SOLUTION GUIDE

How StrongDM Helps with MITRE ATT&CK for Containers

The MITRE ATT&CK Containers Matrix is designed to give adversary tactics and techniques based on real-world observations. It is the foundation to build effective cybersecurity for Enterprises.

Below are the specific requirements where StrongDM can help you mitigate the techniques for the MITRE ATT&CK framework.

Tactic	Description
Initial Access	The adversary is trying to get into your network. Initial Access consists of techniques that use various entry vectors to gain their initial foothold within a network. Techniques used to gain a foothold include targeted spearphishing and exploiting weaknesses on public-facing web servers. Footholds gained through initial access may allow for continued access, like valid accounts and use of external remote services, or may be limited-use due to changing passwords.

Technique	Technique Description	How StrongDM Helps
Exploit Public-Facing Application	Adversaries may attempt to exploit a weakness in an Internet-facing host or system to initially access a network. The weakness in the system can be a software bug, a temporary glitch, or a misconfiguration.	StrongDM is a Dynamic Access Management platform that centralizes privileged access for all technical users to every resource in your infrastructure, on-premises and in the cloud. Every activity and query is logged for complete visibility into who is accessing what, when, and how. End users connect through StrongDM without ever being exposed to credentials. Leverage StrongDM's Access Workflows to implement just in time access to all infrastructure to eliminate standing access and reach zero standing privileges.
External Remote Services	Adversaries may leverage external-facing remote services to initially access and/or persist within a network. Remote services such as VPNs, Citrix, and other access mechanisms allow users to connect to internal enterprise network resources from external locations. There are often remote service gateways that manage connections and credential authentication for these services. Services such as Windows Remote Management and VNC can also be used externally.	StrongDM uses network segmentation, and only makes gateways public, to generate and enforce access control rules.

Technique	Technique Description	How StrongDM Helps
Valid Accounts	Adversaries may leverage external-facing remote services to initially access and/or persist within a network. Remote services such as VPNs, Citrix, and other access mechanisms allow users to connect to internal enterprise network resources from external locations. There are often remote service gateways that manage connections and credential authentication for these services. Services such as Windows Remote Management and VNC can also be used externally.	Grant temporary or Just-in-Time access, with least privilege by default, for managing access to critical infrastructure. Credentials are never exposed to users accessing resources managed by StrongDM. Integrate testing, approving, and implementing changes necessary in emergency situations (e.g. grant temporary access within applications like Slack and Microsoft Teams).
Cloud Accounts	Adversaries may obtain and abuse credentials of a cloud account as a means of gaining Initial Access, Persistence, Privilege Escalation, or Defense Evasion. Cloud accounts are those created and configured by an organization for use by users, remote support, services, or for administration of resources within a cloud service provider or SaaS application. In some cases, cloud accounts may be federated with traditional identity management systems, such as Windows Active Directory.	Grant temporary or Just-in-Time access, with least privilege by default, for managing access to critical infrastructure. Credentials are never exposed to the end user when connecting to resources through StrongDM. Integrate testing, approving, and implementing changes necessary in emergency situations (e.g. grant temporary access within applications like Slack and Microsoft Teams).
Tactic	**Description**	
Persistence	The adversary is trying to maintain their foothold. Persistence consists of techniques that adversaries use to keep access to systems across restarts, changed credentials, and other interruptions that could cut off their access. Techniques used for persistence include any access, action, or configuration changes that let them maintain their foothold on systems, such as replacing or hijacking legitimate code or adding startup code.	
Account Manipulation	Adversaries may manipulate accounts to maintain access to victim systems. Account manipulation may consist of any action that preserves adversary access to a compromised account, such as modifying credentials or permission groups. These actions could also include account activity designed to subvert security policies, such as performing iterative password updates to bypass password duration policies and preserve the life of compromised credentials. In order to create or manipulate accounts, the adversary must already have sufficient permissions on systems or the domain. However, account manipulation may also lead to privilege escalation where modifications grant access to additional roles, permissions, or higher-privileged Valid Accounts.	Access to critical infrastructure aligns with the identity lifecyle, permissions occur only through StrongDM which authenticates the users through your identity provider or through StrongDM with MFA. Leverage StrongDM's Access Workflows to implement just in time access to all infrastructure to eliminate standing access and reach zero standing privileges.

Technique	Technique Description	How StrongDM Helps
Exrernal Remote Services	Adversaries may leverage external-facing remote services to initially access and/or persist within a network. Remote services such as VPNs, Citrix, and other access mechanisms allow users to connect to internal enterprise network resources from external locations. There are often remote service gateways that manage connections and credential authentication for these services. Services such as Windows Remote Management and VNC can also be used externally.	StrongDM uses network segmentation, and only makes gateways public, to generate and enforce access control rules. The StrongDM gateway architecture prevents exposure of remote services.
Valid Accounts	Adversaries may obtain and abuse credentials of existing accounts as a means of gaining Initial Access, Persistence, Privilege Escalation, or Defense Evasion. Compromised credentials may be used to bypass access controls placed on various resources on systems within the network and may even be used for persistent access to remote systems and externally available services, such as VPNs, Outlook Web Access, network devices, and remote desktop. Compromised credentials may also grant an adversary increased privilege to specific systems or access to restricted areas of the network. Adversaries may choose not to use malware or tools in conjunction with the legitimate access those credentials provide to make it harder to detect their presence.	Grant temporary or Just-in-Time access, with least privilege by default, for managing access to critical infrastructure. Credentials are never exposed to users accessing resources managed by StrongDM. Integrate testing, approving, and implementing changes necessary in emergency situations (e.g. grant temporary access within applications like Slack and Microsoft Teams).
Cloud Accounts	Adversaries may obtain and abuse credentials of a cloud account as a means of gaining Initial Access, Persistence, Privilege Escalation, or Defense Evasion. Cloud accounts are those created and configured by an organization for use by users, remote support, services, or for administration of resources within a cloud service provider or SaaS application. In some cases, cloud accounts may be federated with traditional identity management systems, such as Windows Active Directory.	Grant temporary or Just-in-Time access, with least privilege by default, for managing access to critical infrastructure. Credentials are never exposed to users accessing resources managed by StrongDM. Integrate testing, approving, and implementing changes necessary in emergency situations (e.g. grant temporary access within applications like Slack and Microsoft Teams).

Tactic	Description
Privilege Escalation	The adversary is trying to gain higher-level permissions. Privilege Escalation consists of techniques that adversaries use to gain higher-level permissions on a system or network. Adversaries can often enter and explore a network with unprivileged access but require elevated permissions to follow through on their objectives. Common approaches are to take advantage of system weaknesses, misconfigurations, and vulnerabilities.

Technique	Technique Description	How StrongDM Helps
Valid Accounts	Adversaries may obtain and abuse credentials of existing accounts as a means of gaining Initial Access, Persistence, Privilege Escalation, or Defense Evasion. Compromised credentials may be used to bypass access controls placed on various resources on systems within the network and may even be used for persistent access to remote systems and externally available services, such as VPNs, Outlook Web Access, network devices, and remote desktop. Compromised credentials may also grant an adversary increased privilege to specific systems or access to restricted areas of the network. Adversaries may choose not to use malware or tools in conjunction with the legitimate access those credentials provide to make it harder to detect their presence.	Grant temporary or Just-in-Time access, with least privilege by default, for managing access to critical infrastructure. Credentials are never exposed to users accessing resources managed by StrongDM. Integrate testing, approving, and implementing changes necessary in emergency situations (e.g. grant temporary access within applications like Slack and Microsoft Teams).
Cloud Accounts	Adversaries may obtain and abuse credentials of a cloud account as a means of gaining Initial Access, Persistence, Privilege Escalation, or Defense Evasion. Cloud accounts are those created and configured by an organization for use by users, remote support, services, or for administration of resources within a cloud service provider or SaaS application. In some cases, cloud accounts may be federated with traditional identity management systems, such as Windows Active Directory.	Grant temporary or Just-in-Time access, with least privilege by default, for managing access to critical infrastructure. Integrate testing, approving, and implementing changes necessary in emergency situations (e.g. grant temporary access within applications like Slack and Microsoft Teams). Leverage StrongDM's Access Workflows to implement just in time access to all infrastructure, including cloud infrastructure, to eliminate standing access and reach zero standing privileges.

Tactic	Description
Defense Evasion	The adversary is trying to avoid being detected. Defense Evasion consists of techniques that adversaries use to avoid detection throughout their compromise. Techniques used for defense evasion include uninstalling/disabling security software or obfuscating/encrypting data and scripts. Adversaries also leverage and abuse trusted processes to hide and masquerade their malware. Other tactics' techniques are cross-listed here when those techniques include the added benefit of subverting defenses.

Technique	Technique Description	How StrongDM Helps
Impair Defenses	Adversaries may maliciously modify components of a victim environment in order to hinder or disable defensive mechanisms. This not only involves impairing preventative defenses, such as firewalls and anti-virus, but also detection capabilities that defenders can use to audit activity and identify malicious behavior. This may also span both native defenses as well as supplemental capabilities installed by users and administrators.	StrongDM provides session recordings and audit logs for all access to configured data sources, which are critical for identifying root cause in security incidents.
Disable Cloud Logs	An adversary may disable cloud logging capabilities and integrations to limit what data is collected on their activities and avoid detection. Cloud environments allow for collection and analysis of audit and application logs that provide insight into what activities a user does within the environment. If an adversary has sufficient permissions, they can disable logging to avoid detection of their activities.	StrongDM provides session recordings and audit logs for all access to configured data sources, which are critical for identifying root cause in security incidents.
Indicator Removal	Adversaries may delete or modify artifacts generated within systems to remove evidence of their presence or hinder defenses. Various artifacts may be created by an adversary or something that can be attributed to an adversary's actions. Typically these artifacts are used as defensive indicators related to monitored events, such as strings from downloaded files, logs that are generated from user actions, and other data analyzed by defenders. Location, format, and type of artifact (such as command or login history) are often specific to each platform.	StrongDM provides session recordings and audit logs for all access to configured data sources, which are critical for identifying root cause in security incidents.

Technique	Technique Description	How StrongDM Helps
Valid Accounts	Adversaries may obtain and abuse credentials of existing accounts as a means of gaining Initial Access, Persistence, Privilege Escalation, or Defense Evasion. Compromised credentials may be used to bypass access controls placed on various resources on systems within the network and may even be used for persistent access to remote systems and externally available services, such as VPNs, Outlook Web Access, network devices, and remote desktop. Compromised credentials may also grant an adversary increased privilege to specific systems or access to restricted areas of the network. Adversaries may choose not to use malware or tools in conjunction with the legitimate access those credentials provide to make it harder to detect their presence.	Grant temporary or Just-in-Time access, with least privilege by default, for managing access to critical infrastructure. Credentials are never exposed to users accessing resources managed by StrongDM. Integrate testing, approving, and implementing changes necessary in emergency situations (e.g. grant temporary access within applications like Slack and Microsoft Teams).
Cloud Accounts	Adversaries may obtain and abuse credentials of a cloud account as a means of gaining Initial Access, Persistence, Privilege Escalation, or Defense Evasion. Cloud accounts are those created and configured by an organization for use by users, remote support, services, or for administration of resources within a cloud service provider or SaaS application. In some cases, cloud accounts may be federated with traditional identity management systems, such as Windows Active Directory.	Grant temporary or Just-in-Time access, with least privilege by default, for managing access to critical infrastructure. Integrate testing, approving, and implementing changes necessary in emergency situations (e.g. grant temporary access within applications like Slack and Microsoft Teams). Leverage StrongDM's Access Workflows to implement just in time access to all infrastructure, including cloud infrastructure, to eliminate standing access and reach zero standing privileges.

Tactic	Description
Credential Access	The adversary is trying to steal account names and passwords. Credential Access consists of techniques for stealing credentials like account names and passwords. Techniques used to get credentials include keylogging or credential dumping. Using legitimate credentials can give adversaries access to systems, make them harder to detect, and provide the opportunity to create more accounts to help achieve their goals.

Technique	Technique Description	How StrongDM Helps
Credentials from Password Stores	Adversaries may search for common password storage locations to obtain user credentials. Passwords are stored in several places on a system, depending on the operating system or application holding the credentials. There are also specific applications that store passwords to make it easier for users manage and maintain. Once credentials are obtained, they can be used to perform lateral movement and access restricted information.	Credentials are never exposed to users accessing resources managed by StrongDM, including cloud infrastructure

Technique	Technique Description	How StrongDM Helps
Credential Access	The adversary is trying to steal account names and passwords. Credential Access consists of techniques for stealing credentials like account names and passwords. Techniques used to get credentials include keylogging or credential dumping. Using legitimate credentials can give adversaries access to systems, make them harder to detect, and provide the opportunity to create more accounts to help achieve their goals.	Leverage StrongDM's Access Workflows to implement Just -in-Time access to all infrastructure to eliminate standing access and reach Zero Standing Privileges. Credentials are never exposed to users accessing resources managed by StrongDM, including cloud infrastructure
Unsecured Credentials	Adversaries may search compromised systems to find and obtain insecurely stored credentials. These credentials can be stored and/or misplaced in many locations on a system, including plaintext files (e.g. Bash History), operating system or application-specific repositories (e.g. Credentials in Registry), or other specialized files/artifacts (e.g. Private Keys).	Leverage StrongDM's Access Workflows to implement Just -in-Time access to all infrastructure to eliminate standing access and reach Zero Standing Privileges. Credentials are never exposed to users accessing resources managed by StrongDM, including cloud infrastructure

Tactic	Description
Discovery	The adversary is trying to steal account names and passwords. Credential Access consists of techniques for stealing credentials like account names and passwords. Techniques used to get credentials include keylogging or credential dumping. Using legitimate credentials can give adversaries access to systems, make them harder to detect, and provide the opportunity to create more accounts to help achieve their goals.

Technique	Technique Description	How StrongDM Helps
Account Discovery	Adversaries may attempt to get a listing of valid accounts, usernames, or email addresses on a system or within a compromised environment. This information can help adversaries determine which accounts exist, which can aid in follow-on behavior such as brute-forcing, spear-phishing attacks, or account takeovers (e.g., Valid Accounts).	The StrongDM Admin UI maintains a list of all users and resources they have access to. Admins can define and enforce the appropriate access policies based on a user's role or a resource's attributes with comprehensive permissions auditing available. Users can only view a personalized Access Catalog that shows that they have access to based on roles and attributes.

Technique	Technique Description	How StrongDM Helps
Cloud Account	Adversaries may attempt to get a listing of cloud accounts. Cloud accounts are those created and configured by an organization for use by users, remote support, services, or for administration of resources within a cloud service provider or SaaS application.	The StrongDM Admin UI maintains a list of all users and resources they have access to. Admins can define and enforce the appropriate access policies based on a user's role or a resource's attributes with comprehensive permissions auditing available. Users can only view a personalized Access Catalog that shows that they have access to based on roles and attributes.
Permission Groups Discovery	Adversaries may attempt to discover group and permission settings. This information can help adversaries determine which user accounts and groups are available, the membership of users in particular groups, and which users and groups have elevated permissions.	The StrongDM Admin UI maintains a list of all users and resources they have access to. Admins can define and enforce the appropriate access policies based on a user's role or a resource's attributes with comprehensive permissions auditing available. Users can only view a personalized Access Catalog that shows that they have access to based on roles and attributes.
Cloud Groups	Adversaries may attempt to find cloud groups and permission settings. The knowledge of cloud permission groups can help adversaries determine the particular roles of users and groups within an environment, as well as which users are associated with a particular group.	The StrongDM Admin UI maintains a list of all users and resources they have access to. Admins can define and enforce the appropriate access policies based on a user's role or a resource's attributes with comprehensive permissions auditing available. Users can only view a personalized Access Catalog that shows that they have access to based on roles and attributes.
Cloud Infrastructure Discovery	An adversary may attempt to discover infrastructure and resources that are available within an infrastructure-as-a-service (IaaS) environment. This includes compute service resources such as instances, virtual machines, and snapshots as well as resources of other services including the storage and database services.	The StrongDM Admin UI maintains a list of all users and resources they have access to. Admins can define and enforce the appropriate access policies based on a user's role or a resource's attributes with comprehensive permissions auditing available. Users can only view a personalized Access Catalog that shows that they have access to based on roles and attributes.
Container and Resource Discovery	Adversaries may attempt to discover containers and other resources that are available within a containers environment. Other resources may include images, deployments, pods, nodes, and other information such as the status of a cluster.	The StrongDM Admin UI maintains a list of all users and resources they have access to. Admins can define and enforce the appropriate access policies based on a user's role or a resource's attributes with comprehensive permissions auditing available. Users can only view a personalized Access Catalog that shows that they have access to based on roles and attributes.

Tactic	Description
Lateral Movement	The adversary is trying to move through your environment. Lateral Movement consists of techniques that adversaries use to enter and control remote systems on a network. Following through on their primary objective often requires exploring the network to find their target and subsequently gaining access to it. Reaching their objective often involves pivoting through multiple systems and accounts to gain. Adversaries might install their own remote access tools to accomplish Lateral Movement or use legitimate credentials with native network and operating system tools, which may be stealthier.

Technique	Technique Description	How StrongDM Helps
Remote Services	Adversaries may use Valid Accounts to log into a service that accepts remote connections, such as telnet, SSH, and VNC. The adversary may then perform actions as the logged-on user.	Grant temporary or Just-in-Time access, with least privilege by default, for managing access to critical infrastructure. Integrate testing, approving, and implementing changes necessary in emergency situations (e.g. grant temporary access within applications like Slack and Microsoft Teams). Leverage StrongDM's Access Workflows to implement just in time access to all infrastructure to eliminate standing access and reach zero standing privileges.
Remote Desktop Protocol	Adversaries may use Valid Accounts to log into a computer using the Remote Desktop Protocol (RDP). The adversary may then perform actions as the logged-on user.	Grant temporary or Just-in-Time access, with least privilege by default, for managing access to critical infrastructure. Integrate testing, approving, and implementing changes necessary in emergency situations (e.g. grant temporary access within applications like Slack and Microsoft Teams). Leverage StrongDM's Access Workflows to implement just in time access to all infrastructure to eliminate standing access and reach zero standing privileges.
SSH	Adversaries may use Valid Accounts to log into remote machines using Secure Shell (SSH). The adversary may then perform actions as the logged-on user.	Grant temporary or Just-in-Time access, with least privilege by default, for managing access to critical infrastructure. Integrate testing, approving, and implementing changes necessary in emergency situations (e.g. grant temporary access within applications like Slack and Microsoft Teams). Leverage StrongDM's Access Workflows to implement just in time access to all infrastructure to eliminate standing access and reach zero standing privileges.