netskope

SOLUTION BRIEF

Securing Remote Workers with Netskope

Employees are increasingly working from locations outside of the traditional corporate network environment. These remote workers bypass traditional perimeter-based security controls, leaving organizations exposed and vulnerable to data loss and threats. A new, cloud-based, security solution is needed to provide protection, visibility and remote access across the enterprise.

KEY USE CASES

- **Gain visibility into the activities of remote workers.** Understand the actions of users, and risks associated with websites and cloud applications.
- **Enhance the end user experience for remote workers.** Connect users to cloud, web, and private applications using a high-performance, scalable, global network infrastructure.
- **Enforce granular data loss prevention (DLP) and threat protection policies.** Create DLP policies to protect sensitive data, and detect threats hosted within websites or cloud environments.
- **Retire legacy VPN solutions and adopt zero trust network access.** Provide direct, seamless and secure remote access to applications in public cloud environments or data centers.
- **Consolidate security for remote workers.** Combine the Netskope Next Generation Secure Web Gateway (NG SWG) and Netskope Private Access (NPA) products to deliver a modern, unified, cloud-based security platform.

THE CHALLENGE

Working outside of the traditional office environment has become a cultural norm, but employers are struggling with providing security for their remote workers. Legacy security solutions, typically located in the data center, are costly and complex and are bypassed by remote workers connecting directly to the Internet. This leaves remote workers open to threats, and permits data exfiltration to the cloud and web. Meanwhile the remote access VPNs used to connect remote workers to applications in the data center provide crude network-level access, and cannot effectively provide access to applications hosted in public cloud environments.

NETSKOPE FOR REMOTE WORKERS

Netskope provides a globally available, cloud-based security platform for securing remote workers' access to web, cloud, and private applications in the data center or public cloud. Netskope has the unique ability to decode cloud application and website traffic to understand remote workers' activities, inspect data movement, and detect threats hidden in SSL/TLS traffic. Netskope improves users' remote access experience by seamlessly and securely connecting them to their private applications using Zero Trust Network Access. Netskope requires a single, lightweight client installed on a device to manage web and cloud traffic, and tunnel private application traffic.

CAPABILITIES

DATA PROTECTION

Data is increasingly at risk as it moves outside the enterprise perimeter and beyond the visibility and control of traditional security controls. Consistent data protection policies are now required across IT-managed services such as Salesforce, Microsoft Office 365 and AWS, plus thousands of unmanaged cloud services, and websites which allow the uploading of data. Cloud services make it all too easy for employees to put sensitive information in the wrong place or share it with the wrong people. Malicious insiders or disgruntled employees are more likely to attempt exfiltration of company sensitive data when outside the office environment, making robust protection of data all the more critical for remote workers.

Netskope DLP protects sensitive data from being uploaded by remote workers to cloud applications (SaaS), public cloud environments (IaaS), or any website. Netskope is also able to identify and prevent the movement of sensitive data that may indicate the actions of a malicious insider attempting to steal data. Netskope has the most advanced cloud-based DLP capabilities, designed for ease of implementation, low false positive rates, and detailed incident investigation.

THREAT PROTECTION

When remote workers connect directly to the internet and bypass traditional on-premises security controls they expose the organization to greater risk. Remote working ultimately increases an organization's attack surface—the size and extent of the network and devices open to compromise by today's elusive threats.

Netskope decodes TLS-encrypted cloud services and websites, to identify and mitigate against the current wave of cloud-enabled threats that are facing organizations. Cybercriminals are utilizing cloud services as the reliable and scalable infrastructure for implementing their cyber kill chain in the cloud. Consider phishing pages hosted in cloud storage services such as OneNote, Command and Control networks using collaboration apps such as Slack or GitHub, or malware payloads hosted in AWS S3 buckets or Microsoft Azure.

With Netskope, remote workers are secured by a Secure Access Service Edge (SASE), as defined by Gartner. SASE combines Secure Web Gateway (SWG), Cloud Access Security Broker (CASB) and Zero Trust Network Access (ZTNA) in one common platform with unified policy controls.

Backed by Netskope Threat Research Labs, a dedicated team focused on the discovery and analysis of new cloud threats, Netskope uses multi-layer defenses including antivirus, pre-execution script analysis and heuristics, bare-metal sandboxing, machine-learning anomaly detection, plus dozens of 3rd party threat intelligence feeds.

ZERO TRUST NETWORK ACCESS

The Netskope ZTNA solution allows an organization to begin retiring legacy VPN hardware and make a move towards a more secure, cloud-first, remote access architecture. End the high capital investment, refresh cycles, and ongoing management costs of VPN appliances—and adopt ZTNA for your remote workers.

Netskope provides an alternative to backhauling (or hairpinning) remote users through the corporate network to access applications in public cloud environments, an inefficient legacy architecture that typically impacts the user experience. Netskope also removes the need to expose applications publically from public cloud environments, therefore, lowering the risk of compromise through unauthorized access.

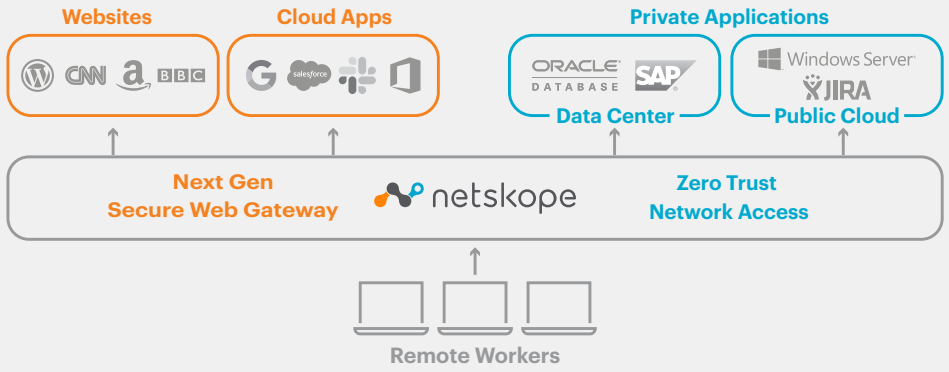

FIGURE 1: Securing Remote Workers with Netskope

Netskope directly and seamlessly connects remote workers to private applications running in public cloud environments or private data centers. Connectivity between remote workers and applications is secured by an end-to-end TLS encrypted tunnel and optimally routed through NewEdge—Netskope's high-performance, scalable global network infrastructure. Integration with strong authentication, and inspection of device security posture, ensures that only authorized users with secure devices can gain access to applications.

> **"62% of organizations say their biggest application security challenge is securing access to private apps that are distributed across datacenter and cloud environments"**
>
> Cybersecurity Insiders, 2019 Zero Trust Adoption Report, November 2019

VISIBILITY

Netskope provides detailed and valuable insight into all the cloud applications and websites an organization's remote workers are visiting. Furthermore, Netskope's Cloud XD™ technology is able to decode cloud and web traffic to understand the activities performed by users and distinguish between corporate and personal instances of cloud apps. With Netskope, you can obtain granular visibility into cloud app activity and the spread of sensitive data within and outside your organization. However, in order to provide a more robust security solution, security teams need to enact granular security controls across both managed and unmanaged cloud apps use. The greatest blindspot for security teams is the unofficial use of unmanaged apps that often proliferate across organizations.

GRANULAR CONTROL

Netskope's Cloud XD is the "engine" of the Netskope platform, Cloud XD makes sense of cloud services, apps, and web traffic to feed context and content into data and threat protection policies. Cloud XD understands the language of the cloud (APIs, JSON, etc.) to provide granular visibility into the users, devices, applications, instances, risk ratings, URL categories, and activities in cloud and web environments. It then takes smart actions, such as allow, block, delete, encrypt, quarantine and more, based on your enforcement policies.

Granular visibility and control of remote workers' activities when they use cloud applications or visit websites plays an important role in reducing the risk of data loss, and protecting against threats. Netskope's NG SWG policies can differentiate between personal and corporate instances of cloud applications. Examples of how this instance-awareness can be used include; preventing uploads of sensitive data to personal instances of cloud storage, or preventing access to rogue instances of public cloud environments used to host phishing pages or malware.

BENEFITS	DESCRIPTION
ADVANCED THREAT PROTECTION	**PROVIDE REMOTE WORKERS WITH PROTECTION FROM CLOUD-BASED AND WEB-BASED THREATS. PLUS PROTECT THE BUSINESS FROM MALICIOUS INSIDERS:** • Automatically detect compromised accounts by examining user behavior such as cloud application login frequency, suspicious geographic login-access, brute-force attacks and unusual login patterns • Detect and stop threats from cloud apps and websites in real-time using multiple anti-malware engines, threat intelligence feeds (40+), pre-execution heuristics, sandboxing and machine learning • Detect and alert on anomalous behavior by identifying unusual amounts of data uploaded, downloaded or deleted • Maximize investment in existing security technologies by integrating Netskope with EDR (Endpoint Detection and Response), SIEM (Security Information and Event Management), SOAR (Security Orchestration, Automation and Response), and RBI (Remote Browser Isolation) solutions
ADVANCED DATA PROTECTION	**DEVELOP GRANULAR DLP POLICIES THROUGH EASY TO USE TEMPLATES, OR BUILD CUSTOM RULES:** • Quickly implement cloud-delivered DLP policies using dozens of predefined policy templates to identify sensitive data in accordance with common regulations • Detect sensitive data accurately by reading data classification tags, finding data using regular expressions, performing EDM, or detecting fingerprinted documents • Selectively apply DLP policies to data based on the context of a transaction. Focus on particular activities, users, apps, instances, devices, etc to build policies that generate fewer false positives • Take appropriate remedial action when DLP policies are triggered, including blocking data transfers, alerting, cautioning users, or encrypting or quarantining a file • Netskope's native investigation tools simplify the analysis of DLP incidents, providing forensic information that includes excerpts of violation data, and allowing incidents to be given priorities and assigned to investigators
ZERO TRUST NETWORK ACCESS	**ALLOW SEAMLESS REMOTE ACCESS TO APPLICATIONS IN DATA CENTERS AND PUBLIC CLOUD ENVIRONMENTS:** • Zero trust network access to private applications. Protect data and resources with application-level access control based on user identity and device security posture • Seamless and direct access to public cloud(s) where remote users are connected directly to applications in public cloud environments—no need to hairpin through corporate infrastructure to access applications hosted in the public cloud • Avoid the need to expose private applications publically from public cloud environments such as AWS or Azure, therefore removing any risk of external compromise by unauthorized users • Simplify IT operations, modernize network architecture, improve the end-user experience and increase the security of Internet use using a scalable, cloud-based platform that unifies ZTNA, CASB, SWG and DLP
VISIBILITY AND CONTROL	**OBTAIN DEEP VISIBILITY INTO REMOTE WORKERS CLOUD APPLICATION AND WEB USAGE, AND DEFINE POLICIES TO CONTROL ACTIVITIES:** • Discover all managed and unmanaged (shadow IT) cloud apps being used by remote workers and view their risk score • Identify the high risk behaviors and activities of remote workers within managed and unmanaged cloud apps • Use Netskope's instance-awareness to prevent the loss of corporate data to personal cloud app instances • Granularly manage share and post activities in cloud apps to prevent sensitive data from being exposed • Detect compromised accounts and insider/ privileged user threats • Capture an audit trail of remote worker activity within cloud apps and websites for forensic investigations

REQUEST A LIVE DEMO:
https://www.netskope.com/request-demo

netskope

The Netskope security cloud provides unrivaled visibility and real-time data and threat protection when accessing cloud services, websites, and private apps from anywhere, on any device. Only Netskope understands the cloud and takes a data-centric approach that empowers security teams with the right balance of protection and speed they need to secure their digital transformation journey. Reimagine your perimeter with Netskope.

©2020 Netskope, Inc. All rights reserved. Netskope is a registered trademark and Netskope Active, Netskope Cloud XD, Netskope Discovery, Cloud Confidence Index, and SkopeSights are trademarks of Netskope, Inc. All other trademarks are trademarks of their respective owners. 02/20 SB-365-1