
November 2023
Security that's ready for anything
MACIO Forum
netskope

Farewell to Network Security as We Know It

Nate Smolenski - CISO - Head of Cyber Intelligence Strategy @ Netskope
CISSP, CISA, CISM, ZTX-I
November 2023

The Changing Business, Technology, & Threat Landscape

Modern Challenges May Catch Organizations' Defenses Off Guard

Unstructured Data Sprawl

80% of the projected 175 zettabytes of data by 2025 will be unstructured

Source code is the most frequently exposed data type

AI-based Threats

Thousands malicious URLs and domains to capitalize on genAI

AI-based malware is a growing security concern

Generative AI Apps

ChatGPT fastest-growing app in history with 100M users 2 months after launch

AI app use up 22.5% over the past two months

ChatGPT
Google Bard
Grammarly

Unpredictable User Behavior

82% of data breaches involve the human element and 61% involve credentials

70% of users continue to work remotely

Connectivity Performance

Network optimization and troubleshooting of access anomalies require analysis of vast amounts of data

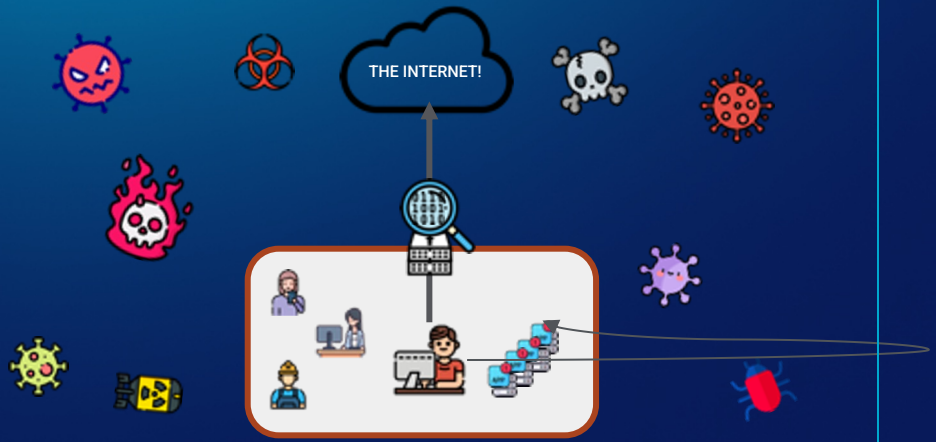
New Connected Devices

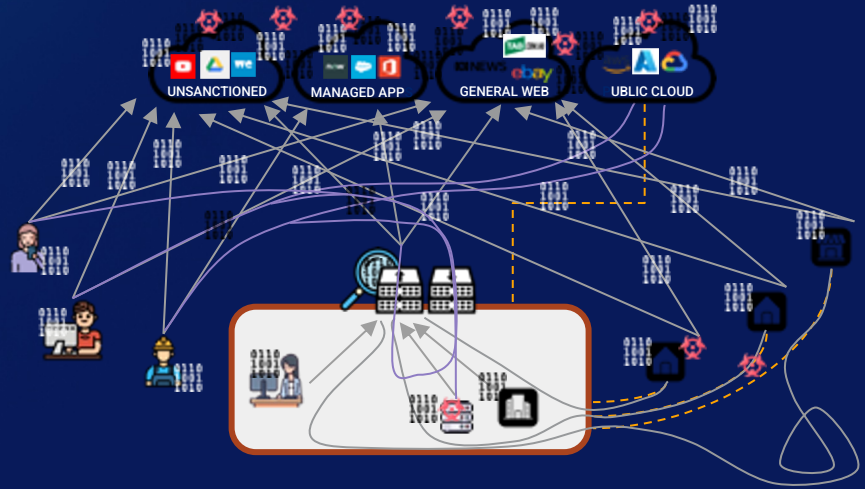
By 2025, ~80 billion devices will be connected to the Internet

More than 25% of cyberattacks against businesses will involve IoT

Yesterday vs Today

Data is now everywhere; including the local office





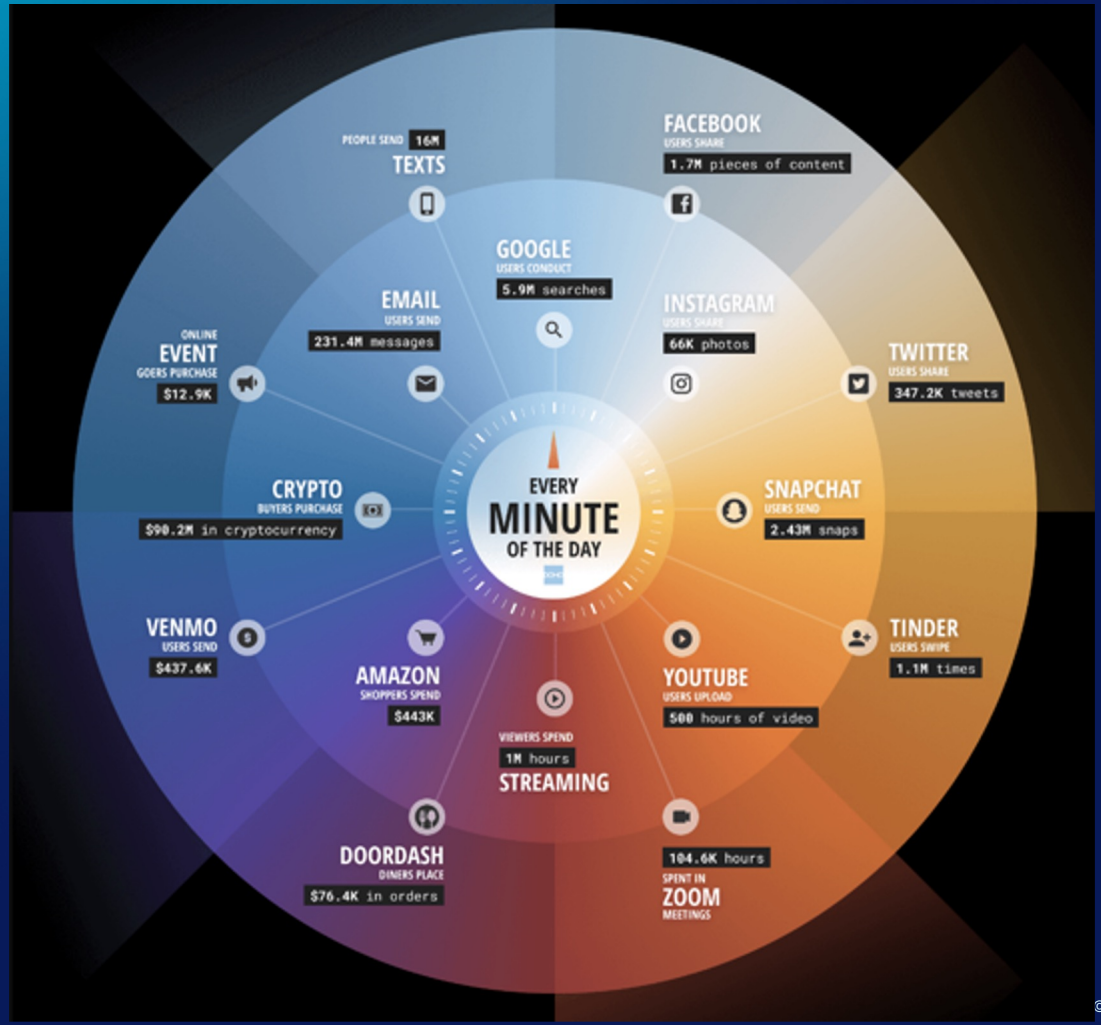
Yesterday

Users, Apps, and Data located **within** the company perimeter
Security on-premises made sense!

Today

Users, Apps, and Data located **outside** the company perimeter
Security on-premises is broken - nothing is there anymore!

netskope



Deteriorating Visibility and Control

Security Leader Challenges

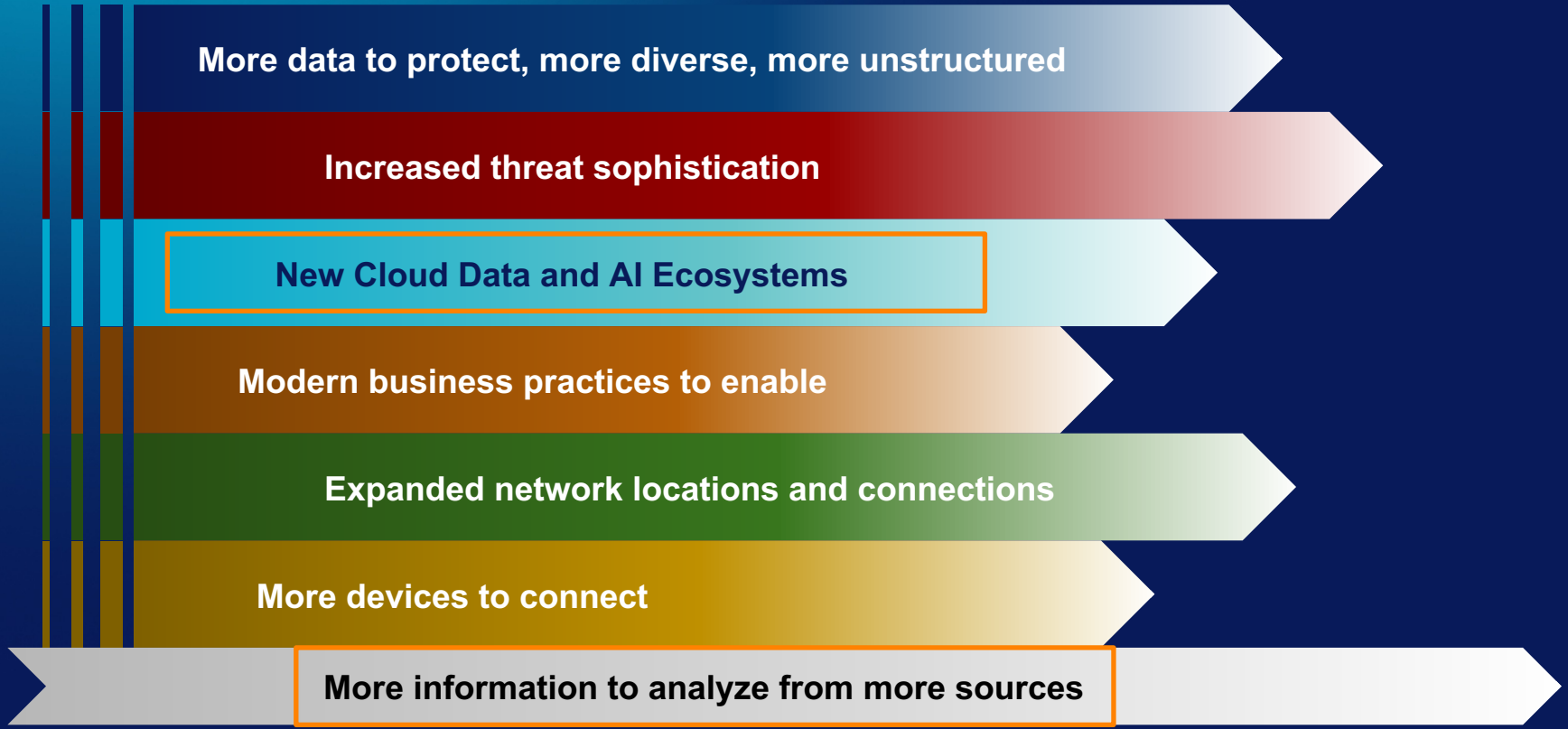
- Movement to SaaS has exposed risks related to our inability to deliver high efficacy controls while at the same time managing our attack surface.

Network Leader Challenges

- Fear that moving to the cloud will cause us to lose capabilities of the data center and what we control?

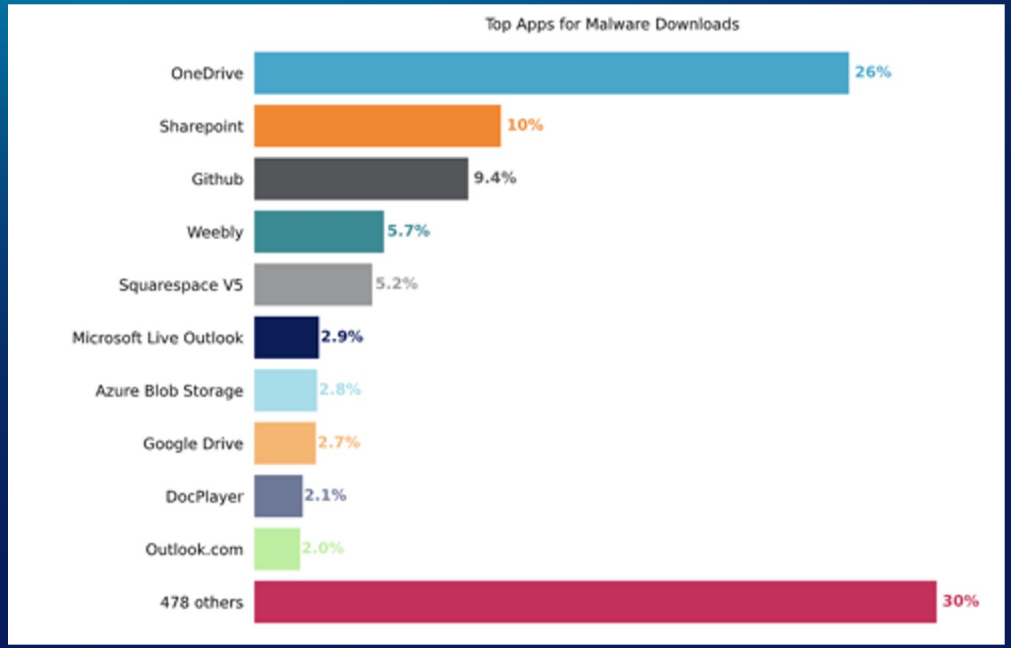
How do you control what users do inside of business-led SaaS applications?

The Era of Rapidly Expanding Data and Threat Landscape



netskope

Increase in Evolved Cloud Threats



Security & Network Leader Challenges

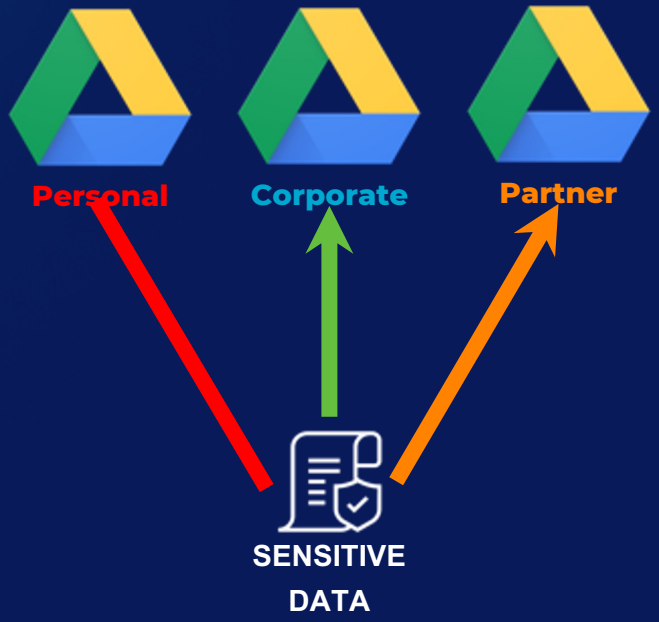
- Inability to detect and prevent malware and phishing from “trusted” SaaS applications
- Increased Ransomware prevents standard operations
- Bypass of common SaaS business traffic (MSFT 365 traffic) creates blind spots for malware infiltration

How do you detect and prevent malware in trusted SaaS apps?

Insufficient Data Protection

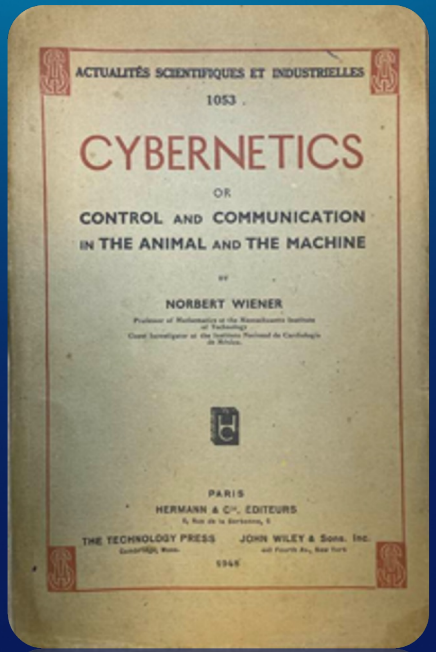
Security & IT Leader Challenges

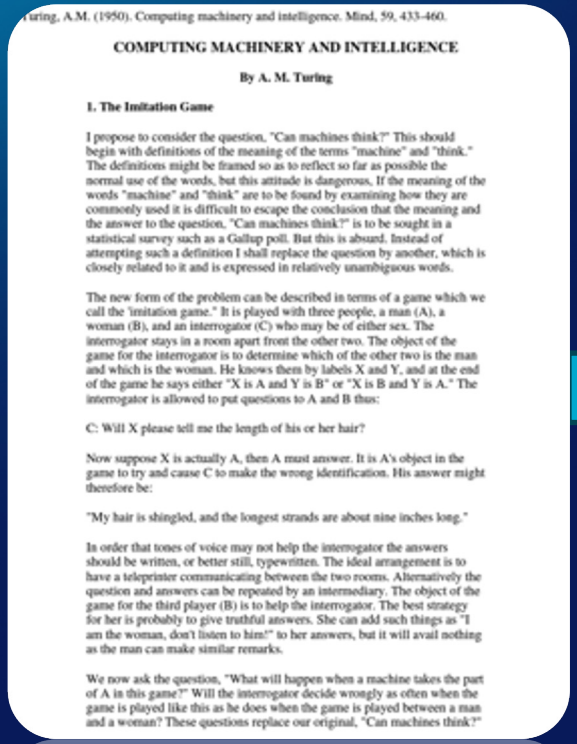
- Movement to cloud has rendered my existing DLP controls ineffective
  - Unable to safely collaborate with 3rd party business partners
  - Unable to control data theft to personal cloud storage
  - Unable to prevent sensitive data movement to exposed public cloud storage



What about AI?

Artificial Intelligence – From 1948 until present day





Turing, A.M. (1950). Computing machinery and intelligence. Mind, 59, 433-460.

COMPUTING MACHINERY AND INTELLIGENCE

By A. M. Turing

1. The Imitation Game

I propose to consider the question, "Can machines think?" This should begin with definitions of the meaning of the terms "machine" and "think." The definitions might be framed so as to reflect so far as possible the normal use of the words, but this attitude is dangerous, If the meaning of the words "machine" and "think" are to be found by examining how they are commonly used it is difficult to escape the conclusion that the meaning and the answer to the question, "Can machines think?" is to be sought in a statistical survey such as a Gallup poll. But this is absurd. Instead of attempting such a definition I shall replace the question by another, which is closely related to it and is expressed in relatively unambiguous words.

The new form of the problem can be described in terms of a game which we call the 'imitation game." It is played with three people, a man (A), a woman (B), and an interrogator (C) who may be of either sex. The interrogator stays in a room apart front the other two. The object of the game for the interrogator is to determine which of the other two is the man and which is the woman. He knows them by labels X and Y, and at the end of the game he says either "X is A and Y is B" or "X is B and Y is A." The interrogator is allowed to put questions to A and B thus:

C: Will X please tell me the length of his or her hair?

Now suppose X is actually A, then A must answer. It is A's object in the game to try and cause C to make the wrong identification. His answer might therefore be:

"My hair is shingled, and the longest strands are about nine inches long."

In order that tones of voice may not help the interrogator the answers should be written, or better still, typewritten. The ideal arrangement is to have a teleprinter communicating between the two rooms. Alternatively the question and answers can be repeated by an intermediary. The object of the game for the third player (B) is to help the interrogator. The best strategy for her is probably to give truthful answers. She can add such things as "I am the woman, don't listen to him!" to her answers, but it will avail nothing as the man can make similar remarks.

We now ask the question, "What will happen when a machine takes the part of A in this game?" Will the interrogator decide wrongly as often when the game is played like this as he does when the game is played between a man and a woman? These questions replace our original, "Can machines think?"

netskope

What Generative AI Apps Can Do: Endless Possibilities

Generative AI use cases, nonexhaustive

Modality	Application	Example use cases
Text	Content writing	Marketing: creating personalized emails and posts Talent: drafting interview questions, job descriptions
	Chatbots or assistants	Customer service: using chatbots to boost conversion on websites
	Search	Making more natural web search Corporate knowledge: enhancing internal search tools
	Analysis and synthesis	Sales: analyzing customer interactions to extract insights Risk and legal: summarizing regulatory documents
Code	Code generation	IT: accelerating application development and quality with automatic code recommendations
	Application prototype and design	IT: quickly generating user interface designs
	Data set generation	Generating synthetic data sets to improve AI models' quality
Image	Stock image generator	Marketing and sales: generating unique media
	Image editor	Marketing and sales: personalizing content quickly
Audio	Text to voice generation	Trainings: creating educational voiceover
	Sound creation	Entertainment: making custom sounds without copyright violations
	Audio editing	Entertainment: editing podcast in post without having to rerecord
3-D or other	3-D object generation	Video games: writing scenes, characters Digital representation: creating interior-design mockups and virtual staging for architecture design
	Product design and discovery	Manufacturing: optimizing material design Drug discovery: accelerating R&D process
Video	Video creation	Entertainment: generating short-form videos for TikTok Training or learning: creating video lessons or corporate presentations using AI avatars
	Video editing	Entertainment: shortening videos for social media E-commerce: adding personalization to generic videos Entertainment: removing background images and background noise in post
	Voice translation and adjustments	Video dubbing: translating into new languages using AI-generated or original-speaker voices Live translation: for corporate meetings, video conferencing Voice cloning: replicating actor voice or changing for studio effect such as aging
	Face swaps and adjustments	Virtual effects: enabling rapid high-end aging; de-aging; cosmetic, wig, and prosthetic fixes Lip syncing or "visual" dubbing in postproduction: editing footage to achieve release in multiple ratings or languages Face swapping and deep-fake visual effects Video conferencing: real-time gaze correction

Data Exposure, Risks and Compliance Implications

First reported incidents

SAMSUNG

Whoops, Samsung workers accidentally leaked trade secrets via ChatGPT

ChatGPT doesn't keep secrets.

Employee used the AI chatbot to summarise minutes from a meeting, which got leaked to the public.

Three Samsung employees reportedly leaked sensitive data to ChatGPT

Source code exposed to the public. Employees inputted code into ChatGPT for debugging and optimization.

Banking giants, high tech companies and entire countries restrict ChatGPT access

J.P.Morgan

JPMorgan Chase, Verizon, Citigroup, and Goldman Sachs Block Access to ChatGPT

By IBL News · February 27, 2023

Other firms are taking a similar approach. **Bank of America**, **Wells Fargo**, **Goldman Sachs** Group, **Citigroup** and **Deutsche Bank** have banned their employees from tapping ChatGPT and OpenAI for business use, people

citi

Amazon Warns Employees to Beware of ChatGPT

At the same time, OpenAI's Chat GPT gave correct answers to interview questions for a software coding position.

ChatGPT banned in Italy over privacy concerns

Goldman Sachs

BANK OF AMERICA

verizon

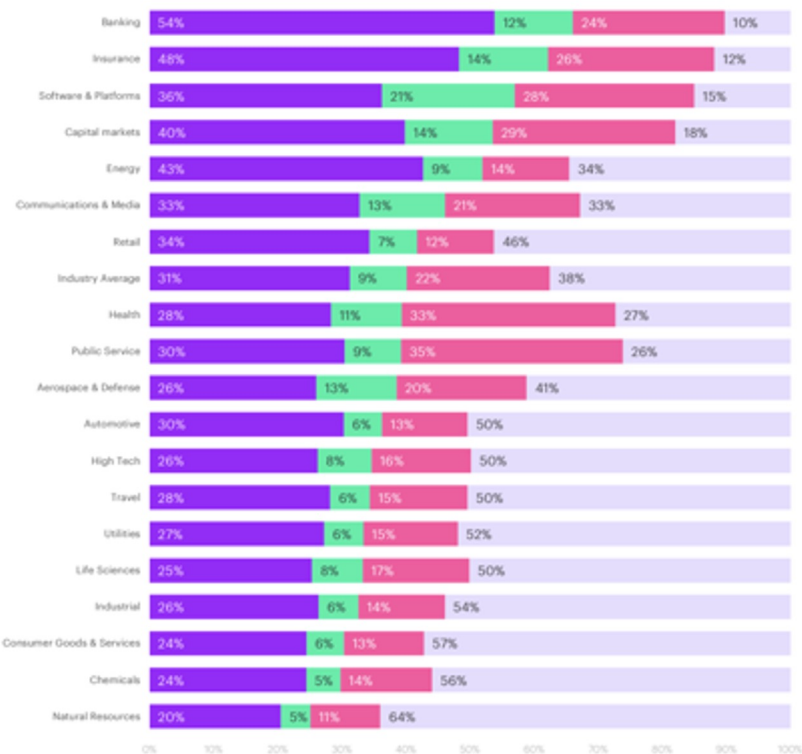
amazon

Deutsche Bank

netskope

Generative AI - Transformational to Work Across Industry

Figure 3: Generative AI will transform work across industries



Work time distribution by industry and potential AI impact

Based on their employment levels in the US in 2021

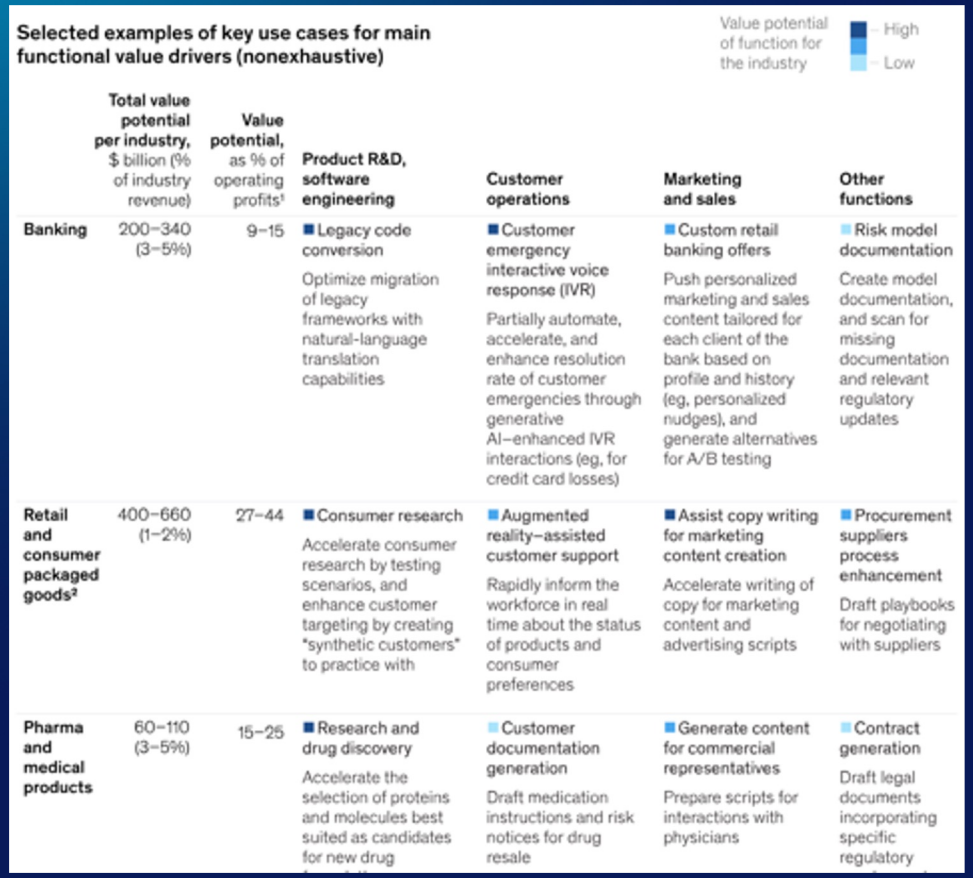
40% of working hours across industries can be impacted by Large Language Models (LLMs)

Why is this the case? Language tasks account for 62% of total worked time in the US. Of the overall share of language tasks, 65% have high potential to be automated or augmented by LLMs.

Source: Accenture Research based on analysis of Occupational Information Network (O*NET), US Dept. of Labor; US Bureau of Labor Statistics.

Notes: We manually identified 200 tasks related to language (out of 332 included in BLS), which were linked to industries using their share in each occupation and the occupations' employment level in each industry. Tasks with higher potential for automation can be transformed by LLMs with reduced involvement from a human worker. Tasks with higher potential for augmentation are those in which LLMs would need more involvement from human workers.

Generative AI - Responsibly Enabling and Protecting Data



Selected examples of key use cases for main functional value drivers (nonexhaustive)

Value potential of function for the industry: High / Low

	Total value potential per industry, $ billion (% of industry revenue)	Value potential, as % of operating profits[1]	Product R&D, software engineering	Customer operations	Marketing and sales	Other functions
Banking	200–340 (3–5%)	9–15	**Legacy code conversion** Optimize migration of legacy frameworks with natural-language translation capabilities	**Customer emergency interactive voice response (IVR)** Partially automate, accelerate, and enhance resolution rate of customer emergencies through generative AI–enhanced IVR interactions (eg, for credit card losses)	**Custom retail banking offers** Push personalized marketing and sales content tailored for each client of the bank based on profile and history (eg, personalized nudges), and generate alternatives for A/B testing	**Risk model documentation** Create model documentation, and scan for missing documentation and relevant regulatory updates
Retail and consumer packaged goods[2]	400–660 (1–2%)	27–44	**Consumer research** Accelerate consumer research by testing scenarios, and enhance customer targeting by creating "synthetic customers" to practice with	**Augmented reality–assisted customer support** Rapidly inform the workforce in real time about the status of products and consumer preferences	**Assist copy writing for marketing content creation** Accelerate writing of copy for marketing content and advertising scripts	**Procurement suppliers process enhancement** Draft playbooks for negotiating with suppliers
Pharma and medical products	60–110 (3–5%)	15–25	**Research and drug discovery** Accelerate the selection of proteins and molecules best suited as candidates for new drug	**Customer documentation generation** Draft medication instructions and risk notices for drug resale	**Generate content for commercial representatives** Prepare scripts for interactions with physicians	**Contract generation** Draft legal documents incorporating specific regulatory

Preparing for Black Swan Events - AI Takeaways

How is your organization balancing new digital transformation objectives?

PRODUCTIVITY

RISK

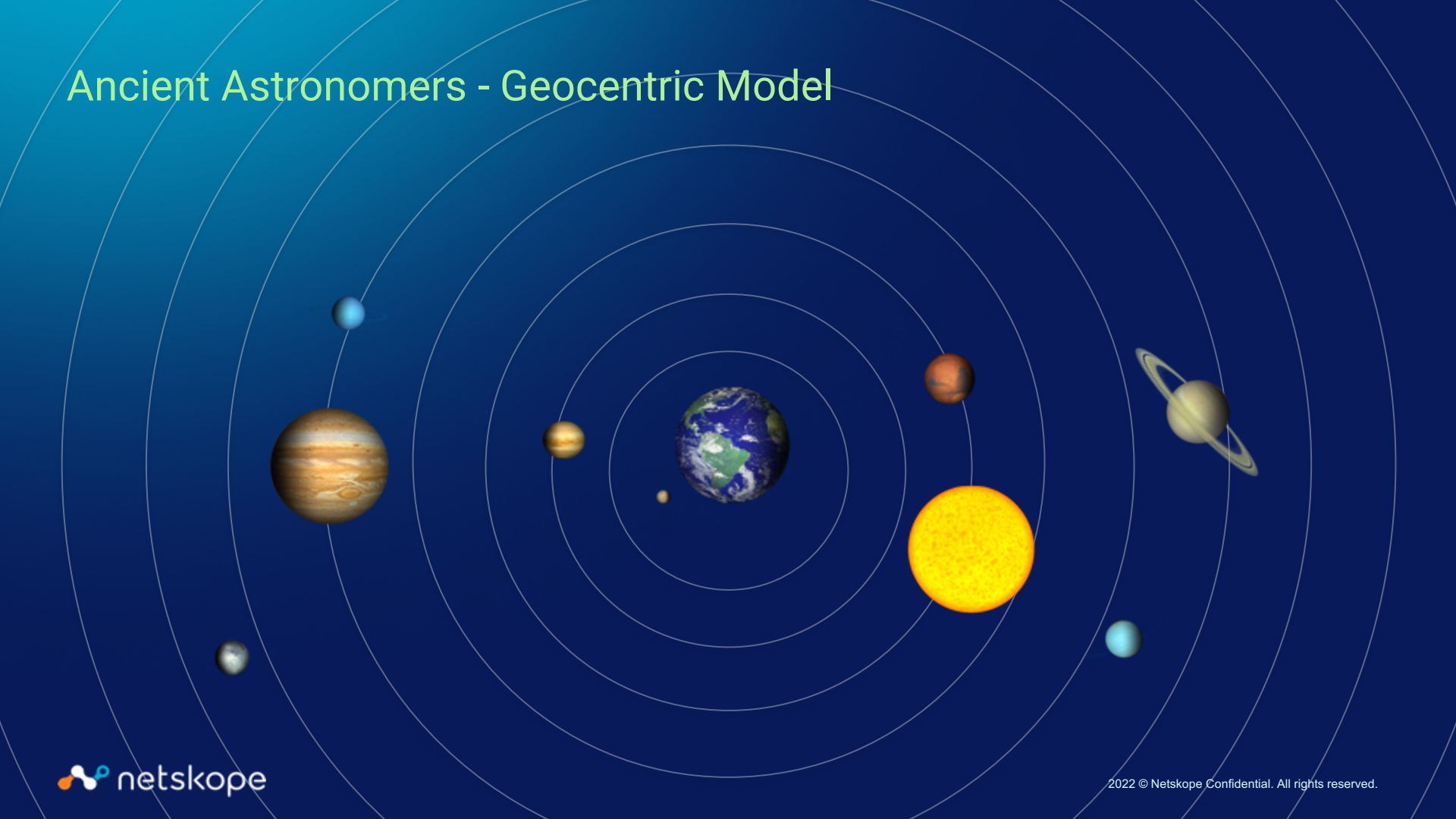
The Expanding Complexity of the Modern Enterprise

TODAY — HYBRID WORK

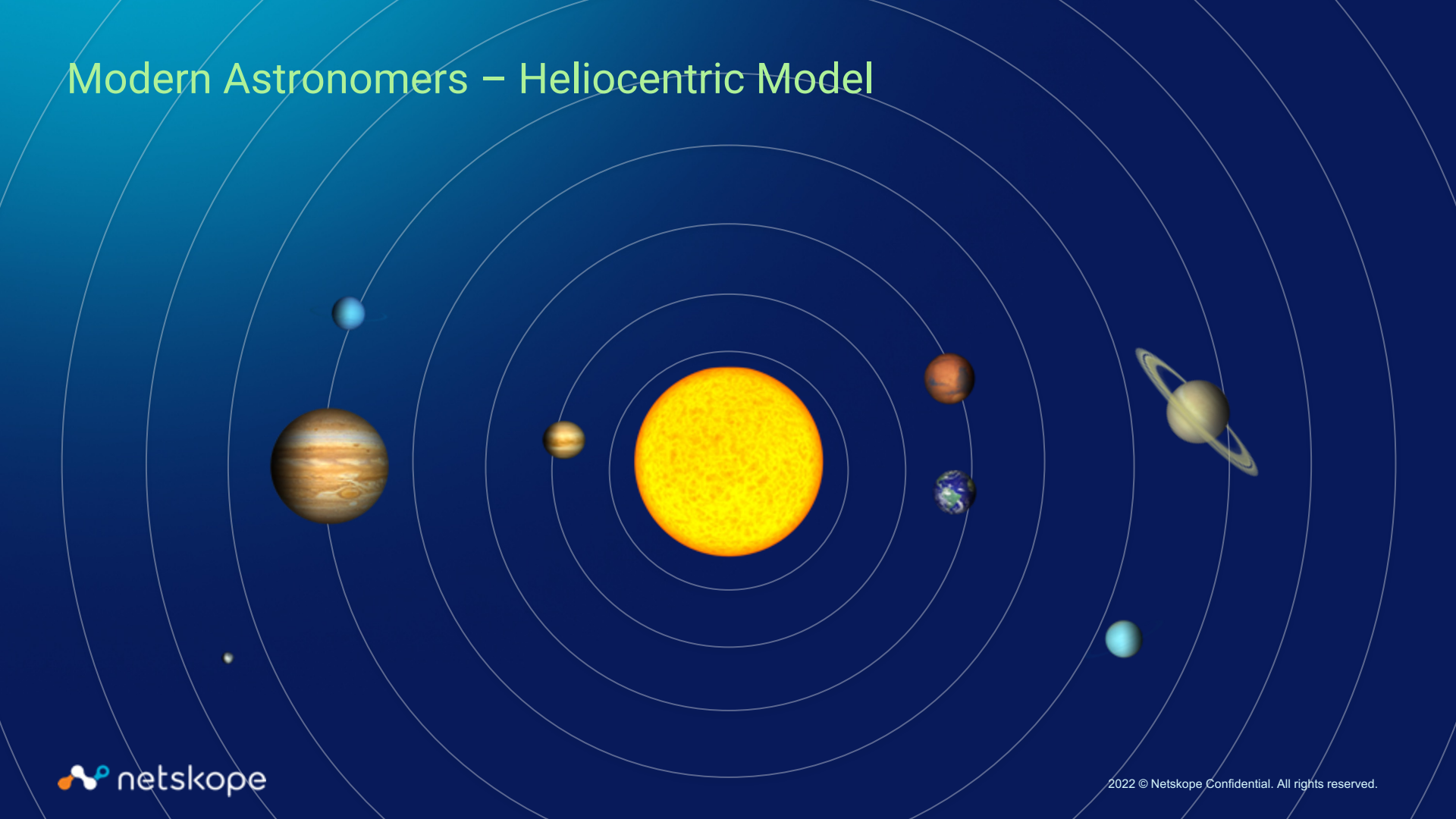
What else will tomorrow bring?

Journey to a Transformed, Adaptive, & Converged Architecture

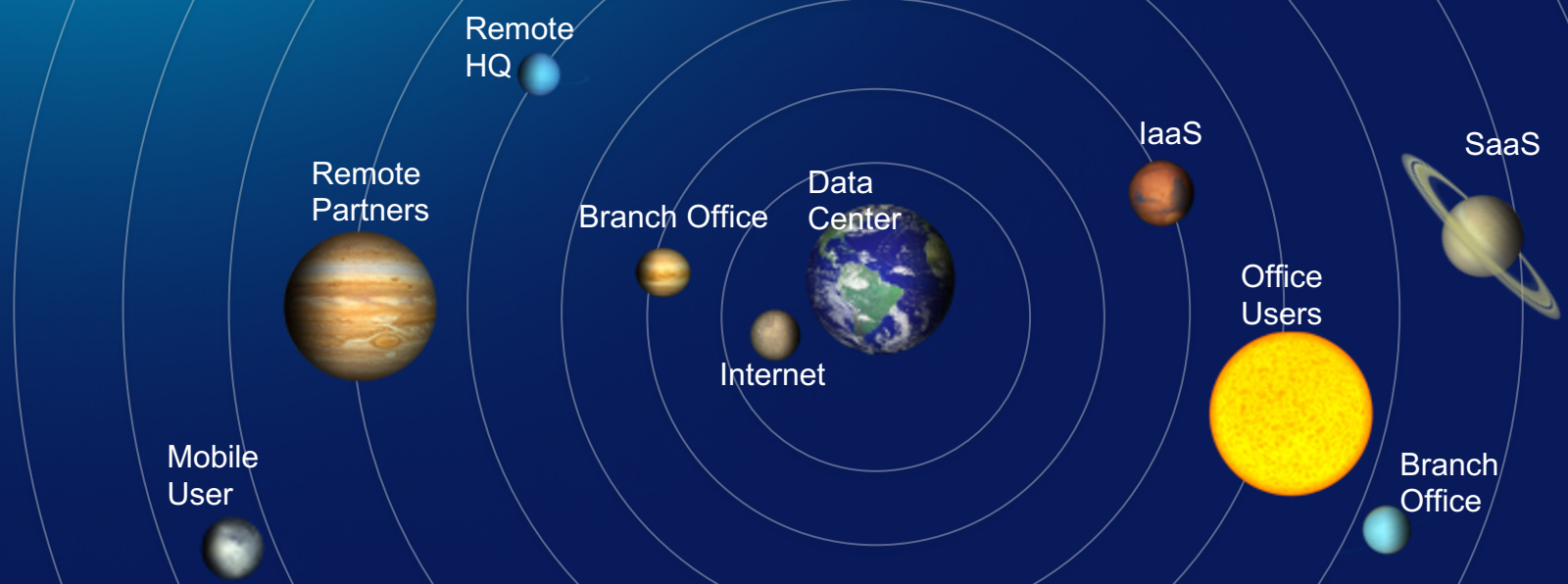
Ancient Astronomers - Geocentric Model



Modern Astronomers – Heliocentric Model

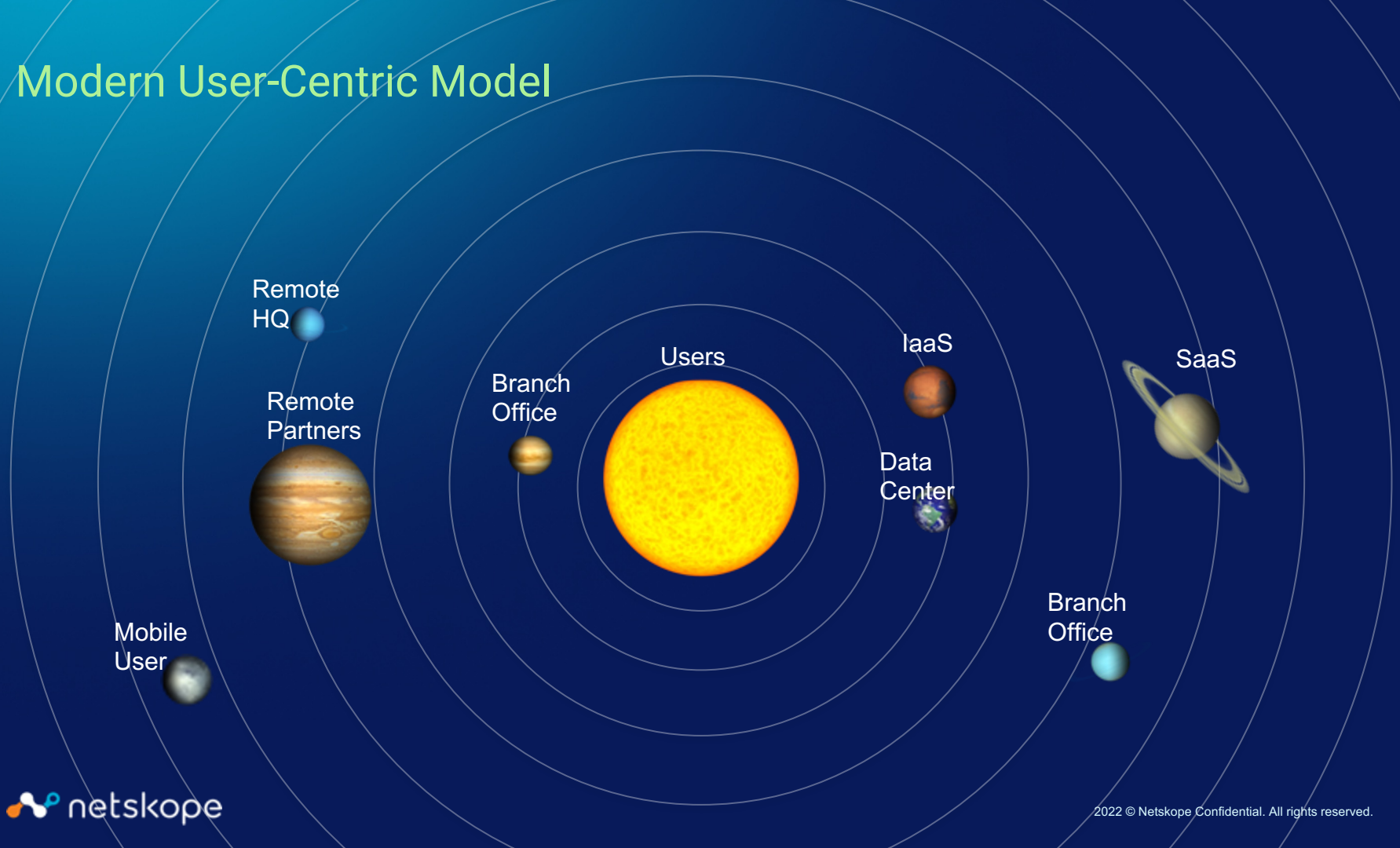


Ancient Data-Center Centric Model



netskope

Modern User-Centric Model



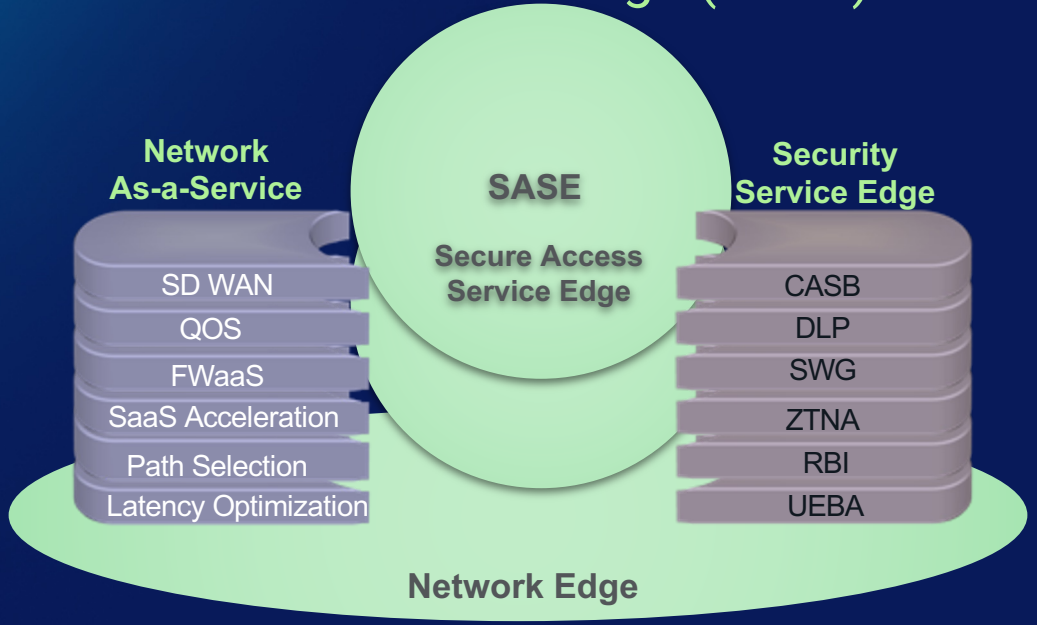
netskope

What If Your Network & Security Worked Together?

- A fast, global security infrastructure to support all your users, in any location, accessible 24x7x365
- Complete data-centric services delivered from the cloud, where and when needed…
- Coverage for all your applications, data and even IoT devices?
- Built for a world moving towards ”any-to-any” communications — a **mesh.**

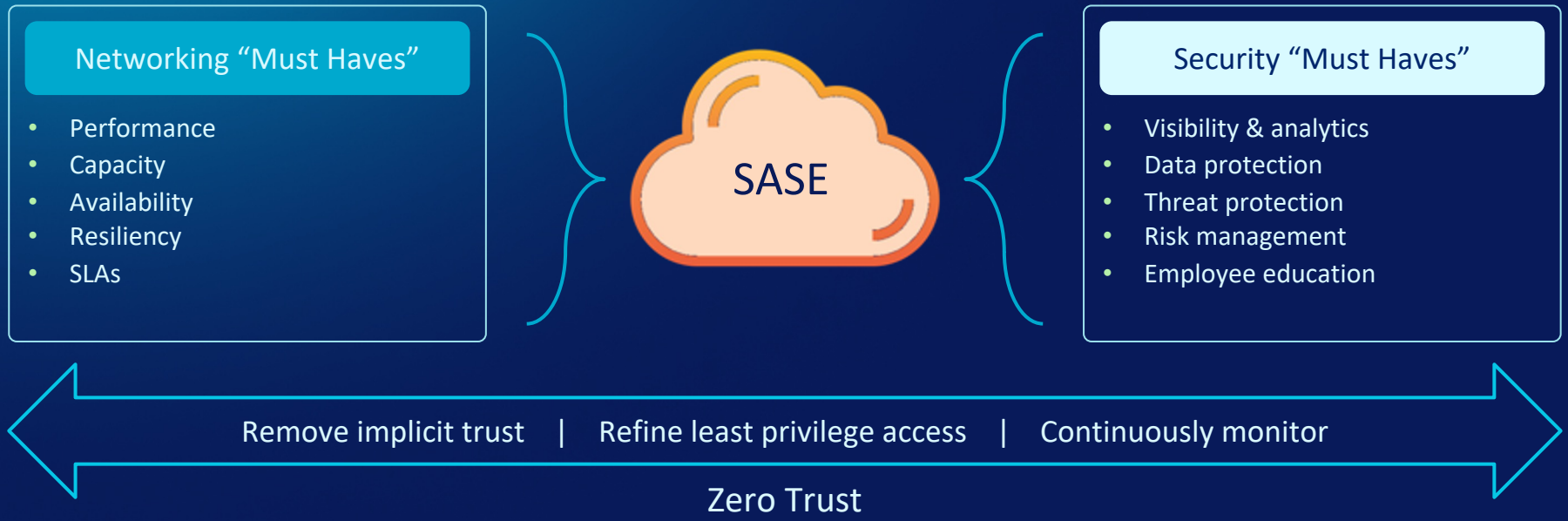
Modern User Centric Model = Secure Access Service Edge (SASE)

- SASE is the convergence of Security-as-a-Service and Network-as-a-Service
- SASE is becoming as disruptive to network and network security architectures as IaaS was to the data center
- Hub-and-Spoke networks are obsolete
- Digital business transformation will require adaptive edge architectures like Secure Access Service Edge



The Future of Network Security Is in the Cloud
Gartner ID G00441737, 8/30/2019

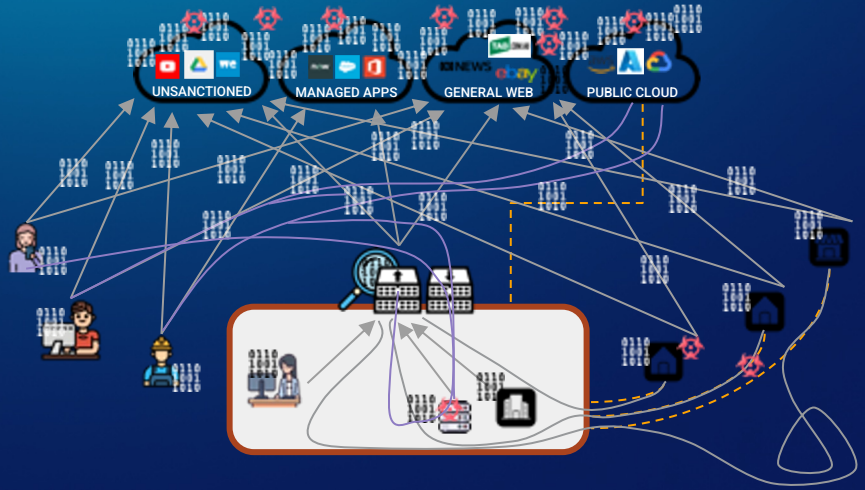
Convergence of Networking & Security Requirements




Controls
Settings
Sunroof
Driving
Cold Weather
Trips
Displays
E-Brake & Power Off
SUSPENSION
STEERING MODE
COMFORT
STANDARD
SPORT
TRACTION CONTROL
REGENERATIVE BRAKING
CREEP
DOORS & LOCKS
LIGHTS
FRONT TRUNK
LOCK
UNLOCK
CHARGE PORT
TRUNK
DOME
AMBIENT
DRL
FOG
HEADLIGHTS
OFF
PARKING
ON
AUTO

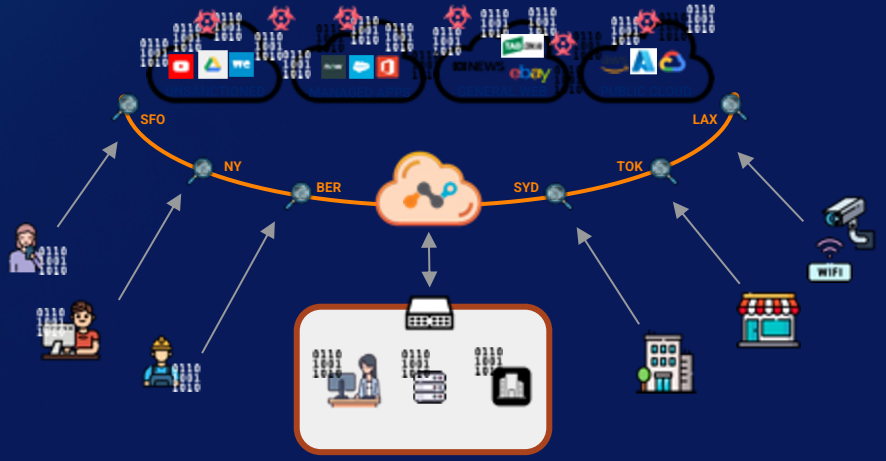
Today VS Tomorrow

Security needs to be decoupled from the corporate network; as per all of your users, apps, and data



Today

Users, Apps, and Data located **outside** the company perimeter
Security on-premises is broken - nothing is there anymore!



Tomorrow

Modern Architectures (SASE & SSE)
Security is *decoupled from the network* and moved **outside** the perimeter

netskope

SASE = Converged, Adaptable, Network & Security Platform

Network & Security Convergence

Secure Access Service Edge (SASE)

Hardware and Virtual SD-WAN
Endpoint SD-WAN
Wireless WAN (4G/5G)
Firewall and IDS/IPS
Multi-Cloud Networking
Intelligent IoT
Voice and Video Optimization
Quality of Experience (QoE)

WAN Edge Services

Security Service Edge (SSE)

Netskope **NewEdge** Private Cloud

Cloud Access Security Broker (CASB)
Secure Web Gateway (SWG)
Zero Trust Network Access (ZTNA)
Data Protection (DLP)
Cloud Firewall (CFW)
Remote Browser Isolation (RBI)
Digital Experience Mgmt. (DEM)
Posture Management (CSPM/SSPM)
genAI Protection (SkopeAI)

netskope

Rich Context For Adaptive Decision Making

Identity/Access
MFA, SSO, ZTNA
Step-up Authentication

Cloud Context
Web, SaaS, IaaS Traffic
Decodes Cloud Traffic
App, Instance, Activity

Threat Protection
Anti-malware, ML Analysis
Malicious Docs, Phishing
Sandbox, RBI, CFW, IPS

Data Protection/DLP
Inline & API for Un/Managed Apps
AI/ML Document/Image Classifiers
Web, SaaS, IaaS, Email, & Endpoint

Analytics Feedback Loop
Continuous Monitoring, Behaviors, Trends,
Unknowns, Closed Loop Policy Refinement

App Trust / 3rd Party Risk
58,000+ apps & services
Actionable in policies
Real-time Coaching

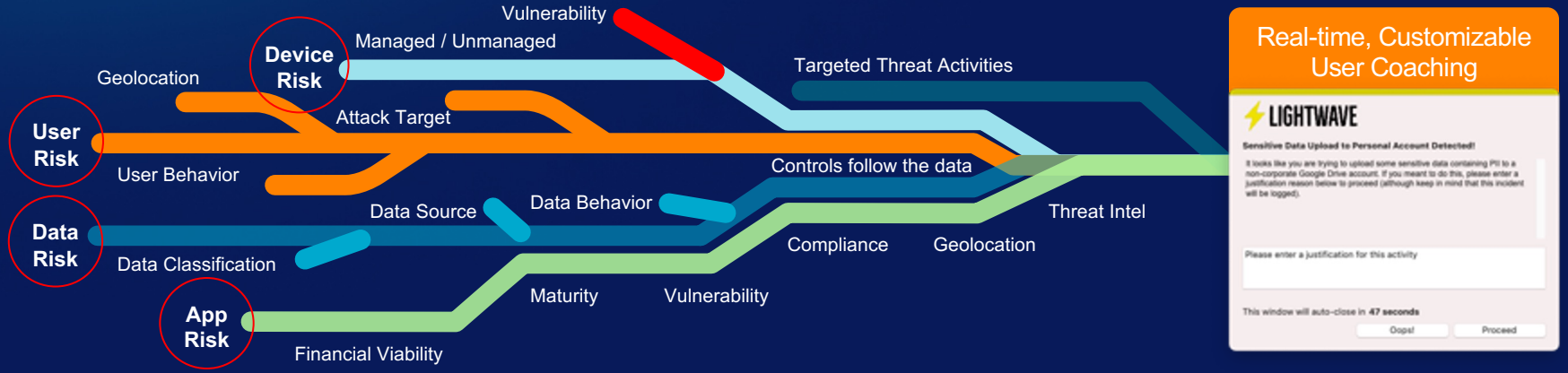
User Trust
Insiders, Compromise, Data Exfiltration
User confidence index scoring (UCI)
Actionable in policies

Device Trust
Posture Checks, SW/Config, Location
Un/Managed, Laptop, Mobile, IoT

Ecosystem Trusts
IOC Sharing, Automation/Workflow
Log Export, Risk Exchange

A Zero Trust Engine - Driven by Dynamic Observability

Identity	Device Risk	SaaS App	App Instance	App Risk	URL Category	Activity Controls	User Risk	Threat	Data Risk (DLP)	Policy Action
Pat Smith Accounting Logged in as psmith@gmail.com	Managed Personal/ BYOD	Google Drive Sanctioned Unsanctioned	Company Personal	93 Excellent rating (low risk) Breadth of 50K+ Apps	Cloud Storage 130+ categories	Upload Share Create Delete Move Download (120+)	↓863 Behavior Tracking (moderate risk) (UEBA)	Threat Intel AV Sandbox IPS ML CTE	GDPR AU Privacy Act Over 3000+ classifiers	Contextual: Allow Coach Block Encrypt Legal Hold Quarantine



netskope

Journey to Secure Access Service Edge (SASE)

	1	2	3	4	5
Digital Transformation	Heavy office use	Emergence of IaaS/PaaS/SaaS	Explosion of API & SaaS Apps	Cloud-first as operating model	Cloud-only as operating model
	Many data centers	Data center consolidation	Cloud Extension	Cloud migration	Mature Hybrid or Full Cloud
	Many branches, Heavy VPN use	Rise of mobile workforce	Hybrid Cloud & Edge Security	Migrate legacy to cloud-based security	Secure Access Service Edge (SASE)
Capability requirements	DDOS Protection, WOC, IDPS, Network DLP, FW, VPN	SSL Inspection, Cloud Discovery, WAF, Content Filtering, SWG, CDN	SD-WAN, CASB, Sandbox, Cloud Threat & Data Protection	Cloud SWG, Cloud UEBA, Public Cloud Security	Cloud Firewall, ZTNA, IoT/OT

netskope

Deriving Business Value With an Adaptive Architecture

High-Value Business Use Cases

Business Agility

Shadow IT Control

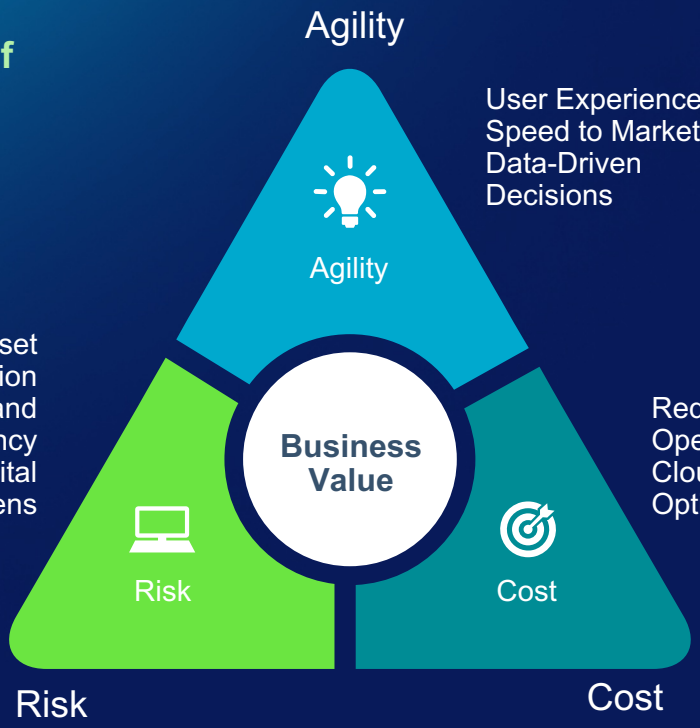
Public Cloud Governance

Reducing User Friction

Data Protection

Transformational Architectures - A Study of Business Value Benefits

Business value is optimized by finding the right balance of agility, risk and cost.



User Experience
Speed to Market
Data-Driven Decisions

19%

Increase in Overall Business Through Better Agility

Critical Asset Protection
Stability and Resiliency
Better Digital Citizens

Decrease in Security Risk

85%

Reduce TCO
Operational Efficiency
Cloud Spend Optimization

51%

Lower Costs for appliances, bandwidth and FTEs

Source: ESG; https://www.netskope.com/lp-esg-economic-validation

Comparative Analysis of Key Technology Consolidation Benefits

	Current State	Future State
High Level Description	**Current on-prem FW, VPN & SWG**	**Secure Access Service Edge (SASE)**
Vendors	Legacy Appliance & MPLS carrier reliance	Full SASE including SD-WAN
Product/Platform	3 Vendors with Multiple Products	1 Platform
“Pane of Glass”	Multiple Consoles + SIEM	1 Console + SIEM
Future Proof Solution for Cloud Needs	No	Yes
Visibility to Security Activity & Behavior	Low	High
Network Architecture & Performance	Hair-pinning to Data Center Sub-optimal performance	New Edge High-Performing Security Cloud
End User Experience	Sub-Optimal	High Performance
3 Year TCO (Network Bandwidth, Security, Resiliency)	$$$$$$	$$$

netskope

Key Outcomes

Improve user experience

The Internet becomes the new corporate network with improved response times

Increase performance with direct access and cloud peering

Securely enable the use of Cloud

Control access to 1000's of cloud apps and cloud infrastructure

Apply inline cloud and retrospective API control

Apply data protection

Apply context-based policies to all web, email and cloud traffic

Govern data use in the cloud. Know where data is, map data flows and

Apply threat protection

Identify and block new threats that emerge from the web, email, cloud and device

Block malware, phishing, drive-by, C&C etc

Manage cloud, third-party, & AI risks

Assess each cloud application/service and apply risk-based policies to block, educate and provision secure access

Reduce third-party risk

Reduce costs through transformation

Consolidate controls with a Zero-trust, Risk-based & Data-centric suite of controls

Reduce existing costs by up to 30%

netskope

Thank you!

Nate Smolenski

Head of Cyber Intelligence Strategy

nsmolenski@netskope.com

@NateSmo1 **nathansmolenski**

netskope