netskope

Compliance Series

Using the Netskope Platform to Achieve Cyber Essentials Certification

Table of Contents

Introduction 2

Firewalls 5

Secure Configuration 7

Security Update Management 9

User Access Control 10

Malware Protection 13

Version	Name	Email	Date
V1.0	Scott Bullock Neil Thacker	sbullock@netskope.com nthacker@netskope.com	30th July 2024

INTRODUCTION

Cyber Essentials is a UK Government-backed initiative designed to help organisations of all sizes protect themselves against the most common cyber threats. Implementing Cyber Essentials effectively can enhance an organisation's cybersecurity by establishing fundamental controls to mitigate attacks. Additionally, achieving certification can reassure potential customers and suppliers that the organisation has taken essential steps to safeguard against cyber threats.

Originally launched in 2014, over 130,000 certificates have since been awarded to businesses across the UK and is seen as a mandatory requirement for any organisations supplying services to the UK public sector. In April 2023, Cyber Essentials was updated to include principles such as zero trust along with secure access to cloud services, securing Bring Your Own Device (BYOD) and malware protection making Netskope a natural technical partner to support Cyber Essential certification.

There are two levels of certification:

Cyber Essentials
This is a self-assessment option that gives organisations a verified checklist of requirements to meet.

Cyber Essentials Plus
Cyber Essentials Plus requires a technical verification by an independent auditor who performs checks and verification that the controls through self assessment have been implemented and are operational.

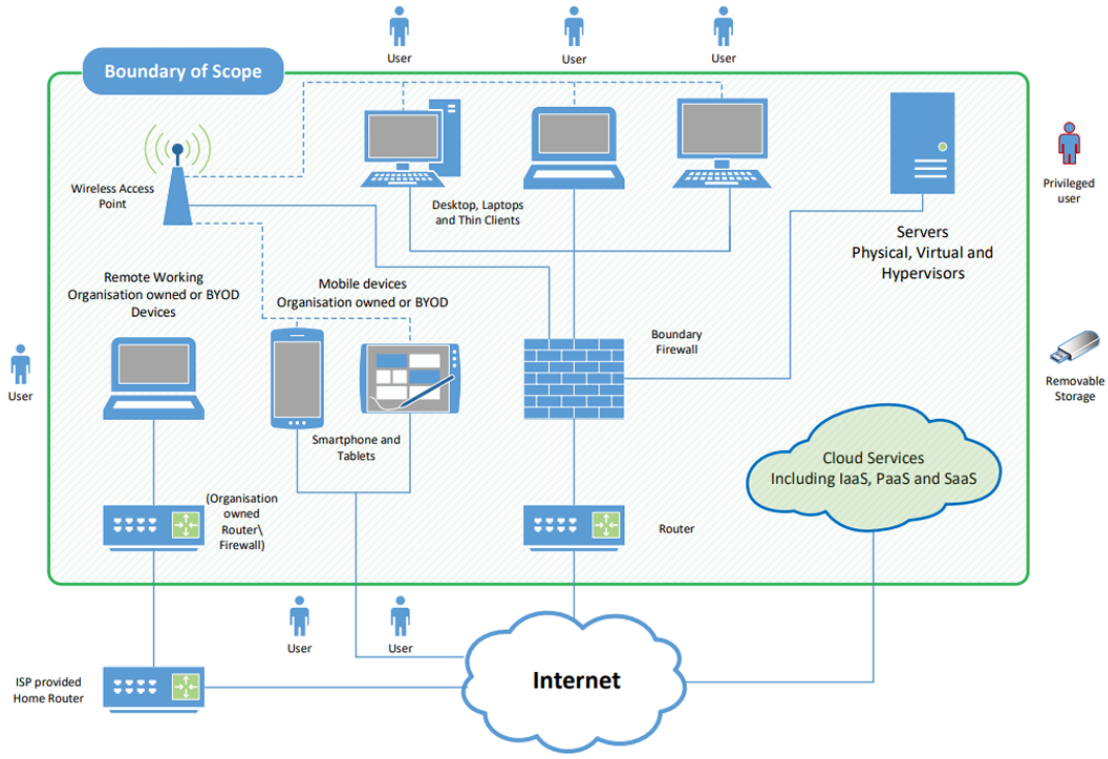
The scope of Cyber Essentials includes devices (including mobile and BYOD), servers, routers, firewalls, gateways and cloud services (including IaaS, PaaS, SaaS).

For cloud services, **the applicant organisation is always responsible** for ensuring all controls are implemented, but some of the controls can be implemented by the cloud service provider (see below).

Requirement	IaaS	PaaS	SaaS
Firewalls	Both your organisation and the cloud provider	The cloud provider and sometimes also your organisation	The cloud provider
Secure configuration	Both your organisation and the cloud provider	Both your organisation and the cloud provider	Both your organisation and the cloud provider
Security update management	Both your organisation and the cloud provider	Both your organisation and the cloud provider	The cloud provider
User access control	Your organisation	Your organisation	Your organisation
Malware protection	Both your organisation and the cloud provider	The cloud provider and sometimes also your organisation	The cloud provider

Source: https://www.ncsc.gov.uk/files/Cyber-Essentials-Requirements-for-Infrastructure-v3-1-April-2023.pdf

The boundary of scope for Cyber Essentials is included in the following diagram.



Source: https://www.ncsc.gov.uk/files/Cyber-Essentials-Requirements-for-Infrastructure-v3-1-April-2023.pdf

HOW TO USE THIS GUIDE

This guide consists of 5 core technical control requirements defined by the UK National Cyber Security Centre (NCSC) requirements for IT infrastructure and elaborates how Netskope can assist organisations in meeting and maintaining these core controls.

These include:

1. Firewalls
2. Secure configuration
3. Security update management
4. User access control
5. Malware protection

Note the following acronyms and/or aliases for the Netskope products:

Industry terminology	Netskope Product Line/Abbreviation
Security Access Service Edge	SASE
Security Service Edge	SSE
Next-Gen Secure Web Gateway	NG-SWG
Cloud Access Security Broker	CASB
Public Cloud Security	Public Cloud Security
Zero Trust Network Access	ZTNA Next
Cloud Security Posture Management	CSPM
SaaS Security Posture Management	SSPM
Data Loss Prevention	DLP (Standard & Advanced)
Firewall as a Service	Cloud Firewall
Reporting and Analytics	Advanced Analytics
Threat Intelligence	Threat Protection (Standard & Advanced)
Remote Browser Isolation	RBI
Artificial Intelligence Security	SkopeAI
Software-Defined Wide Area Network (SD-WAN)	Borderless SD-WAN Secure SD-WAN Endpoint SD-WAN Wireless SD-WAN IoT Intelligent Access
Threat/Risk Sharing	Cloud Exchange Cloud Threat Exchange (CTE) Cloud Risk Exchange (CRE)
IT/IoT/OT Security	Device Intelligence
Proactive Digital Experience Management	P-DEM
Third-Party Risk Management/Supply Chain	Cloud Confidence Index (CCI)
User Risk Metrics	User Confidence Index (UCI)

1. Firewalls

Requirement	Netskope Response	Netskope Products
Protect every device in scope with a correctly configured firewall (or network device with a firewall functionality).	Netskope's Cloud Firewall and NG-SWG applies organisational security policies to egress traffic to the web or cloud applications, for all ports and protocols, without the need to backhaul traffic to an on-prem security stack. Netskope's Cloud Security Posture Management (CSPM) and SaaS Security Posture Management (SSPM) can assess configuration of cloud services, including firewall services, to identify misconfiguration. Netskope Device Intelligence identifies, catalogues, and classifies all managed and unmanaged devices connecting to the organisation's network, and groups devices into network segments to isolate devices as required.	NG-SWG Cloud Firewall CSPM SSPM Device Intelligence
For all firewalls (or devices with firewall functionality), change default administrative passwords to a strong and unique password, or disable remote administrative access entirely.	Netskope's Cloud Firewall and NG-SWG applies organisational security policies to egress traffic to the web or cloud applications, for all ports and protocols, without the need to backhaul traffic to an on-prem security stack. Access to the administration console can be managed via SSO/MFA and IP allow lists can also be configured to limit access to the admin console. Netskope's Cloud Security Posture Management (CSPM) and SaaS Security Posture Management (SSPM) can assess configuration of cloud services, including firewall services, to identify misconfiguration. Netskope Device Intelligence identifies, catalogues, and classifies all managed and unmanaged devices connecting to the organisation's network, and groups devices into network segments to isolate devices as required.	NG-SWG Cloud Firewall CSPM SSPM Device Intelligence
For all firewalls (or devices with firewall functionality), prevent access to the administrative interface (used to manage firewall configuration) from the internet, unless there is a clear and documented business need, and the interface is protected by one of the following controls: - multi-factor authentication - an IP allow list that limits access to a small range of trusted addresses combined with a properly managed	Netskope's Cloud Firewall and NG-SWG applies organisational security policies to egress traffic to the web or cloud applications, for all ports and protocols, without the need to backhaul traffic to an on-prem security stack. Access to the administration console can be managed via SSO/MFA and IP allow lists can also be configured to limit access to the admin console. Netskope's Cloud Security Posture Management (CSPM) and SaaS Security Posture Management (SSPM) can assess configuration of cloud services, including firewall services, to identify misconfiguration.	NG-SWG Cloud Firewall CSPM SSPM Device Intelligence

password authentication approach.	Netskope Device Intelligence identifies, catalogues, and classifies all managed and unmanaged devices connecting to the organisation's network, and groups devices into network segments to isolate devices as required.	
For all firewalls (or devices with firewall functionality), block unauthenticated inbound connections by default.	Netskope's Cloud Firewall and NG-SWG applies organisational security policies to egress traffic to the web or cloud applications, for all ports and protocols, without the need to backhaul traffic to an on-prem security stack. The services by default block unauthenticated connections. Netskope's Cloud Security Posture Management (CSPM) and SaaS Security Posture Management (SSPM) can assess configuration of cloud services, including firewall services, to identify misconfiguration. Netskope Device Intelligence identifies, catalogues, and classifies all managed and unmanaged devices connecting to the organisation's network, and groups devices into network segments to isolate devices as required.	NG-SWG Cloud Firewall CSPM SSPM Device Intelligence
For all firewalls (or devices with firewall functionality), ensure inbound firewall rules are approved and documented by an authorised person, and include the business need in the documentation.	Netskope's Cloud Firewall and NG-SWG applies organisational security policies to egress traffic to the web or cloud applications, for all ports and protocols, without the need to backhaul traffic to an on-prem security stack. Netskope products support Role-Based Access Control (RBAC) and logging and alerting to raise any incidents whereby change control and approval has not been granted. Both Device Intelligence and CSPM/SSPM can also be used to identify rogue devices or misconfiguration of cloud services.	NG-SWG Cloud Firewall CSPM SSPM Device Intelligence
For all firewalls (or devices with firewall functionality), remove or disable unnecessary firewall rules quickly, when they are no longer needed.	Netskope's Cloud Firewall and NG-SWG applies organisational security policies to egress traffic to the web or cloud applications, for all ports and protocols, without the need to backhaul traffic to an on-prem security stack. Netskope products support reporting on rules that are redundant and have not been triggered allowing for the efficient removal of rules. Both Device Intelligence and CSPM/SSPM can also be used to identify rogue devices or misconfiguration of cloud services.	NG-SWG Cloud Firewall CSPM SSPM Device Intelligence
Use a software firewall on devices which are used on untrusted networks, such as public wifi hotspots.	Netskope's Cloud Firewall and NG-SWG applies organisational security policies to egress traffic to the web or cloud applications, for all ports and protocols, without the need to backhaul traffic to an on-prem security stack	NG-SWG Cloud Firewall Device Intelligence

	The service operates on devices as an endpoint client allowing for secure access to web and cloud services whilst devices are on untrusted networks. Device Intelligence can also be used to identify rogue devices on untrusted or segregated networks.	

2. Secure Configuration

Requirement	Netskope Response	Netskope Products
Remove and disable unnecessary user accounts (such as guest accounts and administrative accounts that won't be used).	Netskope's Cloud Security Posture Management (CSPM) and SaaS Security Posture Management (SSPM) continuously monitor an organisation's mission critical IaaS platforms and SaaS functions, respectively, to prevent, detect, and remediate misconfigurations such as deviations from organisational access management policies. Both CSPM and SSPM integrate with Netskope's Cloud Ticket Orchestrator (CTO) for automated remediation of security vulnerabilities.	CSPM SSPM CTO
Change any default or guessable account passwords.	Netskope's Cloud Security Posture Management (CSPM) and SaaS Security Posture Management (SSPM) continuously monitor an organisation's mission critical IaaS platforms and SaaS functions, respectively, to prevent, detect, and remediate misconfigurations such as deviations from organisational access management policies. Both CSPM and SSPM integrate with Netskope's Cloud Ticket Orchestrator for automated remediation of security vulnerabilities. Netskope Device Intelligence identifies, catalogues, and classifies all managed and unmanaged devices connecting to the organisation's network, and groups devices into network segments to isolate high-risk devices. Netskope's Device Intelligence's AI/ML engine creates a baseline of normal behaviour at the device level, detects anomalous behaviour, and can apply granular access and activity controls in accordance with zero trust principles.	CSPM SSPM Device Intelligence CTO
Remove or disable unnecessary software (including applications, system utilities, and network services).	Netskope's CASB and NG-SWG identify and classify all managed and unmanaged apps and cloud services in the organisation's IT ecosystem. Its Cloud Confidence Index (CCI) provides each app a risk-based score, and	CASB NG-SWG CCI

	Advanced Analytics maps data flows throughout the organisation's network. Together, these tools help the organisation determine which apps and services are mission critical, and which ones are redundant or too high-risk to maintain. Device Intelligence can also be used to identify rogue devices, including network devices, on untrusted or segregated networks.	Device Intelligence Advanced Analytics
Disable any auto-run feature which allows file execution without user authorisation (such as when they are downloaded).	Remote Browser Isolation is a built-in feature of Netskope's NG-SWG that isolates high-risk and uncharacterized web sites in a secure, cloud-based container or "sandbox." Any auto-run feature including malware is executed in the container and cannot infect the organisation's network.	NG-SWG RBI
Ensure users are authenticated before allowing them access to organisational data or services.	Netskope's NG-SWG and ZTNA Next integrate with identity providers to extend SSO/MFA across web and cloud-based apps and services. Moreover, NG-SWG and CASB decode and log user activity, developing a baseline of normal behaviour for each user. NG-SWG, CASB, ZTNA Next, and Device Intelligence can all detect anomalous user behaviour and adjust access controls based on zero trust principles. This can include blocking some actions or requesting step-up multi-factor authentication.	NG-SWG CASB ZTNA Next Device Intelligence
Ensure appropriate device locking controls for users that are physically present.	Netskope's products do not map to this requirement	
If a device requires a user's physical presence to access a device's services (such as logging on to a laptop or unlocking a mobile phone), a credential such as a biometric, password, or PIN must be in place before a user can gain access to the services.	Netskope's products do not map to this requirement	
Protect authentication methods against brute force attacks by applying one of the following methods: - 'throttling' the rate of attempts, so that the number of times the user must wait between attempts increases with each unsuccessful attempt (allow no more than 10 guesses in five minutes); or - locking devices after more than 10 unsuccessful attempts.	Netskope's NG-SWG and ZTNA Next integrate with identity providers to extend SSO/MFA across web and cloud-based apps and services. Moreover, NG-SWG and CASB decode and log user activity, developing a baseline of normal behaviour for each user. NG-SWG, CASB, ZTNA Next, and Device Intelligence can all detect anomalous user behaviour and adjust access controls based on zero trust principles. This can include blocking some actions or requesting step-up multi-factor authentication.	NG-SWG CASB ZTNA Next Device Intelligence

Use technical controls to manage the quality of credentials. If credentials are just to unlock a device, use a minimum password or PIN length of at least 6 characters. When the device unlocking credentials are also used for authentication, apply the full password requirements in Table 4 (User Access Controls).	Netskope's NG-SWG and ZTNA Next integrate with identity providers to extend SSO/MFA across web and cloud-based apps and services. Moreover, NG-SWG and CASB decode and log user activity, developing a baseline of normal behaviour for each user. NG-SWG, CASB, ZTNA Next, and Device Intelligence can all detect anomalous user behaviour and adjust access controls based on zero trust principles. This can include blocking some actions or requesting step-up multi-factor authentication.	NG-SWG CASB ZTNA Next Device Intelligence

3. Security Update Management

Requirement	Netskope Response	Netskope Products
All software on in-scope devices must be licensed and supported.	Netskope's NG-SWG and CASB can identify and classify all managed and unmanaged apps and cloud services in the organisation's IT ecosystem. Its Cloud Confidence Index (CCI) assigns each app a risk-based score. An app's CCI score is updated periodically to reflect any improvement or deterioration in its business readiness. Netskope's Device Intelligence identifies, catalogues, and classifies all managed and unmanaged devices connecting to the organisation's network, and groups devices into network segments to isolate high-risk devices. Netskope's Advanced Analytics can be used to create custom dashboards to track in-scope apps and services and support the creation and ongoing management of an inventory.	NG-SWG CASB CCI Advanced Analytics Device Intelligence
All software on in-scope devices must be removed from devices when it becomes unsupported or removed from scope by using a defined subset that prevents all traffic to or from the internet.	Netskope's Cloud Firewall and NG-SWG applies organisational security policies to egress traffic to the web or cloud applications, for all ports and protocols, without the need to backhaul traffic to an on-prem security stack. Netskope Device Intelligence identifies, catalogues, and classifies all managed and unmanaged devices connecting to the organisation's network, and groups devices into network segments to isolate high-risk devices. Netskope's Device Intelligence's AI/ML engine creates a baseline of normal behaviour at the device level, detects anomalous behaviour, and can apply granular access and activity controls in accordance with zero trust principles.	NG-SWG Cloud Firewall Device Intelligence

All software on in-scope devices must have automatic updates enabled where possible.	Netskope Device Intelligence identifies, catalogues, and classifies all managed and unmanaged devices connecting to the organisation's network, and groups devices into network segments to isolate high-risk devices. Netskope's Device Intelligence's AI/ML engine creates a baseline of normal behaviour at the device level, detects anomalous behaviour, and can apply granular access and activity controls in accordance with zero trust principles. Device Intelligence can be integrated with the organisation's incident response tools to generate security alerts based on criteria set by the organisation.	Device Intelligence
All software on in-scope devices must be updated as soon as possible (including applying any manual configuration changes required to make the update effective), and no later than 14 days after an update has been released where: - the update fixes vulnerabilities described by the vendor as 'critical' or 'high-risk'; - the update addresses vulnerabilities with a CVSS v3 base score of 7 or above; or - there are no details of the level of vulnerabilities the update fixes provided by the vendor.	Netskope Device Intelligence identifies, catalogues, and classifies all managed and unmanaged devices connecting to the organisation's network, and groups devices into network segments to isolate high-risk devices. Netskope's Device Intelligence's AI/ML engine creates a baseline of normal behaviour at the device level, detects anomalous behaviour, and can apply granular access and activity controls in accordance with zero trust principles. Netskope's Cloud Security Posture Management (CSPM) and SaaS Security Posture Management (SSPM) continuously monitor an organisation's mission critical IaaS platforms and SaaS functions, respectively, to prevent, detect, and remediate misconfigurations such as deviations from organisational access management policies. Both CSPM and SSPM integrate with Netskope's Cloud Ticket Orchestrator (CTO) for automated remediation of security vulnerabilities.	CSPM SSPM Device Intelligence CTO

4. User Access Control

Requirement	Netskope Response	Netskope Products
Have in place a process to create and approve user accounts.	Netskope's suite of solutions, including CASB, NG-SWG, DLP, and ZTNA-Next, all support Role-Based Access Control (RBAC) to help organisations enforce access management policies. These policies are based on the principle of least privilege, ensuring that users have only the minimum level of access necessary for their roles. In addition, Netskope products integrate with identity providers to extend SSO/MFA across web and cloud-based apps and services.	NG-SWG CASB DLP ZTNA Next

Authenticate users with unique credentials before granting them access to applications or devices.	Netskope's suite of solutions, including CASB, NG-SWG, DLP, and ZTNA-Next, all support Role-Based Access Control (RBAC) to help organisations enforce access management policies. These policies are based on the principle of least privilege, ensuring that users have only the minimum level of access necessary for their roles. In addition, Netskope products integrate with identity providers to extend SSO/MFA across web and cloud-based apps and services.	NG-SWG CASB DLP ZTNA Next
Remove or disable user accounts when they're no longer required (for example, when a user leaves the organisation or after a defined period of account inactivity).	Netskope's suite of solutions, including CASB, NG-SWG, DLP, and ZTNA-Next, all support Role-Based Access Control (RBAC) to help organisations enforce access management policies. These policies are based on the principle of least privilege, ensuring that users have only the minimum level of access necessary for their roles. In addition, Netskope products integrate with identity providers to extend SSO/MFA across web and cloud-based apps and services. Netskope's Advanced Analytics can be used to monitor usage of disabled accounts to ensure account details have not been shared across apps and services. Netskope's User Entity and Behavior Analytics (UEBA) product employs multiple ML-based anomaly-detection models and includes a User Confidence Index (UCI), a dynamic risk score for users. UCI helps adapt policies, recommend security training, and mitigate insider threats, and can share insider threat information through Netskope's Cloud Risk Exchange (CRE).	NG-SWG CASB DLP ZTNA Next Advanced Analytics UEBA UCI CRE
Implement MFA where available (authentication to cloud services must always use MFA).	Netskope's NG-SWG, CASB and ZTNA Next integrate with identity providers to extend SSO/MFA across web and cloud-based apps and services.	NG-SWG CASB ZTNA Next
Use separate accounts to perform administrative activities only (no emailing, web browsing, or other standard user activities that may expose administrative privileges to avoidable risks).	Netskope's suite of solutions, including CASB, NG-SWG, DLP, and ZTNA-Next, all support Role-Based Access Control (RBAC) to help organisations enforce access management policies. These policies are based on the principle of least privilege, ensuring that users have only the minimum level of access necessary for their roles. Netskope's User Entity and Behavior Analytics (UEBA) product employs multiple ML-based anomaly-detection models and includes a User Confidence Index (UCI), a dynamic risk score for users. UCI helps adapt policies, recommend security training, and mitigate insider threats, and can share insider threat information through Netskope's Cloud Risk Exchange (CRE). Netskope's Advanced Analytics can be used to monitor and trend usage of accounts.	NG-SWG CASB ZTNA Next DLP Advanced Analytics UEBA UCI CRE

Remove or disable special access privileges when no longer required (when a member of staff changes role, for example).	Netskope's suite of solutions, including CASB, NG-SWG, DLP, and ZTNA-Next, all support Role-Based Access Control (RBAC) to help organisations enforce access management policies. These policies are based on the principle of least privilege, ensuring that users have only the minimum level of access necessary for their roles. Netskope's Advanced Analytics can be used to monitor usage of accounts to ensure account details are appropriate to the role and monitor for any behavioural changes. Netskope's User Entity and Behavior Analytics (UEBA) product employs multiple ML-based anomaly-detection models and includes a User Confidence Index (UCI), a dynamic risk score for users. UCI helps adapt policies, recommend security training, and mitigate insider threats, and can share insider threat information through Netskope's Cloud Risk Exchange (CRE).	NG-SWG CASB ZTNA Next DLP Advanced Analytics UEBA UCI CRE
Protect passwords against brute-force password guessing by implementing at least one of the following: - multi-factor authentication; - 'throttling' the rate of attempts, so that the number of times the user must wait between attempts increases with each unsuccessful attempt (allow no more than 10 guesses in five minutes); or - locking accounts after no more than 10 unsuccessful attempts.	Netskope's suite of solutions, including CASB, NG-SWG, DLP, and ZTNA-Next, all support Role-Based Access Control (RBAC) to help organisations enforce access management policies. These policies are based on the principle of least privilege, ensuring that users have only the minimum level of access necessary for their roles. In addition, Netskope products integrate with identity providers to extend SSO/MFA across web and cloud-based apps and services.	NG-SWG CASB DLP ZTNA Next
Use technical controls to manage the quality of passwords, including at least one of the following: - multi-factor authentication; - a minimum password length of at least 12 characters, with no maximum restrictions; or - a minimum password length of at least 8 characters, with no minimum length restrictions, and use automatic blocking of common passwords using a deny list.	Netskope's suite of solutions, including CASB, NG-SWG, DLP, and ZTNA-Next, all support Role-Based Access Control (RBAC) to help organisations enforce access management policies. These policies are based on the principle of least privilege, ensuring that users have only the minimum level of access necessary for their roles. In addition, Netskope products integrate with identity providers to extend SSO/MFA across web and cloud-based apps and services.	CASB NG-SWG DLP ZTNA Next
Support users to choose unique passwords for their work accounts by: - educating people about avoiding common passwords, such as a pet's name,	The Netskope platform can enforce organisational policy regarding password management. It also uses pop-up banners and coaching pages to educate users on organisation policy.	All products

common keyboard patterns, or passwords they have used elsewhere. This could include teaching people to use the password generator feature built into some password managers; - encouraging people to choose longer passwords by promoting the use of multiple words (a minimum of three) to create a password; - providing usable secure storage for passwords (for example a password manager or secure locked cabinet) with clear information about how and when it can be used; - not enforcing regular password expiry; or - not enforcing password complexity requirements.		

5. Malware Protection

Requirement	Netskope Response	Netskope Products
Use anti-malware software on all in-scope devices that is configured to be updated in line with vendor recommendations.	Netskope's Public Cloud Security can be enhanced with Advanced DLP, which scans IaaS Storage for hidden malware, providing robust cloud protection. Standard Threat Protection guards against known malware and uses machine learning for new threats, offering real-time phishing detection and web filtering. Advanced Threat Protection extends the capabilities of Standard Threat Protection by using deobfuscation, recursive file unpacking, and multi-stage sandboxing to detect new malware. Netskope integrates these threat protection tools with its Cloud Threat Exchange and other Intelligent Security Service Edge tools, such as Cloud Firewall and User Entity and Behavior Analytics, to provide layered security. SkopeAI, leveraging machine learning, enhances the DLP engine by enabling deep contextual awareness to analyse and protect unstructured data like images. It excels in detecting various attacks, polymorphic malware, novel	NG-SWG CASB Cloud Firewall Public Cloud Security Advanced DLP Advanced Threat Protection Threat Protection SkopeAI

	phishing web domains, zero-day threats, and malicious web content, delivering superior speed and accuracy.	
Use anti-malware software on all in-scope devices that is configured to prevent malware from running.	Netskope's Public Cloud Security can be enhanced with Advanced DLP, which scans IaaS Storage for hidden malware, providing robust cloud protection. The Remote Browser Isolation (RBI) feature in Netskope's NG-SWG secures access to high-risk websites by isolating them in a cloud-based sandbox, preventing malware from infecting the organisation's network. Standard Threat Protection guards against known malware and uses machine learning for new threats, offering real-time phishing detection and web filtering. Advanced Threat Protection extends the capabilities of Standard Threat Protection by using deobfuscation, recursive file unpacking, and multi-stage sandboxing to detect new malware. Netskope integrates these threat protection tools with its Cloud Threat Exchange and other Intelligent Security Service Edge tools, such as Cloud Firewall and User Entity and Behavior Analytics, to provide layered security. SkopeAI, leveraging machine learning, enhances the DLP engine by enabling deep contextual awareness to analyse and protect unstructured data like images. It excels in detecting various attacks, polymorphic malware, novel phishing web domains, zero-day threats, and malicious web content, delivering superior speed and accuracy.	NG-SWG CASB Cloud Firewall Public Cloud Security RBI Advanced DLP Advanced Threat Protection Threat Protection SkopeAI
Use anti-malware software on all in-scope devices that is configured to prevent the execution of malicious code.	Netskope's Public Cloud Security can be enhanced with Advanced DLP, which scans IaaS Storage for hidden malware, providing robust cloud protection. The Remote Browser Isolation feature in Netskope's NG-SWG secures access to high-risk websites by isolating them in a cloud-based sandbox, preventing malware from infecting the organisation's network. Standard Threat Protection guards against known malware and uses machine learning for new threats, offering real-time phishing detection and web filtering. Advanced Threat Protection extends the capabilities of Standard Threat Protection by using deobfuscation, recursive file unpacking, and multi-stage sandboxing to detect new malware. Netskope integrates these threat protection tools with its Cloud Threat Exchange and other Intelligent Security Service Edge tools, such as Cloud Firewall and User Entity and Behavior Analytics, to provide layered security. SkopeAI, leveraging machine learning, enhances the DLP engine by enabling deep contextual awareness to analyse	NG-SWG CASB Cloud Firewall Public Cloud Security RBI Advanced DLP Advanced Threat Protection Threat Protection SkopeAI

	and protect unstructured data like images. It excels in detecting various attacks, polymorphic malware, novel phishing web domains, zero-day threats, and malicious web content, delivering superior speed and accuracy	
Use anti-malware software on all in-scope devices that is configured to prevent connections to malicious websites over the internet.	The Remote Browser Isolation feature in Netskope's NG-SWG secures access to high-risk websites by isolating them in a cloud-based sandbox, preventing malware from infecting the organisation's network. Standard Threat Protection guards against known malware and uses machine learning for new threats, offering real-time phishing detection and web filtering. Advanced Threat Protection extends the capabilities of Standard Threat Protection by using deobfuscation, recursive file unpacking, and multi-stage sandboxing to detect new malware. Netskope integrates these threat protection tools with its Cloud Threat Exchange and other Intelligent Security Service Edge tools, such as Cloud Firewall and User Entity and Behavior Analytics, to provide layered security. SkopeAI, leveraging machine learning, enhances the DLP engine by enabling deep contextual awareness to analyse and protect unstructured data like images. It excels in detecting various attacks, polymorphic malware, novel phishing web domains, zero-day threats, and malicious web content, delivering superior speed and accuracy	NG-SWG CASB Cloud Firewall Public Cloud Security RBI Advanced DLP Advanced Threat Protection Threat Protection SkopeAI
Actively approve any applications before deploying them to in-scope devices.	Netskope’s NG-SWG and CASB identify and inventory all managed and unmanaged apps in the organisation’s IT ecosystem. Moreover, Netskope’s Cloud Confidence Index (CCI) assists with secure acquisition and third party risk management by providing a risk-based score to tens of thousands of different apps. The CCI score is a function of more than thirty variables, including data security, known vulnerabilities, auditability, compliance with major regulatory frameworks, and business continuity capability. Default weights for each variable can be adjusted to provide a custom-tailored risk score for each app based on the organisation's unique risk profile and tolerance.	NG-SWG CASB CCI
Maintain a current list of approved applications, and prohibit users from installing any application that is unsigned or has an invalid signature.	Netskope’s NG-SWG and CASB identify and inventory all managed and unmanaged apps in the organisation’s IT ecosystem. NG-SWG decodes and logs over a hundred inline activities, such as “upload,” “download,” “share,” etc. And CASB gives administrators visibility into, and logging of, user activities in IaaS and SaaS services. The Cloud Confidence Index (CCI) provides each app a risk-based score, which can be used to assist with	NG-SWG CASB CCI

	decisions surrounding asset acquisition, but can also be incorporated dynamically into rules that prevent users from sharing data with apps that have a score below an organisation-defined threshold. CCI scores can be calibrated by the organisation to reflect its specific security needs, and will adjust dynamically as the specific app improves or degrades with respect to various criteria.	