netskope

5 REASONS TO CHOOSE CLOUD SECURITY FOR REMOTE WORKERS

5 REASONS TO CHOOSE CLOUD SECURITY FOR REMOTE WORKERS

Many organizations struggle with providing adequate security for remote workers, and are increasingly challenged by remote access requirements in today's cloud-first world. As a group, remote workers are well suited for migration to a cloud-native security solution; it is possible to deliver a significant risk reduction, and an improvement to user experience, with relatively low effort.

As you evaluate how best to secure remote workers, consider these five reasons to transform your security stack with a cloud-native solution. For each of the 5 reasons, this eBook provides an explanation of the issue and its risks, how Netskope can help address the issue, and how you can test and evaluate your current security solution's effectiveness.

REASON #1 | CLOUD-BASED THREATS

REASON #2 | DATA EXPOSURE AND THEFT

REASON #3 | ACCESS COMPROMISE AND ANOMALIES

REASON #4 | ELASTIC CAPACITY AND GLOBAL PERFORMANCE

REASON #5 | ADOPTION OF ZERO TRUST NETWORK ACCESS

01

CLOUD-BASED THREATS

Cloud is the new attack surface. The number one cloud-based attack is phishing, and the number one phishing target is your employees' credentials for cloud apps and webmail[1]. Legacy web security defenses focused on web reputations to trigger defenses, or endpoint solutions looking for a malicious payload, are missing the transformation.

01

Today, organizations typically use over 2,400 cloud services and apps[2] of which more than 1,600 are known to deliver threats[2].

There are examples at all stages of the cyber kill chain of cloud services, cloud apps, and cloud storage being used to evade legacy defenses. Well known cloud services have trusted domains and valid certificates, and may even be whitelisted to bypass defenses. This provides attacks with 'red carpet' entry to remote workers who typically spend up to 89% of their day[2] accessing the cloud.

FACT:

Cybercriminals now want your cloud identity more than your credit card number. Phishing attacks for SaaS credentials (30.8%) have surpassed phishing attacks on payment systems (19.8%) and financial institutions (19.4%).

APWG Phishing Trends Activity Report, Q4 2019 - https://apwg.org/trendsreports/

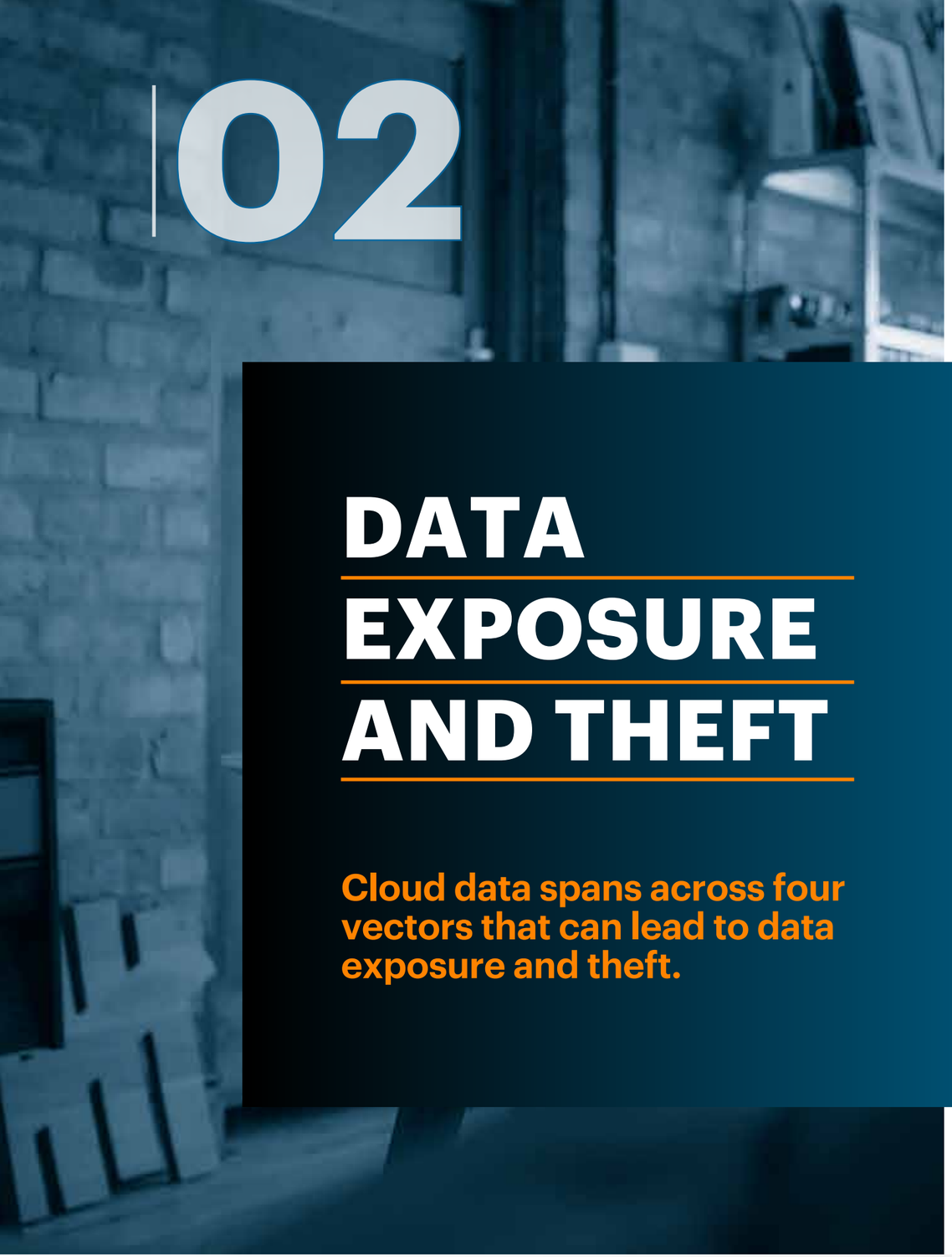
NETSKOPE ADVANTAGE

The Netskope Next Gen Secure Web Gateway (NG SWG) protects all users and devices, from any location, using cloud-native defenses. Netskope has the ability to decode the traffic for thousands of cloud services and cloud apps to understand activity, instance and data, and to provide advanced threat protection. Cloud-enabled kill chains are here to stay. Defenses unable to decode the context of cloud services, cloud apps, and websites simply leave your organization blind to today's threats.

EVALUATE AND TEST

Test your security stack to assess how many of your cloud services and cloud apps, managed and unmanaged, can be inspected for content and context. Check that you have metadata available such as user identity, device type, cloud application, risk level, application instance, user activity, and transferred data. If you had to investigate a cloud phishing attack from a rogue instance of an unmanaged cloud app, do you have the necessary visibility and metadata?

[1] APWG Phishing Trends Activity Report, Q4 2019 - https://apwg.org/trendsreports/
[2] Netskope Cloud and Threat Report - February 2020



02

DATA EXPOSURE AND THEFT

Cloud data spans across four vectors that can lead to data exposure and theft.

Firstly, familiar and trusted managed cloud services including Microsoft Office 365 and G Suite by Google Cloud are often whitelisted. Remote workers can therefore accidently, or with intent, move data between company and personal instances of these cloud services.

Secondly, an organization only has a handful of *managed* cloud services, typically less than 2%, while use of a diverse set of *unmanaged* cloud services account for 98%. Unmanaged cloud apps are usually freely adopted by business units and individual users and data can often flow easily to these services.

Thirdly, data movement between cloud application categories is commonplace, this includes data moving between cloud storage apps, from cloud storage to collaboration apps, and from cloud storage to webmail apps. You need to detect, and then manage, sensitive and private data movement between undesirable categories, apps, and instances.

Fourth and finally, without understanding the risk associated with cloud applications it is impossible to limit the access, or user activities, for those cloud apps where data may be at risk of compromise. Insight into which applications are lower risk (e.g. Microsoft OneDrive, Box) versus those posing higher risk (e.g. WeTransfer, Zippyshare) will help the security team set appropriate data protection policies for remote workers.

STATS:

20% of users have sensitive data moving between cloud apps and 37% of that data is involved in DLP violations

Netskope Cloud and Threat Report - February 2020

NETSKOPE ADVANTAGE

Netskope NG SWG protects remote workers by using cloud-based Data Loss Prevention (DLP). Netskope DLP has a rich understanding; including the content, context, instance, category, and risk level; of cloud applications being used within an organization. These variables, not found in legacy web defenses, can be used to build effective data protection policies directly in the cloud – no need for legacy Internet Content Adaptation Protocol (ICAP) interfaces between web proxies and external DLP appliances.

Netskope is a single cloud security platform, with unified policies for securing both cloud and web. This means DLP policies can be applied across webpage content, files, and forms, as well as thousands of cloud services and apps.

EVALUATE AND TEST

Test your security stack across the four vectors; apply DLP rules and policies to differentiate between sensitive data uploaded to company versus personal instances of managed cloud apps, or managed versus unmanaged cloud apps. Also, if your current security stack has visibility of remote workers, can it profile cloud data movement between cloud app categories, or provide cloud app risk scoring to help with selecting and enabling lower risk cloud apps for use by business units and employees?

03

ACCESS COMPROMISE AND ANOMALIES

Cloud identity and access is the new perimeter, so it should be no surprise that phishing cloud access credentials is now the number one target for cybercriminals, well ahead of payment and financial phishing targets.

When phishing is successful then an enterprise's next defense is identifying the use of those compromised credentials, and associated malicious activities, as quickly as possible. Detecting access compromise and anomalous behavior requires rich metadata gathered from across thousands of cloud services and apps, and an understanding of context for Machine Learning (ML) models and use cases. Legacy defenses which are blind to cloud services, because they are unable to decode the content and context, leave remote workers unprotected and security operations with no ability to detect or investigate access compromise and anomalies.

REMEMBER:

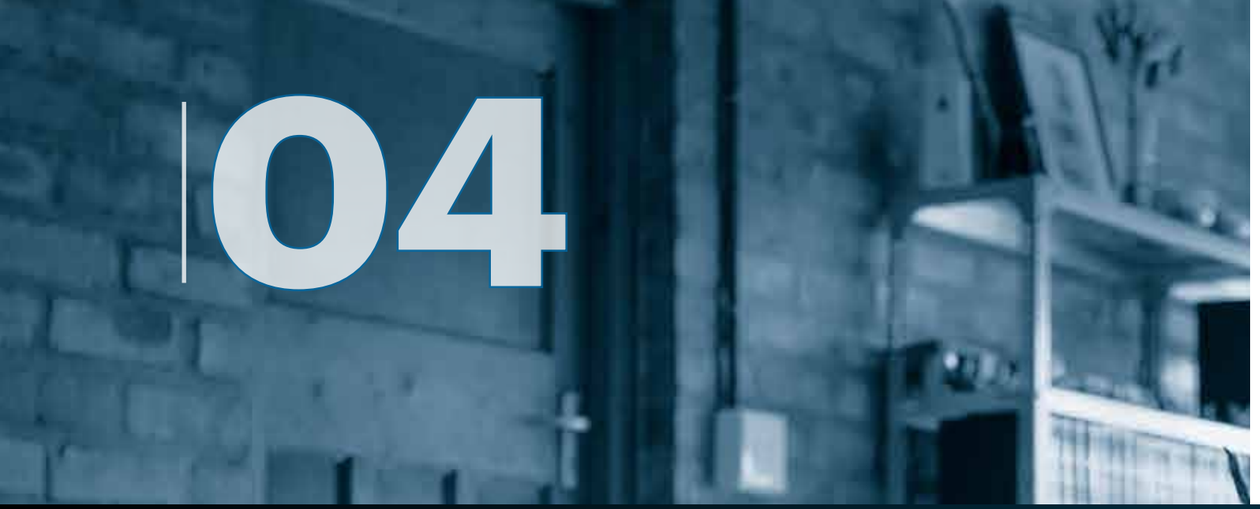
Cloud-enabled attacks can cloud phish credentials using trusted domains, which have valid SSL certificates, and which evade endpoint defenses because there is no detectable payload.

NETSKOPE ADVANTAGE

Netskope provides user and entity behavior analytics (UEBA) based on the rich metadata it collects from remote users' wherever they are and whatever cloud applications and websites they are accessing. Netskope UEBA machine learning anomaly detection allows the detection of compromised accounts, malicious insiders, and data exfiltration. Further insights and alerts are provided by sequential rules analysis of activities such as bulk downloads, bulk uploads, bulk deletes, rare events, geographical proximity analysis, access from high risk countries, and multiple failed logins. A simple question to ask your security team: Can we currently detect or investigate suspected access compromise or anomalous user behavior in cloud applications?

EVALUATE AND TEST

Test your current security stack by simulating suspicious data exfiltration behavior. Download 10 or more files from a company instance of a managed cloud application and then upload them to a personal instance of an unmanaged cloud application, wait 20 mins and then delete the files from the personal instance. Did you get an alert on these activities? Did you get a single alert or two alerts? Could you prevent this behavior with granular policy controls?



04

ELASTIC CAPACITY AND GLOBAL PERFORMANCE

Cybercriminals have adopted the cloud faster than most legitimate organizations, many of whom are still trying to secure cloud usage using web security appliances that they invested in many years ago. Remote workers are often hairpinned (or backhauled) through these appliances via VPN connections. These appliances are typically restricted in compute and storage capacity and this forces security teams to trade-off security capabilities for acceptable performance.

Encrypted SSL/TLS traffic (HTTPS) is now at 84% globally[2] and effective defenses require intensive compute cycles to decode and inspect the content and context of cloud and web usage. Approaches such as whitelisting traffic to try and improve user experience, selectively firing defenses based on risk or reputation, being unable to decode the API-based JSON traffic of cloud, or simply allowing remote workers to bypass security controls, are all huge risks in a cloud first environment. A modern approach to security for remote workers that scales, and delivers an optimal user experience, can only be delivered from the cloud.

ANALYST VIEW:

Read Gartner's thoughts on the future of cloud-native security in their report, "The Future of Network Security is in the Cloud".

Published 30 August 2019 - ID G00441737

https://www.gartner.com/doc/reprints?id=1-6QW0Z4A&ct=190528&st=sb

NETSKOPE ADVANTAGE

Netskope provides cloud-native security microservices in one global platform, with on-demand performance and scale to inspect encrypted traffic, decode cloud services and apps, filter web traffic, and apply advanced data and threat protection. Netskope also provides a global network infrastructure of high-capacity public Points of Presence (PoPs) with unmatched peering relationships with services such as Amazon Web Services (AWS), Microsoft Azure and Google Cloud Platform (GCP)—ensuring the fastest round trip times to Internet services for remote workers wherever they are in the world. This network infrastructure, called NewEdge™, ensures a safe and positive user experience when using the Netskope Security Cloud.

EVALUATE AND TEST

Compare your legacy appliance defense capabilities with the cloud defense capabilities of Netskope. Create your own tests or use the Netskope security check tool—**netskopesecuritycheck.com**

If users are bypassing your existing security controls when out of the office, consider implementing cloud-native defenses. These protections can replace or augment the appliances in your data center. As there's no reason to wait if your remote workers are at higher risk, consider a proof of concept or pilot of Netskope for your remote workers.

05

ADOPTION OF ZERO TRUST NETWORK ACCESS

The migration of private applications to public cloud, and the wide adoption of cloud applications, are removing the need for corporate data centers. Managing legacy VPN solutions which backhaul to appliances in traditional data centers introduces several risks in addition to an undesirable, cumbersome user experience.

05

Firstly, hairpinning remote users via VPNs through central data centers to access apps and resources hosted in public cloud environments will result in poor performance and long round-trip times. Secondly, having open ports and services for VPN connections into network environments provides an open attack surface. And finally, remote VPNs provide compromised accounts or malicious insiders with both access and, more worryingly, the potential for lateral movement within the corporate network.

CONSIDER:

Can your existing appliance-based VPN solution scale to support remote access for all employees should such a need arise?

REASON #5 | ADOPTION OF ZERO TRUST NETWORK ACCESS

NETSKOPE ADVANTAGE

Secure remote users with zero trust network access (ZTNA) solutions, like Netskope Private Access (NPA), to provide direct access to only authorized applications in the data center or public cloud. NPA does not require inbound open ports or services, and, therefore, removes any opportunity for external exposure and attack. NPA is a cloud-native and highly scalable solution. Unlike with VPN appliances, there is no need to worry about the concurrency of users or exhaustion of resources. Now is the time to consider retiring your legacy VPN solution in favor of ZTNA.

EVALUATE AND TEST

Compare your remote worker VPN experience to Netskope Private Access side by side in an evaluation. Consider especially how remote workers access to private applications in public cloud environments is complicated by using traditional remote access VPNs. Also consider whether your existing appliance-based solution and associated licensing could scale to support remote access for all employees should such a need arise.

Netskope has seen entire customer teams adopt ZTNA over their legacy VPN solutions in extremely short timescales due to user and Network Operations (NetOps) experience benefits. An evaluation of NPA can typically be deployed within a few hours and will provide immediate firsthand experience of the benefits. Bear in mind that NPA is part of the same Netskope cloud platform that delivers all the advantages outlined in this eBook for securing remote workers' access to cloud and web.

Remote workers should be your first priority for cloud-native, cloud-first defenses

On any given day around **33% of workers are remote**, and on average they are **spread across more than 8 locations**[1] in today's enterprises.

Remote workers are in the cloud regularly, being targeted by cloud-enabled threats, and freely moving data across a wide breadth of cloud applications and web services. Attempts to hairpin remote users via VPNs back to legacy web security appliances which are restricted in capacity generally result in high end-to-end latency and a poor user experience.

The solution? Separate remote workers from the pack and provide them with the security they need using a globally available, cloud-native, next generation secure web gateway (NG SWG). Use Netskope to control web access, provide data and threat protection, and decode thousands of cloud services and apps to provide policy controls by user, cloud app, cloud app category, cloud app instance, risk level, user activity, data content, and more. Finally, provide remote workers with secure and direct access into corporate data centers and public cloud environments using Netskope Private Access, a ZTNA solution that is another integrated capability of the Netskope platform.

[1] Netskope Cloud and Threat Report - February 2020

For More Information

Netskope can help you secure your remote workers no matter where they are. For more details, please contact your local Netskope sales representative or channel partner or refer to the following web pages:

Securing Remote Workers:
https://www.netskope.com/solutions/securing-remote-workers

Move Beyond VPNs:
https://www.netskope.com/solutions/virtual-private-networks

The network perimeter is dissolving. A new perimeter is needed that can protect data and users everywhere, without introducing friction to the business. 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 delivers data-centric security from one of the world's largest and fastest security networks, empowering the largest organizations in the world with the right balance of protection and speed they need to enable business velocity and secure their digital transformation journey. **Reimagine your perimeter with Netskope.**

netskope.com