

WHITE PAPER
July 2024

Security Outcomes with VMware Tanzu® Platform

Table of Contents

Introduction	3
Identify (ID)	3
Asset Management (ID.AM)	3
Protect (PR)	4
Identity Management and Access Control (PR.AC)	5
Figure 1	6
Data Security (PR.DS)	9
Information Protection (PR.IP)	10
Configuration Management	10
Backups	11
Response and Recovery Plans	12
Vulnerability Management	12
Maintenance (PR.MA)	13
Protective Technology (PR.PT)	14
Logging	14
Least Functionality	16
Figure 2	16
Resilience/Availability	17
Detect (DE)	18
Anomalies and Events (DE.AE)	18
Security Continuous Monitoring (DE.CM)	18
Monitoring for Unauthorized Software	18
Vulnerability Scanning	18
Respond (RS)	19
Mitigation (RS.MI)	19
Recover (RC)	19
Summary	20

VMware Tanzu Platform

Learn more about the full capabilities and components of VMware Tanzu® Platform Cloud Foundry: tanzu.vmware.com/platform

Certain outcomes are generally consistent across security teams globally. While the methods used and the completeness and depth of the outcomes will vary greatly by the size of the organization and the sensitivity of the information they store and process, many outcomes are universal. In the U.S., the [National Institute of Standards and Technology](#) (NIST) has created a framework that can help understand and perform evaluations against these common outcomes, called the [Cybersecurity Framework](#) (CSF). Using the CSF, this document reviews how VMware Tanzu Platform for Cloud Foundry (Tanzu Platform¹) helps security teams achieve a number of key outcomes for applications running on the platform. The five core functions captured in the framework are listed below. Organizations should continuously evaluate their application of the functions and the associated activities as part of their effort to address the dynamic cybersecurity risk.

- **Identify** – Understand the organization and its assets to manage cybersecurity risk.
- **Protect** – Implement the people, processes, and technologies needed to prevent cybersecurity events and incidents from affecting critical services or data.
- **Detect** – Develop integrated measures to identify a cybersecurity event or incident and the affected systems, services, and data.
- **Respond** – Prepare and practice measures to contain the impact of an identified cybersecurity incident
- **Recover** – Maintain effective plans to return to normal operations following a cybersecurity incident.

Identify (ID)

The activities in the Identify function are foundational for an effective security program, but many are out of scope for Tanzu Platform as they are focused on understanding the business context of the organization and identifying and managing risks to critical functions and resources. The one area in this function Tanzu Platform assists with is Asset Management.

Asset Management (ID.AM)

Asset Management encompasses the actions an organization would take to have a complete understanding of what assets they have, both physical and virtual/software. This also includes what communications flows exist across the organization, any external systems that are used, how various resources are prioritized, and the identification of cybersecurity roles and responsibilities. Within this, the activities related to inventorying and controlling software platforms and application is enhanced with Tanzu Platform.

1. Due to changes in product and naming, Tanzu Platform is used to refer to Tanzu Platform for Cloud Foundry, formerly Tanzu Application Service. Read more at tanzu.vmware.com/platform.

How Security Is Layered in Tanzu Platform

- Use cloud-native security principles to automate compliance tasks.
- Build automated systems that log every activity; use an operational toolchain that can rapidly patch and update components as new bits become available.
- Embrace immutable infrastructure.

When applications run on Tanzu Platform, the software ecosystem that sits below the application code itself is actively managed by the platform. This starts with the use of a variation on the operations' traditional use of the golden image called stemcells, which are used as the operating system (OS) for the virtual machines used within the platform. As new vulnerabilities are found in the OS or included third-party software, Tanzu updates the stemcells with the latest patches for Tanzu Platform customers. The [Tanzu Platform Overview and Security Policy](#) provides information on how Tanzu rates the severity of patches and the timelines for the release of updated stemcells.

The second layer managed by Tanzu is the runtime container within which the application code runs, this runtime is determined programmatically by the platform using buildpacks. The buildpacks provide a framework and runtime support for apps. When a developer pushes an app to Tanzu Platform, the platform automatically detects an appropriate buildpack which is then used to compile or prepare your app for launch. Because the platform manages the deployment of the stemcells and buildpacks, along with the root file system for the resulting containers, a full component inventory for all software assets currently used in the deployment can be generated whenever needed. This is a much better scenario than needing to run inventory scripts or other mechanisms to collect updated software inventory information across hundreds if not thousands of individual systems.

Protect (PR)

The Protect Function is likely the area people are most familiar with, and over time has been the one where the most money has been invested. At the core, the focus here is on the safeguards an organization should put in-place to ensure the continued delivery of their critical services, limiting or containing the impact of a cybersecurity event or incident. There are six categories in the Protect Function:

- Identity Management and Access Control (PR.AC)
- Awareness and Training (PR.AT)
- Data Security (PR.DS)
- Information Protection Processes and Procedures (PR.IP)
- Maintenance (PR.MA)
- Protective Technology (PR.PT)

Identity Management and Access Control (PR.AC)

Effective identity management and access control is at the heart of any cybersecurity program designed to protect critical assets and services. Ultimately, organizations need solutions that ensure only properly authenticated users, devices, and services/processes can perform authorized actions. Tanzu Platform provides several features that can be leveraged to provide the desired outcomes in this category. To begin with, Tanzu Platform should be integrated with centralized identity systems so access can be granted or revoked from a centralized place. Integration with a central identity platform also allows the use of strong authentication methods. There are three areas within Tanzu Platform where this identity integration should be implemented:

- At the platform level, the identities used by Platform Engineers within OpsMan can be integrated with SAML or LDAP sources. SAML is recommended because when using this integration, authentication is handed off to the SAML provider, allowing the organization to enforce additional authentication controls such as requiring multi-factor authentication (MFA), which is not available using LDAP.
- For developer access to deploy and support applications on Tanzu Platform, users can also be integrated with SAML or LDAP. As with the Platform Engineer identities, SAML is the recommended choice because the Identity Provider can be used to enforce additional authentication controls, as required by organizational needs. Instructions for configuring this integration is covered in the [Configuring Tanzu Platform](#) section of the documentation. If the organization chooses to use the local User Account and Authentication (UAA) system for developer access, the required Tanzu Platform word policies needed to meet typical security or compliance requirements can be set in the [Configuring Authentication and Enterprise SSO](#) tab of Tanzu Platform configuration.
- For the applications deployed onto Tanzu Platform, provide centralized identity services at the application level, so developers do not need to provide an individual authentication mechanism for each application. This centralized identity can be provided using the single-sign-on (SSO) tile. This tile can be deployed using Operations Manager (OpsMan) and integrated with each application as desired. The SSO tile provides SSO integration for applications to a SAML, OIDC, or an LDAP directory. Documentation on the use, deployment, and integration of the SSO capabilities is covered in the [Single Sign-On documentation](#).

Once authentication is handled, the next step is to ensure properly authenticated individuals are only authorized to perform the actions required for their role. To facilitate this need to assign the appropriate level of permissions to individuals based on their role, Tanzu Platform has a Role-Based Access Control (RBAC) system that provides simplified assignment of permissions based on role. Figure 1 shows the multiple levels within the platform where permissions can be assigned.

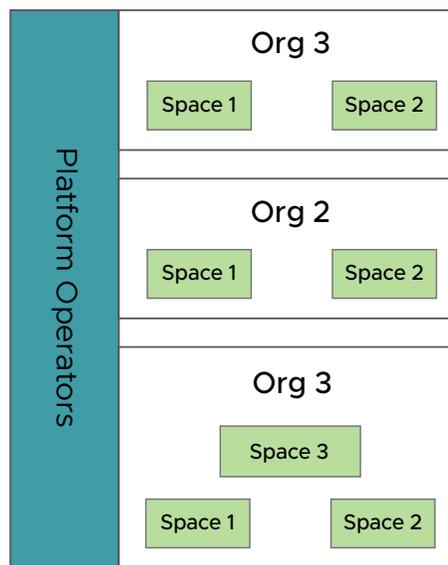


Figure 1: Multiple levels within the platform where permissions can be assigned.

The most fundamental permission layer in Tanzu Platform is the Platform Operators tier. The platform operators are responsible for the day-to-day health of the platform which includes applying updates and upgrades as needed, configuring permissions for developers, and provisioning marketplace services. The platform-level roles apply broad permissions across the platform but do not have permissions within any application orgs or spaces. A detailed list of the platform-level roles and the associated permissions they map to is available in the Tanzu documentation in the section [Configuring Role-Based Access Control \(RBAC\) in Ops Manager](#).

The second permission layer in the system is designed around giving developers the required level of access to deploy applications on the platform. As shown in Figure 1, permissions at this layer are organized into orgs and spaces. Each Tanzu Platform deployment will have at least one org, which in turn has at least one space, with every application and service scoped to a particular space.

An org is a development account that an individual or multiple collaborators can own and use. All collaborators access an org with user accounts. Collaborators in an org share a resource quota plan, applications, services availability, and custom domains. Using the org and space construct provides a flexible permissions structure to meet the unique needs of each organization. For further details on orgs, spaces, and the roles available to developers within each, refer to [Orgs, Spaces, Roles, and Permissions](#) in the Tanzu documentation.

Once the org and space structure is determined, users should be granted access to the orgs and spaces based on their role. Assuming Tanzu Platform has been connected to a centralized identity system, assign the users the appropriate role based on their need following the process for [Adding Existing](#)

[SAML or LDAP Users to a Deployment](#). To facilitate regular reviews of user access, a listing of users and their roles can be generated from the cf CLI or from the [Apps Manager](#) user interface. If the organization has decided to use local user accounts rather than connecting to a central identity service, local users can be managed following the guidelines in the [User Accounts and Communications](#) section of the Tanzu documentation.

Handling authentication and authorization is one major part of the identity story for Tanzu Platform. In addition, the handling of internal secrets is important. The platform requires a number of secrets for platform operation including objects such as the private keys to internal certificate authorities (CAs) and certificates, SSH private keys, and Tanzu Platform words for service accounts. Tanzu uses [CredHub](#) to centralize and secure credential generation, storage, life cycle management, and access for the platform. For those secrets stored in CredHub, the various components of the platform are able to access the needed secrets, without being required to persist them in configuration files or in environment variables.

In a Tanzu Platform deployment, there are two independent CredHub instances deployed. One is the core platform CredHub, often referred to as the BOSH CredHub, which provides a lightweight credential storage instance for the BOSH Director. The BOSH Director, Tanzu Platform, and other tiles store credentials in BOSH CredHub. Additionally, Tanzu Platform deploys an independent CredHub instance on its own VM called the Runtime CredHub. This instance of CredHub is used to store credentials for service instances. When developers want their app to use a service, such as those provided by the Spring Cloud Services tile for Tanzu, they must bind their app to an instance of that service. Service bindings include credentials that developers can use to access the service from their app and these credentials can be stored in the Runtime CredHub instance, providing enhanced security for these service credentials.

The final set of outcomes under Identity Management and Access Control that Tanzu Platform helps with are in the area of network segregation and segmentation. Tanzu Platform provides three main segmentation capabilities that support the need to allow only approved network communications: Application Security Groups (ASGs), Container-to-Container (C2C) Networking, and Isolation Segments.

[Application Security Groups](#) are a collection of egress rules that specify the protocols, ports, and IP address ranges where app or Tanzu Platform instances are allowed to send traffic. ASGs define allow rules, and their order of evaluation is unimportant when multiple ASGs apply to the same space or deployment. ASGs can be applied at the org or space level, but not applied to individual applications. This means that every application within a given space will need to be able to successfully run with the same egress rules. [Istio](#), [Envoy](#), and the [Dynamic Egress](#) feature allow egress rules to be applied to individual applications.

Isolation Segments

Isolation Segments help you address your most important compliance obligations. Once you've created the right level of isolation for your apps, developers and platform engineers are free to innovate with Tanzu Platform as they always have.

While ASGs are egress rules, the Container-to-Container Networking feature provides for ingress rules that enables app instances to communicate with each other directly using an internal overlay network. C2C Networking uses an overlay network to manage communication between app instances. These overlay networks are not externally routable, and traffic sent between containers does not exit the overlay. C2C rules are specified using the source app, destination app, protocol, and port to provide granular control over apps that are allowed to communicate using the C2C network. Refer to [Configuring Container-to-Container Networking](#) for information on how to manage the C2C rules.

The final segmentation capability in Tanzu Platform is called an [Isolation Segment](#). Isolation segments provide dedicated pools of resources (network and compute) to which apps can be deployed to isolate workloads. Using isolation segments separates app resources as completely as if they were in different Tanzu Platform deployments but avoids redundant management components and unneeded network complexity. You can designate isolation segments for exclusive use by orgs and spaces which guarantees that apps within the org or space use resources that are not also used by other orgs or spaces. Customers can use isolation segments for different reasons, including the following:

- To follow regulatory restrictions that require separation between different types of applications. For example, a healthcare company may not be able to host medical records and billing systems on the same machines.
- To dedicate specific hardware to different isolation segments. For example, to guarantee that high-priority apps run on a cluster of high-performance hosts.
- To separate data on multiple clients, to strengthen a security story, or to offer different hosting tiers.

Deploy Tanzu Platform in a way that it's segregated from the rest of the network with a firewall or other filtering mechanism, only allowing access to the applications running on the platform from the larger environment, denying access to management service/ports. With the platform segregated from the rest of the network, implement a [jumpbox](#) or bastion host for platform operators to have SSH and cf CLI access Tanzu Platform, requiring MFA for access to the jumpbox. Only provide accounts to access the jumpbox to platform operators, and require each one use a unique identity. Because privileged account misuse remains a main source of cybersecurity incidents, make sure every single command issued through the jumpbox will be logged and is traceable back to an individual user using a privileged access management (PAM) tool or other audit mechanism.

Tanzu Platform with VMware Tanzu® Data Services

VMware Tanzu® Data Services provide a rich portfolio of secure data solutions that help businesses support the analysis, movement, storage and utilization of data at scale.

Features

- Modern software development platform
- Advanced analytics for innovative insights
- Your choice of storage services from message queuing to a diverse collection of databases
- Robust built-in security
- Business continuity and resilience
- One-click data service provisioning for developers

Data Security (PR.DS)

Tanzu Platform intersects the Data Security category of outcomes in the area of data encryption, for data-at-rest and data-in-transit. Encryption of data-at-rest for the Tanzu Platform starts with the capabilities of the underlying infrastructure. Use virtual disks that are encrypted at the infrastructure layer for Tanzu Platform. This ensures a base level of encryption for all data stored in the platform. The specific infrastructure being used will ultimately dictate how this encryption is configured. Refer to [Disk Encryption](#) for additional details.

In addition to the underlying storage being encrypted, application data stores that hold sensitive data should also have their own encryption mechanisms, to ensure only authorized people and services can access the data. The encryption methods used will vary by the type of data store (relational database, NoSQL database, object storage) and by the type of data being stored (test data, binary objects). Tanzu Platform does not provide any specific capabilities in this area, however, some of the add-on data services available for the platform do. Refer to the documentation for the specific services being used for information on the encryption options available.

Encryption of data-at-rest is one of the areas where CredHub also provides an advantage for the platform. CredHub data is encrypted at rest using a unique key, and the Runtime CredHub can be connected to a Hardware Security Module (HSM) to store the encryption key. This makes sure the secrets stored in CredHub are always encrypted on disk.

For data-in-transit, Tanzu Platform has robust Transportation Layer Security (TLS) capabilities. Ensure TLS is used all the way from the browser/client-side application to the application instance running on Tanzu Platform. There are a variety of ways to configure this depending on the customer's unique infrastructure and requirements. Review the section titled [TLS Connections in TAS for VMs](#) topic in the Tanzu documentation.

Internal to Tanzu Platform, mutually authenticated TLS (mTLS) is used in a number of areas to provide for both authentication and encryption. For example, inbound HTTP/HTTPS traffic for applications running on Tanzu Platform is routed to each application by the Gorouter. The platform can be configured so application instances will only accept a properly authenticated mTLS connection from the Gorouter, thus protecting the applications from attacks.

For situations where additional network-level security is required, Tanzu offers an IPsec add-on for the platform. The IPsec add-on provides security to the network layer of the OSI model with a strongSwan implementation in FIPS mode for each BOSH-deployed VM. IPsec encrypts IP data flow between hosts, between security gateways, between service tiles, and between security gateways and hosts. The IPsec add-on secures network traffic within a Tanzu Platform deployment and provides internal system protection if a malicious actor breaches your firewall. Information on configuring the add-on, as well as its limitations, are covered in the [IPSec Add-on for Tanzu](#) documentation.

Information Protection (PR.IP)

Information protection is a rather broad category of outcomes focused on having policies, processes, and procedures used to manage the protection of information systems and assets. The subcategories here cover topics such as configuration management, software development life cycle, change control, backup and recovery, and recovery planning and testing. Tanzu Platform provides a number of capabilities to help achieve these outcomes.

Configuration Management

Configuration management can be a challenging outcome for many technology organizations due to the breadth of technologies used and the constant changes happening with those technologies. The same stemcell and buildpack components that support the outcomes under [Asset Management](#) also provide useful capabilities in the area of configuration management because the configuration of these items is enforced programmatically by the platform, rather than left to the individual developers to handle.

As the foundational element for the platform, the stemcells used for all VMs are hardened in line with published benchmarks such as those from the Center for Internet Studies (CIS) and the DISA Security Technical Implementation Guides (STIGs), with minor variations as needed to support containers, etc. Details on stemcell hardening are available from the [Stemcell Security](#) section of the Tanzu documentation. Leveraging the capabilities of the core platform automation engine [BOSH](#), Tanzu Platform ensures the configuration is consistent across all BOSH-deployed VMs.

Because the BOSH-deployed VMs are recreated from the base stemcells each time a BOSH deployment is performed, if someone makes a configuration change to one of the running VMs, that change will be erased at the next deployment. This feature prevents configuration drift, especially if deployments are performed regularly; deployments at least weekly are recommended. For those cases where customers need to make changes to the configuration of the VMs that differ from what is delivered in the default stemcells (add login banners, customize audit rules) the changes can be added programmatically as a [BOSH add-on](#). This ensures the configuration changes are properly approved and tracked to ensure the running configuration always matches the desired configuration without the need for additional tooling.

With stemcells and BOSH providing configuration management for the VMs used in Tanzu Platform, buildpacks along with the hardened [stack](#) or rootfs provide the same level of configuration control for the runtime containers. As mentioned earlier in [Asset Management](#), buildpacks provide framework and/or runtime support for the applications. This means developers don't need to spend time configuring and deploying these components, as they are provided automatically by the platform. In addition, because the buildpack (when combined with the rootfs) drives the contents and configuration of the container in which the application instances will ultimately run, it provides the configuration management layer for these containers.

Buildpacks typically examine your apps to determine which dependencies to download and how to configure the apps to communicate with bound services. When a developer pushes an app, Tanzu Platform automatically detects an appropriate buildpack for it and then uses that buildpack to compile or prepare the app for launch. Because all of this happens programmatically, there is no variance in the configurations; the containers are launched with the same configuration each time. Each time an application is pushed or is restaged, the containers for that application will be rebuilt from scratch, ensuring that the running container matches the specified configuration in the buildpack. This eliminates the concern over configuration drift in the containers.

There is one caveat to the buildpack/rootfs configuration management mechanism, in the scenario where the customer [deploys their own containers](#) to Tanzu Platform rather than using the containers built by the platform. In this case, the developer is directly providing the container to use when running the application, so the platform is not able to enforce configuration controls. In this case, the responsibility is on the developer or the broader organization to ensure the configuration of the container matches organizational standards and is enforced throughout the container life cycle.

Backups

The next area under the Information Protection subcategory for which Tanzu Platform provides capabilities is maintaining and testing backups. The key to this outcome is making sure all critical data and the applications and services used to access it are properly backed up and can be restored when needed. There are many layers which need to be considered to ensure the backups provide adequate coverage, one of which is Tanzu Platform. To gain an overview of the backup and recovery process for Tanzu Platform, review the [Disaster Recovery in Tanzu Platform](#) topic in the Tanzu documentation.

Tanzu leverages a utility called BOSH Backup and Restore (BBR) to provide a backup mechanism for Tanzu Platform, and provides [starter Concourse pipelines](#) that can be used to automate the process.

- Carefully review the information on [Backing Up Tanzu Platform](#) with BBR in the Tanzu documentation to ensure the environment is prepared for successful backup operations.
- The BBR utility will back up the configuration information for the BOSH Director and Tanzu Platform installation, but doesn't back up application data or data stored by services like the MySQL tile. Each service will have instructions on how to properly perform backups. The back up and recovery plan needs to include these dependencies in order for the applications running on the platform to be fully recovered.
- The backup created by BBR consists of a folder with the backup artifacts and metadata files. When the BBR process is complete, encrypt and compress the backup artifacts and move them to your preferred storage space.

- Make redundant copies of your backup artifacts and store them in multiple locations, based on the needs of the response and recovery plans, to ensure they will be available at alternate locations in the event of a disaster.
- Regularly restore the backups to validate the artifacts; see the [instructions for validating the backup](#) in the Tanzu documentation.

Response and Recovery Plans

These subcategories cover the requirement to maintain and test the plans that will be used to implement the Respond and Recover functions when necessary. While Tanzu Platform does not provide any specific tools to assist with creating, maintaining, or testing these plans, the capabilities provided by the platform do allow organizations to simplify and streamline the steps in the response or recovery processes. The same stemcell, VM, buildpack, container, and rootfs features referenced in the [Configuration Management](#) section also help streamline response and recovery.

In a typical response or recovery scenario, applications need to be re-deployed or restored by deploying and configuring each of the many layers upon which the application runs. In addition, each application has historically had its own unique, customized implementation of this stack, so re-deploying or restoring many applications becomes highly complex. Tanzu Platform removes these complexities. Because the platform is standardized using the common building blocks discussed previously, it removes much of this complexity and allows teams to have greater confidence in their ability to respond to and recover from an incident.

For Tanzu Platform, the BBR tool is also used to restore the backups. The process for restoring applications running on Tanzu Platform will generally follow the steps listed below, which are provided in detail in the [Restoring Tanzu Platform From Backup with BBR](#) topic in the Tanzu documentation.

- If the restore is being performed on new or replacement infrastructure, rebuild the infrastructure or IaaS layer so that it is configured to match the environment it is replacing.
- Follow the steps outlined in the Tanzu documentation to restore Tanzu Platform.
- Once Tanzu Platform is confirmed to be operating properly, rolling out the applications is as simple as executing the required automation pipelines, or running cf push targeting the restored Tanzu Platform.

Vulnerability Management

The outcomes in this subcategory are well understood by security teams, and are at times some of the most challenging to achieve. The goal is easy to state: remediate all vulnerabilities in all systems, applications, and services, as quickly as possible once they are known. Unfortunately, due to the complexity and variability of most technology environments, achieving these goals can be nearly impossible. Tanzu considers fast, consistent patching or repairing of vulnerabilities to be one of the Four Rs of [Cloud-Native Security](#) and is a core

The Four Rs of Enterprise Security

Following the four Rs of enterprise security will help your organization practice good security postures.

- **Rotate:** Change data center credentials every few hours
- **Repace:** Apply to every server and application in the data center every few hours from a known good state.
- **Repair:** Apply to vulnerable operating systems and application stacks consistently within hours of patch availability.
- **Replicate:** Auto-replicate app resources across multiple availability targets.

capability of Tanzu Platform. With Tanzu, organizations can repair vulnerable operating systems (OSs) and application stacks consistently, within hours of patch availability leveraging stemcells and buildpacks, as covered in the [Configuration Management](#) section.

Once notified that an updated stemcell is available for their environment, platform engineers use the OpsMan UI or API to [associate the updated stemcell to the affected tiles on the platform](#). After applying the stemcell, the engineers review and apply the changes to the affected tiles. The platform will then automatically rotate all managed VMs for the selected products and services to the new stemcell version, including all Tanzu Platform VMs on which custom applications are running. To ensure the VMs are always running on the most updated stemcells, this process should be automated with standard CI/CD tools like [Concourse](#).

This process also leverages a second one of the Four Rs, because the patches are not just applied to a running virtual machine image, which is prone to failure for a large number of reasons. With Tanzu, all the virtual machines are rebuilt or repaved from the new stemcell (golden image). This not only ensures the needed fixes are applied properly, but it also removes any possibility that an attacker could gain a foothold in a VM and use that to exfiltrate data or as a link to external control systems. Should an attacker have gained a foothold in the system, rebuilding from a known good image removes them from the environment and forces them to start over. This presents a major disruption to the typical attack life cycle. Because of these benefits, and the fact the platform can be architected so that repaving all VMs can be done with no impact to the running applications, customers should repave their environment as often as possible, even when there are no updates to apply.

Maintenance (PR.MA)

The focus of this subcategory is to make sure maintenance activities for information systems are properly authorized, performed only by authorized people, and are logged and monitored. For organizations using Tanzu Platform, maintenance activities will generally look different than they might for other parts of the organization. This is because the platform is optimized for automation, and enforces strict configuration control through regularly rebuilding the environment to a known good state, rather than allowing manual or one-off changes to be made in the environment. This changes the way the organization needs to approach traditional maintenance activities.

One big shift enabled by Tanzu Platform is to remove the need to access or make changes to a running application instance. In production environments, the ability to access a running container interactively using SSH should be unnecessary and turned off. If updates or changes are needed for an application running on the platform, the changes should run through the standard application deployment automation, which is where the needed approvals, user authentication, authorization, and logging would occur.

When the changes or updates are deployed by the automation, all of the applicable application instances will be recreated, ensuring there are no one-off or snowflake systems.

This same model generally applies at the platform level. The platform is designed for maintenance activities to be performed through automation, removing the need for manual changes or updates. Updated software versions, patched stemcells, and configuration changes can all be deployed using automated pipelines which can include the required testing and approval workflows to ensure only authorized people can make approved changes.

In cases where maintenance activities require interactive SSH access to the virtual machines in Tanzu Platform environment, the following recommendations help ensure access is properly secured and all activity can be logged.

- As discussed in [Identity Management and Access Control \(PR.AC\)](#), deploy Tanzu Platform on an isolated network segment, with a jumpbox used to access the administrator interfaces and integrated with a PAM solution to provide advanced access control and logging.
- The standard system auditing features can be customized using the [os-conf-release](#) BOSH add-on to log any changes to critical system files which can then be compared to authorized maintenance activity. Alternatively, the Tanzu-provided File Integrity Monitoring (FIM) tool can be deployed and customized to alert on changes to monitored files.

Protective Technology (PR.PT)

Protective Technology is something of a catch-all subcategory that covers the remaining technical controls that are designed to ensure the security and resilience of systems and assets. The outcomes where Tanzu Platform plays a part here are audit logging, implementing the principle of least functionality, and resilience mechanisms.

Logging

Tanzu Platform provides robust logging capabilities to support a variety of outcomes, creating a standard way to collect logs from all the applications running on Tanzu Platform. This relieves application developers from needing to create logging solutions and capabilities for each application they develop. Ensure the applications log to stderr and stdout and the platform will take care of the rest. The section on [Configuring Logging in Tanzu Platform](#) from the Tanzu Platform documentation provides a good overview of the logging mechanisms and options available in the platform.

To provide for the typical outcomes most organizations will be targeting, all logs from production environments should be forwarded to an external system for storage and analysis. For Tanzu Platform, there are multiple levels where this needs to be configured to ensure all needed logs are sent to the target system:

- Operations Manager is the base environment for Tanzu Platform installation. To configure syslog forwarding for this layer, see the Settings section in the [Operations Manager](#) documentation.

VMware Tanzu Operations Manager

Tanzu Operations Manager works alongside BOSH Director for life cycle management across Tanzu Platform.

Features

- Web-based interface allows platform engineers to avoid creating and maintaining complex manifest files
- Ability to install, remove and upgrade products within your deployment
- Provides information on your running virtual machines

Learn more about [Tanzu Operations Manager](#).

- BOSH Director handles life cycle management for the whole platform. Logs from this layer should be forwarded to the target system using syslog. To configure log forwarding for BOSH Director, see the applicable section in the Tanzu Platform installation documentation under [Configuring BOSH Director](#). NOTE: BOSH Director logs contain sensitive information that should be considered privileged. For example, these logs may contain cloud provider credentials. Configure the forwarding to use TLS encryption to prevent information from being intercepted by a third party.
- The Tanzu Platform layer is next. These logs should also be sent to the collection/analysis system using syslog. Instructions for configuring syslog forwarding for this layer can be found in the Tanzu Platform documentation in the [Configuring Logging in Tanzu Platform](#) section.
 - To ensure all relevant events are forwarded to the log collection system, make sure the **Enable Cloud Controller security event logging** checkbox is selected when configuring Tanzu Platform.
- The fourth layer is application logging. This is where the power of Tanzu Platform to enhance developer productivity shines through. Developers who deploy applications on the platform need to make sure their application logs to stderr and stdout so the platform logging system called Loggregator will collect the logs and provide a central way to configure sending those logs to an external system. The section titled [App Logging in Cloud Foundry](#) from Tanzu Platform documentation provides a good overview of this topic.
 - The easiest way to forward application logs to an external log management and analysis system is to create syslog drains, which can be scaled up as needed, based on the amount of log traffic. The process for configuring these drains is covered in the section of the Tanzu Platform documentation called [Streaming App Logs to Log Management Services](#).
 - The alternative method to send application logs to an external platform is to deploy a nozzle to the Cloud Foundry (CF) Loggregator Firehose. To understand the nozzle method, first review the [Loggregator Architecture](#).
 - Many popular log management/analysis platforms have pre-built nozzles available from the Tanzu Network. These include Splunk and Sumo Logic, as well as platform-specific nozzles for GCP, Azure, and VMware.
 - Custom nozzles can be created and deployed if needed, following the guidance in the [Deploying a Nozzle to the Loggregator Firehose](#) documentation.
- A fifth (optional) level of logging is available in Tanzu Platform: application traffic logging. Not every organization will need to undertake this level of logging. It should only be used if the organization requires that every single network connection to applications running on Tanzu Platform needs to be logged and analyzed for malicious activity. Application traffic logging can be turned on for the entire platform (recommended) or for specific Application Security Groups. Refer to [App Traffic Logging](#) for information on turning on this type of logging. When enabled, this feature will capture the following information for applications deployed on Tanzu Platform:

- TCP traffic – Logs the first packet of every new TCP connection.
- UDP traffic – Logs UDP packets sent and received, up to a maximum per-second rate for each container.
- Packets denied – Logs packets blocked by either a container-specific networking policy or by [Application Security Group \(ASG\)](#) rules applied. Logs packet denials up to a maximum per-second rate for each container.

Least Functionality

The stemcell hardening process described earlier in the [Configuration Management](#) section coupled with the buildpack mechanism used when deploying applications ensures all platform components are built with the least amount of functionality possible. Each component is built from a base that has no extra functionality. Specific functionality is then added at the appropriate layer only when needed to support the specific requirements of the application. As an example of this, consider the deployment of a typical Java application on the platform.

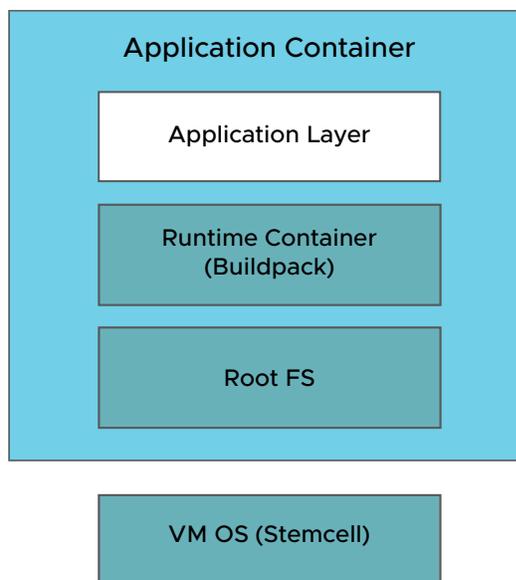


Figure 2 - An application container constructed from three main building blocks

The virtual machines on which the application instances will ultimately run do not have the components needed to run a Java application. They are standardized VMs based on the hardened stemcell, each one built from the same image for consistency. There are no unnecessary services enabled on the VM.

The application container is then constructed from three main building blocks, as shown in Figure 2. The first is the rootfs or stack. Like the other components, the rootfs is specifically tuned to only have the required binaries and OS support to run the application container. There are no additional applications or services in this layer.

Modern Spring Applications

Java applications run seamlessly on Tanzu Platform with Spring. Learn how Spring can make your Java applications more modern, simple, and effective.

Learn more: spring.io

On top of the roots is the buildpack. The buildpack is where specific environments are built based on the needs of the application. In the example of a Java application, this is where the Java runtime will be introduced, along with the specific dependencies required for Java. Because the buildpack is centrally managed and is specific to the language/runtime needed for the specific application being deployed, it only has the functionality needed for that specific application, providing the least amount of functionality possible. The final layer is the application code itself, which is the responsibility of the organization to have controls in-place to ensure it only has the required functionality.

Resilience and Availability

Some of the main advantages of leveraging Tanzu Platform are in the areas of resilience and availability. The platform is designed to leverage multiple levels of availability and resilience, and is used by a number of large global organizations to meet their most aggressive availability requirements for public-facing applications. The four main layers of high availability in the platform are availability zone, virtual machine, process, and application instance:

- The core platform components and application instances can be scaled horizontally and spread out across availability zones. Coupled with external load balancers that provide load balancing to each of the Tanzu Platform Router IP addresses, this allows the application to continue serving requests even when a data center goes down.
- At the virtual machine level, BOSH detects if a VM is present by listening for heartbeat messages that are sent from the BOSH agent every 60 seconds. When BOSH finds a VM is not responding, it sends an alert to the Resurrector component. If the Resurrector is enabled, it sends the IaaS a request to create a new VM instance to replace the one that failed.
- Tanzu Platform uses a BOSH agent and a process called monit to monitor the processes on the component VMs that work together to keep applications running, such as nsync, BBS, and Cell Rep. If monit detects a failure, it restarts the process and notifies the BOSH agent on the VM. The BOSH agent notifies the BOSH Health Monitor, which triggers responders through plugins such as email notifications or paging.
- If application instances are lost for any reason, such as a bug in the app or an AZ going down, Tanzu Platform restarts new instances to maintain capacity. The system tracks the number of instances of each application that are running across the environment. When there is a discrepancy between the actual state of the app instances running and the desired state, Tanzu Platform will initiate the deployment of new application instances.

Learn how to [achieve high availability](#) with Tanzu Platform.

Detect (DE)

This function is focused on enabling timely discovery of cybersecurity events. The focus is on developing and implementing activities to identify the occurrence of a cybersecurity event or incident. Tanzu Platform provides capabilities that can help achieve outcomes in two of the categories under this area: Anomalies and Events and Security Continuous Monitoring.

Anomalies and Events (DE.AE)

The platform has logging capabilities that support the outcomes in this category. See the Protective Technology category of the [Logging](#) section for details on configuring logging to send information into a centralized platform for detection. To support anomaly detection, enable application traffic logging and use analysis tools on that data to detect unusual traffic patterns.

Security Continuous Monitoring (DE.CM)

With Tanzu Platform, Tanzu provides capabilities that directly help achieve the outcomes in the subcategories of monitoring for unauthorized software and performing vulnerability scans.

Monitoring for Unauthorized Software

For customers using Tanzu Platform for Linux, Tanzu provides an optional component customers can install to monitor the file system of the VMs and containers called the File Integrity Monitoring Add-on for PCF. This add-on can be configured to alert on any changes to the file system for the VMs and containers in Tanzu Platform, which would include the installation of any unauthorized software. Information on how to configure the add-on can be found in the Tanzu [documentation](#) for the add-on.

Vulnerability Scanning

As covered in the [Vulnerability Management](#) section, Tanzu provides robust vulnerability remediation capabilities for Tanzu Platform which can make vulnerability scanning at the platform level unnecessary, depending on organizational risk assessments. Leveraging the automation capabilities provided using [Concourse](#) and the Platform Automation for Tanzu Platform product, customers can completely automate the speedy deployment of updated platform components (stemcells, buildpacks, rootfs) as they are released by Tanzu to remediate newly discovered CVEs. This automation can be monitored to ensure vulnerabilities in the environment have been removed.

For those customers who require additional scanning and monitoring to ensure the running VMs and containers do not have known vulnerabilities present, there are a number of partner solutions available for Tanzu Platform that will monitor the running VMs and containers and generate alerts if a vulnerability is discovered. For those organizations that require this level of vulnerability monitoring, review the list of solutions listed under the Identity and Security section of the [Tanzu documentation site](#).

While Tanzu Platform provides vulnerability remediation capabilities that cover the platform and the runtime environment for applications via the standard buildpacks, customers need to provide vulnerability monitoring for their application code. Customers should use a variety of testing tools in their application integration/testing/deployment pipelines to check the code for the presence of vulnerabilities. In addition, customers should conduct routine scans of the running applications to check for vulnerabilities. These capabilities are not provided by Tanzu Platform.

Respond (RS)

The Respond function is used for the activities an organization will perform when taking action in response to a detected cybersecurity incident. The outcome categories covered include communications concerning the incident, analysis of the incident, and actions performed to contain the impact of the incident and mitigate its effects. Tanzu Platform capabilities map to the Mitigation category.

Mitigation (RS.MI)

The Four Rs (repair, repave, rotate, replicate) of Cloud Native Security were introduced earlier in the [Vulnerability Management](#) section. One of the main benefits of regularly repaving Tanzu Platform and the running applications is how it mitigates the impacts of a cybersecurity incident. Whenever a cybersecurity incident affects Tanzu Platform or applications running on the platform, repaving should be a key part of the mitigation plan. Performing a full repave of Tanzu Platform during a cybersecurity incident will provide the benefits highlighted below, which are key components of mitigating the effects of an incident.

- Using the most recent versions of stemcells, buildpacks, and root file systems to perform the repave ensures the known vulnerabilities in each platform layer have been properly eliminated.
- By repaving the environment from the gold images, any malicious software including persistence mechanisms and backdoors that was introduced by the attacker is removed.
- Repaving also removes any Command and Control (CnC) capabilities the attacker may have established within the VMs or containers on the platform.

Recover (RC)

While the Respond function is focused on containing and mitigating a cybersecurity incident, the Recover function covers the plans and processes implemented to return to normal operations following an incident. This includes restoring or repairing any services that were impaired as a result of the incident. The back up and recovery capabilities of Tanzu Platform were covered previously in the [Backups](#) section. The general recovery process with Tanzu Platform would be as follows:

Accelerate Software Delivery with VMware Tanzu® Labs™

[VMware Tanzu Labs](#) partners with organizations worldwide to accelerate software delivery and modernize legacy apps. If you're looking for consulting support for the Tanzu portfolio, please contact your sales representative.

- If the restore is being performed on new or replacement infrastructure, rebuild the infrastructure or IaaS layer so that it is configured to match the environment it is replacing. Refer to the [Compatibility of Restore](#) section in the Tanzu documentation for the important considerations.
- Follow the steps outlined in the Tanzu documentation to restore Tanzu Platform.
- Once Tanzu Platform is confirmed to be operating properly, rolling out the applications is as simple as executing the required automation pipelines, or running a push targeting the restored Tanzu Platform.

The backup and recovery functionality of Tanzu Platform typically does not apply to the persistent data stores used by the applications running on the Tanzu Platform. These data stores will need their own backup and recovery plans, which would also need to be executed as part of the Recover function, if they were affected by the cybersecurity incident.

Summary

The NIST Cybersecurity Framework identifies five core functions for an effective cybersecurity program: Identify, Protect, Detect, Respond, and Recover. Using this framework provides security teams a common mechanism they can use to assess their cybersecurity program and how successful they are in achieving the key outcomes needed to aid their organization in defending against and responding to cybersecurity incidents. As described throughout this document, the capabilities Tanzu Platform provides to an organization map directly to certain key categories and subcategories within the framework, helping security teams achieve some of their key outcomes.

