Netskope Policies (Current State)

By Palak 12 min 3

Block Malware Upload/Download - Threat Protection

If a user—whether intentionally or unintentionally—attempts to upload or download a malicious file from any application category monitored by Netskope, the platform will restrict the action using this policy, ensuring enhanced security across your cloud environment.

Benefits:

- **Proactive Threat Prevention:** Blocks malware before it can enter or spread within your environment, reducing the risk of data breaches, ransomware, and other cyber threats.
- **Data Integrity:** Ensures that files shared within and outside the organization remain clean and trustworthy.
- **Compliance Support:** Helps meet regulatory and industry standards that require malware scanning and threat protection in cloud environments.
- **Reduced Incident Response Effort:** Minimizes the need for remediation and incident handling caused by malware infections.

Potential Negative Impacts:

- **False Positives:** Legitimate files may be mistakenly flagged as malicious, leading to unnecessary disruptions in business operations.
- **User Frustration:** Users may experience workflow interruptions, especially when urgent file transfers are blocked.
- **Operational Delays:** Blocking downloads/uploads can delay collaboration, particularly when working with third-party vendors or clients who may unknowingly share flagged files.

Block Malicious Sites

Websites that are widespread, exploitative, or capable of directly impacting business availability and operations are categorized as malicious based on their associated security risks. Blocking access to such high-risk domains is a crucial component of a proactive risk management strategy, helping us minimize vulnerabilities and prevent potential threats from reaching users or endpoints.

Benefits:

- **Improved Security Posture:** Prevents users from accessing sites known for distributing malware, phishing content, or hosting exploit kits.
- **Business Continuity:** Reduces the risk of service disruptions and data breaches caused by threat actors using malicious web domains.

- **Compliance and Governance:** Supports adherence to cybersecurity regulations by enforcing safe browsing practices.
- **Enhanced Threat Visibility:** Leverages Netskope's threat intelligence to provide real-time insights into emerging threats and risky destinations.

Potential Negative Impacts:

- **Access Limitations:** Some sites may be blocked due to aggressive categorization, potentially affecting research or legitimate use cases.
- **False Positives:** Legitimate websites might be misclassified, leading to user confusion or operational slowdowns.
- **User Experience Friction:** Blocking access may result in user dissatisfaction and support requests.

Following are the different categories under malicious sites:

Security Risk	Description
Ad Fraud	Sites that are being used to commit fraudulent online display advertising transactions using different ad impression boosting techniques, including but not limited to ads stacking, iframe stuffing, and hidden ads. Sites that have high non-human web traffic and with rapid, large, and unexplained changes in traffic. Web analysts should not use this category.
Attack	Sites that attempt to gain unauthorized access to information resources or services or cause harm or damage to information systems.
Botnets	Sites or compromised web servers running software that is used by hackers to send spam, phishing attacks, and denial of service attacks.
Command and Control Server	Internet servers and compromised command and control (C2 or C&C) servers and centers used to send commands to infected machines called bots. And sites that are a security risk because call-home malware is detected.
Compromised/Malicious Sites	Sites that appear to be legitimate, but house malicious code or link to malicious websites hosting malware. These sites have been compromised by someone other than the site owner. If Firefox blocks a site as malicious, use this category. Examples are defaced, hacked by, etc.
Cryptocurrency Mining	Sites that use cryptocurrency mining technology without user permission. This is considered a malicious category.
DGA	Domains that are generated algorithmically using a domain generation algorithm (DGA). These domains are used by DGA-based malware as their C2 channel, and they aim to hide the location of the active C2 server.
Hacking	Sites with information or tools specifically intended to assist in online crime, such as the unauthorized access to computers, but also pages with tools and information that enables fraud and other online crime.
Malware Distribution Point	Sites that host viruses, exploits, and other malware are considered Malware Distribution Points. Web analysts might use this category if their antivirus program triggers on a particular website. Other categories should also be added if applicable.
Miscellaneous	Sites with security risk indicators that aren't mapped to any of the other listed security risk types (e.g., high risk, medium risk, and possible risk).
Phishing/Fraud	Sites that impersonate other web pages, usually with the intent of stealing passwords, credit card numbers, or other information. Also includes websites that are part of scams such as a 419 scam where a person is convinced to hand over money with the expectation of a big payback that never comes (e.g., con, hoax, scam, etc.).
Spam	URLs that frequently occur in spam messages. Web analysts shouldn't use this.

Spyware & Questionable Software	Software that reports information back to a central server such as spyware or keystroke loggers. It also includes software that may have legitimate purposes, but some people may object to having on their system. Web analysts shouldn't use this category.

Block Prohibited Sites

To enforce acceptable use policies blocking access to web content across a wide range of inappropriate or high-risk categories becomes necessary . These include adult content, gambling, drugs, criminal activities, and other themes that could pose legal, ethical, or operational risks to Atlan. This categorization is continually updated using real-time analysis and threat intelligence, ensuring accurate enforcement and risk reduction across all user traffic.

Benefits:

- **Policy Compliance Enforcement:** Supports internal governance and legal requirements by restricting access to non-compliant, unethical, or regulated content types.
- **Workplace Productivity:** Minimizes distractions by blocking access to content categories unrelated to professional responsibilities, such as games, pornography, or alcohol-related pages.
- **Risk Reduction:** Helps protect users from inadvertently accessing harmful, exploitative, or illegal content, including child abuse, aggressive media, and remote access tools that enable shadow IT.
- **Customizable Enforcement:** Allows organizations to apply differentiated controls by department or user group, ensuring balance between security and operational flexibility.

Potential Negative Impacts:

- **False Positives:** Websites may occasionally be misclassified, impacting business operations and requiring manual whitelisting or policy updates.
- **User Frustration:** Users may encounter blocked pages during routine browsing, leading to dissatisfaction or increased support requests.
- **Policy Maintenance Burden:** Ensuring alignment between evolving business needs and categorical enforcement may require periodic review and tuning of blocked categories.

Following are the different categories under prohibited sites in Atlan:

Category	Description	Sample URLs
Abortion	Web pages discussing abortion from historical, medical, or legal viewpoints (not overtly biased).	abortion.com, http://gynpages.com , http://abortionfacts.com
Adult Content – Other	Adult content excluding pornography (e.g., sex, nudity, adult shopping).	http://mature-sexcontacts.com
Adult Content – Pornography	Sites that portray explicit sexual content.	http://xvideos.com , http://youporn.com
Aggressive	Content promoting or displaying violence, torture, or militancy (e.g., crime scenes, mutilation).	http://murders.ru , malaprensa.com, alombredelespoir.org
Alcohol	Sites showing or promoting alcoholic beverages.	http://thewinecellarinsider.com , http://johnniewalker.com
Child Abuse	Sites showing physical or sexual abuse of children.	NULL
Criminal Activities	Sites promoting illegal acts like bomb-making, theft, or necrophilia.	http://sosvox.org , uggsheepskinboots.us

Drugs	Sites endorsing or glamorizing drug use and culture.	http://magicmushroom.com , buyecstasy.com, http://buy-magic-mushrooms.com
Gambling	Sites involving betting or gambling strategies.	http://betfair.com , http://lotterypost.com
Games	Sites hosting non-gambling games or related content.	http://gamespot.com , http://epicgames.com
Peer-to-Peer (P2P)	Sites that provide or support file sharing software (e.g., emule, frostwire).	http://thepiratebay.org , http://1337x.tw , torlock.com
Remote Access	Sites offering remote desktop or VPN access services.	http://teamviewer.com , http://remotepc.com
Tobacco	Sites selling or promoting tobacco products.	http://cigarsinternational.com , http://allcigs.com , thompsoncigars.com
Web Proxies/Anonymizers	Services that anonymize browsing and mask user identity (e.g., VPNs, web proxies).	http://kproxy.com , http://hidemyass.com , http://expressvpn.com

Block Ads (Already applied on Firewall)

Ads are often a vector for **malvertising**—a tactic where malicious code is embedded in legitimate ad networks to target users without their knowledge. By blocking ads, we can improve security, reduce distractions, and enhance overall web performance.

Benefits:

- **Reduced Exposure to Malvertising:** Prevents users from being targeted by malicious ads that could lead to malware infections or phishing sites.
- **Improved User Productivity:** Eliminating distracting ads can help employees stay focused on work-related tasks.
- **Faster Web Browsing:** Blocking ad content can significantly reduce page load times, improving overall browsing experience.
- **Lower Bandwidth Usage:** Ads consume network resources; blocking them can optimize bandwidth usage across the organization.

Potential Negative Impacts:

- **Website Functionality Issues:** Some websites rely on ad frameworks for functionality, and blocking ads might break site layouts or prevent access to content.
- **Impact on Freemium Services:** Users may be unable to access ad-supported content or services, such as free tools, streaming platforms, or news websites.
- **End User Complaints:** Users might encounter blocked pages without understanding why, leading to support tickets and frustration.

Restrict Personal Account Access

By leveraging deep application context, Netskope can differentiate between **corporate and personal instances** of cloud services, applying controls based on user identity, instance type, or activity.

Restricting personal account access—especially in critical categories like **Cloud Storage**, **Webmail**, **Collaboration Tools**, and **Development Platforms**—is a key strategy for enforcing **data governance policies**, particularly in environments with **high adoption of multi-tenant SaaS** platforms.

For instance:

- **Cloud Storage platforms** (e.g., Google Drive, Dropbox) often enable seamless file syncing via browser or sync clients. While corporate drives can be monitored and protected, personal drives can act as a blind spot for exfiltrating sensitive data.
- **Webmail services** (e.g., Gmail, Outlook) offer users a convenient way to send or forward documents—but these accounts often fall outside enterprise visibility and DLP inspection.

- **Collaboration apps** (e.g., Slack, Zoom) can retain shared files or chat history in unmanaged personal instances, exposing confidential communication.
- **Development Tools** (e.g., GitHub) accessed via personal repositories may lead to inadvertent exposure of intellectual property or code artifacts.

In such cases, Netskope's ability to enforce **instance-aware policy controls** becomes critical. Where app architecture does not support identity distinction—such as desktop clients or certificate-pinned tools—**blocking personal usage altogether** is the most effective safeguard.

Benefits:

- **Data Loss Prevention:** Prevents employees from uploading, sharing, or downloading sensitive corporate data through personal accounts on platforms like Gmail, Google Drive, Dropbox, or Zoom.
- **Shadow IT Control:** Reduces visibility gaps and unmanaged app usage by blocking personal instances of cloud services not sanctioned by IT.
- **Compliance Assurance:** Helps meet regulatory requirements by ensuring data handling only occurs through authorized and monitored channels.
- **Granular Enforcement:** Netskope supports instance-level policy enforcement—allowing personal instances to be blocked while allowing corporate accounts to function normally.

Potential Negative Impacts:

- **Productivity Disruption:** Some users may rely on personal tools for convenience, and restrictions could temporarily impact workflows if alternatives aren't in place.
- **Misidentification of Accounts:** Mistakenly categorizing a corporate account as personal (or vice versa) can lead to improper blocking or unintended data exposure.
- **User Pushback:** Blocking access to familiar tools may result in friction or resistance from users, especially in hybrid or BYOD environments.
- **Policy Maintenance:** Requires consistent policy tuning to accommodate new applications, domains, and user patterns across different departments.

Following are the different categories under Personal Login Restriction:

Category	Description	Sample URLs
Application Suite	Applications that include multiple products from the same company, often used across various categories and business functions.	http://gsuite.google.com , atlassian.net, http://axway.com
Cloud Backup	Applications used for backing up consumer or enterprise data to the cloud to mitigate data loss due to device failure, corruption, or disasters.	http://druva.com , http://crashplan.com , http://jungledisk.com
Cloud Storage	Services for uploading and storing data in the cloud, often accessible through web apps, APIs, or desktop tools. **High risk of data exfiltration via personal accounts.**	drive.google.com, http://box.com , http://dropbox.com
Collaboration	Platforms that support group interaction, communication, or joint efforts to achieve shared goals. **Personal accounts can host confidential chats or shared files.**	http://sharepoint.com , http://slack.com , http://zoom.us
Content Management	Systems used for creating, managing, and publishing digital content including multimedia and documents.	http://cloudinary.com , http://clearvoice.com , http://drupal.org

Development Tools	Services used by software developers for source control, issue tracking, and application lifecycle management. **Risk of source code leaks via unmanaged personal repos.**	http://developer.salesforce.com , http://visualstudio.microsoft.com , http://github.com
Generative AI	Platforms leveraging AI/ML models to generate text, visuals, or code from existing datasets.	http://chat.openai.com , http://jasper.ai , http://beautiful.ai
IaaS/PaaS	Infrastructure and platform services offering scalable compute, storage, and application hosting capabilities.	http://aws.amazon.com , http://azure.microsoft.com , http://cloud.google.com
Identity and Access Management	Tools that enable secure user authentication, single sign-on (SSO), and user provisioning across enterprise applications.	http://onelogin.com , auth0.com, http://okta.com
Web Conferencing	Tools for conducting virtual meetings, webinars, or remote collaboration sessions via video and audio communication.	http://webex.com , http://zoom.us , http://gotomeeting.com
Webmail	Web-based email platforms that allow users to access email through a browser interface, typically used for both personal and business communication. **Primary exfiltration vector if left unmanaged.**	mail.google.com, http://outlook.com , http://protonmail.com

Block Upload of PII, PHI, and PCI Across all Categories

To protect sensitive data and maintain regulatory compliance, **Blocking the upload of Personally Identifiable Information (PII), Protected Health Information (PHI), and Payment Card Information (PCI)** across **all application categories by default is required** .This control is enforced using **Advanced Data Loss Prevention (DLP)** policies that inspect content in real-time before allowing uploads to proceed.

Benefits:

- **Regulatory Compliance:** Helps meet standards such as GDPR, HIPAA, PCI DSS, and other data protection regulations.
- **Risk Reduction:** Prevents accidental or intentional data exposure through uploads to unauthorized or unsanctioned platforms.
- **Consistent Protection:** Ensures sensitive data is blocked regardless of the application or user location (on-network, remote, or mobile).
- **Auditability:** Provides detailed logging and reporting for all blocked events, supporting security investigations and audits.

Implications:

- **False Positives:** Strict DLP rules may block legitimate business uploads if the content contains patterns resembling sensitive data (e.g., test data or IDs).
- **User Friction:** Users may encounter blocked actions, leading to confusion or support requests if exception workflows are not clearly defined.
- **Exception Handling Required:** Critical workflows (e.g., HR uploading to secure HR platforms) may require granular exception policies to avoid disruption.

Allow Upload of PII, PHI, and PCI to Approved Atlan Instances with Monitoring

To support business productivity while maintaining data governance, **allowing the upload of sensitive data types—including PII, PHI, and PCI—to trusted Atlan instances** listed in the **Atlan SaaS Cloud Apps List** , while ensuring full **monitoring and visibility** through DLP logging and analytics is required.

This approach empowers users to work efficiently in Atlan with regulated data, without compromising on oversight or compliance tracking.

Benefits:

- **Supports Business Productivity:** Enables data teams to perform critical tasks in Atlan (e.g., metadata management, compliance mapping) without DLP blocks.
- **Governed Enablement:** Restricts uploads to approved, sanctioned Atlan tenants only—no broad access.
- **Full Visibility:** DLP policies continue to log all uploads, providing audit trails and enabling security teams to review and respond to anomalies.
- **Minimizes Workflow Disruptions:** Prevents unnecessary upload blocks while still ensuring security oversight.
- **Compliance Alignment:** Allows for safe handling of sensitive data within known, trusted cloud applications.

Negative Implications:

- **Monitoring Without Blocking:** While data is logged, it is not actively blocked—requires robust alerting and quick incident response.
- **Risk of Misuse:** If misconfigured, users could potentially upload sensitive data to incorrect or impersonated Atlan instances.
- **Over-reliance on Trust:** Assumes the Atlan environment is properly secured and monitored internally.
- **Policy Maintenance Required:** Regular review is necessary to ensure only current and trusted tenants remain on the allow list.

Block All Upload

Allowing users to upload files to unmanaged or non-corporate platforms—such as chat applications, file converters, and social media—poses significant risks to Atlan's data security posture. These platforms often fall outside the visibility and control of enterprise security tools, making them attractive vectors for intentional or accidental **data exfiltration**.

With **Netskope's deep contextual controls**, organizations can enforce **"Block All Upload"** policies on such categories to ensure sensitive files do not leave approved channels, while still allowing read-only or monitoring access where necessary.

This is particularly important for:

- **Chat & IM Platforms**, which enable fast, informal file sharing with no audit trails.
- **File Converter Sites**, which may allow format shifting to bypass content controls (e.g., converting `.docx` to `.jpg`).
- **Social Media**, where users can post files or screenshots of confidential information to a public or semi-public audience.

Benefits:

- **Prevents Data Leakage:** Stops file transfers to unmanaged and risky platforms, reducing the threat of unintentional leaks or insider abuse.
- **Mitigates Compliance Risk:** Helps enforce data protection policies (e.g., GDPR, HIPAA, PCI-DSS) by eliminating unmonitored outbound channels.
- **Neutralizes Bypass Attempts:** File converters are often used to alter file types to evade detection. Blocking uploads thwarts this vector entirely.
- **Controls Shadow IT:** Many communication and social apps used personally or unofficially (e.g., WhatsApp, Snapchat) are invisible to IT without upload restrictions.

Potential Negative Impacts:

- **User Frustration:** Employees may feel limited or frustrated when blocked from uploading to familiar tools they use for quick communication or personal productivity.
- **Collaboration Challenges:** Cross-functional teams or external partners relying on personal chat or social apps may encounter barriers in communication.
- **Increased Support Requests:** Blocking uploads can lead to helpdesk tickets, especially if the rationale and alternatives are not clearly communicated.

Following are the different categories under Block All Upload:

Category	Description	Sample URLs

Chat, IM & Other Communication	Web pages with real-time chat rooms and messaging allowing strangers and friends to chat in groups both in public and private chats. Includes Internet Relay Chat (IRC).	http://whatsapp.com , hangouts.google.com, http://line.me
File Converter	Sites that allow conversion of files from one type to another, such as documents (including PDF files), images, audio, video, etc.	pdf.online, http://freepdfconvert.com , http://onlineconvertfree.com
Social	Websites and applications that enable users to create and share content or to participate in social networking.	http://facebook.com , http://snapchat.com , twitter.com

SSL Bypass

To ensure seamless user experience, Netskope recommends the following best practices for configuring traffic steering and SSL inspection:

Bypass Steering for Collaboration Applications

Netskope advises bypassing traffic steering for widely-used collaboration platforms such as **Microsoft Teams, Zoom, WebEx, and Slack (calls)**. These apps often utilize dynamic IPs, peer-to-peer connections, and real-time media protocols, which can be disrupted by SSL inspection or proxy routing.

Benefits:

- Preserves **call/video quality** and connection reliability.
- Reduces **latency and jitter** during live meetings.
- Minimizes **IT troubleshooting** for real-time communication issues.

Implications:

- Collaboration traffic is **not inspected**, which slightly reduces visibility for those specific flows.
- Requires **ongoing monitoring** to ensure newly introduced domains/IPs are also bypassed.

Sensitive Sectors

Sensitive sectors such as **Government , Finance etc** often rely on secure, authenticated platforms and encrypted services to access portals, applications, and cloud storage (e.g., **banking sites**, **tax platforms**).

To avoid disrupting access and ensure seamless functionality, **Netskope recommends bypassing SSL inspection and traffic steering** for these categories.

Benefits:

- **Preserves Functionality:** Avoids broken logins or page errors caused by interception of encrypted traffic.
- **Ensures Compliance:** Supports uninterrupted access to regulatory platforms (e.g., tax portals, medical systems).
- **Reduces Operational Risk:** Prevents false positives or blocks that could impact business-critical transactions.

Implications:

- **Reduced Visibility:** Bypassing SSL inspection limits Netskope's ability to inspect and apply DLP or threat protection to these specific flows.
- **Trust-Based Access:** Assumes that the sites categorized under Finance, Government, and Healthcare are legitimate—requires continuous category accuracy and validation.

- **Monitoring Still Recommended:** Traffic should still be monitored at a high level (e.g., URL categorization and access logs) even if content is not decrypted.