netskope

Digital Transformation Needs a More Perfect Union

The Business Case for Stronger Networking-Security Team Collaboration in the SASE Era

In most enterprises, it's no secret that network and security teams have conflict; some are mis-aligned on priorities, others are fully at-odds. In a more siloed era, where each team had a strategy, a resource pool, and a set of priorities it controlled, this conflict was seen as a cost of doing business. But this is the era of Secure Access Service Edge (SASE) architecture, where networking and security teams and the products and services they manage converge into a shared set of priorities tied to business objectives. In this landscape, network and security teams must not only align, but also collaborate to ensure an increasingly remote workforce can safely access data from anywhere, using cloud applications, and have a good experience doing it, with no degradation in network connectivity.

Easier said than done. Network-security team collaboration isn't just a "kumbaya" moment, and the reality is that its absence is costing teams real money and real time, and, from an executive viewpoint, limiting the organization's ability to successfully deliver on the digital transformation projects that will fuel business growth and keep them competitive.

New research from Censuswide, commissioned by Netskope, underscores the very real tensions between network and security teams, and how CIOs, networking leads, and security leads view the current state of the union—or lack thereof.

This document will outline several of the key findings and point a way forward for teams that seek better collaboration as they strive for the benefits of a secure, cloud-first SASE architecture.

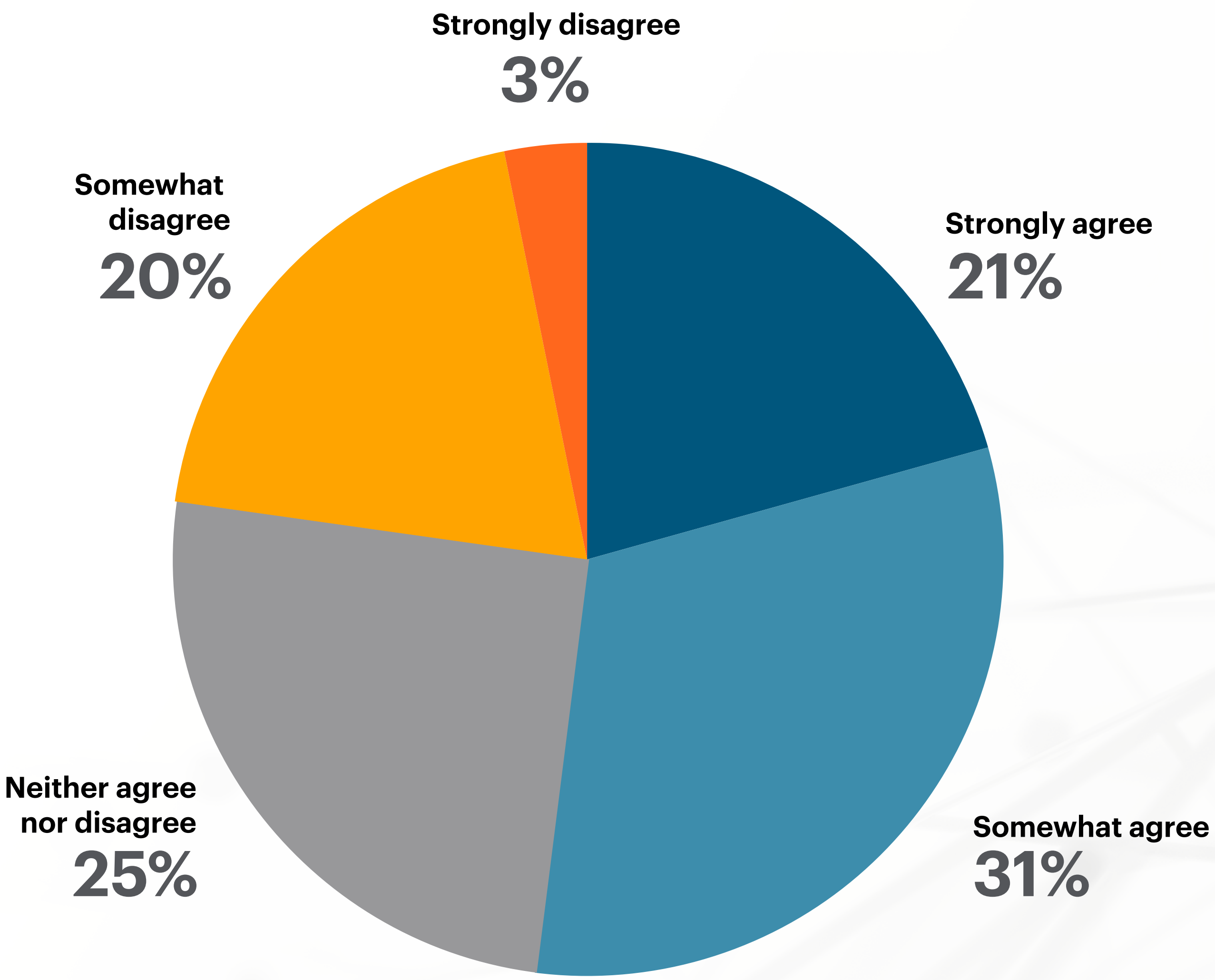
50% of CIOs believe that a lack of collaboration between specialist teams stops their organization from realizing the benefits of digital transformation.

About $6.8 trillion will be spent by enterprises on digital transformation (Dx) projects through 2023*—a number expected to increase over the successive three years. The benefits of digital transformation, even loosely defined, ensure that businesses will stay agile, competitive, and cloud-first, turning functional IT and security cost centers into true business enablers. 87% of Censuswide survey respondents are either actively working on a Dx project or have just completed one.

However, the ongoing schism between network and security professionals points to challenges that inhibit the timely success of Dx projects. This is known to CIOs often in charge of setting Dx priorities with the buy-in from executive leadership.

*IDC FutureScape: Worldwide Digital Transformation 2021

A LACK OF COLLABORATION BETWEEN SPECIALIST TEAMS STOPS US FROM REALIZING THE BENEFITS OF DIGITAL TRANSFORMATION



The Key Thing

Individual Dx projects may be able to proceed without the necessary collaboration between network and security teams. But the same won't be true for substantial architectural shifts where that collaboration is required for success—such as the move toward SASE to right-fit organizations for secure cloud adoption.

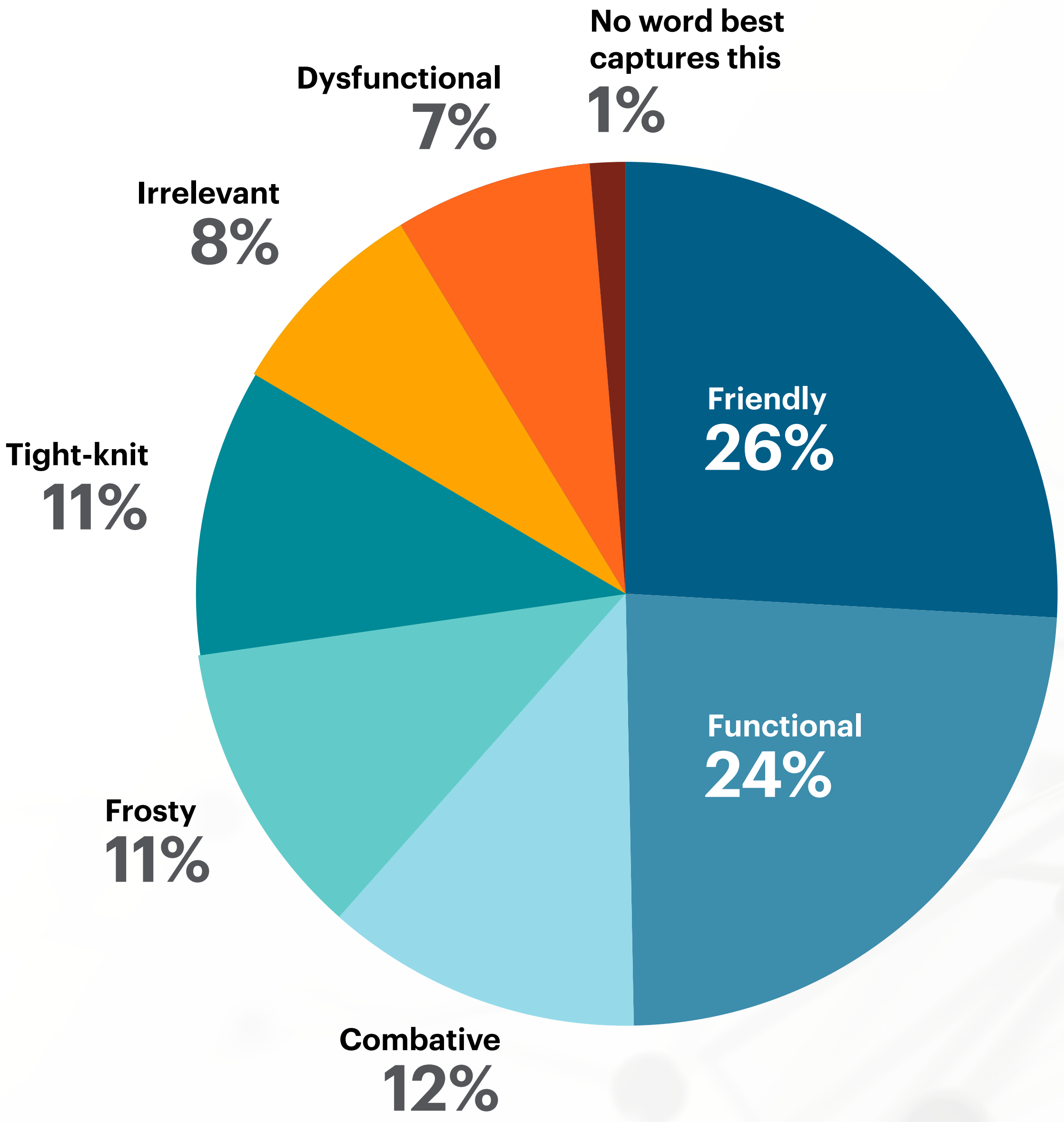
Nearly half of network and security professionals describe the relationship between the two teams in strongly negative terms such as ‘combative’, ‘dysfunctional’, ‘frosty’ or ‘irrelevant’.

Did you know that 45% network and security professionals have never even met a member of the other team? That may seem far fetched considering nearly half (49%) sit within the same larger group and report to the same leaders, but those same respondents clearly cite that “the security and networking teams don’t really work together much.”

The problem may be one of leadership and prioritization. Both network and security professional respondents to the Censuswide data selected the same three top priorities for 2021:

- Supporting increased productivity for the organization as a whole
- Expansion of infrastructure to support business growth
- Increasing visibility and control

WHAT WORD, IF ANY, BEST CAPTURES FOR YOU THE RELATIONSHIP BETWEEN YOUR SECURITY AND NETWORKING TEAMS:



The Key Thing

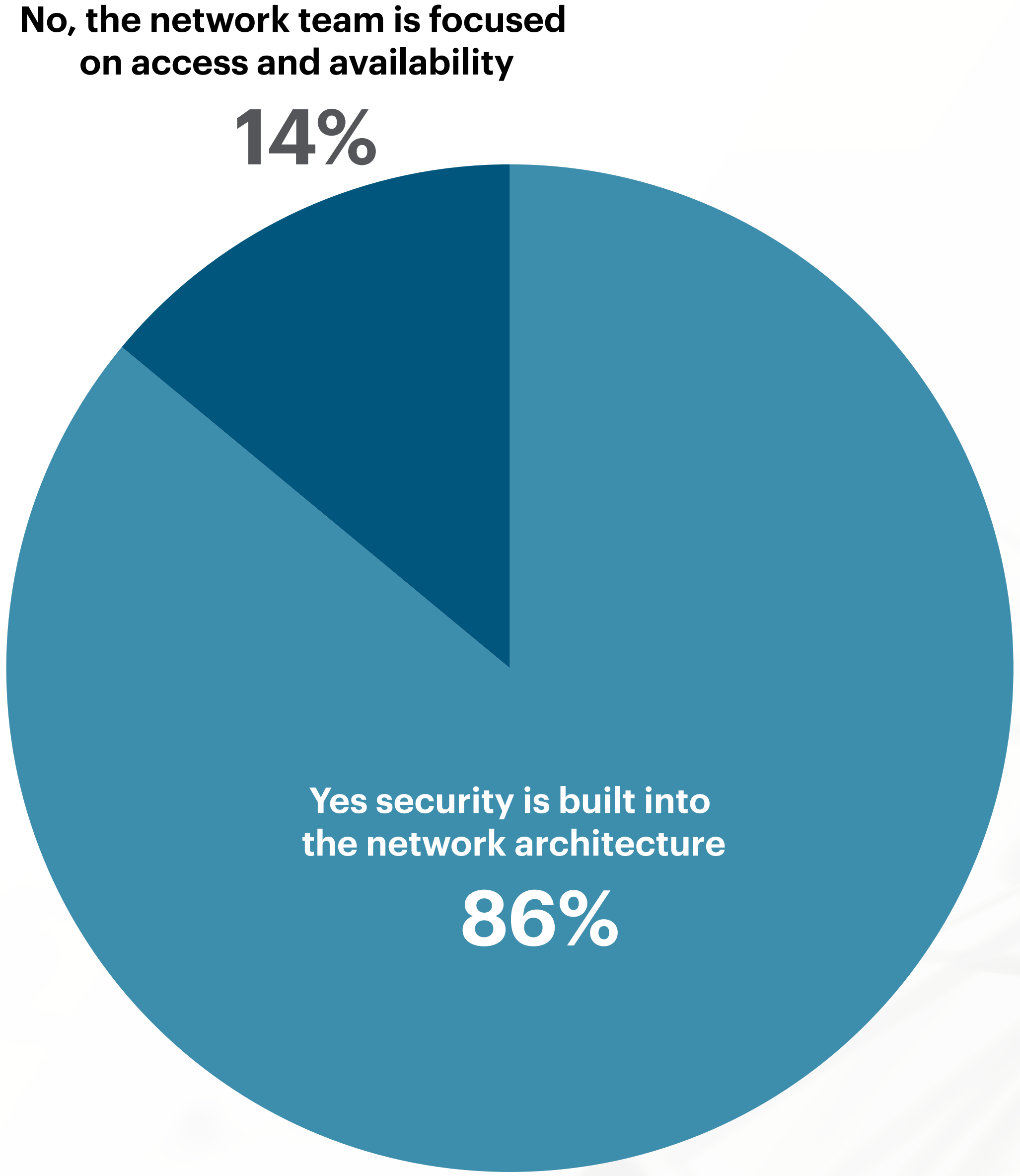
Network and security teams are often far apart—and their relationships downright unproductive–despite being situated in the same organizations of the company, working for the same senior leaders, and identifying the same business-level priorities that highlight the value they can bring.

86% of network and security respondents stated that security is part of the network team's responsibility

Security and networking were once the same organization within a company, and despite appearances, have remained inextricably linked even as each function grew and expanded. Consider that the role of security is to find problems (often in network infrastructure) and orchestrate how they're fixed, and that part of the role of networking is to maintain uptime and connectivity—deploying the tools and techniques the security team helps to select or at least consult on.

Teams aren't ideologically opposed to collaboration, the research found. A majority of security and network groups stated that security is part of the network team's responsibility, and built into the network architecture. More than half also shared that Dx projects have a sponsor within both networking and security teams.

IS SECURITY PART OF THE NETWORK TEAM'S RESPONSIBILITY?



The Key Thing

The foundation is already in place for better collaboration. It's on leadership to effectively activate it.

60% of enterprises will have a SASE strategy by 2025*

Whether it's called SASE, which is the Gartner term first coined in 2019, or something else, the evolution in IT and security that the cloud era portends is fast coming. Much like the term cloud 10 years ago or the concept of Zero Trust principles five years ago, SASE is the subject of lots of noise and lots of trendy vendor marketing—without much step-by-step, "here's how this is done" practical advice.

But as people, processes, and technology all evolve toward a SASE future, any definition of success depends on networking-security convergence.

The Key Thing

The right path to SASE has been hotly debated ever since Gartner coined the term, and will be for the foreseeable future. But what isn't in dispute is the role of network-security convergence in a successful SASE architecture—nor that SASE architecture is the wave of the future.

*Gartner, "2021 Strategic Roadmap for SASE Convergence," published March 25, 2021

What You Can Do Today

Change management is difficult in "normal" times, and made more so by significant macro trends in technology (cloud adoption, SASE architecture) and once-in-a-generation crises with significant business and interpersonal effects, such as the COVID-19 pandemic. The following are process suggestions from Fortune 500 CIOs successfully tackling the problem of network-security collaboration, effectively driving Dx projects, and setting a course for a SASE future in their teams.

Embrace What DevOps Has Taught Us

DevOps (and its variations, including DevSecOps) became a movement because it acknowledges inherent conflicts and points of misalignment between development teams and operational teams in large, layered organizations. Much DevOps-inspired thinking and tactics, from the creation of cross functional project teams to the use of kanban boards and agile processes, can be easily transferred to network-security collaboration or any spot in the organization that would benefit from stronger cross-functional teamwork.

Consider the SNOC

The idea of a combined SOC and NOC—known in some circles as a security and network operations center (SNOC)—is catching on as more teams realize that the business-imperative goal of secure, robust, resilient corporate network infrastructure is common to each. A SNOC blends critical functions under that commonality, and further relies on next-generation technologies such as AI/ML to augment human analysis and ensure nothing slips below anyone's radar.

Focus On a (Short) List of Business-Critical Metrics That Transcend Network-Security Boundaries

How best would you communicate to executive leadership, particularly the non-technical C-suite, that networking and security are working in harmony to maintain infrastructure and support business objectives? That kind of reporting wouldn't be the time for anecdotal highlights—or even "kumbaya"!

Exact metrics will depend on the nature of the business and the maturity of the teams, but CIOs recommend the following for consideration:

- Improved Mean Time to Respond (MTTR)
- Improved Mean Time to Failure (MTTF) or Mean Time Between Failures (MTBF)
- Increased Customer Satisfaction (internal or external customers—measured by robust survey)

For More Information

Visit netskope.com

> “Netskope’s progress in the SASE framework is the farthest along than any other vendor in the Magic Quadrant.”
>
> - Gartner, Magic Quadrant for Cloud Access Security Brokers, Nov 2020

Netskope, the SASE leader, safely and quickly connects users directly to the internet, any application, and their infrastructure from any device, on or off the network. With CASB, SWG, and ZTNA built natively in a single platform, Netskope is fast everywhere, data centric, and cloud smart, all while enabling good digital citizenship and providing a lower total-cost-of-ownership.

netskope.com

netskope