cedrus
digital transformation solutions

Who is Cedrus?

We're a professional services firm that designs, architects, and implements technology-powered solutions for the digital age. Our Cloud Security practice advises organizations on how to safely embrace the Cloud.

The on-premise to cloud journey creates new vulnerabilities that need be addressed by:

• Creating the right policies and procedures
• Effectively monitoring and managing cloud activity
• Implementing the appropriate technologies to enforce the necessary security controls

Our Partnership with Netskope

As a trusted Netskope partner, we help customers:

• Select the right components in the Netskope platform to meet requirements
• Implement the technology to meet standards & integration specifications
• Establish governance oversight and process models to make the implementation effective

THE CHALLENGE

Organizations must protect critical data and infrastructure from loss, theft, misuse, and an expanding array of compliance regulations. Adding to this challenge is the fact that security teams often have limited bandwidth or do not have experience in new cloud security tools.

How do you establish a proper security risk posture in the cloud?

• Create policies to control access and protect data to manage business risk and compliance obligations
• Prioritize the most critical security controls and use cases
• Implement in key areas such as Data Leakage Prevention (DLP), Single Sign-On (SSO) federations, and access control
• Create plans and processes to handle security alerts or incidents
• Monitor, refine, and address change and business enablement in an ongoing fashion

WORKSHOP DELIVERABLE

The goal of this half-day workshop is to provide you with a clear set of goals to expand industry-specific policy, process, and security controls beyond the initial deployment. The deliverable is a prioritized plan for implementation and oversight that aligns to your unique business risk and key use cases.

• Critical criteria for risk assessment in discovery (HIPAA, PCI, etc.)
• Policy configuration criteria (DLP, Access Control, etc.)
• Networking concerns and integration plans
• Governance processes, roles, and responsibilities
• Operational and executive reporting requirements

WHO IS THIS FOR?

This offering is ideal for any Netskope subscriber that is new to the platform, has specific industry regulatory or compliance requirements, or would like to greater leverage the platform and understand their current maturity.

Activities	Description	Time (min)
Pre-Workshop		*N/A*
Cedrus and Netskope prep session	Cedrus gathers pertinent data about customer Netskope environment	
Intros and overview of session		*15*
Introductions		
How we run this workshop	Overview of the topics, roles, and workshop mechanics	
Customer led overview of the use cases/business case	Reasons for Netskope purchase, use cases, & vision for cloud security	
Best practice rollout/implementation plan discussion based upon customer use cases		*30*
Planning for Netskope Professional Services (PS)	Best practices to prepare for engaging with Netskope PS	
What goes into Netskope PS Activation	Netskope Activation Services and how they work	
Customer priorities discussion	Prioritization of feature implementation for customer risk & compliance	
What comes after Netskope PS (Finer Grained Policy Design)	Areas that will need internal evolution after initial activation	
Operationalization	Overview of operationalization of the Netskope platform	
How to establish policies that meet business risk requirements based upon customer use cases		*75*
Netskope Client and Directory Integration	Directory structure, client rollout plan, directory importer	
Access Control and Reverse Proxy	Requirements by user type, device type, location, & reverse proxy	
Risk Assessment (Discovery)	Key risk thresholds for customer to optimize discovery process	
Data Leakage Prevention (DLP)	Customer concerns, data types, advanced DLP, & user interaction	
Threat Protection	Policy application to cloud apps and integration with third party tools	
Continuous Infrastructure-as-a-Service (IaaS) Compliance	Customer current approach to security & capture a benchmark plan	
Unique Networking, Log, or Routing Considerations	Topology requirements such as forwarding or on premise log parser	
Secure Web Gateway	Transition to Netskope for Web, network, & the key controls	
Break		*15*
How to establish a working group for cloud security decisions		*45*
Decisions overview	Security decisions for effective risk-driven approach to cloud security	
Roles/personnel for participation	Types of roles or personnel required to participate in decisions	
Governance processes for healthy operation	Governance processes that will be required to operate maturely	
Operationalization		*60*
Roles/Responsibilities	Types of roles & their responsibilities for successful adoption	
Ops Training & Personnel	Training mechanisms to ensure success in operations with Netskope	
Incident Handling	Integrating Netskope into current or creating new Incident Handling	
Business Engagement	How to engage business for change & unsanctioned app migration	