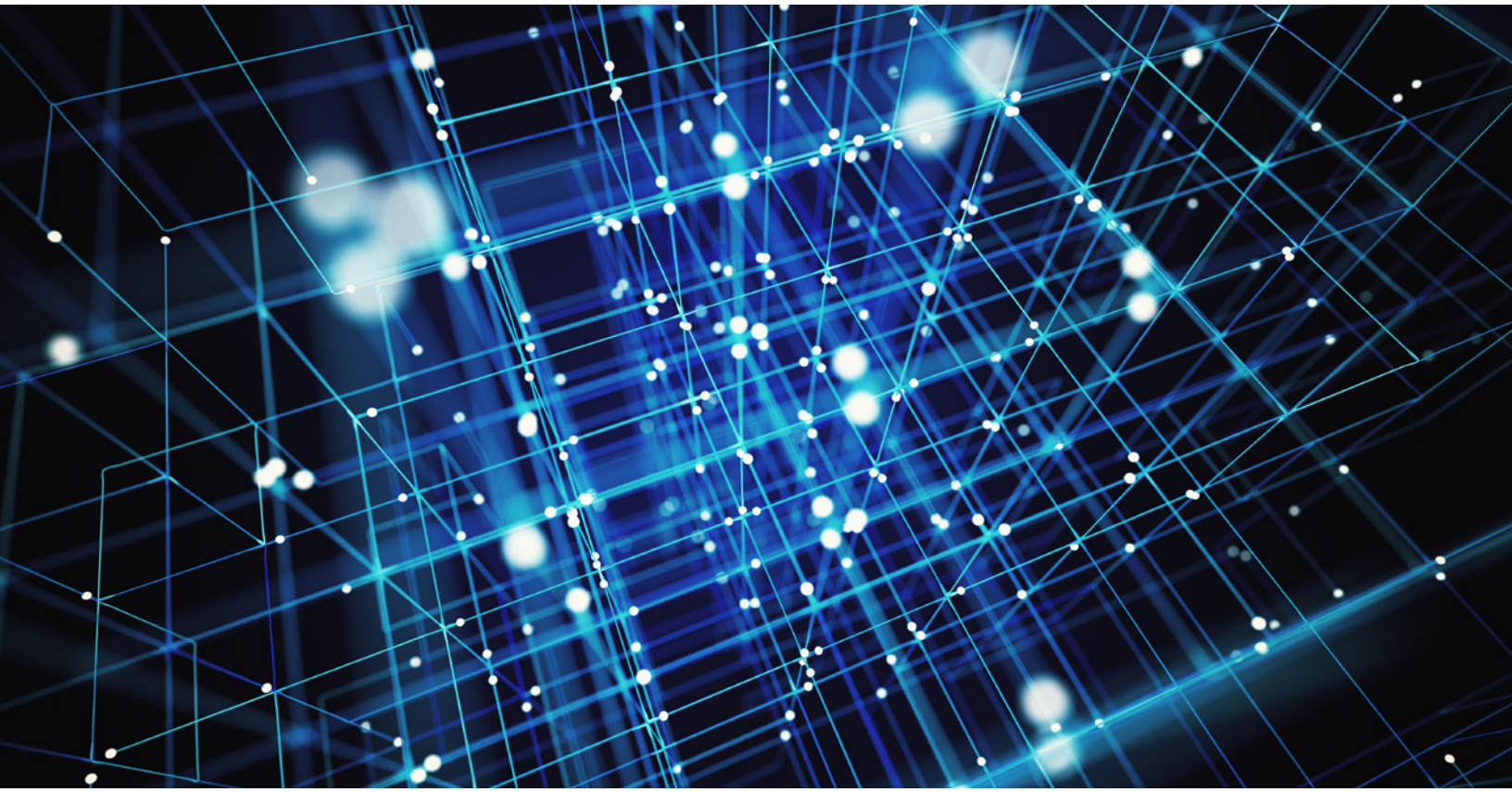
netskope

WHITE PAPER



How the Netskope Platform can assist with MITRE ATT&CK

MITRE Adversarial Tactics, Techniques and Common Knowledge (ATT&CK) is a curated knowledge base and model for cyber adversary behavior, reflecting the various phases of an adversary's attack lifecycle and the platforms they are known to target. The tactics and techniques abstraction in the model provide a common taxonomy of individual adversary actions understood by both offensive and defensive sides of cybersecurity. It also provides an appropriate level of categorization for adversary action and specific ways of defending against it.

The behavioral model presented by ATT&CK contains the following core components:

Tactics denoting short-term, tactical adversary goals during an attack (the columns);

Techniques describing the means by which adversaries achieve tactical goals (the individual cells); and

Documented adversary usage of techniques and other metadata (linked to techniques).

Implementing MITRE ATT&CK typically involves either manual mapping or integration with cybersecurity tools and processes. Subsequently, Netskope has produced this artifact to assist customers to understand how the Netskope platform contributes to an organization’s ability to address the attack technique and tactics defined in MITRE ATT&CK, allowing an organization to understand how they can leverage this platform to mitigate or minimize the impact of these well-known and well-documented attacks.

Category	Technique	Capability	Mitigation	Detection	Source	Page	Solution	Justification
Reconnaissance	Active Scanning	N	N/A	N/A	N/A	N/A	N/A	N/A
Reconnaissance	Gather Victim Host Information	N	N/A	N/A	N/A	N/A	N/A	N/A
Reconnaissance	Gather Victim Identity Information	N	N/A	N/A	N/A	N/A	N/A	N/A
Reconnaissance	Gather Victim Network Information	N	N/A	N/A	N/A	N/A	N/A	N/A
Reconnaissance	Gather Victim Org Information	N	N/A	N/A	N/A	N/A	N/A	N/A
Reconnaissance	Phishing for Information	Y	Restrict Web-Based Content	Navigation to known-bad sites	Netskope Platform Overview v3.pdf	11	NG-SWG	Before compromising a victim, adversaries may send phishing messages to elicit sensitive information that can be used during targeting. Often, adversaries will utilize websites and portals which have been previously identified as known-bad sites by threat intelligence and heuristic analysis. Netskope NG-SWG can detect and prevent navigation to these sites, limiting the impact of this technique.
Reconnaissance	Search Closed Sources	N	N/A	N/A	N/A	N/A	N/A	N/A
Reconnaissance	Search Open Technical Databases	N	N/A	N/A	N/A	N/A	N/A	N/A
Reconnaissance	Search Open Websites/ Domains	N	N/A	N/A	N/A	N/A	N/A	N/A
Reconnaissance	Search Victim-Owned Websites	N	N/A	N/A	N/A	N/A	N/A	N/A
Resource Development	Acquire Infrastructure	N	N/A	N/A	N/A	N/A	N/A	N/A
Resource Development	Compromise Accounts	N	N/A	N/A	CIS Controls v1.pdf	2	N/A	N/A
Resource Development	Compromise Infrastructure	N	N/A	N/A	N/A	N/A	N/A	N/A
Resource Development	Develop Capabilities	N	N/A	N/A	N/A	N/A	N/A	N/A
Resource Development	Establish Accounts	N	N/A	N/A	CIS Controls v1.pdf	2	N/A	N/A
Resource Development	Obtain Capabilities	N	N/A	N/A	N/A	N/A	N/A	N/A
Resource Development	Stage Capabilities	N	N/A	N/A	N/A	N/A	N/A	N/A

Category	Technique	Capability	Mitigation	Detection	Source	Page	Solution	Justification
Initial Access	Drive-by Compromise	Y	Restrict Web-Based Content	Inspect URLs for potentially known-bad domains or parameters.			NG-SWG	In drive-by compromises, adversaries compromise a legitimate website and inject some form of malicious code such as JavaScript, iFrames, or cross-site scripting. Adversaries may also insert malicious advertisments to webpages, in order to compromise victims. Netskope NG-SWG provides SSL/TLS inspection and can restrict navigation to known-bad domains. This can help mitigate and detect drive-by compromises by alerting when malicious code is detected.
Initial Access	Exploit Public-Facing Application	N	N/A	N/A	NS-Mitre-ATT&CK-Framework-WP-00 (1).pdf	3	N/A	N/A
Initial Access	External Remote Services	Y	Limit Access to Resource Over Network, Multi-factor Authentication, Network Segmentation	Detecting adversary use of valid accounts with UEBA			UEBA, NPA	Organizations traditionally manage remote access through VPNs, Citrix, or exposed RDP consoles. Adversaries often target these external remote services as they are publically available and provide network-level access to organizational resources. Netskope Private Access can provision internal applications to remote users without the need for inbound access rules and traditional VPNs. This Zero Trust Network Access capability ensures that remote users access only the applications they have been provisioned and do not gain remote access to the internal network (such as occurs with a VPN).
Initial Access	Hardware Additions	N	N/A	N/A	N/A	N/A	N/A	N/A
Initial Access	Phishing	Y	Restrict Web-Based Content, Anti-Virus Analysis	URL inspection, SSL/TLS inspection	NS-Mitre-ATT&CK-Framework-WP-00 (1).pdf	3	NG-SWG, CTEP	Phishing attacks are an extremely common method to gain initial access to a victim's network. Netskope NG-SWG can detect navigation to known-bad domains and websites, and provide real-time user coaching when users navigate to these websites.

Category	Technique	Capability	Mitigation	Detection	Source	Page	Solution	Justification
Initial Access	Replication Through Removable Media	N	N/A	N/A	N/A	N/A	N/A	N/A
Initial Access	Supply Chain Compromise	Y	No mitigation capability	Scan downloads for malicious signatures			NG-SWG	Supply chain compromises are an advanced attack technique used by adversaries, where products are manipulated before reaching the final customer. While these types of attacks can be difficult to detect, Netskope NG-SWG Advanced Threat Protection provides malware analysis and bare-metal sandboxing of downloaded executables. This capability can detect malicious installers which may have been inserted as a result of a software supply chain compromise.
Initial Access	Trusted Relationship	Y	Network Segmentation	Monitoring for activity conducted by second- and third-party providers	NS-Mitre-ATT&CK-Framework-WP-00 (1).pdf	4	NPA, NG-SWG	Adversaries may breach or otherwise leverage organizations who have access to intended victims, such as IT service providers. Organizations can utilize the zero trust model of Netskope Private Access to expose only required applications to their IT service partners, while enforcing conditional access policies such as OS version requirements, MFA enforcement, and geo-location. Further, Netskope NG-SWG can monitor and detect activity conducted by third-party providers in managed SaaS applications.

Category	Technique	Capability	Mitigation	Detection	Source	Page	Solution	Justification
Initial Access	Valid Accounts	Y	Privileged Account management	Suspicious account behavior across systems that share accounts	NS-Mitre-ATT&CK-Framework-WP-00 (1).pdf	4	NG-SWG, UEBA	Adversaries may obtain and abuse credentials of existing accounts as a means of gaining Initial Access, Persistence, Privilege Escalation, or Defense Evasion. Netskope can provide insights into the use of cloud and SaaS accounts across multiple applications, including detecting when an account is being used across multiple devices or sessions, which may indicate account compromise. Further, Netskope can enforce MFA for specific actions in SaaS applications, mitigating the impact of a compromised valid accounts
Execution	Command and Scripting Interpreter	Y	Restrict Web-Based Content	Malicious file detection			NG-SWG	Adversaries may abuse command and script interpreters to execute commands, scripts, or binaries. Netskope NG-SWG can detect and prevent the execution of malicious JavaScript in webpages which are accessed by victims.
Execution	Container Administration Command	N	N/A	N/A	N/A	N/A	N/A	N/A
Execution	Deploy Container	N	N/A	N/A	N/A	N/A	N/A	N/A
Execution	Exploitation for Client Execution	Y	Remote Browser Isolation	Malicious file detection	N/A	N/A	NG-SWG	Adversaries may exploit software vulnerabilities in client applications to execute code. Netskope NG-SWG can detect malicious office documents, and our RBI offering can help isolate exploitation attempts.
Execution	Inter-Process Communication	N	N/A	N/A	N/A	N/A	N/A	N/A
Execution	Native API	N	N/A	N/A	N/A	N/A	N/A	N/A
Execution	Scheduled Task/ Job	N	N/A	N/A	N/A	N/A	N/A	N/A
Execution	Shared Modules	N	N/A	N/A	N/A	N/A	N/A	N/A
Execution	Software Deployment Tools	N	N/A	N/A	N/A	N/A	N/A	N/A
Execution	System Services	N	N/A	N/A	N/A	N/A	N/A	N/A

Category	Technique	Capability	Mitigation	Detection	Source	Page	Solution	Justification
Execution	User Execution	Y	Restrict Web-Based Content	None	N/A	N/A	NG-SWG	An adversary may rely upon specific actions by a user in order to gain execution (often follow-on behavior from phishing). While Netskope does not actually detect the user interaction on an OS, Netskope NG-SWG detects malicious files that are being delivered to the users.
Execution	Windows Management Instrumentation	N	N/A	N/A	N/A	N/A	N/A	N/A
Persistence	Account Manipulation	Y	Privileged Account Manage-ment	Monitor for use of credentials at unusual times or to unusual systems or services. This may also correlate with other suspicious activity. Monitor for unusual permissions changes that may indicate excessively broad permissions being granted to compromised accounts.	CIS Controls v1.pdf	2	UEBA, CSA	Account manipulation may consist of any action that preserves adversary access to a compromised account, such as modifying credentials or permission groups. Netskope UEBA provides alerting around strange credential use and Netskope CSA will alert on lack of multi-factor authentication for IaaS platforms and other insecure practices.
Persistence	BITS Jobs	N	N/A	N/A	N/A	N/A	N/A	N/A
Persistence	Boot or Logon Autostart Execution	N	N/A	N/A	N/A	N/A	N/A	N/A
Persistence	Boot or Logon Initialization Scripts	N	N/A	N/A	N/A	N/A	N/A	N/A
Persistence	Browser Extensions	Y	Restrict Web-Based Content	Malicious file detection	N/A	N/A	NG-SWG	Adversaries may abuse internet browser extensions to establish persistent access to victim systems. Netskope NG-SWG restricts web traffic, which could interrupt any C2 communications happening. In addition, it may block download of the extension if it's recognized as malicious.
Persistence	Compromise Client Software Binary	N	N/A	N/A	N/A	N/A	N/A	N/A
Persistence	Create Account	N	N/A	N/A	NS-Mitre-ATT&CK-Framework-WP-00 (1).pdf	4	N/A	N/A

Category	Technique	Capability	Mitigation	Detection	Source	Page	Solution	Justification
Persistence	Create or Modify System Process	N	N/A	N/A	N/A	N/A	N/A	N/A
Persistence	Event Triggered Execution	N	N/A	N/A	N/A	N/A	N/A	N/A
Persistence	External Remote Services	Y	Limit Access to Resource Over Network, Multi-factor Authentication, Network Segmentation	Detecting adversary use of valid accounts with UEBA			NPA, UEBA	Organizations traditionally manage remote access through VPNs, Citrix, or exposed RDP consoles. Adversaries often target these external remote services as they are publically available and provide network-level access to organizational resources. Netskope Private Access can provision internal applications to remote users without the need for inbound access rules and traditional VPNs. This Zero Trust Network Access capability ensures that remote users access only the applications they have been provisioned and do not gain remote access to the internal network (such as occurs with a VPN). Netskope UEBA can also detect anomalous use of valid account.
Persistence	Hijack Execution Flow	N	N/A	N/A	N/A	N/A	N/A	N/A
Persistence	Implant Container Image	N	N/A	N/A	N/A	N/A	N/A	N/A
Persistence	Modify Authentication Process	N	N/A	N/A	N/A	N/A	N/A	N/A
Persistence	Office Application Startup	N	N/A	N/A	N/A	N/A	N/A	N/A
Persistence	Pre-OS Boot	N	N/A	N/A	CTEP v1.pptx.pdf	11	N/A	N/A
Persistence	Scheduled Task/ Job	N	N/A	N/A	N/A	N/A	N/A	N/A
Persistence	Server Software Component	N	N/A	N/A	N/A	N/A	N/A	N/A
Persistence	Traffic Signaling	N	N/A	N/A	N/A	N/A	N/A	N/A

Category	Technique	Capability	Mitigation	Detection	Source	Page	Solution	Justification
Persistence	Valid Accounts	Y	Multi-factor Authentication	Suspicious account behavior across systems that share accounts	NS-Mitre-ATT&CK-Framework-WP-00 (1).pdf	4	NG-SWG, UEBA	Adversaries may obtain and abuse credentials of existing accounts as a means of gaining Initial Access, Persistence, Privilege Escalation, or Defense Evasion. Netskope can provide insights into the use of cloud and SaaS accounts across multiple applications, including detecting when an account is being used across multiple devices or sessions, which may indicate account compromise. Further, Netskope can enforce MFA for specific actions in SaaS applications, mitigating the impact of a compromised valid accounts
Privilege Escalation	Abuse Elevation Control Mechanism	N	N/A	N/A	CIS Controls v1.pdf	2	N/A	N/A
Privilege Escalation	Access Token Manipulation	N	N/A	N/A	N/A	N/A	N/A	N/A
Privilege Escalation	Boot or Logon Autostart Execution	N	N/A	N/A	N/A	N/A	N/A	N/A
Privilege Escalation	Boot or Logon Initialization Scripts	N	N/A	N/A	N/A	N/A	N/A	N/A
Privilege Escalation	Create or Modify System Process	N	N/A	N/A	N/A	N/A	N/A	N/A
Privilege Escalation	Domain Policy Modification	N	N/A	N/A			N/A	N/A
Privilege Escalation	Escape to Host	N	N/A	N/A			N/A	N/A
Privilege Escalation	Event Triggered Execution	N	N/A	N/A	N/A	N/A	N/A	N/A
Privilege Escalation	Exploitation for Privilege Escalation	N	N/A	N/A	N/A	N/A	N/A	N/A
Privilege Escalation	Hijack Execution Flow	N	N/A	N/A	N/A	N/A	N/A	N/A
Privilege Escalation	Process Injection	N	N/A	N/A	N/A	N/A	N/A	N/A
Privilege Escalation	Scheduled Task/ Job	N	N/A	N/A	N/A	N/A	N/A	N/A

Category	Technique	Capability	Mitigation	Detection	Source	Page	Solution	Justification
Privilege Escalation	Valid Accounts	Y	Multi-factor Authentication	Suspicious account behavior across systems that share accounts	NS-Mitre-ATT&CK-Framework-WP-00 (1).pdf	4	NG-SWG	Adversaries may obtain and abuse credentials of existing accounts as a means of gaining Initial Access, Persistence, Privilege Escalation, or Defense Evasion. Netskope can provide insights into the use of cloud and SaaS accounts across multiple applications, including detecting when an account is being used across multiple devices or sessions, which may indicate account compromise. Further, Netskope can enforce MFA for specific actions in SaaS applications, mitigating the impact of a compromised valid account.
Defense Evasion	Abuse Elevation Control Mechanism	N	N/A	N/A	N/A	N/A	N/A	N/A
Defense Evasion	Access Token Manipulation	N	N/A	N/A	N/A	N/A	N/A	N/A
Defense Evasion	BITS Jobs	N	N/A	N/A	N/A	N/A	N/A	N/A
Defense Evasion	Build Image on Host	N	N/A	N/A	N/A	N/A	N/A	N/A
Defense Evasion	Deobfuscate/ Decode Files or Information	N	N/A	N/A	NS-Mitre-ATT&CK-Framework-WP-00 (1).pdf	4	N/A	N/A
Defense Evasion	Deploy Container	N	N/A	N/A	N/A	N/A	N/A	N/A
Defense Evasion	Direct Volume Access	N	N/A	N/A	CIS Controls v1.pdf	2	N/A	N/A
Defense Evasion	Domain Policy Modification	N	N/A	N/A	N/A	N/A	N/A	N/A
Defense Evasion	Execution Guardrails	N	N/A	N/A	N/A	N/A	N/A	N/A
Defense Evasion	Exploitation for Defense Evasion	N	N/A	N/A			N/A	N/A
Defense Evasion	File and Directory Permissions Modification	N	N/A	N/A	N/A	N/A	N/A	N/A
Defense Evasion	Hide Artifacts	N	N/A	N/A	N/A	N/A	N/A	N/A
Defense Evasion	Hijack Execution Flow	N	N/A	N/A	N/A	N/A	N/A	N/A
Defense Evasion	Impair Defenses	N	N/A	N/A	N/A	N/A	N/A	N/A
Defense Evasion	Indicator Removal on Host	N	N/A	N/A	N/A	N/A	N/A	N/A
Defense Evasion	Indirect Command Execution	N	N/A	N/A	N/A	N/A	N/A	N/A

Category	Technique	Capability	Mitigation	Detection	Source	Page	Solution	Justification
Defense Evasion	Masquerading	N	N/A	N/A	N/A	N/A	N/A	N/A
Defense Evasion	Modify Authentication Process	N	N/A	N/A	NS-Mitre-ATT&CK-Framework-WP-00 (1).pdf	5	N/A	N/A
Defense Evasion	Modify Cloud Compute Infrastructure	Y	No mitigation capability	CSPM detects configuration drift			CSPM	An adversary may attempt to modify a cloud account's compute service infrastructure to evade defenses. A modification to the compute service infrastructure can include the creation, deletion, or modification of one or more components such as compute instances, virtual machines, and snapshots. Netskope CSPM can detect configuration drift in AWS, Azure, and GCP infrastructure, and even actively remediate this activity.
Defense Evasion	Modify Registry	N	N/A	N/A	N/A	N/A	N/A	N/A
Defense Evasion	Modify System Image	N	N/A	N/A	N/A	N/A	N/A	N/A
Defense Evasion	Network Boundary Bridging	N	N/A	N/A	CIS Controls v1.pdf	2	N/A	N/A
Defense Evasion	Obfuscated Files or Information	Y	No mitigation capability	SSL/TLS inspection	NS-Mitre-ATT&CK-Framework-WP-00 (1).pdf	4	NG-SWG	Adversaries may attempt to make an executable or file difficult to discover or analyze by encrypting, encoding, or otherwise obfuscating its contents on the system or in transit. Netskope NG-SWG performs SSL/TLS inspection of all web traffic transiting an organization, which can assist organizations in detecting and identifying obfuscated malware.
Defense Evasion	Pre-OS Boot	N	N/A	N/A	N/A	N/A	N/A	N/A
Defense Evasion	Process Injection	N	N/A	N/A	N/A	N/A	N/A	N/A
Defense Evasion	Rogue Domain Controller	N	N/A	N/A	N/A	N/A	N/A	N/A
Defense Evasion	Rootkit	N	N/A	N/A	N/A	N/A	N/A	N/A
Defense Evasion	Signed Binary Proxy Execution	N	N/A	N/A	N/A	N/A	N/A	N/A
Defense Evasion	Signed Script Proxy Execution	N	N/A	N/A	N/A	N/A	N/A	N/A
Defense Evasion	Subvert Trust Controls	N	N/A	N/A	NS-Mitre-ATT&CK-Framework-WP-00 (1).pdf	4	N/A	N/A

Category	Technique	Capability	Mitigation	Detection	Source	Page	Solution	Justification
Defense Evasion	Template Injection	N	N/A	N/A	NS-Mitre-ATT&CK-Framework-WP-00 (1).pdf	5	N/A	N/A
Defense Evasion	Traffic Signaling	N	N/A	N/A	N/A	N/A	N/A	N/A
Defense Evasion	Trusted Developer Utilities Proxy Execution	N	N/A	N/A	N/A	N/A	N/A	N/A
Defense Evasion	Unused/ Unsupported Cloud Regions	Y	No mitigation capability	CSPM detects configuration drift			CSPM	Adversaries may create cloud instances in unused geographic service regions in order to evade detection. Netskope CSPM can detect and alert on cloud configuration drift, including cloud resources created in unsupported or unused regions.
Defense Evasion	Use Alternate Authentication Material	Y	N/A	UEBA combined with API CASB logs can identify account compromise, such as when an attacker uses stolen access tokens	N/A	N/A	API CASB	Adversaries may use application access tokens to access cloud apps and services. Netskope's API CASB and UEBA capabilities identify account compromise resulting from adversaries abusing alternative authentication material.
Defense Evasion	Valid Accounts	Y	Multi-factor Authentication	Suspicious account behavior across systems that share accounts	NS-Mitre-ATT&CK-Framework-WP-00 (1).pdf	4	NG-SWG	Adversaries may obtain and abuse credentials of existing accounts as a means of gaining Initial Access, Persistence, Privilege Escalation, or Defense Evasion. Netskope can provide insights into the use of cloud and SaaS accounts across multiple applications, including detecting when an account is being used across multiple devices or sessions, which may indicate account compromise. Further, Netskope can enforce MFA for specific actions in SaaS applications, mitigating the impact of a compromised valid account.

Category	Technique	Capability	Mitigation	Detection	Source	Page	Solution	Justification
Defense Evasion	Visualization/ Sandbox Evasion	Y	N/A	Netskope uses multiple sandbox envinronments, including a bare metal sandbox designed to trigger malware, even malware that employ evasion techniques	N/A	N/A	API CASB, NG-SWG	Adversaries may use several methods to accomplish Virtualization/Sandbox Evasion such as the use of sleep timers or loops within malware code to avoid operating within a temporary sandbox. Netskope's multi-layered sandbox uses a variety of techniques to detect even evasive malware.
Defense Evasion	Weaken Encryption	N	N/A	N/A	N/A	N/A	N/A	N/A
Defense Evasion	XSL Script Processing	N	N/A	N/A	N/A	N/A	N/A	N/A
Credential Access	Brute Force	Y	User Account Management	Failed logins	NS-Mitre-ATT&CK-Framework-WP-00 (1).pdf	5	NG-SWG, NPA	Adversaries may use brute force techniques to gain access to accounts when passwords are unknown. Netskope Private Access and NG-SWG provide MFA enforcement for cloud, SaaS, and even internal applications. This can prevent successful brute force attacks.
Credential Access	Credentials from Password Stores	N	N/A	N/A	N/A	N/A	N/A	N/A
Credential Access	Exploitation for Credential Access	Y	N/A	N/A	N/A	N/A	NG-SWG	Adversaries may use exploits to steal credentials or bypass authentication. Netskope NG-SWG includes a client traffic exploit prevention (CTEP) module to prevent web-delivered exploits that can steal credentials or provide remote access, bypassing authentication.
Credential Access	Forced Authentication	N	N/A	N/A	CIS Controls v1.pdf	2	N/A	N/A
Credential Access	Forge Web Credentials	N	N/A	N/A	N/A	N/A	N/A	N/A
Credential Access	Input Capture	N	N/A	N/A	N/A	N/A	N/A	N/A

Category	Technique	Capability	Mitigation	Detection	Source	Page	Solution	Justification
Credential Access	Man-in-the-Middle	Y	Limit Access to Resource Over Network, Network Segmentation	No detection capability			NPA	Adversaries may attempt to position themselves between two or more networked devices using a man-in-the-middle (MiTM) technique to support follow-on behaviors such as Network Sniffing or Transmitted Data Manipulation. Netskope Private Access operates on a zero trust model, where internal applications are exposed via the Netskope platform at the application level. This means that internal applications which may be vulnerable to MiTM attacks, such as those with unencrypted legacy protocols, are protected.
Credential Access	Modify Authentication Process	N	N/A	N/A	NS-Mitre-ATT&CK-Framework-WP-00 (1).pdf	5	N/A	N/A
Credential Access	Network Sniffing	N	N/A	N/A			N/A	N/A
Credential Access	OS Credential Dumping	N	N/A	N/A	N/A	N/A	N/A	N/A
Credential Access	Steal Application Access Token	Y	User Account Management	Hunt for malicious apps in CASB, "High severity app permissions" policy			NG-SWG	Adversaries can steal user application access tokens as a means of acquiring credentials to access remote systems and resources. Adversaries can construct a malicious application designed to be granted access to resources with the target user's access token; often this is done via phishing links sent to the user. Netskope NG-SWG can be configured to block access to unknown or unmanaged SaaS applications, effectively preventing this type of attack. Further, threat hunters can use the NG-SWG to hunt for new and unseen applications which may have requested access tokens from users. For example, they can filter for apps that are authorized by a small number of users, apps requesting high-risk permissions, permissions incongruous with the app's purpose, or apps with old "Last authorized" fields.

Category	Technique	Capability	Mitigation	Detection	Source	Page	Solution	Justification
Credential Access	Steal or Forge Kerberos Tickets	N	N/A	N/A	N/A	N/A	N/A	N/A
Credential Access	Steal Web Session Cookie	Y	No mitigation capability	CTEP signatures	N/A	N/A	NG-SWG	An adversary may steal web application or service session cookies and use them to gain access to web applications or internet services as an authenticated user without needing credentials. Netskope NG-SWG contains a client traffic exploit protection module that includes signatures to detect and block many known cookie stealers.
Credential Access	Two-Factor Authentication Interception	N	N/A	N/A	N/A	N/A	N/A	N/A
Credential Access	Unsecured Credentials	Y	DLP	No detection capability	NS-Mitre-ATT&CK-Framework-WP-00 (1).pdf	5	NG-SWG, API CASB	Adversaries may search compromised systems to find and obtain insecurely stored credentials. Netskope DLP can identify credentials being uploaded to cloud apps or the web where they may be exposed, as commonly occurs with secrets in code repositories.
Discovery	Account Discovery	N	N/A	N/A	NS-Mitre-ATT&CK-Framework-WP-00 (1).pdf	5	N/A	N/A
Discovery	Application Window Discovery	N	N/A	N/A	N/A	N/A	N/A	N/A
Discovery	Browser Bookmark Discovery	N	N/A	N/A	N/A	N/A	N/A	N/A
Discovery	Cloud Infrastructure Discovery	Y	CSPM can help with reviews of IAM users, roles, and policies	Netskope API decoding can detect a large number of describe/view actions by new users			NG-SWG, CSPM	An adversary may attempt to discover resources that are available within an Infrastructure-as-a-Service (IaaS) environment. The discovery of these available resources may help adversaries determine their next steps in the cloud environment, such as establishing Persistence. Netskope NG-SWG can detect and identify users with a large number of API calls to IaaS platforms, including activities from newly identified users.
Discovery	Cloud Service Dashboard	Y	N/A	N/A	N/A	N/A	N/A	N/A

Category	Technique	Capability	Mitigation	Detection	Source	Page	Solution	Justification
Discovery	Cloud Service Discovery	N	N/A	N/A			N/A	N/A
Discovery	Containter and Resource Discovery	N	N/A	N/A			N/A	N/A
Discovery	Domain Trust Discovery	N	N/A	N/A	N/A	N/A	N/A	N/A
Discovery	File and Directory Discovery	N	N/A	N/A	N/A	N/A	N/A	N/A
Discovery	Network Service Scanning	N	N/A	N/A	N/A	N/A	N/A	N/A
Discovery	Network Share Discovery	N	N/A	N/A	N/A	N/A	N/A	N/A
Discovery	Network Sniffing	N	N/A	N/A	N/A	N/A	N/A	N/A
Discovery	Password Policy Discovery	N	N/A	N/A	N/A	N/A	N/A	N/A
Discovery	Peripheral Device Discovery	N	N/A	N/A	N/A	N/A	N/A	N/A
Discovery	Permission Groups Discovery	N	N/A	N/A	NS-Mitre-ATT&CK-Framework-WP-00 (1).pdf	5	N/A	N/A
Discovery	Process Discovery	N	N/A	N/A	N/A	N/A	N/A	N/A
Discovery	Query Registry	N	N/A	N/A	N/A	N/A	N/A	N/A
Discovery	Remote System Discovery	N	N/A	N/A	N/A	N/A	N/A	N/A
Discovery	Software Discovery	N	N/A	N/A	N/A	N/A	N/A	N/A
Discovery	System Information Discovery	N	N/A	N/A	N/A	N/A	N/A	N/A
Discovery	System Location Discovery	N	N/A	N/A	N/A	N/A	N/A	N/A
Discovery	System Network Configuration Discovery	N	N/A	N/A	N/A	N/A	N/A	N/A
Discovery	System Network Connections Discovery	N	N/A	N/A	N/A	N/A	N/A	N/A
Discovery	System Owner/ User Discovery	N	N/A	N/A	N/A	N/A	N/A	N/A
Discovery	System Service Discovery	N	N/A	N/A	N/A	N/A	N/A	N/A
Discovery	System Time Discovery	N	N/A	N/A	N/A	N/A	N/A	N/A
Discovery	Virtualization/ Sandbox Evasion	Y	N/A	Netskope uses multiple sandbox envinronments, including a bare metal sandbox designed to trigger malware, even malware that employ evasion techniques	N/A	N/A	API CASB, NG-SWG	Adversaries may use several methods to accomplish Virtualization/Sandbox Evasion such as the use of sleep timers or loops within malware code to avoid operating within a temporary sandbox. Netskope's multi-layered sandbox uses a variety of techniques to detect even evasive malware.

Category	Technique	Capability	Mitigation	Detection	Source	Page	Solution	Justification
Lateral Movement	Exploitation of Remote Services	N	N/A	N/A	N/A	N/A	N/A	N/A
Lateral Movement	Internal Spearphishing	N	N/A	N/A	N/A	N/A	N/A	N/A
Lateral Movement	Lateral Tool Transfer	N	N/A	N/A	N/A	N/A	N/A	N/A
Lateral Movement	Remote Service Session Hijacking	N	N/A	N/A	N/A	N/A	N/A	N/A
Lateral Movement	Remote Services	Y	Multi-factor Authentication, User Account Management	No detection capability	NS-Mitre-ATT&CK-Framework-WP-00 (1).pdf	5	NPA	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, including moving laterally. Netskope Private Access can provision RDP access to only a specified list of users, while enforcing conditional access policies and MFA. This prevents RDP from being exposed to the internet, while ensuring that only legitimate users are using the remote service.
Lateral Movement	Replication Through Removable Media	N	N/A	N/A	N/A	N/A	N/A	N/A
Lateral Movement	Software Deployment Tools	N	N/A	N/A	N/A	N/A	N/A	N/A
Lateral Movement	Taint Shared Content	Y	No mitigation capability	Cloud storage scan	NS-Mitre-ATT&CK-Framework-WP-00 (1).pdf	5	NG-SWG, API CASB	Content stored on cloud-hosted locations may be tainted by adding malicious programs, scripts, or exploit code to otherwise valid files. Once a user opens the shared tainted content, the malicious portion can be executed to run the adversary's code on a remote system. Netskope's Cloud Storage Scan continuously monitors cloud storage for malicious files, detecting and alerting when malware is present on a cloud storage repository.
Lateral Movement	Use Alternate Authentication Material	N	N/A	N/A	N/A	N/A	N/A	N/A

Category	Technique	Capability	Mitigation	Detection	Source	Page	Solution	Justification
Collection	Archive Collected Data	Y	No mitigation capability	DLP	N/A	N/A	NG-SWG	An adversary may compress and/or encrypt data that is collected prior to exfiltration. Compressing the data can help to obfuscate the collected data and minimize the amount of data sent over the network. Netskope NG-SWG leverages DLP to detect and block uploads of encrypted data.
Collection	Audio Capture	N	N/A	N/A	N/A	N/A	N/A	N/A
Collection	Automated Collection	Y	Encrypt Sensitive Information, Remote Data Storage	No detection capability	NS-Mitre-ATT&CK-Framework-WP-00 (1).pdf	6	NG-SWG, CSPM	Once established within a system or network, an adversary may use automated techniques for collecting internal data. Netskope Cloud Storage Scan can identify sensitive data in cloud repositories and encrypt it, mitigating the impact of an adversary's automated collection.
Collection	Clipboard Data	N	N/A	N/A	N/A	N/A	N/A	N/A
Collection	Data from Cloud Storage Object	Y	Audit File Permissions, Encrypt Sensitive Information, Multi-factor Authentication	Mass file download			NG-SWG, CSPM	Adversaries may access data objects from improperly secured cloud storage. Netskope CSPM can detect incorrectly configured cloud storage locations, including public S3 buckets, and alert organizational security teams to remediate. Further, Netskope NG-SWG can detect and prevent mass file download events from SaaS and IaaS instances, both managed and unmanaged. This can help mitigate an adversary's data collection attempts.
Collection	Data from Configuration Repository	N	N/A	N/A	N/A	N/A	N/A	N/A

Category	Technique	Capability	Mitigation	Detection	Source	Page	Solution	Justification
Collection	Data from Information Repositories	Y	User Account Management	Privileged users access monitoring	NS-Mitre-ATT&CK-Framework-WP-00 (1).pdf	6	NG-SWG	Adversaries may leverage information repositories to mine valuable information. Information stored in a repository may vary based on the specific instance or environment. Specific common information repositories include SharePoint and Confluence. Netskope NG-SWG audits all API activity in cloud SaaS applications, including SharePoint and Confluence, which can help security teams identify risky users who are accessing sensitive information repositories.
Collection	Data from Local System	N	N/A	N/A	N/A	N/A	N/A	N/A
Collection	Data from Network Shared Drive	N	N/A	N/A	N/A	N/A	N/A	N/A
Collection	Data from Removable Storage	N	N/A	N/A	N/A	N/A	N/A	N/A
Collection	Data Staged	N	N/A	N/A			N/A	N/A
Collection	Email Collection	Y	No mitigation capability	Email DLP	CIS Controls v1.pdf	2	Email DLP	Adversaries may target user email to collect sensitive information. Emails may contain sensitive data, including trade secrets or personal information, that can prove valuable to adversaries. Netskope email DLP can prevent sensitive information from being exfiltrated over email.
Collection	Input Capture	N	N/A	N/A	N/A	N/A	N/A	N/A
Collection	Man in the Browser	N	N/A	Detect malicious JavaScript content	CTEP v1.pptx.pdf	11	NG-SWG	Adversaries can take advantage of security vulnerabilities and inherent functionality in browser software to change content, modify behavior, and intercept information as part of various man in the browser techniques. Netskope NG-SWG contains client threat exploit protection, content inspection, and threat intelligence modules that can detect malicious content loaded by browsers as a result of MiTB attacks like malicious browser extensions.

Category	Technique	Capability	Mitigation	Detection	Source	Page	Solution	Justification
Collection	Man-in-the-Middle	Y	Limit Access to Resource Over Network, Network Segmentation	No detection capability			NPA	Adversaries may attempt to position themselves between two or more networked devices using a man-in-the-middle (MiTM) technique to support follow-on behaviors such as Network Sniffing or Transmitted Data Manipulation. Netskope Private Access operates on a zero trust model, where internal applications are exposed via the Netskope platform at the application level. This means that internal applications which may be vulnerable to MiTM attacks, such as those with unencrypted legacy protocols, are protected.
Collection	Screen Capture	Y	No mitigation capability	Advanced DLP	N/A	N/A	NG-SWG	Adversaries may attempt to take screen captures of the desktop to gather information over the course of an operation. Screen capturing functionality may be included as a feature of a remote access tool used in post-compromise operations. Netskope NG-SWG Advanced DLP includes a screenshot detection mechanism that can detect screenshots being uploaded to cloud apps or to the web.
Collection	Video Capture	N	N/A	N/A	N/A	N/A	N/A	N/A
Command and Control	Application Layer Protocol	Y	Malware Detection Over HTTP/S	Monitor for web traffic to/from known-bad or suspicious domains.			NG-SWG	Adversaries may communicate using application layer protocols associated with web traffic to avoid detection/network filtering by blending in with existing traffic. Netskope NG-SWG inspects SSL/TLS network traffic transiting an organisation and can monitor and alert on connections to known-bad domains.
Command and Control	Communication Through Removable Media	N	N/A	N/A	N/A	N/A	N/A	N/A
Command and Control	Data Encoding	N	N/A	N/A			N/A	N/A

Category	Technique	Capability	Mitigation	Detection	Source	Page	Solution	Justification
Command and Control	Data Obfuscation	N	N/A	N/A	N/A	N/A	N/A	N/A
Command and Control	Dynamic Resolution	Y	N/A	DGA and NRD detection	N/A	N/A	NG-SWG	Adversaries may dynamically establish connections to command and control infrastructure to evade common detections and remediations. Netskope NG-SWG includes advanced DGA detection to detect and block suspicious domains and can also block all newly registered domains.
Command and Control	Encrypted Channel	Y	No mitigation capability	SSL/TLS inspection			NG-SWG	Adversaries may employ a known encryption algorithm to conceal command and control traffic rather than relying on any inherent protections provided by a communication protocol. Netskope NG-SWG inspects SSL/TLS network traffic transiting an organization and can detect command and control traffic with encrypted communication channels.
Command and Control	Fallback Channels	N	N/A	N/A	N/A	N/A	N/A	N/A
Command and Control	Ingress Tool Transfer	Y	Restrict Web-Based Content	In-line malware detection			NG-SWG	Adversaries may transfer tools or other files from an external system into a compromised environment. Netskope NG-SWG Advanced Threat Protection provides unpacking and de-obfuscation, pre-execution analysis, with cloud and bare-metal sandboxing for 30+ file types. This analysis is combined with open- and close-source threat intelligence, which can detect and alert on known malicious adversarial tools.
Command and Control	Multi-Stage Channels	N	N/A	N/A	N/A	N/A	N/A	N/A
Command and Control	Non-Application Layer Protocol	N	N/A	N/A	N/A	N/A	N/A	N/A
Command and Control	Non-Standard Port	N	N/A	N/A	N/A	N/A	N/A	N/A
Command and Control	Protocol Tunneling	N	N/A	N/A	N/A	N/A	N/A	N/A

Category	Technique	Capability	Mitigation	Detection	Source	Page	Solution	Justification
Command and Control	Proxy	Y	Restrict Web-Based Content	SSL/TLS inspection			NG-SWG	Adversaries may take advantage of routing schemes in Content Delivery Networks (CDNs) and other services which host multiple domains to obfuscate the intended destination of HTTPS traffic or traffic tunneled through HTTPS. Netskope NG-SWG performs SSL/TLS inspection for all web traffic, which can be used to identify C2 traffic which is domain fronting.
Command and Control	Remote Access Software	Y	Restrict Web-Based Content	Traffic to TeamViewer and other services	CIS Controls v1.pdf	2	NG-SWG	An adversary may use legitimate desktop support and remote access software, such as Team Viewer, Go2Assist, LogMeIn, Ammyy Admin, etc., to establish an interactive command and control channel to target systems within networks. Netskope NG-SWG can detect and alert on outgoing traffic to sites and services used by remote access tools.
Command and Control	Traffic Signaling	N	N/A	N/A	N/A	N/A	N/A	N/A
Command and Control	Web Services	Y	Network Intrusion Prevention, Restrict Web-Based Content	No detection capability	NS-Mitre-ATT&CK-Framework-WP-00 (1).pdf	6	NG-SWG	Adversaries may use an existing, legitimate external web service as a means for relaying data to/from a compromised system. Netskope NG-SWG can block web traffic to known-bad external web services, such as Ngrok.
Exfiltration	Automated Exfiltration	Y	No mitigation capability	UEBA	NS-Mitre-ATT&CK-Framework-WP-00 (1).pdf	6	NG-SWG	Adversaries may exfiltrate data, such as sensitive documents, through the use of automated processing after being gathered during Collection. Netskope NG-SWG can detect exfiltration of data to cloud apps, using UEBA to identify uploads of unusually large quantities of data, or uploads to unusual apps and instances.

Category	Technique	Capability	Mitigation	Detection	Source	Page	Solution	Justification
Exfiltration	Data Transfer Size Limits	Y	No mitigation capability	UEBA	NS-Mitre-ATT&CK-Framework-WP-00 (1).pdf	6	NG-SWG	An adversary may exfiltrate data in fixed size chunks instead of whole files or limit packet sizes below certain thresholds. This approach may be used to avoid triggering network data transfer threshold alerts. Netskope NG-SWG can detect exfiltration of data to cloud apps, using UEBA to identify uploads of unusually large quantities of data, or uploads to unusual apps and instances.
Exfiltration	Exfiltration Over Alternative Protocol	Y	Restrict Web-Based Content	SSL/TLS inspection	NS-Mitre-ATT&CK-Framework-WP-00 (1).pdf	6	NG-SWG	Adversaries may steal data by exfiltrating it over a different protocol than that of the existing command and control channel. Netskope NG-SWG can detect C2 HTTP/S traffic and perform SSL/TLS inspection to identify data being exfiltrated.
Exfiltration	Exfiltration Over C2 Channel	Y	Restrict Web-Based Content	SSL/TLS inspection	NS-Mitre-ATT&CK-Framework-WP-00 (1).pdf	6	NG-SWG	Adversaries may steal data by exfiltrating it over an existing command and control channel. Netskope NG-SWG can detect C2 HTTP/S traffic and perform SSL/TLS inspection to identify data being exfiltrated.
Exfiltration	Exfiltration Over Other Network Medium	N	N/A	N/A	N/A	N/A	N/A	N/A
Exfiltration	Exfiltration Over Physical Medium	N	N/A	N/A	N/A	N/A	N/A	N/A
Exfiltration	Exfiltration Over Web Service	Y	Restrict Web-Based Content	Large upload actions	Netskope Platform Overview v3.pdf	2	NG-SWG	Adversaries may use an existing, legitimate external web service to exfiltrate data rather than their primary command and control channel. Netskope NG-SWG audits all API activity to cloud SaaS apps, including cloud storage. Netskope can alert and block mass-upload actions initiated by users, and alert security teams to exfiltration attempts.
Exfiltration	Scheduled Transfer	N	N/A	N/A			N/A	N/A

Category	Technique	Capability	Mitigation	Detection	Source	Page	Solution	Justification
Exfiltration	Transfer Data to Cloud Account	Y	Prevent upload to unmanaged Cloud Storage	Large upload actions	Netskope Platform Overview v3.pdf	11	NG-SWG	Adversaries may exfiltrate data by transferring the data, including backups of cloud environments, to another cloud account they control on the same service to avoid typical file transfers/downloads and network-based exfiltration detection. Netskope NG-SWG can detect the use of unmanaged cloud applications, even identifying different IaaS cloud accounts. Netskope can be configured to prevent data transfers to unmanaged cloud account instances.
Impact	Account Access Removal	N	N/A	N/A	N/A	N/A	N/A	N/A
Impact	Data Destruction	Y	Multi-factor Authentication	Delete API actions	CIS Controls v1.pdf	2	Inline and API CASB, UEBA	Adversaries may destroy data and files on specific systems or in large numbers on a network to interrupt availability to systems, services, and network resources. Netskope NG-SWG can prevent delete API actions on managed cloud SaaS applications, preventing the destruction of data by adversaries. Further, Netskope NG-SWG can enforce an MFA step-up when a delete API action is attempted.
Impact	Data Encrypted for Impact	N	N/A	N/A	CIS Controls v1.pdf	2	N/A	N/A
Impact	Data Manipulation	N	N/A	N/A	CIS Controls v1.pdf	2	N/A	N/A
Impact	Defacement	N	N/A	N/A	NS-Mitre-ATT&CK-Framework-WP-00 (1).pdf	5	N/A	N/A
Impact	Disk Wipe	N	N/A	N/A	N/A	N/A	N/A	N/A
Impact	Endpoint Denial of Service	N	N/A	N/A	N/A	N/A	N/A	N/A
Impact	Firmware Corruption	N	N/A	N/A	N/A	N/A	N/A	N/A
Impact	Inhibit System Recovery	N	N/A	N/A	N/A	N/A	N/A	N/A
Impact	Network Denial of Service	N	N/A	N/A	CTEP v1.pptx.pdf	11	N/A	N/A

Category	Technique	Capability	Mitigation	Detection	Source	Page	Solution	Justification
Impact	Resource Hijacking	Y	N/A	Detect downloads of miners and miner-related network	N/A	N/A	NG-SWG	Adversaries may leverage the resources of co-opted systems in order to solve resource intensive problems which may impact system and/or hosted service availability. One common purpose for Resource Hijacking is to validate transactions of cryptocurrency networks and earn virtual currency. Netskope NG-SWG can detecty downloads of crypto-minters and crypto-miner related network communication using our client traffic exploit protection module, threat scanning, and NSIQ, our threat intelligence.
Impact	Service Stop	N	N/A	N/A	N/A	N/A	N/A	N/A
Impact	System Shutdown/ Reboot	N	N/A	N/A	N/A	N/A	N/A	N/A