTV surveillance? (Y/N)	Y	24 x 7 CCTV surveillance for entire facility

Do you do background checks for staff? (Y/N)	Y	NetEnrich HR staff conducts extensive background checks on all new hires. We also use extensive third-party background checks for certain employees for management and project -pecific requirements.
Do you allow cameras into the ODC? (Y/N)	N	
Workstations		
Are laptops used? (Y/N)	Y	USB port(s) are disabled
Do you have antivirus and antispyware (including key logger protection)? (Y/N)	Y	
Do you run a vulnerability scanner like Qualys, n*Circle, or Nessus? (Y/N)	Y	NetEnrich uses QualysGuard for vulnerability scanning.
Do you have an antispyware program with a signature service? Do signatures need to be updated weekly? (Y/N)	Y	Sophos Anti-Spyware is corporate standard.
Are your AV and antivirus/antispyware events centrally logged and reviewed periodically? (Y/N)	Y	Standard procedure as part of proactive checklist process.
Are users prevented from overriding virus protection? (Y/N)	Y	Users cannot make changes to configuration.
Do workstations have the ability to write to portable storage devices (e.g., CD/DVD ROM and thumb drives)? (Y/N)	N	Workstations do not contain any ports for attaching portable media.
Are USB ports disabled? (Y/N)	Y	USB ports are not present in workstations; they are disabled on laptops.
Are external devices (e.g., USB drives or eternal disk drives) used? (Y/N)	N	USB ports are not present in workstations; they are disabled on laptops.
Are you running a supported OS on the desktop, with an active support/maintenance contract? (Y/N)	Y	
Do you have robust weekly patching practices? (e.g., security patches) (Y/N)	Y	All security and critical patches are tested and installed on periodic intervals.
Are workstations able to access the nternet? (Y/N)	Y	They are controlled through a proxy server.
If workstations have access to the internet, are they protected via firewalls and IDS with current signatures? (Y/N)	Y	All communication between workstations and desktops with client sites is via Proxy/HTTPS.
Do you have Periodic (Quarterly) vulnerability scans (desktop & network) (Y/N)	Y	Part of our Security Compliance audit process. Reviewed and approved by ISO 27001 auditor.
Are databases on local workstations? (Y/N)	N	No data is kept on workstations or laptops.
Are users able to overwrite or change critical system configuration parameters (e.g., virus protection software)? (Y/N)	N	All the administrative settings on the workstation and laptop are controlled using GPO
Do users have local admin privileges? (Y/N)	N	
Do you have an asset disposal policy/practice (get details)? (Y/N)	Y	All storage devices containing sensitive information will be physically destroyed or securely overwritten using systems approved by the IS Coordinator.

Do you use an endpoint security product (get details)? (Y/N)	Y	NetEnrich uses a combination of network firewall, Email quarantine, Antivirus, Proxy, VLAN, and personal firewall for mobile devices along with risk assessment and reporting to create a complete security infrastructure for end-point devices.
Are printers located in NOC area? (Y/N)	N	
Are printers located outside NOC? (Y/N)	Y	
If there are printers located outside NOC, can they be printed to from inside the NOC? (Y/N)	N	The network printer is seggregated from the NOC VLAN
Are print jobs recorded and reviewed? (Y/N)	Y	All print jobs are reviewed
Is there an enforcement mechanism? (Y/N)	Y	
Network		
Is there an enforcement mechanism for remote access? (Y/N)	Y	This is part of remote access policy, which is enforced and documented through the Information Security Manual. The effectiveness of the policy enforcement has been audited as part of internal checkpoint audits and yearly third-party audit.
Email Transport Security: All email communication should transit over TLS or a secure channel? (Y/N)	Y	
Do you have Email content filtering? (Y/N)	Y	
Do you have Internet content filtering to prevent downloading of malware from malicious or risk sites? (Y/N)	Y	
Do you have Controls to prevent unauthorized network connections? (Y/N)	Y	
Are communications closets secured/monitored? (Y/N)	Y	NetEnrich NOCs are all secure facilities.
Do you use Active Directory (AD) with defined domains? (Y/N)	Y	
Are Security events logged and reviewed (get details) (Y/N)	Y	NetEnrich has a proactive checklist with regular IT management review for necessary action.
Are AD domains mapped to RBAC and provide access to specific resources? (Y/N)	Y	
Do you have a password strength policy (get details)? (Y/N)	Y	NetEnrich’ s policy is to require a combination of: both upper- and lower-case letters (case sensitivity) and inclusion of one or more numerical digits/special characters; prohibition of words found in a dictionary or the user's personal information. Minimum charaters required is 12
Confirm that there are no local file servers? (Y/N)	Y	
Is SIEM in place? (Y/N)	Y	Complete IT infrastructure covered by IBM Qradar
For laptops only		
Do you have a personal firewall program with a support contract (recommended products are IBM ISS Proventia Desktop, McAfee Personal FW, Norton Personal FW, Checkpoint Zone Alarm, Kaspersky etc.)? Do electronic signatures need to be updated weekly? (Y/N)	Y	Sophos, signatures update on a daily basis.

Are personal firewall actions centrally logged and reviewed? (Y/N)	Y	
Backup		
Desktop and laptops are backed up weekly? (Y/N)	N	Only few identified critical Laptops backup is enabled
Remote Access		
Confirm that no client data should be moved to local file servers? (Y/N)	Y	Access to client site will be via OR, which restricts access by role, time, or ticket and does not expose data.
Additional Responses		
Do you have cube privacy /privacy filters on screens? (Y/N)	Y	
Is there lockable storage for media and hardcopy files? (Y/N)	Y	
Do you have Windows MS Office (with support contract) (Y/N)	Y	

8.1. NetEnrich on EU GDPR

Territorial Scope

The scope of the GDPR is extended so that many companies based outside the EU that are processing personal data about persons who are in the EU will need to comply and appoint a representative in the EU.

NetEnrich has business across geographies including the EU region. Data protection is being taken care of and the services from NetEnrich access only the metadata of the customer and does not port any data across borders. The only tool we use is OpsRamp to support the customer requirement. OpsRamp will be deployed in the EU data center to ensure that the data is not stored across the border. Service delivery will use metadata for performance and capacity and not for any personal data.

Supervisory authority

The GDPR requires national data protection authorities (Supervisory Authorities) to respond to complaints and enforce the GDPR and local data protection laws where only data subjects in that member state are affected. Where there is cross border processing, a lead Supervisory Authority system (determined by the location of the “main establishment” of the organisation) applies through which that authority enforces the GDPR in consultation with the other “concerned” Supervisory Authorities.

The CISO and DPO at the delivery center will be representative for any kind of issues arising due to the cross border processing and data protection. The incident is considered as high priority and concerned members will be on the call till the issue is resolved.

Data governance and accountability

The GDPR places onerous accountability obligations on controllers and processors to demonstrate compliance with the GDPR. Some of the elements that must be demonstrated are explicit but some are implied, such as the implementation of appropriate governance models so that data protection receives an appropriate level of attention within the organisation. The net effect is that all large organisations will need to implement a formal data protection programme.

NetEnrich has already been certified as ISO27001:2013 company adhering to the Information security on the data handled on behalf of the customer. The existing customer requirement on data protection are being fulfilled .

DPO is responsible for the core activities of the organisation and consist of processing operations which require “regular and systematic monitoring” of data subjects on “a large scale”; or (b) where the core activities consist of processing of special categories of data on a “large scale”; or (c) where required under Member State law.

Export of personal data

Customer environment is being monitored and supported using OpsRamp and third party tools which are compliant on data protection and handling. The OpsRamp tool does not port any data across the borders only the metadata are being collected for Dashboard and reports preparation. Any data which is marked a PII information will not be available to the monitoring or NOC teams.

Personal data breach

The GDPR introduces new timeframes for notifying Supervisory Authorities and data subjects and requirements regarding the details that are required to be recorded and provided in such circumstances.

Any data breach identified are brought to the DPO's notification within 72 hours for minor incidents and immediate notification is required for major incidents. Incident SLAs are in line with the delivery and customer requirement.

8.2. EU GDPR FAQ's

When is the GDPR coming into effect?

The General Data Protection Regulation (GDPR) was approved and adopted by the EU Parliament in April 2016. The regulation will take effect after a two-year transition period and, unlike a Directive it does not require any enabling legislation to be passed by government; meaning it will be in force May 2018.

Who does the GDPR affect?

The GDPR not only applies to organizations located within the EU but it will also apply to organizations located outside of the EU if they offer goods or services to, or monitor the behavior of, EU data subjects. It applies to all companies processing and holding the personal data of data subjects residing in the European Union, regardless of the company's location.

What are the penalties for non-compliance?

Organizations can be fined up to 4% of annual global turnover for breaching GDPR or €20 Million. This is the maximum fine that can be imposed for the most serious infringements, e.g. not having sufficient customer consent to process data or violating the core of Privacy by Design concepts. There is a tiered approach to fines, e.g. a company can be fined 2% for not having their records in order (article 28), not notifying the supervising authority and data subject about a breach or not conducting impact assessment. It is important to note that these rules apply to both controllers and processors -- meaning 'clouds' will not be exempt from GDPR enforcement.

What constitutes personal data?

Any information related to a natural person or 'Data Subject' that can be used to directly or indirectly identify the person. It can be anything from a name, a photo, an email address, bank details, posts on social networking websites, medical information, or a computer IP address.

What is the difference between a data processor and a data controller?

A controller is the entity that determines the purposes, conditions and means of processing the personal data, while the processor is an entity which processes personal data on behalf of the controller.

Do data processors need 'explicit' or 'unambiguous' data subject consent - and what is the difference?

The conditions for consent have been strengthened, as companies will no longer be able to utilise long illegible terms and conditions full of legalese, as the request for consent must be given in an intelligible and easily accessible form, with the purpose for data processing attached to that consent - meaning it must be unambiguous. Consent must be clear and distinguishable from other matters and provided in an intelligible and easily accessible form, using clear and plain language. It must be as easy to withdraw consent as it is to give it. Explicit consent is required only for processing sensitive personal data - in this context, nothing short of "opt in" will suffice. However, for non-sensitive data, "unambiguous" consent will suffice.

What about Data Subjects under the age of 16?

Parental consent will be required to process the personal data of children under the age of 16 for online services; member states may legislate for a lower age of consent but this will not be below the age of 13.

What is the difference between a regulation and a directive?

A regulation is a binding legislative act. It must be applied in its entirety across the EU, while a directive is a legislative act that sets out a goal that all EU countries must achieve. However, it is up to the individual countries to decide how. It is important to note that the GDPR is a regulation, in contrast the previous legislation, which is a directive.

Does my business need to appoint a Data Protection Officer (DPO)?

DPOs must be appointed in the case of: (a) public authorities, (b) organizations that engage in large scale systematic monitoring, or (c) organizations that engage in large scale processing of sensitive personal data (Art. 37). If your organization doesn't fall into one of these categories, then you do not need to appoint a DPO.

How does the GDPR affect policy surrounding data breaches?

Proposed regulations surrounding data breaches primarily relate to the notification policies of companies that have been breached. Data breaches which may pose a risk to individuals must be notified to the DPA within 72 hours and to affected individuals without undue delay.

Will the GDPR set up a one-stop-shop for data privacy regulation?

The discussions surrounding the one-stop-shop principle are among the most highly debated and are still unclear as the standing positions are highly varied. The Commission text has a fairly simple and concise ruling in favor of the principle, the Parliament also promotes a lead DPA and adds more involvement from other concerned DPAs, the Council's view waters down the ability of the lead DPA even further. A more in depth analysis of the one-stop-shop policy debate can be found at http://www.eugdpr.org/controversial-topics.html.