Vistara Security Overview

Table of Contents

List of Figures

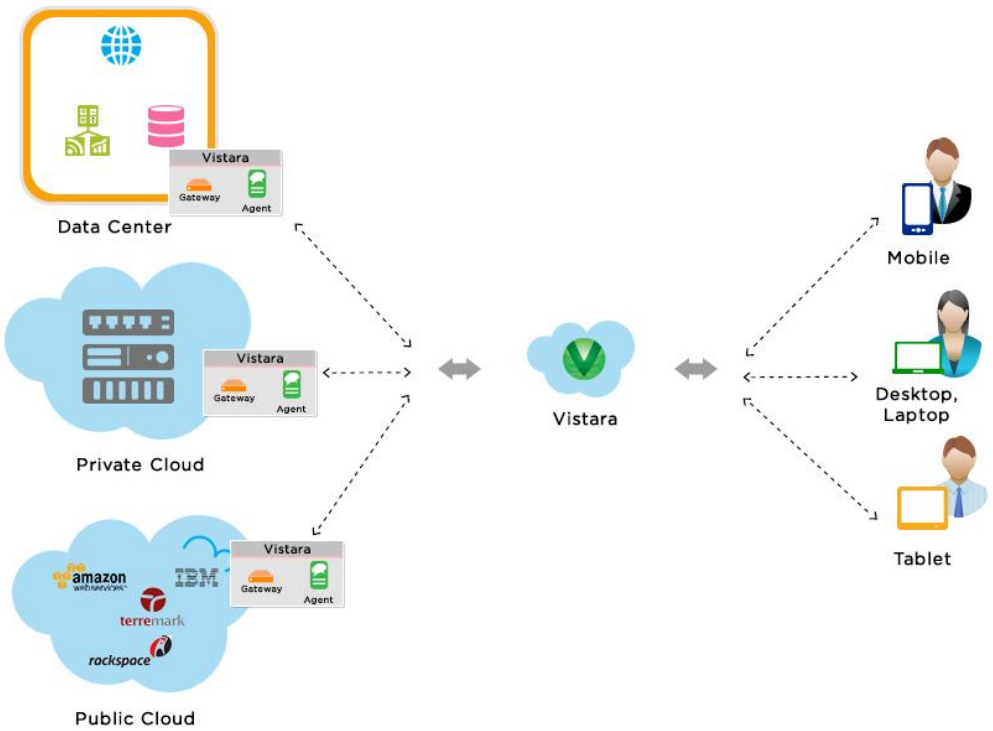
1. Introduction

Vistara is a SaaS based operations management platform for modern IT. This document covers the security model and practices behind Vistara. This documented is intended for Vistara customers and partners interested in understanding how Vistara ensures the security and integrity of the data that Vistara collects in managing their IT environments.

2. Architecture

The figures below shows Vistara's high level architecture and components.

Figure 1



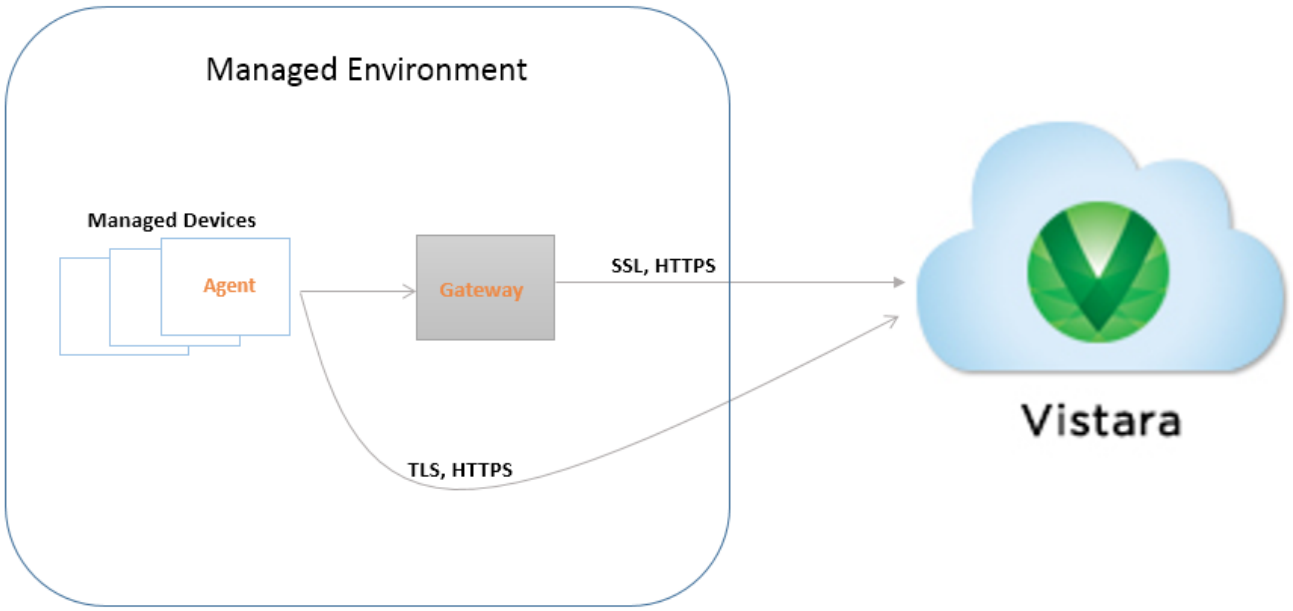


Figure 2

Vistara Gateway

Description	A virtual appliance that collects data from the managed environment. The Gateway establishes a secure connection to the Vistara Cloud over the internet via: 1) SSL version 3.0 with 256-bit encryption 2) HTTPS
Form Factor	The Gateway is a Virtual Appliance that runs on VMware vSphere and Citrix XenServer platforms.
Operating System	Hardened configuration of Ubuntu Server. Hardening includes the following measures: • Minimal software is installed • All unnecessary services are turned off • Applying latest patches and updates • All unnecessary users and groups are removed

Access Controls	All configuration updates for the Vistara Gateway are pushed from the Vistara servers using a 256-bit encrypted channel created by the Vistara Gateway. End users do not have access to the Vistara Gateway.

Vistara Agent

Description	A lightweight agent that runs on Windows and Linux systems in the managed environment. The agent collects data and performs management actions on servers and desktops. The Agent establishes a secure connection to the Vistara Cloud over the internet via: 1) TLS version 1.1 with 256-bit encryption 2) HTTPS
Form Factor	Windows and Linux binaries. The Windows Agent runs as Windows Service and Linux binary runs as a python script.

Vistara Cloud

Description	The Vistara application running in datacenters.
Infrastructure	Vistara runs on company owned physical hardware within co-location facilities in the two U.S based datacenters. Vistara does not run in a Public Cloud.

3. Datacenters

The Vistara Cloud is comprised of the various components of the Vistara application, running on company owned infrastructure in co-location facilities within two enterprise class, U.S based datacenters. The two datacenters are owned and operated by two different 3rd party datacenter providers. Both datacenter providers are publicly listed U.S firms.

Locations	Datacenter 1: Santa Clara, California Datacenter 2: Rancho Cordova (Sacramento), California
Security Certifications	Security certifications that the two 3rd party datacenters have include SAS 70, PCI DSS, and others.

4. Types of data Vistara collects

Vistara collects and stores only data necessary to perform IT operations management functions on devices that it manages. The table below summarizes the type of data Vistara 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 Vistara 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 Vistara Cloud via a 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	The Vistara Gateway and Agent sent configuration data to the Vistara Cloud via a secure channel.
Device Credentials	Credentials (username / password) necessary to discover devices, access performance and configuration data, and log into devices to run automation scripts.	The IT administrator provides device credential to Vistara via its user interface. Device credentials are stored in the Vistara Cloud, using industry standard 1024-bit RSA encryption.

5. Types of data Vistara does not collect

Vistara does not collect, and has no means to collect, any data processed by applications that Vistara monitors. Examples of such data includes data within database tables, content of application transactions, user credentials of applications, etc.

6. Application security

Vistara supports an extensive set of security features that ensure that management data collected by Vistara is accessed only by authorized users. The following is a summary security features in Vistara.

Role Based Access Control	Vistara supports a comprehensive role based access controls. Users' access to devices and actions within Vistara is controlled by fine-grained permissions. Permissions are assigned based on users' roles.
Identity Management	Vistara provides multiple options to manage user identity: - Built-in user management system within Vistara - Integration with Microsoft Active Directory - Integration with single sign-on service OneLogin via SAML 2.0.
Authentication and Passwords	Vistara follows standard practices for passwords: - Rules of password strengths - CAPTCHA code based validation - Automated lockout after multiple unsuccessful login attempts Vistara supports two-factor authentication using yubico YubiKey.

7. Security of operational processes

Vistara's operations and development processes follow methodologies that ensure security of data managed by Vistara. The table below highlight specific processes.

ISO Processes	The Vistara product development organization is ISO 27001 certified: - First certification was in January 2009 - Latest certification was in February 2013 - Certifying auditors: TUV SUD GmbH

Infrastructure Management	The infrastructure on which Vistara runs is managed to industry standard practices: - The network is protected by a **perimeter firewall** and **Intrusion Detection System** - Servers are **patched** monthly - **Vulnerability checks** are performed on servers regularly - **Penetration checks** are performed regularly - All changes to infrastructure are governed by a **Change Advisory Board** per ITIL standards

8. Further Information

Please contact your Vistara representative for further information on Vistara security.