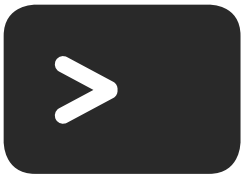
Terminal

Elegant, Fast Software Defined Datacenters



This paper is intended to provide insight into the reasons for developing a new Cloud Computing product and the competitive differentiation of such offerings. After reading this paper, you should understand the contrast between traditional and Terminal Computing systems.

Terminal Private Software-Defined Datacenter

Enterprises demand more from their service than traditional users but their needs are ill-matched to existing products. Today, Cloud provisioning is outside of Enterprise control, Policy is executed in a haphazard manner and Applications run unsecured by design.

Terminal was designed to address these concerns. Terminal delivers a new kind of Virtual Machine (called Terminals) that are full Linux computers with bare-metal performance.

After much effort, the Terminal Research team identified three areas of operational concern for Modern Enterprises.

- Fast, On-Demand Computing
- Centralized Security Policy
- Automatic Disaster Recovery

The solutions presented here today are proprietary Terminal designs and are provided by Terminal as a service to its customers. After reading this paper, you should understand the differentiation between existing industry solutions and Terminal design patterns.

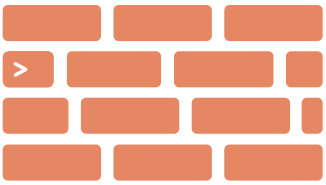
On-Demand Computing

Today, provisioning of virtual machines on public clouds can take anywhere from a few minutes to multiple days. The Enterprise has no direct control over the infrastructure and is entirely reliant on operator staff for support, who may not be available or equipped to provide service. Frustrating IT staff further is the inability to onboard and offboard new workloads through a consistent web-accessible interface.

Terminal is a different kind of cloud, one that provisions your machines in less than five seconds exactly to your specifications.

Terminal features on-demand provisioning accessible through a web dashboard. Simply choose the size of your machine and a base image and go. No more waiting for someone else to provide you with equipment or for slow provisioning systems to turn your service on. Just click a button and your machine is online, it's that easy.

Competitive differentiation: Terminal provides a web dashboard with provisioning controls that provision new machine in less than 5 seconds.



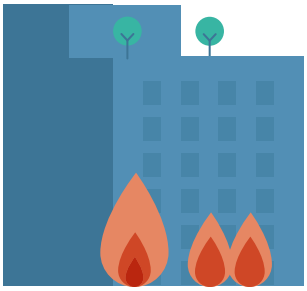
Centralized Policy

Security is a hard task for Enterprise IT organizations. Most solutions are difficult to maintain, require specialized training and are prohibitively expensive. Role-based policy and explicit security are actually hard things to deliver, but Terminal provides best-in-class security easily and quickly.

The Terminal solution is to integrate Policy control directly into the cloud and present centralized control through a web dashboard without additional hoops to jump through. With a few clicks, propagate policy settings to every machine for applications like Network Access Control, Firewall and Single Sign On.

Competitive differentiation: Terminal provides a web dashboard with policy controls that automatically propagate in just a few clicks.

Automatic Disaster Recovery



Things break. When things break, it's important that systems return to normalcy as quickly as possible. Terminal provides automatic disaster recovery so you never have to say "sorry" again.

Using Terminals proprietary snapshot technology, users can create RAM-perfect copies of their systems at any time (even while the system is running). This snapshotting can be scripted so that it occurs on every update to the filesystem. Since snapshots can be booted in less than 5 seconds, if a machine fails because of an application error, the most recent snapshot can be brought online almost instantly. Best of all, since the snapshots are RAM-perfect, the recovered image doesn't require you to recover state. All of the processes that were running pick up exactly where they left off.

Competitive Differentiation: Terminal has the best backup and recovery setup in the industry because of RAM-perfect snapshots.

Data Center Architecture

This section discusses Terminal's unique approach to Data Center architecture. Terminal's easy-to-use interfaces are backed by an infrastructure working behind the scenes to ensure fast, reliable service that works automatically with minimal action on the part of end users. To make that happen, we're continually evolving our product and architecture to speed data transfer, improve reliability and adjust to changes in the environment. In this section, we'll explain how your services are delivered, processed and managed securely.

DISTRIBUTED STORAGE

The Terminal approach begins with a reimagining of how cloud architectures should be designed. Terminal has tried to design a cloud that automates almost all aspects of operations, provisioning and disaster recovery. To this end, Terminal has implemented a number of strategic technological decisions.

Specifically, one of the technical achievements Terminal is most proud of is the development of a custom virtual file system that is distributed, rack-aware, and fault-tolerant. This file system shares RAM and Disk across virtual hosts on the same machine and includes both RAM and Disk deduplication. This file system also permits the migration of Terminals across physical servers without performance penalty.

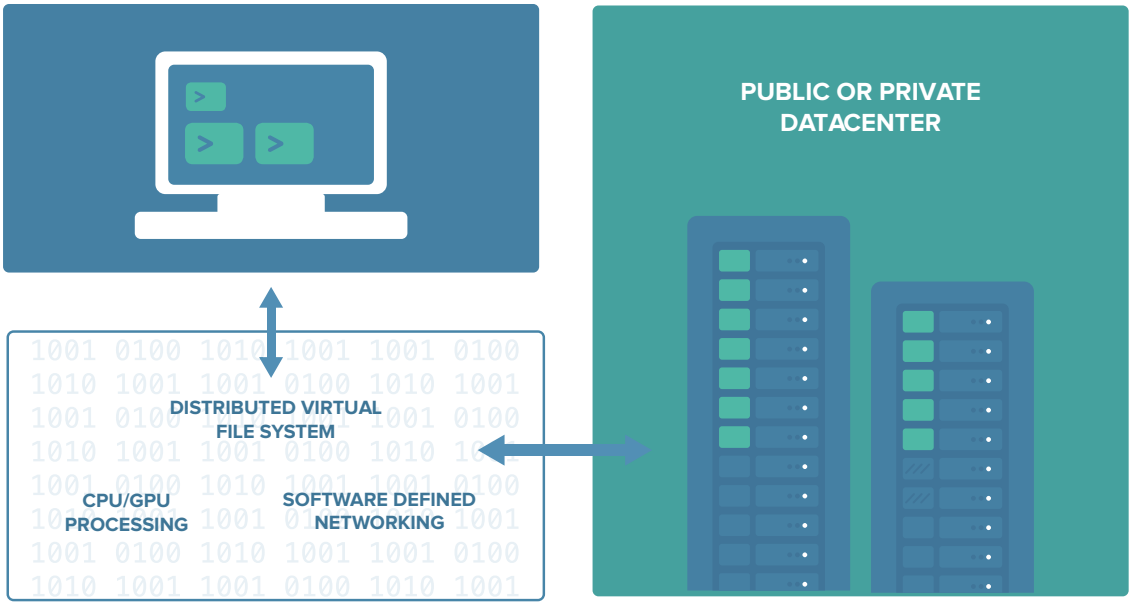
Since migration does not mute a users ability to use their Terminal, the backend can simply migrate the user across servers to ensure optimal use of available resources. When a user requests a Terminal, the entire cloud rebalances to give that user the resources they want in the most optimal fashion, and all of this takes place automatically and without performance penalty.

SOFTWARE DEFINED NETWORKING

Terminal operates a proprietary software defined network that covers enterprise applications end to end. Towards that effort, Terminal exerts control over multiple aspects of the experience. Terminal provides an extremely fast virtualized network layer that allows provisioning of rules-based access policy quickly and easily. The network is secure, fast and fault-tolerant.

Each Terminal can receive exactly the network configuration it needs for its workload, automatically. Access policy can be configured from both the command line and the web interface and deployed across the entire infrastructure in just a few clicks.

Terminal features a programmable IP access management layer that can integrate with any number of deployment tools from Ansible to Chef.



SNAPSHOTS

One of Terminal's key technologies is the snapshot. Snapshots are RAM-perfect copies of a Terminal at a specific instant in time. Snapshots can be stored in geographically diverse locations, and can occur as often as a user might like. Snapshots can be used to create new Terminals that begin at the exact state of the snapshot. This includes Datasets already loaded into Memory, processes running at the time of the snapshot, and any other data cached in the RAM.

By leveraging the programmatic nature of snapshots, users can create a disaster recovery environment that is perfect up to the last change in the file system. That is to

say that the worst case in the event of a catastrophic datacenter failure is to restore to the last change in the file system.

Some of the use cases we have seen for Snapshots include:

- Distributing an Application package that is secure, ready for production and customized for a specific workload
- Deployment of any number of machines in parallel across any number of heterogeneous public or private datacenters
- Loading a data analysis application with the dataset already in memory
- Rolling back a database to the last change very quickly

Snapshots are the best way to protect and manage your applications.

Terminal Datacenter Design

Terminal's key competitive differentiation stems from the Terminal cloud, a set of of interconnected server environments designed for reliability and efficacy. This cloud is tightly connected to infrastructure which allows Terminal to provide secure, fast and responsive computing environments. The Terminal cloud can be deployed in public, private or hybrid cloud environments and automatically scales when new hardware is introduced.

Terminal operates datacenters which contain application servers which provide the following services:

- Distributed Storage and Memory
- Compute and Graphical processing
- Software-defined Networking

These servers are connected over a fast, low-latency network typically running at 10 gigabits per second, and leverage rack-aware design functionality to always target the closest resources for consumption. This provides more security and latency guarantees than might otherwise be available. Terminal's datacenters automatically scale, heal and perform better than any other cloud in the industry.

Terminal only hosts in datacenters that are Tier 4, SAE-16 certified and managed by global partners.

Reliability

A cloud is only as good as it is reliable, and to that end, we've developed Terminal with multiple layers of redundancy to guard against connectivity loss and ensure availability. By positioning Terminal in multiple discrete world-class datacenters, Terminal gains geographic diversity, performance reliability and consistent availability. Redundant copies of all configuration information are distributed across independent devices within a datacenter with an N+2 availability model. Backups of all changes to configuration files are saved hourly and incrementally.

Constant load balancing across multiple servers ensures redundancy and a consistent user experience for the end user.

Product Features

This section describes the specific product features Terminal brings to bear for its customers. After reading this, you should have a concrete understanding of Terminal security practices, customer offerings and detailed service management controls.

The Terminal service can be utilized and accessed through a number of interfaces. Each has security settings and features that protect user data while ensuring ease of access.

- Web: This interface can be accessed through any modern web browser. It allows users to managed, configure and control their devices.
- Command Line: Terminal supports full SSH connections to the Terminal cloud which function just like your existing local machine.

Our security team performs automated and manual application security testing on a regular basis to identify and patch potential security vulnerabilities and bugs. We also work with third-party security specialists, as well as other industry security teams and the security research community, to keep our applications safe and secure.

ADMIN MANAGEMENT FEATURES

As no two organizations are alike, we've developed a number of tools that empower admins to customize Terminal to their team's particular needs. Below are several key control and visibility features available via the Terminal admin panel.

Controls

- User provisioning methods
    - **Email Invitation** - A Tool for generating manual invitations to the platform
    - **Active Directory** - Administrators can automate the creation and removal of accounts from an existing active directory system. Once integrated, Active Directory can be used to manage membership.
    - **Single Sign On (SSO)** - Terminal can be configured to allow team members

access by signing into a central identity provider. Our SSO implementation, which uses the industry standard SAML (Security Assertion Markup Language), makes life easier and more secure by placing a trusted identity provider in charge of authentication giving team members access to Terminal without an additional password to manage.

- **Password Reset** - As a proactive security measure, admins can reset passwords for the entire team or on a per-user basis.

Visibility

- **User Activity Reports** - Terminal admins can generate activity reports at any time for several types of events, filtered by date range. Reports are available for individual users or entire team accounts and can be downloaded in CSV (comma-separated values) format for analysis with SIM/SEM (Security Incident/Event Management) tools. The following information is available to admins in user activity reports.
  - **Passwords** - Changes to password or two-step verification settings. Admins do NOT have visibility into users' actual passwords.
  - **Logins** - Successful and Failed logins to the Terminal Website and Enterprise Applications
  - **Admin actions** - Changes to settings in the admin console such as application permissions
  - **Devices** - Linking of Computer, Tablet and Mobile Devices to a Terminal account
  - **Membership** - Additions to and Removals from the team.
  - **Usage** - Per machine usage reporting
- Technical Support identity Verification - Before any troubleshooting or account information is provided by Terminal Support, the account admin must provide a one-time use, randomly generated security code to verify his or her identity. This PIN is only available through the admin console.

USER MANAGEMENT FEATURES

Terminal also includes tools for end users to further protect their accounts and data. The authentication, recovery, logging, and other security features below are available through the various Terminal interfaces.

- **Two-Step Verification** - This optional -- but highly recommended -- security feature adds an extra layer of protection to a users Terminal account and Enterprise applications. Once two-step verification is enabled, Terminal will require a six-digit security code in addition to a password upon sign-in or when adding a new device.
  - Account administrators can track which team members have two-step verification enabled.
  - Terminal two-step authentication codes can be received via text message or with the Terminal secure login application (or other apps which conform to the Time-Based One-Time Password (TOTP) algorithm standard. In the event a user cannot receive security codes via these methods, they may opt to use a 16-digit one-time-use emergency backup code.

    - Once a user enables two-step verification, admins can mandate that they keep it enabled on their accounts. Additionally, admins can generate a reminder email for all users with the service disabled, prompting them to enable it.
- **Password strength estimator** - Accessible to all users when they create an account or change their password, the password strength estimator helps users generate a secure password for individual account protection.
- **Terminal User Dashboard** - Tevnos users receive access to the Terminal User Dashboard, a one-stop web application for managing all of their Tevnos devices and policies. A user can provision new equipment, disable old, lost or stolen equipment, and get a quick overview of their monthly usage.

Terminal Information Security

Terminal has established an information security framework and regularly reviews and updates security policies, provides security training, performs application and network security testing, monitors compliance with security policies, and conducts internal and external risk assessments.

OUR POLICIES

We've established a thorough set of security policies covering the areas of information security, physical security, incident response, logical access, physical production access, change management, and support. These policies are reviewed and approved at least annually. Employees, interns, and contractors are notified of updates to these policies, as well as ongoing security training, by email and/or via our security policies intranet page.

- **Information Security** - Policies pertaining to user and Terminal information, with key areas including device security, authentication requirements, data and systems security, employee use of resource guidelines and handling of potential issues.
- **Physical Security** - How we maintain a safe and secure environment for people and property at Terminal.
- **Incident Response** - Our requirements for responding to potential security threats, including assessment, communication, and investigation procedures.
- **Logical Access** - Policies for securing Terminal systems, user information and usage information covering access control to corporate and production environments.
- **Physical Production Access** - Our procedures for restricting access to the physical production network, including management review of personnel and de-authorization of terminated personnel.

- **Change Management** - Policies for code review and managing changes that impact security by authorized developers to application source code, system configuration and production releases
- **Support** - User metadata access policies for our support team regarding viewing, providing support for or taking action on accounts.

EMPLOYEE POLICY AND ACCESS

Employee access to the Terminal environment is maintained by a central directory and authenticated using a combination of strong passwords, passphrase protected SSH keys and OTP tokens. For remote access, we require the use of 2-Factor authentication (SSL/VPN) and any special access is reviewed and vetted by our security team.

Access between networks is extremely limited to the minimum number of employees and services. For example, production network access is SSH key-based and restricted to engineering teams requiring access as a part of their jobs. Firewall configuration is tightly controlled and limited to a small number of administrators. Terminal Network connections in external datacenters are governed under tightly controlled secure agreements with potent onsite physical authentication practices.

NETWORK SECURITY

Terminal diligently monitors and maintains the security of our back-end network. Terminal identifies and mitigates risks via regular application, network and other security testing and auditing by both dedicated internal security teams and third-party security specialists. This includes third party penetration testing.

Our Network security and monitoring techniques are designed to provide multiple layers of protection, defense and redundancy. We employ industry-leading security techniques including firewalls, network security monitoring and access control, and intrusion detection systems to ensure only eligible traffic is able to reach our infrastructure.

Terminal' internal private network is segmented according to risk profile and usage. The primary networks are:

- Internet Facing DMZ
- VPN Front-end DMZ
- Production Network
- Corporate Network

Access to the Terminal production network is restricted to only authorized IP addresses. IP addresses with access are associated with the corporate network or approved Terminal personnel. Authorized IP addresses are reviewed on a quarterly basis to ensure a secure production environment. Access to modify the IP list is restricted to authorized individuals.

Strict separation is maintained between Terminal's internal network and the public Internet. All internet bound traffic to and from the production network is carefully controlled through a dedicated proxy service, and those, in turn, are protected by restrictive firewall rules.

These are the same services Terminal offers to its customers and are a great example of eating your own dog food.

Summary

Terminal offers easy-to-use tools to help teams collaborate effectively, without sacrificing the security that organizations require. With a multi-layered approach that combines a robust back-end infrastructure with a customizable set of policies, we provide businesses a powerful solution that can be tailored to their unique needs. To learn more about Terminal, contact our sales team at enterprise@terminal.com.