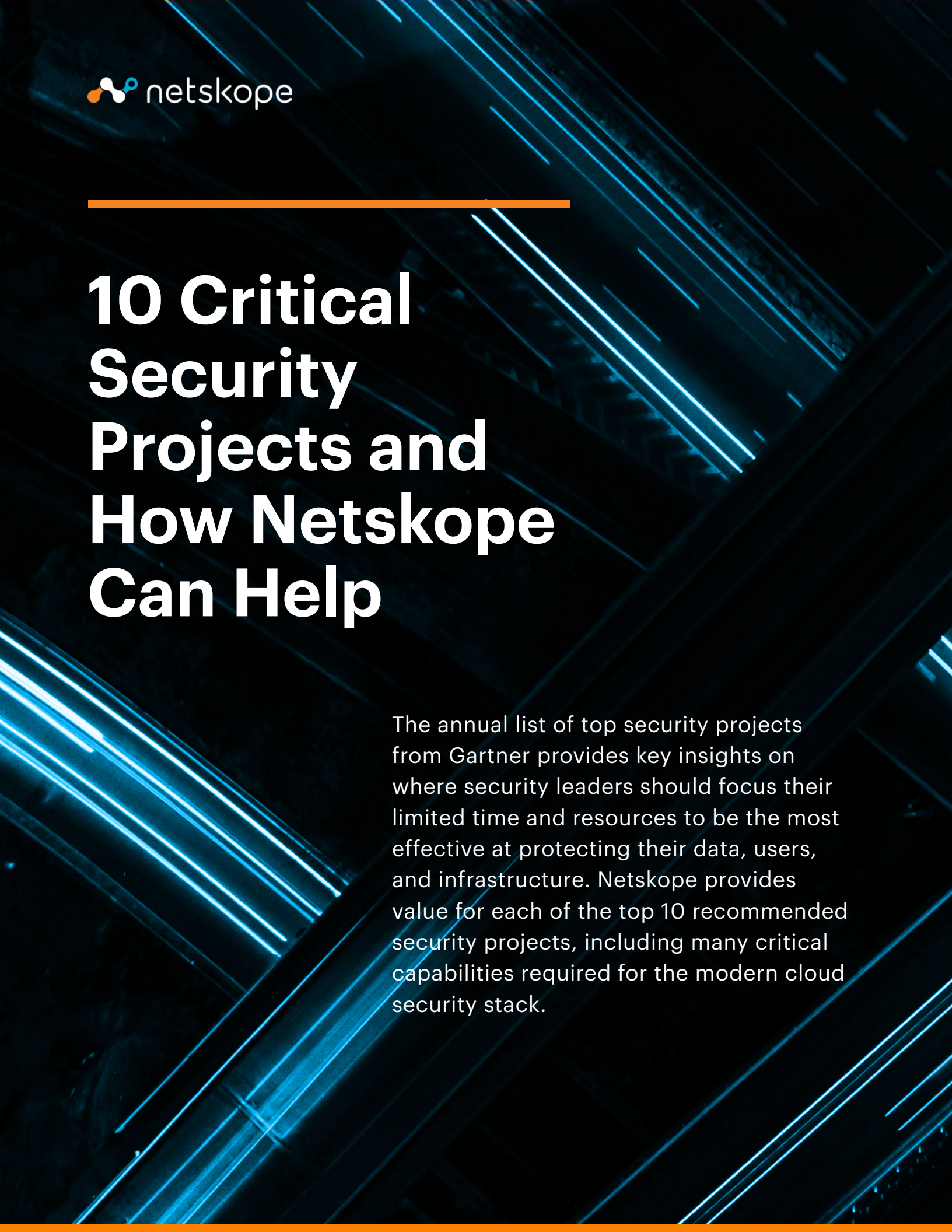


10 Critical Security Projects and How Netskope Can Help

The annual list of top security projects from Gartner provides key insights on where security leaders should focus their limited time and resources to be the most effective at protecting their data, users, and infrastructure. Netskope provides value for each of the top 10 recommended security projects, including many critical capabilities required for the modern cloud security stack.

#1

Securing your remote workforce

As Gartner notes, "Focus on business requirements and understand how users and groups access data and applications. Now that a few months have passed since the initial remote push, it's time for a needs assessment and review of what has changed to determine if access levels are correct and whether any security measures are actually impeding work."

Netskope provides a single-pass, cloud-native security access service edge (SASE) architecture to inspect web, managed SaaS, unmanaged SaaS, public cloud services, and custom app user traffic with data and threat protection alongside granular policy controls.

The average company has 2,415 apps, but less than 2% are typically managed by IT, making inline, Next-Gen Secure Web Gateway (SWG) with data context for 1,000s of apps and web a key component of SASE. Netskope also provides zero-trust network access (ZTNA) so remote users can access private apps and resources in public cloud services or private data centers.

#2

Risk-based vulnerability management

As Gartner notes, "Don't try to patch everything; focus on vulnerabilities that are actually exploitable. Go beyond a bulk assessment of threats and use threat intelligence, attacker activity and internal asset criticality to provide a better view of real organizational risk."

Netskope recognizes that digital transformation and the wide adoption of apps and cloud services shifts security into a shared partnership with apps and cloud services. Companies own securing their data and users and the inherent risks. Netskope provides a risk profile for over 20,000 apps using its Cloud Confidence IndexTM (CCI), enabling policy controls by app risk level with real-time coaching to advise users to safer alternatives, proceed or cancel with a warning, provide a justification, or blocking access.

Netskope also provides a User Confidence IndexTM (UCI) based on multiple methods of machine learning analyzing user activity and baselines to enable user risk profile policy controls. **Combined with Netskope's advanced data protection and cloud DLP, you can invoke risk-based controls by app, user, and data for your security transformation.**

#3

Extended detection and response (XDR)

As Gartner notes, "XDR is a unified security and incident response platform that collects and correlates data from multiple proprietary components. The platform-level integration occurs at the point of deployment rather than being added in later. This consolidates multiple security products into one and may help provide better overall security outcomes. Organizations should consider using this technology to simplify and streamline security."

Netskope provides over 500 attributes of rich cloud metadata of web and cloud user traffic for cloud detection and response (CDR) as part of a larger XDR program. Metadata can be exported to data lakes, SIEMs or centralized analytics platforms via a RESTful API.

Netskope Advanced Analytics also provides 16 predefined dashboards, support for any ad-hoc request or query, and an Explore tool with almost unlimited possibilities to analyze and view analytics. Netskope Behavior Analytics also provide UEBA use cases for data exfiltration, account compromise, and insider threats based on machine learning anomalies, plus a series of sequential anomaly rules with customization to detect bulk downloads, uploads, deletes, failed logins, proximity, risky countries, and many others including by app instance (e.g., business vs. personal).

#4

Cloud security posture management

As Gartner notes, "Organizations need to ensure common controls across IaaS and PaaS, as well as support automated assessment and remediation. Cloud applications are extremely dynamic and need an automated DevSecOps style of security. It can be challenging to secure the public cloud without a means to ensure policy uniformity across cloud security approaches."

Netskope provides Continuous Security Assessment (CSA) for AWS, Microsoft Azure, and Google Cloud Platform IaaS/PaaS public cloud service environments. **Netskope provides a single, consistent view of multiple cloud resources to maintain compliance while auditing and maintaining security configurations.** Netskope also provides IaaS Storage Scans for AWS S3 buckets and Azure Blobs to detect insider threats with real-time controls, and assess data-at-rest to identify sensitive data with cloud DLP and threat protection to find malware and malicious files.

#5

Simplify cloud access controls

As Gartner notes, "Cloud access controls typically are done through a CASB. They offer real-time enforcement through an in-line proxy that can provide policy enforcement and active blocking. CASBs also offer flexibility by, for example, starting out in monitoring mode to better ensure fidelity of traffic and understand security access."

Netskope understands CASB better than any other vendor. One side, CASB API-mode, covers managed apps and data-at-rest, which is likely the majority of your data, but less than 2% of the apps and cloud services your company utilizes. The other side is inline CASB for 1,000s of unmanaged apps, where data is obscured in motion from legacy web gateways. For a single-pass solution, Netskope has united secure web gateway (SWG) and inline CASB into a Next Gen SWG solution for web, managed SaaS, unmanaged SaaS, public cloud services, and custom app user traffic analysis for data and threat protection with the data context required for SASE architecture. Netskope simplifies cloud access using one cloud platform, one service, one console, one policy engine, and one client for remote users, or IPsec/GRE tunnels for offices, plus the option of Zero Trust Network Access (ZTNA) fully integrated.

#6 DMARC

As Gartner notes, "Organizations use email as the single source of verification, and users struggle to determine real messages from fakes. DMARC, or domain-based message authentication, reporting and conformance, is an email authentication policy. DMARC is not a total solution for email security and should be one piece of a holistic security approach. However, it can offer an additional layer of trust and verification with the sender's domain. DMARC can help domain spoofing but will not address all email security issues."

Netskope researches and understands cloud enabled threats, including cloud phishing. SaaS apps provide trusted domains, valid certificates, and in some cases may bypass inline defenses by design or DNS reputation checks. Cloud phishing common modus operandi begins with a personal webmail with a link to cloud storage, often OneDrive, Box, or G-Drive where the file is opened to expose a form requesting login credentials for Microsoft Office 365 as the most impersonated brand in phishing attacks.

These fake logins compromise credentials of company and personal app instances for users and evade endpoint defenses, plus legacy web and email defenses. Netskope protects by knowing approved app instances from rogue ones, when credentials are put into forms via cloud DLP, activities, and assessing any downloads for threats having access to app content and context.

Any cloud-enabled threats exposed provide IOCs that the Netskope Cloud Threat Exchange (CTE) can automatically share with other defenses including endpoints, firewalls, SIEMs, SOAR, and IR solutions within a customer's security stack. CTE is also bi-directional to share IOCs including file hashes and malicious URLs from other defenses with a customer's environment.

#7

Password-less authentication

As Gartner notes, "While employees may not think twice about using the same password for their work computer as they do for the personal email, it can cause major security headaches. Password-less authentication, which can functionally work in a few different ways, offers a better solution for security. The goal should be to increase trust and improve the user experience."

Netskope can federate multi-factor authentication (MFA) from popular identity providers (e.g. Okta) to over 30,000 apps and cloud services where most are not managed by IT and likely use common passwords and weak authentication.

Digital transformation is accelerating projects, enabling remote work, reducing expenses, and exposing risk where 98% of cloud services and apps are unmanaged. Netskope provides forward and reverse proxies within its Next Gen SWG solution connecting into identity services for managed devices via forward proxy, and for unmanaged devices and BYOD via reverse proxy. **Protect your users data, and apps with strong authentication and risk-based policy controls to step-up authentication when desired.**

#8

Data classification and protection

As Gartner notes, "All data is not the same. A one-size-fits-all security approach will create areas of too much security and others of too little, increasing the risk for the organization. Start with policies and definitions to get the process right before beginning to layer in the security technologies."

Netskope provides data protection policies alongside advanced data loss prevention (DLP) rules and policies for data-in-motion and data-at-rest. The majority of users and data are now in the cloud as apps transform into SaaS or custom cloud apps outside of data centers. Netskope understands unintentional and unapproved data movement that crosses boundaries between apps instances, app to app, app suites, and app categories. Data protection policies should come first to phase out high risk apps, reduce high risk user activities with real-time coaching, and understand the content and context so sensitive data does download to unmanaged devices or undesired third parties. Then, advanced DLP can focus on the remaining use cases desired for compliance regulations and data security.

#9

Workforce competencies assessment

As Gartner notes, "Install the right people with the right skills in the right roles. It's critical but challenging to combine hard technical skills with softer leadership expertise. There are no perfect candidates, but you can identify five or six must-have competencies for each project. Assess competencies in a range of ways, including cyber-ranging and cyber simulations and softer skill assessments."

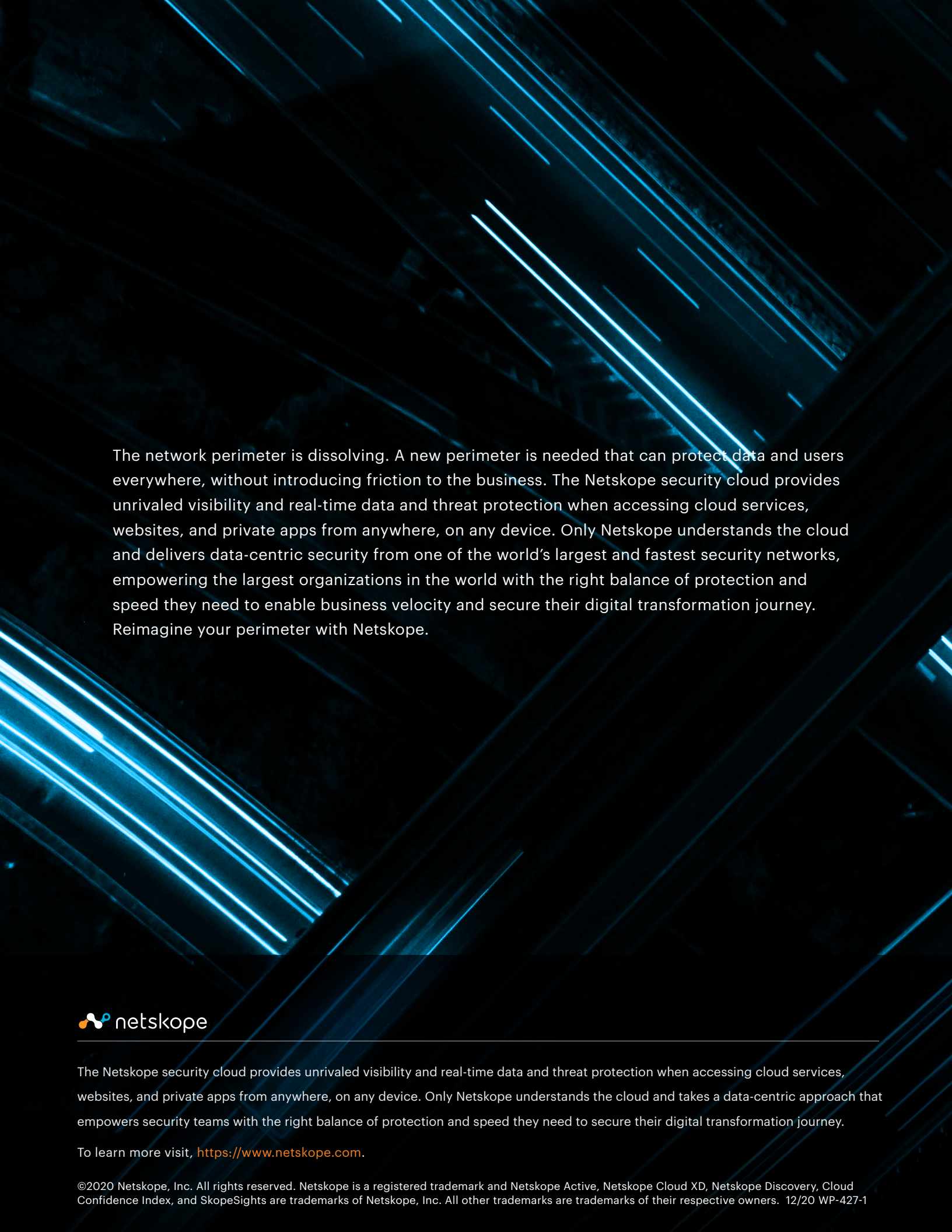
On-premise appliance-based security engineer skills are transforming into cloud security engineer skills, and this transformation also includes networking engineers evolving into cloud infrastructure engineers. **Netskope provides training and certifications to transform your team for these new roles and competencies.** We offer Cloud Security Workshops for a hands-on experience, and Prove It sessions where we demonstrate seven challenges for Next Gen SWG solutions. Your analysts with business intelligence (BI) skills can assess our new Netskope Advanced Analytics using 16 predefined dashboards and unlimited explore capabilities for over 500 metadata attributes—cloud visibility like you have never seen before.

#10

Automating security risk assessments

As Gartner notes, "This is one way to help security teams understand risks related to security operations, new projects or program-level risk. Risk assessment tends to be either skipped entirely or done on a limited basis. These assessments will allow for limited risk automation and visibility into where risk gaps exist."

Netskope Advanced Analytics includes an automated Cloud Risk Assessment (CRA) to analyze all your apps and cloud services utilized, app risk profiles, Sankey charts showing data flows from company app instances to personal ones, plus analysis of data risks and threats. Netskope Advanced Analytics also includes a CxO dashboard for key performance indicators of your security program, a data risk security dashboard, and threats dashboard. **While most security risk assessments are external, one-time scorecards, Netskope provides an internal continuous risk assessment of your users, apps, and data.**



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

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.

To learn more visit, https://www.netskope.com.