

CLOUD SECURITYACCELERATION WORKSHOP

JUMPSTART YOUR CLOUD SECURITY JOURNEY

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.



CLOUD SECURITY ACCELERATION WORKSHOP

AGENDA

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