IronDefense in the Cloud: Security Controls and Access

Introduction

IronNet is dedicated to defending your network from security vulnerabilities that can occur during the daily workflow. Security controls such as traffic encryption, access control lists (ACL), and more are in place to prevent insecure or unauthorized transfer of customer data. This document describes how IronNet keeps your data secure in our cloud deployment via infrastructure, data protection, logging and monitoring, user access, and multi-tenancy.

Infrastructure

Each IronNet cloud deployment receives its own account. This means that Identity and Access Management (IAM) and security policies, such as access controls and security keys, are not shared between IronNet customers but are instead kept separate to ensure users only have access to their organization's data.

Each IronDefense deployment also has a virtual private cloud (VPC) or virtual private network (VPN) with access control list rules that are only open to your organization's IP space and IronNet's IP space. This is to protect your organization's privacy and ensure only authorized users can access your data.

Data Protection

Data in Transit

Communication is encrypted within IronDefense, which is hosted in a cloud account. All communication from the customer network to IronDefense is encrypted as well.

Data at Rest

Our cloud storage system utilizes best practices to secure customer data. Each customer has a unique bucket or object store. IAM credentials are required to access all data, and access is restricted to only nodes and applications that need it. Similarly, access to the instance's storage is only given to authorized applications.

Logging and Monitoring

IronNet uses cloud provider security best practices, including notifications when changes are made to security policies, such as when a new user is added to the environment. This security policy generates logs for all resources created and all changes made. Log files are then aggregated to a centralized location where IronNet's Cyber Operations Center (CyOC) monitors them for suspicious activity and reviews them for audit purposes.

User Access

IronNet Admin Users

To perform administrative actions, IronNet has a select group of admin users who can access IronDefense instances and services. However, a number of controls are in place to ensure only those who need access have it. For example, in order to SSH to a host in IronDefense, the user must have SSH keys and access the host from an IP space that has been whitelisted, such as IronNet HQ or VPN.

IronNet and Customer IronVue Users

IronDefense's access management system organizes users into groups with customized role-based permissions. This provides a flexible and powerful means to enable user workflows while enforcing the principle of least privilege. A user's access to pages, components, and functionalities in IronVue is contingent upon the user's group memberships and the roles associated with those groups. The role-based access control (RBAC) approach provides a more efficient way for administrators to manage access than can be achieved with per-user permission assignments.

Your organization can also manage password policies in IronVue to comply with corporate guidelines. IronVue allows Super Administrators to set a variety of password characteristics, such as the number of days before a password expires, the number of failed login attempts allowed before a user is locked out, and various criteria a password must meet, such as number of digits and special characters.

Multi-tenancy

IronNet understands the need for strong security in multi-tenant infrastructure. To preserve best practices and provide data security for your organization, each customer has its own unique account and a VPN which creates a secure repository for customer data.

All customer data is single-tenancy for both database (flows and users) and file system. The credentials needed to access customer data are generated at the creation of the deployment and isolated from other customer accounts.

Compute resources may be shared by physical machines, but this is managed by the cloud provider, not IronNet. IronDefense applications are run in Docker containers in a customer-specific cluster, but individual IronDefense instances are kept separate from other customers.

What Data Leaves Your Network

There are a few different types of data that leave your network, including metadata, logs, metrics, and (on user request) PCAP. In this section, we will describe why and where this data is needed and how it is securely transmitted from your network to the cloud.

IronDefense sensors, called IronSensors, process PCAP and create metadata called IronFlows. IronFlows are streamed to the cloud. Raw PCAP is stored on the sensors themselves for retrieval later. When a user requests details on a specific IronFlow, the PCAP is retrieved from the sensor and securely transmitted to the cloud back-end to render and download from IronVue. Requested PCAP is retained for one hour on the back-end before being removed. The ability to get flow details and download PCAP is enabled or disabled for users using role-based access controls.

If your organization has elected to do so, your IronSensors can also be configured to forward logs (e.g., DHCP, Proxy) to the cloud for processing and enrichment. Logs can help IronNet gain a better understanding of your network to better defend it against potential attacks.

IronDefense's Health and Monitoring service, IronMon, transmits performance metrics to the cloud to help diagnose problems and track usage. IronMon also sends health alarms to IronNet to ensure product availability. No customer-specific data is shared during these communications.

Data sent to CloudConnect and IronDome follow the same configuration as IronNet's on-premise offerings. Please refer to *CloudConnect Orchestrator for IronDefense* and the IronDome Product Brief for more information.