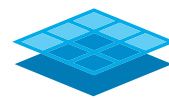


WHITE PAPER

Platform9's Security Practices



PLATFORM9

Introduction	2
Product	3
Platform9 Managed Kubernetes	3
Platform9 Managed OpenStack	4
Product Security	5
Authentication and Authorization	5
Local Credentials (Password-based Authentication)	6
Single Sign-On Support	7
Robust, Extensible Permissions Model	7
Architectural Security	7
Metadata	8
TLS with Mutual Authentication	8
Elimination of Open Ports	8
Restricted Access User	8
Code Signing	8
Operational Security	9
Secure Operations	9
Secure Development	10
Secure Customer Data	10
Protecting Against Web Application Attacks	11
Vulnerability Assessments	11
Key Management and Passwords	11
Secure Hiring Practices	11
Other Security Practices	12
Information Security Policy	12
Physical Security	12
Network Security	13
Compute Security	13
Management Plane Security	13
Disaster Recovery by Public Cloud	13
High Availability and Disaster Recovery	13
Least Privilege Access Policy	14
Privacy Policy	14
Conclusion	15

Introduction

As a multi cloud and hybrid cloud company, security is front and center at Platform9. We take a number of steps to protect our customers' data regardless of their operating model: on-premises infrastructure, colocation facilities, or public clouds such as Amazon Web Services, Microsoft Azure and Google Cloud Platform. The goal of this document is to cover topics related to product security, operational security and other security practices at Platform9.

The Platform9 product comprises Platform9 Managed Kubernetes and Platform9 Managed OpenStack. The product includes a Platform9 management plane that is used to provision, deprovision and perform management tasks on other hosts. These hosts include VMs, containers, bare-metal servers, and public cloud instances that are used by customers for their production workloads.

The following document provides insight into the security practices at Platform9, starting with product security. To get an overview of Platform9, please refer to the [Executive Summary](#), [Platform9 Managed Kubernetes Datasheet](#) and [Platform9 Managed OpenStack Datasheet](#).

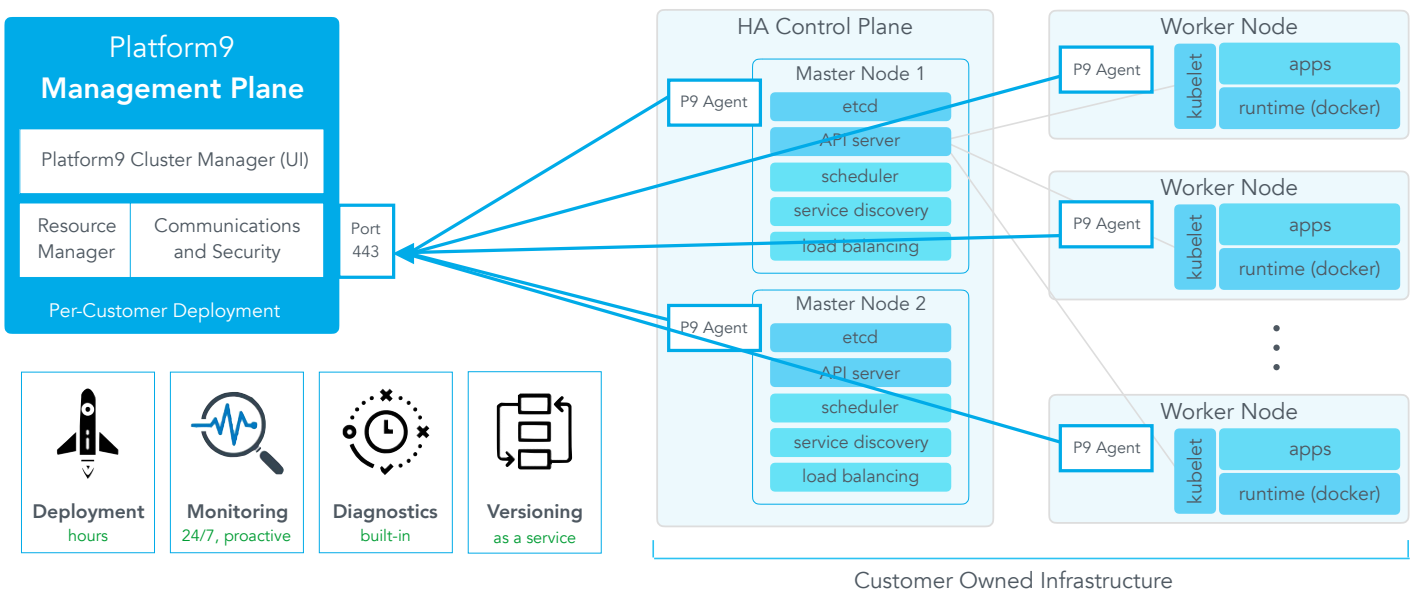
Product

Platform9's SaaS-Managed OpenStack and Kubernetes product consists of multiple components that can be classified in either the management plane or the data plane:

- **Management Plane:** Components in this plane consist of Platform9 instances that enable on-premises or public cloud orchestration of bare-metal servers, virtual machines and containers.
- **Data Plane:** These are bare-metal servers, VMs, containers and apps in the customer datacenter or public cloud. Data plane infrastructure is provisioned, deprovisioned, monitored and managed using the control plane. However, a catastrophic failure in the control plane will not disrupt the workloads in your data plane.

Platform9 Managed Kubernetes

For Platform9 Managed Kubernetes, the management plane is installed in the Platform9 hosted cloud and has access to orchestrate the on-premises control plane and worker nodes through the use of the Platform9 agent. These master nodes receive API requests and schedule creation, deletion and management actions on a number of worker nodes. A diagram of the Platform9 Managed Kubernetes architecture is shown below.

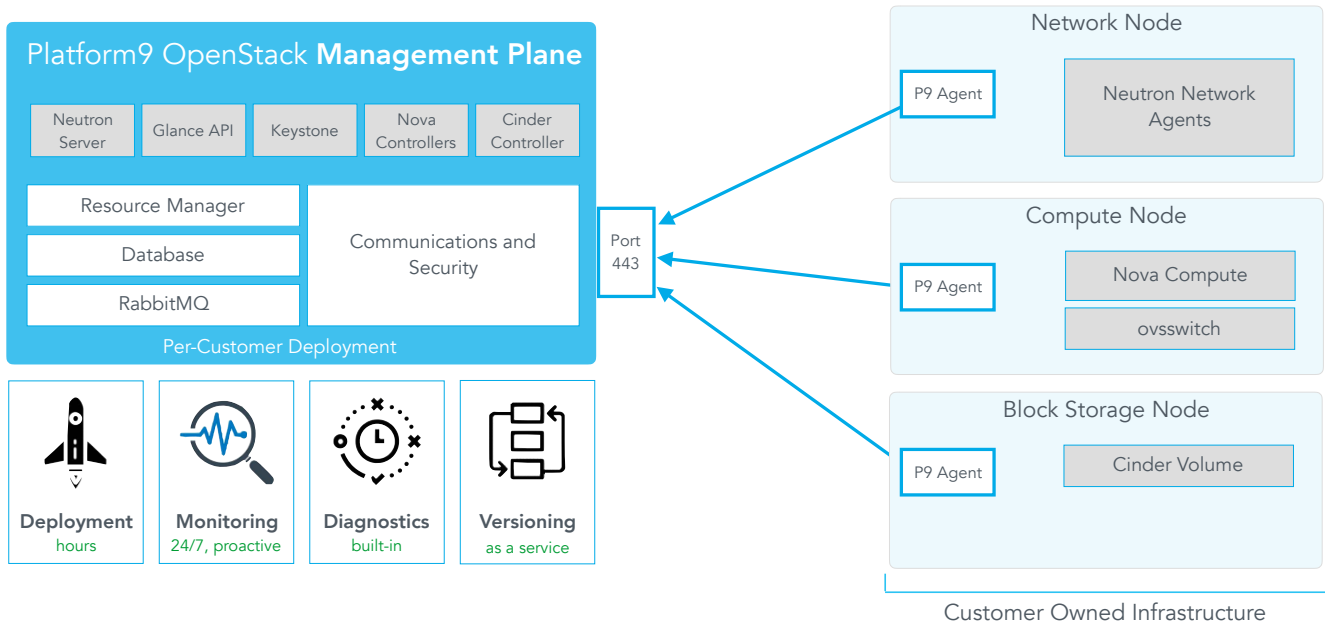


For simplicity, the diagram above shows a single management plane and control plane. Each customer has a separate management plane that does not share resources with those of other customers. The agents communicate with the management plane over a secure TLS channel.

Platform9 Managed Kubernetes can be deployed on vSphere, most Enterprise Linux platforms, public clouds, and on-premises. When a customer decides to onboard Platform9 Managed Kubernetes, the master nodes will be deployed by the Platform9 management plane through the use of an agent.

Platform9 Managed OpenStack

Like Platform9 Managed Kubernetes, Platform9 Managed OpenStack includes a management plane installed in the public cloud and additionally the OpenStack control plane components. The management plane receives requests from the administrator/user and schedules creation, deletion and management of compute, network, and storage nodes which reside in the data plane. A diagram of the Platform9 Managed OpenStack architecture is shown below.

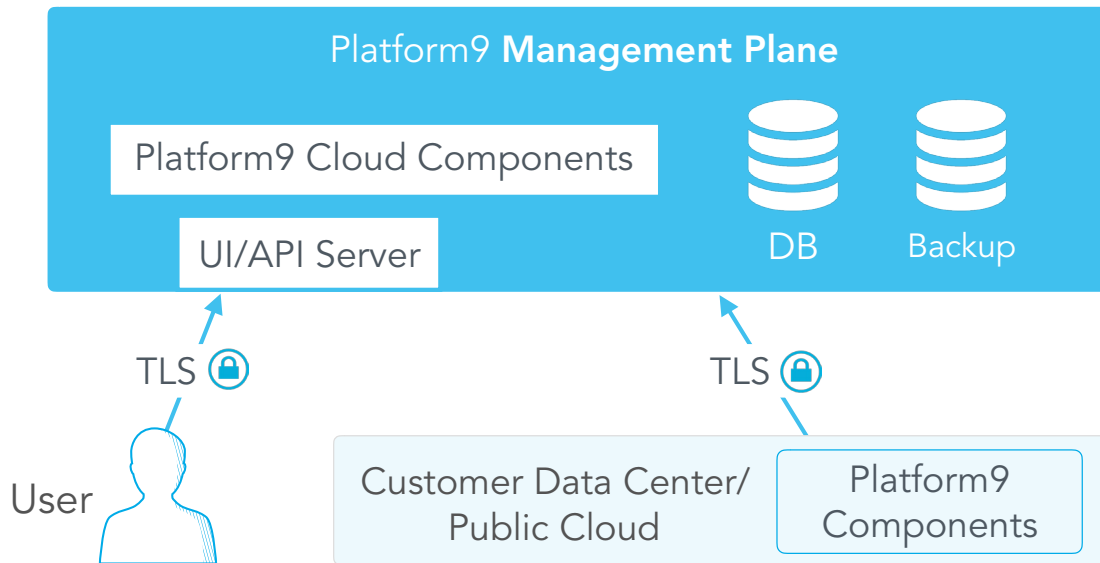


For simplicity, the diagram above shows a single management plane and control plane. Each customer has a separate management plane that does not share resources with those of other customers. The agents communicate with the management plane over a secure TLS channel.

Platform9 Managed OpenStack compute, block storage, and network nodes can be deployed on-premises or in a colocation facility. Using the OpenStack Omni project, the Platform9 management plane can also natively interact with public cloud APIs to provision, deprovision and manage public cloud infrastructure. Other deployment options include KVM-based or VMware-based virtualization and bare-metal servers. When a customer decides to onboard Platform9 Managed OpenStack, the control nodes will be deployed by the management plane in the Platform9 hosted cloud. Once deployment is complete, administrators can provision compute, network, and storage nodes that can then be leveraged by end users for VM-based or bare-metal based workloads.

Product Security

The diagram below highlights key components of the Platform9 network architecture.



The Platform9 management plane, consisting of the Platform9 cloud components, database and backup services, are accessed by both end users and customer data centers. End users can access the Platform9 UI (Clarity) and Platform9 API server. Also shown at the bottom of the diagram are customer data center/public cloud OpenStack hosts and Kubernetes nodes. These sets of infrastructure communicate using TLS v1.2 encryption with the Platform9 cloud components in the management plane.

In order to manage a client's Kubernetes worker nodes or OpenStack hosts, Platform9 uses management planes that reside in the hosted cloud. Each management plane consists of cloud management services deployed for a Platform9 customer. All management environments are centrally managed by Platform9 and are not shared amongst customers.

Authentication and Authorization

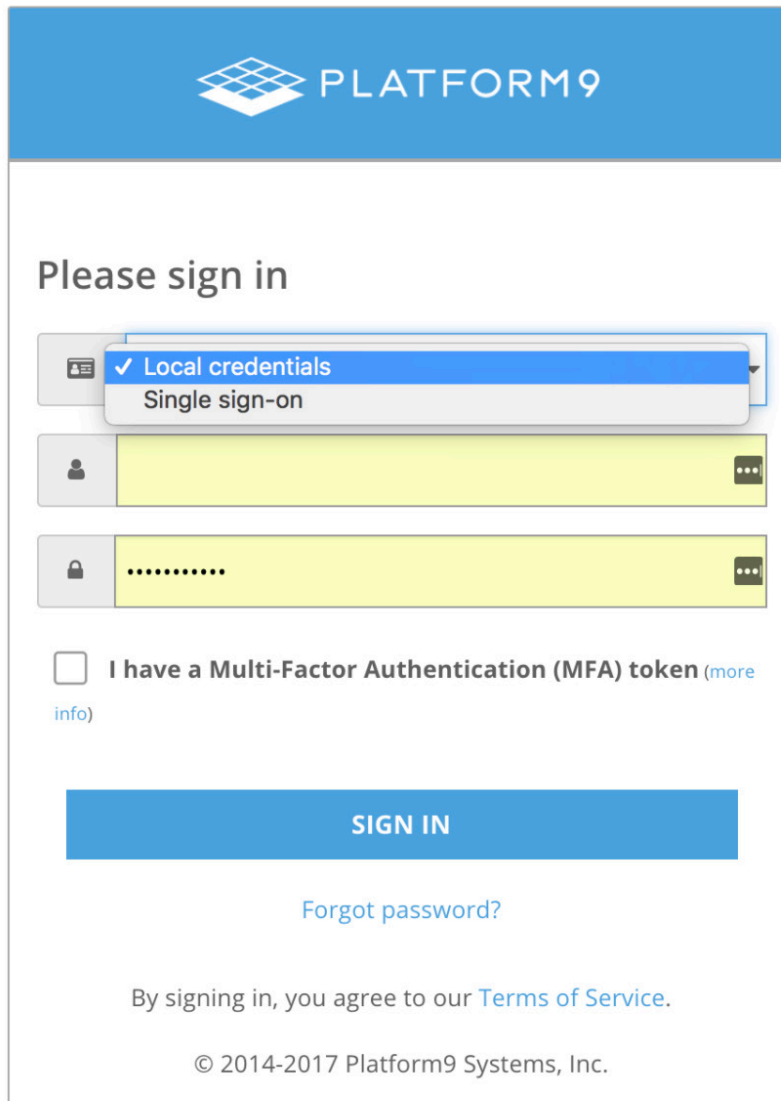
HTTPS connections are used for browser-based access to and communication with Platform9. TLS v1.2 is negotiated with client browsers. Each customer is provisioned to his/her own unique subdomain (ex. customer1.platform9.net).

Customers authenticate to Platform9 with a username and password. After successful authentication, they are provided with a token which is used for subsequent API requests. The token is also sent encrypted and it provides details about the user and user permissions. The Platform9 management plane allows or denies requests by a user or administrator based on their assigned role, and permissions. Lifetime of the token is typically 24 hours, but it can be adjusted based on the security requirements of the customer.

The following sections provide details on authentication with local credentials, SAML-based credential authentication, and the permissions model.

Local Credentials (Password-based Authentication)

In password-based authentication, users login to their Platform9 environment through a dedicated subdomain, such as customer1.platform9.net. Platform9 encrypts customer passwords with a high number of rotations using the SHA512 algorithm.



The screenshot displays the Platform9 login interface. At the top, the Platform9 logo is centered in a blue header. Below the header, the text "Please sign in" is prominently displayed. A dropdown menu is open, showing two options: "Local credentials" (which is selected and highlighted in blue) and "Single sign-on". Below the dropdown, there are two input fields: the first is for the username, and the second is for the password, both with yellow backgrounds and masked with dots. Below the password field, there is a checkbox labeled "I have a Multi-Factor Authentication (MFA) token" with a link to "more info". A large blue "SIGN IN" button is positioned below the form. Underneath the button, there is a link for "Forgot password?". At the bottom of the form, a line of text states "By signing in, you agree to our Terms of Service." and a copyright notice "© 2014-2017 Platform9 Systems, Inc." is at the very bottom.

Single Sign-On Support

SAML, or Security Assertion Markup Language, is an open standard for exchanging authentication and authorization information between an identity provider and service provider (Platform9). Platform9 supports integration with SAML identity providers such as Okta, OneLogin, Microsoft ADFS, Azure Active Directory, and others. Enterprises can have a single login policy (such as MFA token, password length/complexity) across all applications. SAML also alleviates the need for adding/ updating/removing individual users on Platform9 portal.

MFA (time-based one-time password): Platform9 supports use of time-based one-time password (TOTP).

Robust, Extensible Permissions Model

Platform9 uses a role-based permissions model. This model has users and administrators.

- **Self-Service Users:** These users have limited access within the customer environment. A self-service user has access to images that the administrator has shared. A self-service user can create new instances using images, flavors and networks on the infrastructure available to their tenant. A user cannot control resources that belong to other tenants/projects.
- **Administrators:** These users have access to all operations within the customer environment.

Role-based access for Kubernetes was only introduced in v.1.8 (October 2017). Platform9 Managed Kubernetes does not include RBAC currently, but will support it in 2018.

Architectural Security

The Platform9 product has been architected with security in mind. Platform9 services hosted by the management plane are accessed using REST APIs that are secured by TLS. Each API request is also validated through an authentication token, which is sent over the encrypted connection. This ensures that only those authorized to view and modify a particular customer environment are able to do so. It is impossible for a customer to gain control of another customer's environment without gaining possession of an unexpired token from the other customer.

Binary communications, such as AMQP, which are used by some datacenter-side Platform9 components (e.g. nova-compute) are secured using 2-way TLS certificate authentication.

Metadata

Platform9 only receives a limited amount of metadata from agent software installed on customer hosts/nodes. Only the following metadata is collected:

- **For Kubernetes environments:** Host server's operating system, memory, cpu, storage, network and virtual machine attributes (usage and capacity).
- **For Linux/KVM environments:** Host server's operating system, memory, cpu, storage, network and virtual machine attributes (usage and capacity).
- **For vSphere environments:** Datastores, clusters, hosts, and virtual machine attributes (usage and capacity)

The Platform9 management plane does not receive data from running or offline virtual machines, or any other data from hosts.

TLS with Mutual Authentication

Mutual authentication using TLS v1.2 is required for communication between the agent software and Platform9 management plane. Each Platform9 management plane has its own unique, self-signed root certificate authority. This certificate authority is used to generate 2048-bit keys that are in turn used to secure all communications between the management plane and agent software which communicates with it. Both the management plane and any agent software (including host agent, OpenStack agent, and Kubernetes agent) use these keys to mutually authenticate via TLS. This mechanism ensures that other customers cannot mistakenly or maliciously access instances or data in another customer's environment.

Elimination of Open Ports

The Platform9 management plane or any software therein does not initiate a network session into customer hosts. Authorized agents that are installed on hosts initiate a bi-directional channel to the management plane using outbound TLS connections. Attack surface area is limited since customers are not required to open ports to enable communication with Platform9's management plane.

Restricted Access User

Platform9's on-premises components run under a dedicated Unix user account as user "pf9," and group "pf9group." The set of "sudo" privileges required by this user are well documented and can be requested from Platform9.

Code Signing

Platform9 software packages for upgrades, patches, or host reconfiguration are scheduled during maintenance windows defined by each customer. These software packages are cryptographically signed to ensure that the author is Platform9, and no changes have been made by third-parties.

Operational Security

The following list outlines some of the measures Platform9 takes in order to maintain a secure environment for our customers:

- **Isolated customers:** No two customers of Platform9 share a management plane.
- **Virtual firewall:** Customers can restrict access to the management plane by specifying one or more allowable source IP networks.
- **Monthly updates:** The management plane, OpenStack and Kubernetes nodes are patched for security updates regularly. Updates are pushed monthly to include the latest security patches. Critical vulnerabilities are addressed and patched within 3 days.
- **Encryption at rest:** Platform9 performs regular backups and all backups are encrypted.
- **Physical security:** Platform9's server equipment is secured in a Tier 3 data center and access is provided only to authorized employees. Employees develop software using computers with strong passwords and encrypted disk storage in case of loss or theft.
- **Datacenters:** Platform9 uses a well-known hosted cloud provider to host customer production environments. These environments are configured for multi-geographical availability in case of a disaster or other outage in any specific geography.
- **Incident response:** If despite all other protection in place, customer data is accessed without authorization, Platform9 will notify you. If personal information about customers is breached from Platform9, we will notify customers in accordance with California Law (California Civil Code Section 1798.29 and Section 1798.82).

Secure Operations

Access to the management plane is only permitted from the Platform9 secure network and is restricted via firewall rules.

Authentication to management plane servers is done using SSH key-based authentication. As part of the public-private key pair, a private key is generated by each employee. Each employee utilizes his/her own public-private key pair and keys are not shared. All access to the management plane is audited.

Root access is extremely limited in the management plane environment. Permissions to the environment are controlled and access is given to users on an as-needed basis.

Wireless networks are not used by production systems that run the management plane. Within the Platform9 premises, wireless networks secured with WPA2-Enterprise are limited to employees and used only for desktop connectivity.

Secure Development

Platform9 uses the Agile methodology for software development and testing. Systems and applications used for development are regularly patched to remove security vulnerabilities. Platform9 uses a distributed version control system that is gated by public-private key-based authentication system. All changes are tracked and audited and are only committed after multiple peer code reviews and extensive testing.

In the distributed version control system, repositories are controlled on a per account basis. Each team has access to repositories that cannot be accessed externally and updates are cryptographically signed. This implies that any change in code is done as a new update, i.e. it is impossible to commit in the past and without breaking subsequent code changes. By using such a system, the repository is updated linearly based on peer reviews and automated checks.

Secure Customer Data

Platform9 employees are subject to the following access controls:

- Only a limited set of employees have access to customer accounts. These include limited members of our DevOps team and senior engineering management only.
- Customer support engineers are given access to a customer account on a “lease” basis when needed. Further changes are being worked on lease based access for ALL users.
- Access to customer accounts is audited.
- Physical access to servers that hold customer data is secured in a facility which is monitored 24x7.

Platform9 has implemented a layered security model, to help mitigate security issues:

- Each customer account is separately maintained.
- New TLS certificates are generated for each customer.
- Platform9 uses code signing and all components installed on customer premises are signed by Platform9 keys. So malicious code cannot be installed through Platform9.
- These code-signing keys are kept separate from customer accounts. In the event a customer account is hacked, no new malicious component can be installed by the hacker.
- Platform9 on-premises components runs as user ‘pf9’ which has limited and published set of sudo privileges.
- In the event that Platform9 finds evidence of a compromised cloud controller, the cloud controller instance is terminated.

Protecting Against Web Application Attacks

Web Application attacks can include cross-site scripting (XSS) and SQL injection attacks.

Cross-Site Scripting (XSS) attacks inject malicious scripts into benign and trusted web sites. Platform9 UI uses trusted frameworks like Angular.js that work to perform the necessary escaping of the user input and avoid cross site scripting.

SQL injection attacks can be used to gain unauthorized access to a database. Platform9 and other open source frameworks use different libraries to sanitize the user input along with libraries that take care of properly formatting the data before it is submitted to database which mitigates these attacks.

Vulnerability Assessments

Platform9 performs vulnerability assessments on a periodic basis. The vulnerability scans are done using Tenable's [Nessus Vulnerability Scanner](#). These scans are periodically executed for each of Platform9's customer environments. Additional scans are performed upon product releases and product upgrades.

Key Management and Passwords

Platform9 uses mutual TLS authentication (certificate-based mutual authentication). This process uses certificates to establish an encrypted channel and bidirectionally authenticate the Platform9 management plane and the customer's hosts. Platform9 rotates public key certificates every 12 months and when requested by the customer.

Access to the management plane is controlled through the use of SSH keys, and password authentication is disabled. Only a small number of individuals in the Platform9 DevOps team and management have access to the management plane.

Secure Hiring Practices

Platform9 conducts background checks for criminal history, which identify those that may be sex offenders, as well as those on global watchlists, and those with national, and county, criminal records. In the case of positions that require extensive driving, DMV history checks are also performed. These checks ensure we are able to make informed hiring decisions. An employee's eligibility to work and identity is also verified using the I9/E-Verify system. All employees are asked to sign a Confidential Invention Assignment Agreement (CIAA) that restricts discussion of knowledge deemed confidential by Platform9. Upon termination, employees return company hardware and physical keys, and their software logins and keys are revoked.

New hires receive in-house training on security best practices. The training is also provided to existing employees on an annual basis. Topics covered in the training include:

- Architectural security practices
- Operational security practices
- Security code review practices
- Process around incidents
- Desktop and personal security practices

Other Security Practices

Information Security Policy

Platform9 has an information security policy with assigned owners in the Information Security function that has been approved by management. These policies are reviewed every 12 months and include guidelines such as:

- External parties must not have access to scoped systems and data processing facilities
- Firewalls are used for internal and external connections, and working as desired
- Vulnerability scans and test results of internal and external networks are performed periodically
- Security related logs are monitored for configuration changes, access attempts, and other events
- Ensure that VPN access and IP whitelisting have been properly enforced
- Proper precautions are taken to ensure that application instances and database instances are not shared with other clients
- Encryption keys for clients are rotated when requested

Physical Security

Platform9 ensures physical security on-premises and in the management plane in the hosted cloud through the following ways:

- The Platform9 corporate premises is secured using electronic alarm systems, surveillance cameras, and electronic key entries.
- Server rooms are secured using surveillance and periodically rotated entry codes.
- The use of removable disks such as tapes, disk drives, USB drives, CDs, and DVDs is strictly controlled.
- All data residing on Platform9 employee workstations is encrypted.
- Records retention policies covering paper and electronic records, including email, in accordance to contractual agreements, regulations, and standards.
- Customer management planes are created through an automated process. Platform9's datacenters are protected by security staff, two-factor authentication systems, video surveillance, intrusion detection systems, routine logging and auditing. Access to data centers is only provided to active employees and contractors with a legitimate business need. Access for terminated employees is immediately revoked.

Network Security

The management plane, hosted in Platform9's cloud, provides the safeguards against the following attacks:

- Port scanning: Strict access rules are enforced by the management plane. These access rules only allow incoming connections to ports 80 and 443. Platform9 provides the option for customers to lock-down their environment further so that access is only provided to specific IP addresses.
- Packet sniffing: It is impossible for a Platform9 customer to "sniff" another customer's packets. Each customer is deployed in a separate management plane, or virtual cloud, that consists of dedicated instances, networks and access rules. The Platform9 hosted cloud provides further security that prevents a virtual machine from sniffing traffic that has been intended for another virtual machine.
- Distributed denial of service attacks (DDoS): The Platform9 hosted cloud has significant expertise in ensuring uptime for SaaS-based services, and protects against DDoS attacks through the use of several specialized mitigation techniques.

Compute Security

Instances within the management plane use hardened operating systems, firewalls that permit incoming connections only on ports 80 and 443, and signed API calls using session tokens.

Management Plane Security


The hosting provider does not have access rights to Platform9's compute instances in the management plane. Multi-factor authentication is enforced for operations team at Platform9 access to the management plane, and all logins are logged and monitored.

Disaster Recovery by Public Cloud

Each customer account resides in Platform9's management plane in a Platform9 administered cloud that can provide protection against disasters.

High Availability and Disaster Recovery

Platform9 monitors individual services and system connectivity. A single failure in an environment will not be noticeable by its customer, and Platform9 has home-grown monitoring tools to detect and alleviate such issues.



In the event of multiple cascaded failures, Platform9 adheres to a 99.9% uptime guarantee while ensuring that the customer's operational environment is not affected:

- The customer's virtual machines, storage and network components continue to function without interruption.
- An email notification is sent to the customer and remediation steps are taken.
- Platform9 uses backups, if needed, to recover the environment.

Platform9 takes the following measures to protect customer data and recover from backups, if necessary:

- Database replicas and snapshots: Database replicas are created in multiple availability zones. Continuous backups of the database, using point-in-time snapshots, enable the Platform9 operations team to recover customer data from the failed environment.
- S3 backups: Object storage is used for daily backups of the database. These backups span multiple regions and can be used in the event that a region becomes inaccessible.

Least Privilege Access Policy

Platform9 tightly controls access to the management plane, wherein customer data is contained. In addition, different accounts are used for development and production environments. Production environments are restricted to Platform9's operations team and access to support individuals is given on a lease basis, which expires after the necessary work is complete.

Privacy Policy

Guarding user's privacy and that of their business data is paramount, and we work hard to protect user information from unauthorized access. Our [privacy policy](#) is available along with our [terms and conditions](#).

Conclusion

Platform9's Managed Kubernetes and Managed OpenStack product is built with security in mind. Through the use of TLS v1.2 encryption and mutual authentication, end users can securely access the Platform9 Clarity UI and the Platform9 APIs. Other product security features include, but are not limited to, secure single sign-on capability, multi-factor authentication, and roles and privileges.

In addition to product security, Platform9 enforces secure operational practices such as restrictions to management plane access, vulnerability assessments, secure key management/passwords, and secure hiring practices.

Product security and operational security measures complement other practices such as maintaining an Information Security Policy that is reviewed and updated every 12 months, ensuring physical, network, compute and management plane security, and enforcing a least privilege access policy within Platform9.

Securing our customers' data is paramount at Platform9. For further questions regarding security practices, please contact us at info@platform9.com.