netskope

Compliance Series

ISO/IEC 27001:2022 Annex A

Control Mapping to Netskope Products

Table of Contents

Version	Name	Email	Date
v1 [ISO/IEC 27001:2013]	Neil Thacker Vladimir Klasnja	nthacker@netskope.com vladk@netskope.com	Feb 4, 2020
v2 [ISO/IEC 27001:2022]	Aditya Sahu Neil Thacker	asahu@netskope.com nthacker@netskope.com	September 15, 2023

Introduction

The following information covers a mapping of the ISO/IEC 27001:2022 standard and the associated controls available from Netskope products.

ISO/IEC 27001:2022 is an improved standard over ISO/IEC 27001:2013 and all previous versions. The rationale to revise the previous standard is to address the ever-evolving cyber security challenges faced by organisations and improve their overall information security posture.

Core changes

Amendments to ISO/IEC 27001:2022 consider that risk management is increasingly expanding to more organizational functions.

As a result, 24 controls have been merged and 58 and controls have been revised.

The following 11 new controls have been added to the revised standard:

- 5.7 Threat intelligence
- 5.23 Information security for use of cloud services
- 5.30 ICT readiness for business continuity
- 7.4 Physical security monitoring
- 8.9 Configuration management
- 8.10 Information deletion
- 8.11 Data masking
- 8.12 Data leakage prevention
- 8.16 Monitoring activities
- 8.23 Web filtering
- 8.28 Secure coding

Further, the structure of the standard is such that it focusses on the following four aspects:

- Organizational
- People
- Physical
- Technological

Netskope offer a series of controls that can be applied across many of these aspects including Organizational, People and Technological aspects. Whilst Netskope can supplement the Physical aspect such as protecting physical media via a technical control, the focus of this mapping guide is to illustrate how the Netskope suite of products can help support alignment to the ISO standard for the Organizational, People and Technological domains.

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	Private Access for ZTNA
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 Threat Exchange (CTE) Cloud Risk Exchange (CRE)
IT/IoT/OT Security	Device Intelligence
Digital Experience Management	DEM

This information is based on the alignment of organizational, people and technological controls. Netskope may not offer these controls directly out-of-the-box however policies, processes or reports can be created or tuned to support these controls and requirements.

Each of the following sections highlights the Annex reference, Control, Netskope Control and Netskope Product. Not all subsections or references to ISO/IEC 27001:2022 Annex A are referenced, only the areas where Netskope can offer a supplemental or direct control.

Annex A.5 – Organizational Controls

Reference	Control	Netskope Controls	Netskope product
5.1	Policies for information security	Netskope can enforce organizational policies defined by the organization. Netskope additionally can assist communication and track acknowledgement of policies through implementation of pop-up banners/coaching pages across its product that can notify employees of potential policy infringements in line with organizational requirements.	▪ All Products
5.2	Information security roles and responsibilities	Netskope offers Role Based Access Control (RBAC) that support role-based access based on an organizations policy or similar requirements.	▪ All Products
5.3	Segregation of duties	Netskope offers Role Based Access Control (RBAC) that offer segregation of duties and areas of responsibility for the administration of networks and cloud, web, and private applications.	▪ All Products
5.4	Management responsibilities	Netskope can enforce organizational policies defined by organization.	▪ All Products
5.7	Threat Intelligence	Netskope has built a comprehensive threat protection capability including anti-malware (signature-based, behavior-based, AI/ML-based, and sandbox-based) that allows organizations to defend against threats. In addition, Netskope offers Cloud Threat Exchange which allows for exchanging of Cyber Threat Intelligence (CTI) across ecosystems i.e., with Endpoint, Identity, Email and SIEM/SOAR security services.	▪ Threat Protection ▪ Cloud Threat Exchange
5.8	Information security in project management	Netskope can control access to cloud and on-prem based project management solutions through user policy management, threat protection and Data Loss Prevention (DLP) engines.	▪ NG-SWG ▪ CASB ▪ Private Access for ZTNA ▪ DLP

5.9	Inventory of information and other associated assets	Netskope offers controls to identify and protect information assets including assets across web and cloud applications and/or cloud infrastructure along with devices. These controls can be used to create an inventory of information assets across sanctioned or unsanctioned services.	▪ NG-SWG ▪ CASB ▪ Public Cloud Security ▪ Private Access for ZTNA ▪ DLP ▪ Device Intelligence
5.10	Acceptable use of information and other associated assets	Netskope offers controls to identify and protect data and use of cloud applications, cloud infrastructure (IaaS) or private application and their associated information assets. Policies can be implemented to ensure acceptable use of assets based on organizational requirement.	▪ NG-SWG ▪ CASB ▪ Public Cloud Security ▪ Private Access for ZTNA ▪ DLP
5.11	Return of assets	Netskope offers controls to access cloud applications and/or cloud infrastructure and associated information assets. Controls can be used to retrieve or delete information assets through an Application Programming Interface (API) if configured for cloud apps and infrastructure. In addition, Netskope offers controls around IT/IoT/OT devices for access control and asset management.	▪ CASB ▪ Public Cloud Security ▪ Device Intelligence
5.12	Classification of information	Netskope offers controls to identify labelled classified information and can associate policies to protect this information. In addition, Netskope can apply controls around unclassified information based on its Data Loss Prevention (DLP) engines including fingerprinting and natural language processors.	▪ NG-SWG ▪ CASB ▪ Public Cloud Security ▪ Private Access for ZTNA ▪ DLP
5.13	Labelling of information	Netskope offers controls to identify labelled classified information and can associate policies to protect this information in line with organizational procedures.	▪ NG-SWG ▪ CASB ▪ Public Cloud Security ▪ Private Access for ZTNA ▪ DLP
5.14	Information transfer	Netskope offers transfer controls between web, cloud, and private applications. Netskope offer source and destination controls that identify traffic and data flows between client and web, client and cloud application,	▪ NG-SWG ▪ CASB

		client, and private application where configured. Reporting is available via Advanced Analytics to report on data flows including cross-border transfers.	▪ Public Cloud Security ▪ Private Access for ZTNA DLP ▪ Advanced Analytics
5.15	Access control	Netskope offers example access control security policy templates and can enforce organizational policies defined by organization. Netskope offers in line controls that can block, notify, or allow employees access to web, cloud or private application information assets or services. Further, Netskope can be used to identify misconfiguration of access control policy for cloud apps and infrastructure and report on issues or anomalies.	▪ NG-SWG ▪ CASB ▪ Public Cloud Security ▪ Private Access ▪ CSPM ▪ SSPM ▪ Device Intelligence
5.16	Identity management	Netskope offers synchronization services that can register users for access to web, cloud or private application services. Netskope can also integrate into identity services that can control access to web, cloud and on-prem services.	▪ NG-SWG ▪ CASB ▪ Public Cloud Security ▪ Netskope Private Access
5.17	Authentication information	Netskope integrate with third-party identity providers to manage secure and secret authentication including support for SAML, SSO and MFA.	▪ NG-SWG ▪ CASB ▪ Public Cloud Security ▪ Netskope Private Access
5.18	Access rights	Netskope offers asset owners visibility into user access rights to web, cloud and private applications. Reports can be customized to report regularly of user access rights.	▪ NG-SWG ▪ CASB ▪ Public Cloud Security ▪ Private Access
5.19	Information security policy for supplier relationships	Netskope offer reverse proxy capabilities to protect cloud applications along with Zero-Trust Network Access (ZTNA) capabilities for supplier and 3rd-Party access. Protection includes reverse proxy capabilities for corporate and personal devices configured to manage suppliers' access to organizational assets.	▪ CASB ▪ ZTNA

5.20	Addressing security within supplier agreements	Netskope can be used to apply controls and baseline assessments required for and by suppliers in line with security requirements. Policies can be predefined and applied also for SaaS and shared cloud infrastructure components.	▪ CASB ▪ Public Cloud Security
5.21	Managing information security in the ICT supply chain	Netskope can audit web and cloud applications. Netskope can provide metadata to understand if supplier is using underlying cloud infrastructure to support supply chain discovery.	▪ CASB ▪ Public Cloud Security
5.22	Monitoring, review and change management of supplier services	Netskope can audit web and cloud applications. For cloud applications, Netskope produce a Cloud Confidence Index (CCI) score that can be used for audit requirements. Netskope maintain a list of 75,000+ cloud applications including specific audit measurements that can be used to support review of supplier services. Netskope can also continuously monitor SaaS and Public Cloud services for changes to posture.	▪ CASB ▪ Public Cloud Security ▪ CSPM ▪ SSPM
5.23	Information Security for Use of cloud services	Netskope provide controls for protection of cloud services from SaaS to IaaS. Netskope can identify use of cloud services, identify, and improve security posture of services and identify threats that originate from services. In addition, Netskope can assist with continuous assessments and potential data loss incidents from cloud services.	▪ CASB ▪ Public Cloud Security ▪ DLP ▪ CSPM ▪ SSPM ▪ CTE ▪ CRE
5.24	Information Security Incident Management Planning and Preparation	Netskope offers Role Based Access Control (RBAC) that support role-based access based on an organizations RACI policy or similar requirements to support responsibilities and procedures in the event of a security incident. Multiple levels of access including data obfuscation can be applied to protect incident information on a need-to-know basis.	▪ NG-SWG ▪ CASB ▪ Public Cloud Security ▪ Private Access
5.25	Assessment and decision on information security events	Netskope can be configured to collate and report on events and generate alerts based on a series of suspicious events. Netskope have capabilities to identify new anomalies and can use Machine Learning and Artificial Intelligence (ML/AI) to detect new security events from baseline activity.	▪ NG-SWG ▪ CASB ▪ Public Cloud Security ▪ Private Access ▪ Advanced Analytics ▪ SkopeAI

5.26	Response to information security incidents	Netskope has built in ticketing systems, log analysis, forensic reporting, and advanced analytic capabilities to aid organisation in response to an information security incident. Multiple levels of access including data obfuscation can be applied to protect incident information on a need-to-know basis.	▪ NG-SWG ▪ CASB ▪ Public Cloud Security ▪ CTE ▪ CRE ▪ Private Access ▪ Device Intelligence
5.27	Learning from information security incidents	Netskope can be configured to collate and report on events and generate alerts based on a series of suspicious events. Netskope have capabilities to identify new anomalies and can use Machine Learning and Artificial Intelligence (ML/AI) to detect new security events from baseline activity or previous incidents.	▪ NG-SWG ▪ CASB ▪ Public Cloud Security ▪ Private Access ▪ Advanced Analytics ▪ Device Intelligence
5.28	Collection of evidence	Netskope offer a ticketing system to escalate high risk information security events and can store forensic data in forensic tools or repositories defined by customer. In addition, Netskope offer legal hold capabilities that allow for preservation of data in a forensic repository for legal requirements.	▪ NG-SWG ▪ CASB ▪ Public Cloud Security ▪ Private Access ▪ Advanced Analytics ▪ Device Intelligence
5.30	ICT readiness for Business continuity	Netskope can help support ICT readiness and business continuity through implementation of a SASE (Secure Access Service Edge) architecture. Designed with over 100+ locations and 99.999% availability, Netskope NewEdge supports high availability of services not reliant on public cloud infrastructure.	▪ SASE
5.31	Legal, Statutory, Regulatory and Contractual Requirements	Netskope maintain a list of 75,000+ cloud applications including specific audit measurements that can be used to identify and support documentation of legislation and contractual requirements for information systems.	▪ CASB ▪ Public Cloud Security ▪ DLP ▪ CSPM ▪ SSPM
5.32	Intellectual Property Rights	Netskope Data Loss Prevention (DLP) engine can be configured to detect and prevent intellectual property leaving organization. In addition, reports can be configured to identify use of cloud applications that	▪ NG-SWG ▪ CASB

		may be categorized as proprietary software products (subject to licensing). In addition, Netskope can assist with identifying use of Generative AI services and support controls to inspect input queries and outcome generate from services.	▪ Public Cloud Security ▪ DLP ▪ SkopeAI
5.33	Protection of records	Netskope offer controls to meet certain legal and compliance requirements. Netskope Data Loss Prevention (DLP) engine can be configured to detect and prevent records, including personal data, financial data etc. leaving organization.	▪ NG-SWG ▪ CASB ▪ Public Cloud Security ▪ DLP
5.34	Privacy and protection of personally identifiable information (PII)	Netskope offer controls to meet certain legal and compliance requirements. Netskope Data Loss Prevention (DLP) engine can be configured to detect and prevent personal data leaving organization.	▪ NG-SWG ▪ CASB ▪ Public Cloud Security ▪ Private Access ▪ DLP
5.36	Compliance with policies, rules, and standards for information security	Netskope maintain a list of 75,000+ cloud applications including specific audit measurements that can be used to identify and support compliance with security policies and standards. The Netskope product capability maps to many standards and regulatory frameworks including but not limited to ISO, NIST, CSA, CIS, SSAE18, HIPAA, PCI-DSS, GDPR etc.	▪ All Products

Annex A.6 – People Controls

Reference	Control	Netskope Controls	Netskope product
6.2	Terms and conditions of employment	Netskope offers pop-up banners/coaching pages across its product that can notify employees of terms and conditions in line with organizational employment requirements. Netskope can offer controls prior to employment using reverse-proxy capabilities to protect HR systems and applications.	▪ NG-SWG ▪ CASB ▪ Public Cloud Security ▪ Private Access
6.3	Information security awareness, education, and training	Netskope offers pop-up banners/coaching pages across its product that can notify employees of policy infringements in line with organizational requirements. Netskope offers reporting on employee high-risk activities in relation to activities, threats, and Data Loss Prevention (DLP) engines.	▪ NG-SWG ▪ CASB ▪ Public Cloud Security ▪ Private Access
6.4	Disciplinary process	Netskope offers forensic information that may be required in the event of initiating the organizations disciplinary process. Organizations can choose to integrate Netskope with their existing forensic repository or HR system.	▪ NG-SWG ▪ CASB ▪ Public Cloud Security ▪ Private Access
6.5	Responsibilities after termination or change of employment	Netskope offers controls, reporting, and auditing to manage terminated employees or change in employment responsibilities. Netskope offers reporting on employee high-risk activities in relation to activities, threats, and Data Loss Prevention (DLP) engines.	▪ NG-SWG ▪ CASB ▪ Public Cloud Security ▪ Private Access ▪ DLP
6.7	Remote working	Netskope offers supporting security measures to manage risks through remote working from remote sites and remote users. Netskope offer cloud-based proxies that can apply security measures for web, cloud, and private applications.	▪ NG-SWG ▪ CASB ▪ Public Cloud Security ▪ Netskope Private Access
6.8	Information Security Event Reporting	Netskope offer a ticketing system to escalate high risk information security events and can store forensic data in forensic tools or repositories defined by customer. Netskope can identify security weaknesses across web, cloud infrastructure and cloud	▪ NG-SWG ▪ CASB ▪ Public Cloud Security ▪ Private Access

		applications including both misconfiguration and threats originating from these information systems and services.	▪ Advanced Analytics

Annex A.8 – Technological Controls

Reference	Control	Netskope Controls	Netskope product
8.1	User endpoint devices	Netskope can support use of endpoint devices including mobile and BYOD devices. Netskope offers a client to securely connect device to web, cloud and on-prem services and offers Cloud Firewall and SD-WAN hardware and software to ensure devices can connect site-to-site.	▪ SASE ▪ NG-SWG ▪ CASB ▪ Private Access ▪ Cloud Firewall ▪ SD-WAN
8.2	Privileged access rights	Netskope can help identify misuse of privileged accounts in cloud services and perform continuous assessments.	▪ CSPM ▪ SSPM
8.3	Information access restriction	Netskope can identify and make recommendations to restrict access to cloud infrastructure functions based on industry best practice guidelines. Netskope can utilize threat and data protection engines to restrict access to information access based on organizational requirements.	▪ NG-SWG ▪ CASB ▪ Public Cloud Security ▪ Private Access
8.4	Access to source code	Netskope can discover source code across cloud applications and retrospectively can apply remediation controls for certain applications. In addition, Netskope can apply controls around source code based on its Data Loss Prevention (DLP) engines.	▪ NG-SWG ▪ CASB ▪ Public Cloud Security ▪ Private Access ▪ DLP
8.5	Secure authentication	Netskope can monitor and log failed log-on connections to certain cloud apps. Netskope can also match list of used credentials with list of known compromised credentials from 3rd party sources.	▪ CASB ▪ Public Cloud Security
8.6	Capacity Management	Netskope can help support capacity management through implementation of a SASE (Secure Access Service Edge) architecture. Designed with over 100+ locations and 99.999% availability, Netskope NewEdge supports high availability of services not reliant on public cloud infrastructure.	▪ NG-SWG ▪ CASB ▪ Public Cloud Security ▪ Private Access ▪ SD-WAN ▪ DEM

		In addition, Netskope offer a Borderless SD-WAN product that can assist with networking capacity and tuning and Digital Experience Management (DEM) capabilities to ensure capacity is managed.	
8.7	Protection against malware	Netskope offers multiple threat detection engines to detect and prevent malware. Netskope offers additional sandboxing capabilities also to quarantine and execute malware in a sandbox environment. Netskope offers Remote Browser Isolation (RBI) to secure device against drive-by malware attacks and Cloud Threat Exchange (CTE) to distribute new IOC threat intelligence.	▪ NG-SWG ▪ CASB ▪ Public Cloud Security ▪ RBI ▪ Threat Protection ▪ CTE
8.8	Management of technical vulnerabilities	Netskope can inspect cloud infrastructure instances and SaaS services to identify new or existing technical vulnerabilities that exist against industry baselines and can offer auto-remediation where required. In addition, Netskope can identify devices including IT, IOT and OT services that may have technical vulnerabilities.	▪ Public Cloud Security ▪ CSPM ▪ SSPM ▪ Device Intelligence
8.9	Configuration Management	Netskope can help identify misconfigurations made in public cloud and SaaS services and can offer auto-remediation where required. Netskope offer continuous scanning of these services.	▪ Public Cloud Security ▪ CSPM ▪ SSPM
8.10	Information deletion	Netskope offers the ability to discover data-at-rest using the Netskope DLP engine. The engine can be used to discover data based on usage and attributes that match patterns i.e., exact data match or identifying certain categories of data, i.e., personal data records.	▪ DLP
8.11	Data Masking	Netskope offers the ability to discover data-at-rest using the Netskope DLP engine. Data that is processed by the Netskope service can also be obfuscated in the Netskope console if required.	▪ DLP
8.12	Data Leakage Prevention	Netskope offers the ability to discover data-at-rest and data-in-motion using the Netskope DLP engine across all common egress channels i.e., Web, Cloud, On-Prem, and Endpoint. The engine can be used to identify data based on usage and attributes that	▪ DLP

		match patterns i.e., exact data match or identifying certain categories of data, i.e., personal data records.	
8.13	Information backup	Netskope can discover information assets across cloud applications and can identify duplication of data from backups. In addition, Netskope offer legal hold capabilities that allow for preservation of data in a forensic repository for legal requirements.	▪ NG-SWG ▪ CASB ▪ Public Cloud Security
8.14	Redundancy of Information Processing Facilities	Netskope has implemented a high availability cloud-based architecture that allows operations to continue in the event of a failure. Netskope uses a global data centre footprint to replicate systems and backup data between regional data centres for reliability, high availability, and disaster recovery.	▪ SASE ▪ NG-SWG ▪ CASB ▪ Private Access
8.15	Logging	Netskope logs activity across all services including web, cloud and network including application events, page events and alerts. In addition, Netskope offer integration with log and SIEM solutions. Netskope protects log information and keeps full audit trail to identify tampering. Netskope logs administrator and operator logs. Logs can be protected using Role-Based Access Control (RBAC).	▪ SASE ▪ NG-SWG ▪ CASB ▪ Public Cloud Security ▪ Private Access
8.16	Monitoring Activities	Netskope can assist in monitoring use of systems and networks and can be used to detect anomalous behavior with policies set to take action to prevent security incidents for both outbound and inbound network, system, and application traffic.	▪ SASE ▪ NG-SWG ▪ CASB ▪ Public Cloud Security ▪ Private Access ▪ Advanced Analytics ▪ SD-WAN
8.19	Installation of software on operational systems	Netskope can restrict access to software download sites and perform continuous assessment of cloud services across IT, IoT and OT systems.	▪ NG-SWG ▪ CASB ▪ Device Intelligence
8.20	Networks security	Netskope can ensure in line end-to-end encryption (TLS) from client to web and cloud services through Netskope. Netskope offer a secure private access service to on-prem services and offer SD-WAN capabilities from hardware or software to securely connect sites.	▪ SASE ▪ NG-SWG ▪ CASB ▪ Public Cloud Security ▪ Cloud Firewall

			▪ Private Access ▪ SD-WAN
8.21	Security of network services	Netskope can audit web and cloud services and offer visibility into direct-to-net traffic flows and network services.	▪ NG-SWG ▪ CASB ▪ Public Cloud Security
8.22	Segregation of networks	Netskope supports segregation of networks using ZTNA, SD-WAN and Cloud Firewall capabilities.	▪ Private Access ▪ Cloud Firewall ▪ SD-WAN
8.23	Web Filtering	Netskope offers a Next Generation Secure Web Gateway (NG-SWG) that includes web filtering based on dynamic categorisation of websites including blocking malicious sites, command and control services and sites serving illegal content. Netskope offers TLS inspection for encrypted traffic.	▪ NG-SWG
8.24	Use of cryptography	Netskope can encrypt data-at-rest within certain cloud application subject to organizational requirement. Netskope can ensure in line end-to-end encryption (TLS) from client to web, cloud and on-prem application through the Netskope services.	▪ NG-SWG ▪ CASB ▪ Private Access
8.25	Secure development life cycle	Netskope can be used to manage access to apps and services used during SDLC i.e., GitHub, Public Cloud etc. With instance awareness, services can also be managed to separate dev, test, and production environments.	▪ NG-SWG ▪ CASB ▪ Private Access ▪ Cloud Firewall
8.26	Application security requirements	Netskope offers in line controls that can block, notify, or allow employees access to web, cloud or private application information assets across the public internet. Netskope can ensure in line end-to-end encryption (TLS) from client to web, cloud application and private application through the Netskope platform.	▪ NG-SWG ▪ CASB ▪ Public Cloud Security ▪ Private Access
8.27	Secure system architecture and engineering principles	Netskope can be used to continuously assess new technology systems i.e., Cloud for security risks such as misconfigurations and sensitive data that is not securely appropriate i.e., not encrypted.	▪ NG-SWG ▪ CASB ▪ Public Cloud Security ▪ CSPM ▪ SSPM ▪ Private Access

			▪ DLP
8.28	Secure Coding	Netskope can be used to continuously assess and protect movement of source code including the use of proprietary source code in Generative AI services.	▪ NG-SWG ▪ CASB ▪ Public Cloud Security ▪ CSPM ▪ SSPM ▪ Private Access ▪ DLP ▪ SkopeAI
8.30	Outsourced development	Netskope offer reverse proxy capabilities to protect development environments hosted on cloud infrastructure and cloud applications. Protection includes reverse proxy capabilities for corporate and personal devices where configured.	▪ CASB ▪ Public Cloud Security ▪ Netskope Private Access
8.31	Separation of development, test, and production environments	Netskope offers in line controls that can block, notify, or allow employees access to web, cloud or private application information assets. Netskope is also instance aware and can identify different instances of cloud applications including applications used for development, testing and production environments and apply data protection rules to ensure separation of environments.	▪ NG-SWG ▪ CASB ▪ Public Cloud Security ▪ Netskope Private Access
8.32	Change management	Netskope can be integrated with change management solutions. Specific controls and baseline assessments can be completed for cloud infrastructure tied to change management and business processes.	▪ Public Cloud Security ▪ CSPM ▪ SSPM ▪ SD-WAN ▪ Cloud Firewall
8.33	Test information	Netskope can utilize threat and data protection engines to restrict and protect access to information, including test data, based on organizational requirements.	▪ NG-SWG ▪ CASB ▪ Public Cloud Security ▪ Private Access ▪ Public Cloud Security ▪ DLP