Solution Brief +

Netskope for UK Public Sector

Public Sector organisations across all aspects of government - regional and local, healthcare, transport and other public services - are adopting cloud and web services because of the flexibility, scalability, and cost savings that these services provide. But with so many cyber incidents and breaches happening, it's critical to protect cloud and web usage and secure sensitive data for compliance and privacy.

Key Use Cases

- Comply with data privacy regulations including GDPR, UK Data Protection Act and international requirements including US FISMA and DoD.
- Address privacy and security concerns over sensitive data.
- Monitor cloud and web risks and control costs.
- Enforce security and access controls over cloud and web services.
- Protect against cloud threats and malware.

> "47% of malware downloads originate from cloud apps compared to 53% from traditional websites. This is a reflection of both attacker activity and user behaviour."

Netskope Cloud and Threat Report May 2022

The Challenge

Public Sector organisations are increasingly under attack from state-sponsored groups and hackers and face scrutiny over their budgets and use of resources. At the same time hackers are becoming smarter and utilising an increasing number of cloud applications to target users. The same cloud applications are being adopted to users to increase their productivity, potentially exposing sensitive data. Added to this, organisations need to continue to meet regulations and protections including the EU General Data Protection Regulation (GDPR), the UK Data Protection Act 2018 (DPA), the Common Law Duty of Confidentiality (CLDC) and more.

The Solution

Netskope Intelligent Security Services Edge (SSE) helps UK public sector, government agencies and departments comply with local and regional regulations, protect sensitive data, and defend against threats across SaaS, IaaS, and web. Following recognised industry standards, best practices, frameworks and recommendations for cyber security, data protection, incident response and threat management, including NIST, ISO and CSA (Cloud Security Alliance), Netskope Intelligent SSE is easy to use, and secures your transactions wherever your people and data go.

Deep visibility and risk assessment of cloud and web usage

Netskope finds and assesses all cloud services in use, sanctioned or unsanctioned, as well as web use. IT Teams can evaluate cloud and web usage in the organisation with full contextual detail including users, sessions, performance, devices, browsers, time periods, locations, content (including type), and even user activity (e.g., "share" or "upload") and size of traffic per cloud service.

With rich context from CloudXD and trust scores for users and apps, Netskope Intelligent Security Service Edge (SSE) enforces the most adaptive, single pass policy controls across all cloud, web and private applications for stronger risk management with simplified operations.

The Netskope Cloud Confidence Index (CCI) also allows public sector organisations to:

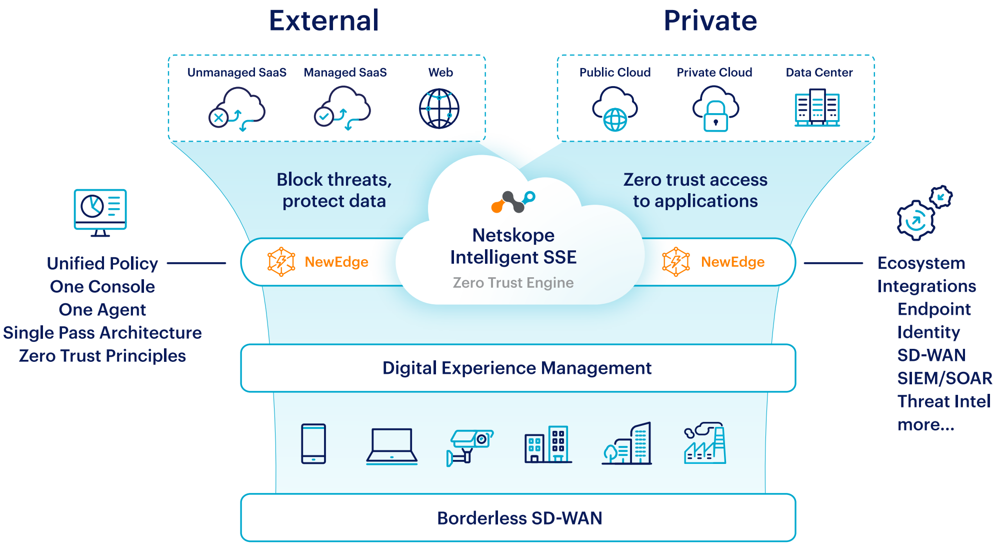
- assess the enterprise's readiness of cloud services based on a set of objective criteria across security, auditability, data privacy, and more.
- Use ad hoc queries and dynamic reports in real time for a dashboard of usage and risk.
- Answer questions like "Who is sharing sensitive content outside of the organisation?" or "Which cloud services in use are high risk to the organisation?"

Granular security policies and access controls over cloud and web services

Netskope provides granular, contextual control over sanctioned and unsanctioned cloud services and websites in real time and in data at rest in sanctioned services. Rather than take a coarse-grained approach of blocking services, security teams can set security policies at a contextual level based on service or website, user, activity, device, and more, choosing from a variety of policy enforcement actions such as block, alert, bypass, encrypt, quarantine, and coach.

For sanctioned services and suites like Microsoft Office 365, G Suite, Box, and more, Netskope provides governance across identity, services, activities, devices, and data. You can therefore enforce policies such as "Encrypt all PII content uploaded to cloud services" or "Alert on the download of PII from any cloud service to a mobile device," and more. For unsanctioned and ecosystem services, Netskope provides visibility and control at the service and category level or globally with set-it-once policies like "No download of PII to a mobile device" or "Allow people to receive content from their partners' cloud storage services, but block them from uploading to or sharing from any except our organisations's sanctioned one." This allows organisations to enforce these policies across all users, even if they are remote, mobile, or using a native app or sync client.

Netskope Intelligent SSE delivers visibility into more than 41,000 cloud applications, with inline user coaching and controls for activities across these applications and their application instances.



Fast everywhere, data-centric, and cloud-smart.

Comprehensive DLP

Netskope provides unmatched, machine learning-enhanced, 4-in-1 data loss prevention (DLP) for SaaS, IaaS, web, and email environments to help reduce risk. Combining protection for data-at-rest and data-in-motion, with a unique understanding of the modern context of cloud and web access, Netskope accurately and effectively detects and protects sensitive content no matter where it is.

Reduce false positives with Netskope DLP, which detects sensitive content accurately across 1000+ file types and across structured and unstructured data, using 3,000+ pre-defined data identifiers, metadata extraction, proximity analysis, fingerprinting, exact match, and more. Netskope also offers incident management capabilities with closed-loop administration and remediation workflows to facilitate the end-to-end incident management process. Included in this are privacy features such as role-based access controls (RBAC). Predefined and customisable templates and reports help comply with regulations, such as: AMRA, EC Directive, EU-GDPR, GLBA, HIPAA, PCI-DSS, PHI, PII, SSN Confidentiality Act, US FTC Rules, and more. Analytics and reporting based on 90-day data retention.

Finally, forensic information of excerpts of DLP violations offer enhanced focus, so organisations can use predefined and customisable workflows and assign incidents to investigate or override alert severity, setting actions such as 'quarantine and restore' and 'restrict file permissions'.

Cloud threat and malware protection

With a comprehensive vantage point over cloud and web service usage, Netskope combines threat intelligence, static and dynamic analysis, and machine-learning based anomaly detection to enable real-time detection, prioritised analysis, and remediation of threats that may originate from — or be further propagated by — the cloud and web.

Using threat intelligence, static and dynamic analysis, and anomaly detection and cloud sandboxing, Netskope detects and remediates the latest viruses, advanced persistent threats (APTs), spyware, adware, worms, ransomware, and other malware. Netskope also guards against cloud threats such as compromised credentials (re-used or shared), privileged user and access abuse such as data exfiltration from a sanctioned service to an unsanctioned one, or access to malicious sites.

BENEFITS	DESCRIPTION
GDPR AND DPA REQUIREMENTS	• Controllers close a 'data processing agreement' with processors - Find processors (specifically those that deal with personal data) in use throughout organisations with Netskope to decide which to sanction (close agreement with) and which to restrict. • Personal data is collected only as necessary to the purpose of use with limitations on processing of 'special data' and 'sensitive data'. • Restrict upload or download of "special data" and "sensitive data" per definition with Netskope Cloud DLP. • Controllers and processors know the location where personal data is stored or otherwise processed. • Use Netskope Cloud Confidence Index (CCI) to assess where data is stored and/or processed for each processor (cloud service) and enforce policies with the Netskope for processors that do not store/transfer data in secure locations (on List of Adequate Jurisdictions maintained by the European Commission of approved countries and territories) or process data in undetermined locations, such as blocking cloud service from being used. • Controllers take adequate security measures to protect personal data from loss, alteration, or unauthorised processing. • eDiscover and protect sensitive data at rest in a sanctioned processor (cloud service) or for real-time activities in all cloud services with Netskope DLP. Apply security policies such as "Block use of cloud storage services rated 'Medium' or below from use" to ensure organisational usage of secure, vetted processors only. Detect and automatically remediate cloud threats and malware like ransomware resident in sanctioned services or in real-time activities like uploads and downloads to prevent information from being stolen. • Controllers prevent personal data from being uploaded to personal cloud services and personal devices (BYOD) or enforce the organisation's security measures in personal clouds and devices. - Understand and query on all access and activities by device and device classification, for example, BYOD. Enforce access and activity-level policies based on device type and classification. Enforce policies to ensure that corporate and personal data only go into processors approved by the company and not personal instances on the same processor, for example, allow upload of confidential data to corporate Box but not to personal instances of Box. Differentiate between processor (service) instances to ensure corporate policies and visibility only in place for sanctioned processors and personal data related to organisational and business processes. • Controllers know the privacy and security standards the processor adheres to and assess those standards. • Track personal data with cloud forensic analysis to log and audit which processors have processed and/or possess personal data to comply with requests for information on individual's personal data. Assess enterprise-readiness of processors on 40 parameters with CCI (including privacy features like whether service enables sub-processors or does anything else with data as well as data security features such as encryption of data at rest and cipher type). Netskope also determines GDPR-readiness of apps on a high, medium, low scale based on the parameters.
FISMA AND NIST FEDERAL REQUIREMENTS	In order to strengthen information security systems, FISMA outlines multiple guidelines that can be applied to cloud usage, including the summarized ones below: • Overall visibility and continuous monitoring. Netskope can continuously inventory all cloud and web services in use with contextual data on users, devices, locations, cloud activity, data being shared, and more. Ad hoc reports and dynamic queries can be run in real time to fulfill auditing requirements. • Risk and vulnerability assessments in services used. The Netskope Cloud Confidence Index evaluates over 20,000 cloud services across objective criteria. Services with vulnerabilities or other attributes that may impact organisational continuity or security can be evaluated and rated according to risk based on usage. • Security controls and data protection. Security policies based on contextual information like use of an unmanaged device or risky activity like sharing can be restricted with granular security controls from Netskope. Sensitive data can be secured with AES 256-bit encryption. Access controls are included in these controls, as well as cloud threat and malware protection. Administrators can follow up with suspected violations with full cloud incident management capabilities.