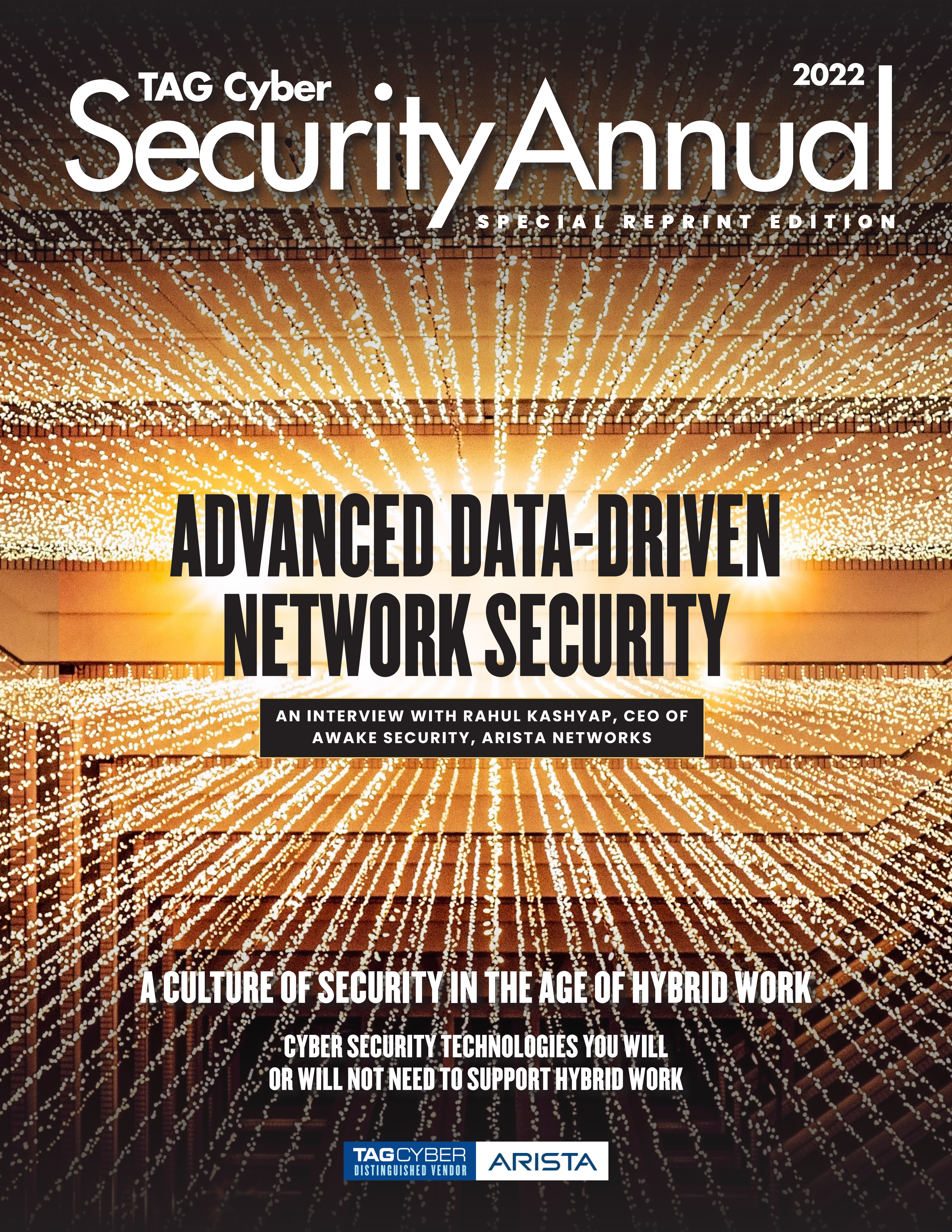


TAG Cyber Security Annual 2022

SPECIAL REPRINT EDITION

ADVANCED DATA-DRIVEN NETWORK SECURITY

AN INTERVIEW WITH RAHUL KASHYAP, CEO OF AWAKE SECURITY, ARISTA NETWORKS

A CULTURE OF SECURITY IN THE AGE OF HYBRID WORK

CYBER SECURITY TECHNOLOGIES YOU WILL OR WILL NOT NEED TO SUPPORT HYBRID WORK

TAG CYBER DISTINGUISHED VENDOR

ARISTA

TAG CYBER 2022 DISTINGUISHED VENDOR

The need to reduce cyber risk has never been greater, and Arista Networks has demonstrated excellence in this regard. The TAG Cyber analysts have selected Arista Networks as a 2021 Distinguished Vendor, and such award is based on merit. Enterprise teams using Arista Networks's platforms will experience world-class risk reduction. Nothing is more important in enterprise security today.

The Editors,
TAG Cyber Security Annual
www.tag-cyber.com

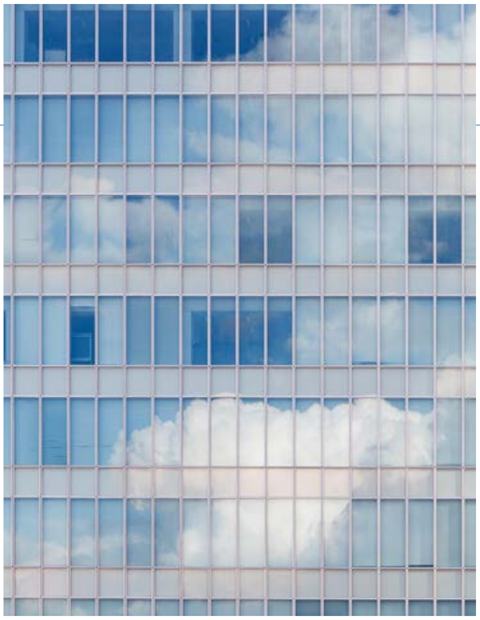
REPRINTED FROM THE TAG CYBER SECURITY ANNUAL

AN INTERVIEW WITH RAHUL KASHYAP,
CEO OF AWAKE SECURITY,
ARISTA NETWORKS

ADVANCED DATA-DRIVEN NETWORK SECURITY

The technical and operational interaction between networking and security has always been close, and experts in each area will attest to the need to cooperate when dealing with cyber threats. Founded in 2004 and headquartered in Santa Clara, California, Arista is a large public company that fully understands this interaction and has championed the delivery of world-class products in each area.

Arista specifically addresses important new issues such as cloud-grade routing, programmable switching, converged infrastructure networking, telemetry and analytics, IP storage and big data, media and entertainment support, electronic trading, and cognitive cloud computing. To this portfolio, Arista has developed a strong security solution, spearheaded by its acquisition of Awake Security.



TAG Cyber: Tell us about Arista. And what acquisitions have you been involved with recently?

ARISTA: We are an industry leader in data-driven cloud networking solutions for large data center and campus environments. Many of the largest cloud service providers, financial services institutions, retailers, and technology providers rely on Arista's infrastructure to provide reliable and high-performance network services. Arista invests heavily in improving business outcomes for our customers through organic innovations and acquisitions of best-of-breed solution providers. Our two most recent acquisitions were Awake Security, an AI-driven network detection and response provider, and Big Switch Networks, which delivers pervasive and programmable network observability.

TAG Cyber: What are some emerging trends you see in network security?

ARISTA: We see two technology trends and one business trend. Starting with the business trend, we see more and more customers that look at security as an adjective rather than a noun. They are expecting a network that, in a sense, is self-securing rather than bolting on a myriad of "security solutions" on top of the network infrastructure. In other words, customers want to see the underlying switches, routers, etc. as part of the security defenses.

On the technology front, with the rapid pace of the ongoing digital transformation, we see customers struggling to understand and secure all the unmanaged devices on the network. In many cases, north of 50 percent of devices on the network fall in the unmanaged bucket, which means no EDR agents deployed, no logs being pulled off the device, etc. These devices are everything from BYO devices to DevOps and shadow IT, as well as IoT. Of course, cloud workloads and SaaS applications also contribute to this lack of visibility. All of this contributes to a significantly larger attack surface that we already see being exploited by nation state-sponsored ransomware gangs and other threat actors.

Finally, we see a continuous increase in the amount of encrypted traffic on the network, even in east-west corridors. Traditional network security solutions rely on visibility into the clear text payload, typically achieved by TLS interception. Unfortunately, given the privacy implications and some of the changes with protocols like TLS 1.3, decryption is simply not a viable option.

No discussion on threats can go very far without talking about ransomware. We are seeing trends like the use of a double tap strategy where data is both encrypted and exfiltrated.

Therefore, we see a trend toward encrypted traffic analysis. The objective is to use data science methods to get smarter about threats buried within the encrypted traffic without ever performing decryption.

TAG Cyber: Do most enterprise teams understand the importance of software-driven network solutions?

ARISTA: I believe so. In fact, if anything, the last 18 months of "work from anywhere" have almost forced most organizations to adopt a software-driven approach. The adoption of the cloud and SaaS applications has also accelerated this trend.

Interestingly, today we find that our customers are moving one step further on this continuum by asking for a data-driven approach: What is the ground-truth data from the network telling us about the threats in the environment? Is there risky insider behavior? Are there basic hygiene issues like weak passwords that might be driving risk? They are also looking for this approach to come with broad programmability. This applies to real-time, network-state streaming, a programmable monitoring fabric, and programmable threat detection and response. For instance, we see organizations that want to evolve from traditional black box "AI-based" solutions to a system where the detection models are open and can be tweaked or adapted using a simple set of tools without the need for data scientists on staff.

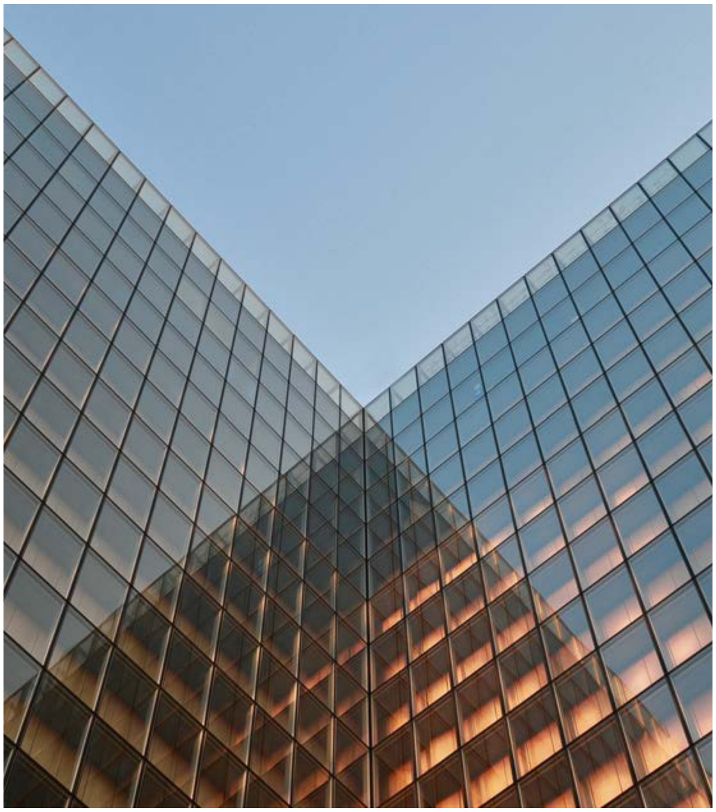
TAG Cyber: Do you have any predictions about emerging cyber threats to network infrastructure?

ARISTA: Well, clearly no discussion on threats can go very far without talking about ransomware. We are seeing trends like the use of a double tap strategy where data is both encrypted and exfiltrated. This way, even if the target restores from backups, the threat actor will simply threaten to publicly release the data. The prediction here is that customers are going to get a lot more focused on detecting the early warning signs in order to intercept and remediate before the encryption event.

We see more threats specifically looking to exploit IoT devices and other unmanaged infrastructure. Along similar lines, the lack of comprehensive visibility into the network is leading to unpatched infrastructure, from firewalls and VPN concentrators to remote access solutions. The point is that hygiene around passwords and patches is becoming "cool" again.

We also believe we will see more "hybrid" attacks—attacks that move between a customer's on-premise and cloud-based infrastructure. For instance, we recently saw a targeted attack that used malicious browser extensions to steal the password from the organization's cloud administrator. Those credentials were then used to login to the cloud console and compromise workloads.

Finally, we believe the mantra "every threat is an insider threat" will continue to be proven right. This is not to say that behind every threat is a malicious insider. Instead, we are seeing "innovative" ways through which external attackers are gaining legitimate insider access—whether through bribery, extortion, or tricking an unsuspecting victim.



A CULTURE OF SECURITY IN THE AGE OF HYBRID WORK

OUR SURVEY SHOWS COMPANIES HAVE REMOTE AND HYBRID WORK PLANS, BUT THEY ALSO HAVE REASON FOR CONCERN

KATIE TEITLER

A mere two years ago, the idea of “hybrid work,” that is, working partly in a dedicated corporate office environment and partly from various and fluctuating remote locations, was the privilege of a select few. While remote work had more than taken hold in the corporate world by that same time period, hybrid work wasn’t yet part of the corporate lexicon.

When COVID-19 hit in full force in the United States, starting in March 2020, offices were shuttered and workers were forced into their living rooms, dining rooms, basements, and even bedrooms as their new work environments. Coffee shops weren’t open for a change of scenery. Business travel had ground to a halt. Businesses were operating at near 100 percent remote capacity wherever and whenever possible.

As signs of improvement arose, especially following the release of COVID-19 vaccines, some office workers tentatively started returning to office environments for at least part-time in-office work. Today, in Q4 2021, as we weather the roller coaster of COVID cases in the U.S., 61 percent of organizations report that their workforces continue to function remotely, according to a recent survey of 258 IT and security professionals conducted by TAG Cyber. (Figure 1)

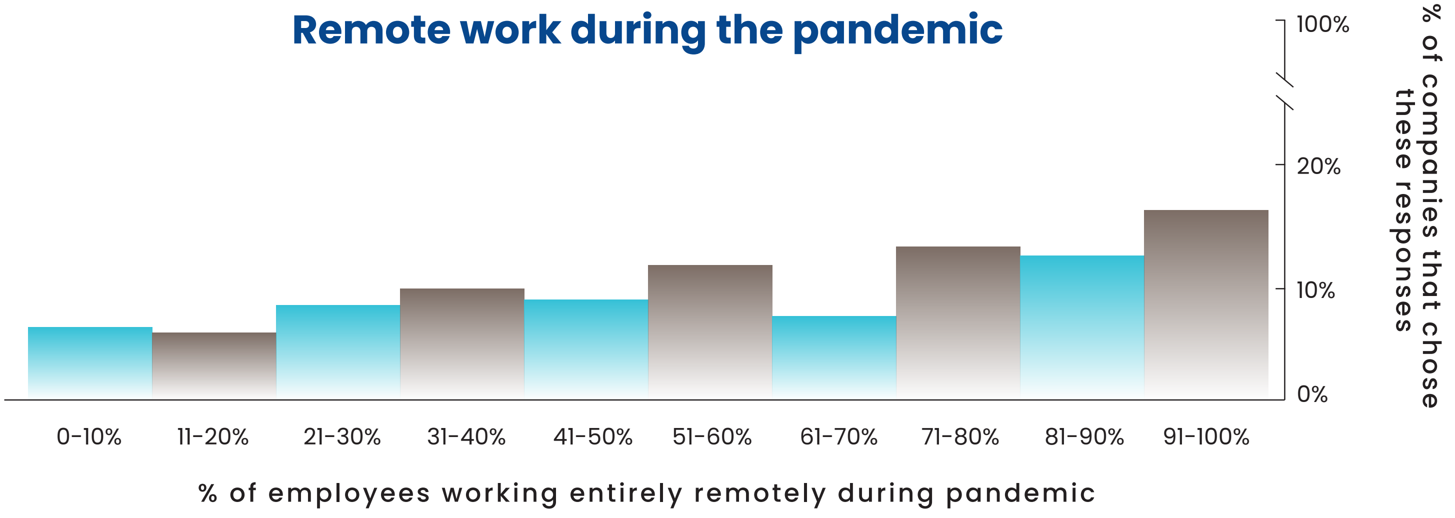


Figure 1

When broken down by company size, organizations with 1,000-4,999 employees have more employees working remotely than any other category (29.5 percent of those companies have more than 51 percent of employees working remotely).

However, when looking at companies with 91-100 percent of employees working remotely, smaller companies, those with 100-999 employees, report the highest percentage of employees working remotely (41 percent of those companies have more than 90 percent of employees working remotely).

Looking ahead to 2022, hybrid work seems to be the future. To level set, according to TAG Cyber's definition, hybrid work differs from remote work in that hybrid workers function part time in the corporate office environment and part time in other, remote locations. Remote work, in contrast, means that the preponderance of time is spent working in out-of-office locations. This does not mean that remote workers will never visit the corporate office, nor does it mean that their working location will be static. However, remote workers are likely to have a dedicated office and spend the majority of their time working from there.

When it comes to post-pandemic working conditions, 60 percent of our survey respondents said they expect fewer than half their companies' employees to work remotely when offices are able to reopen. (Figure 2)

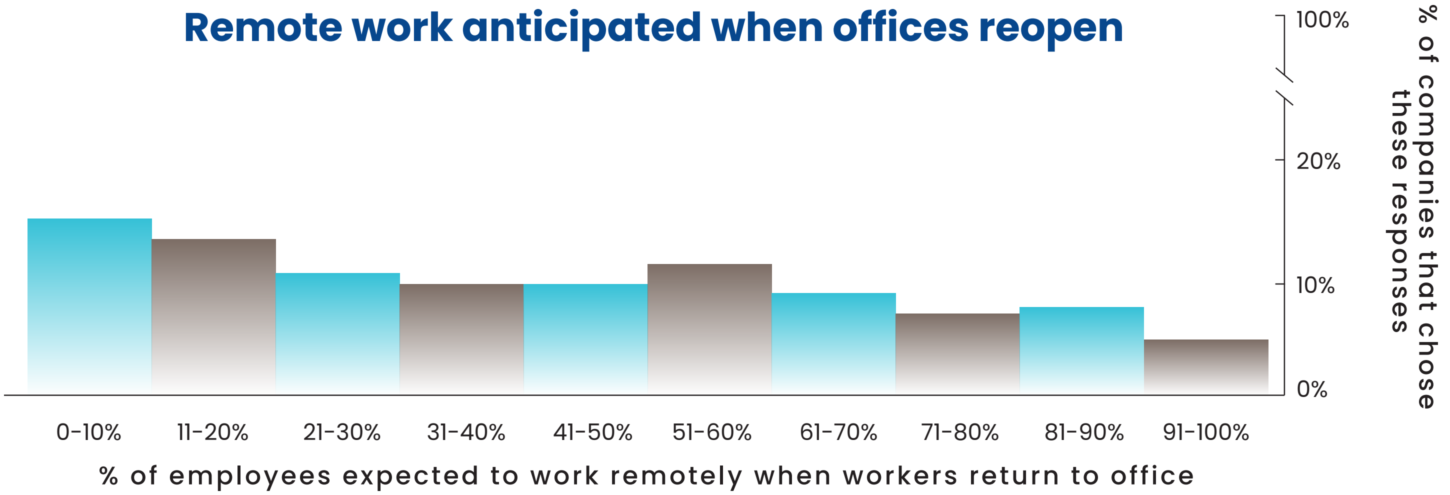


Figure 2

Smaller companies, those with 100-999 employees, are the least likely to anticipate remote and hybrid work. By contrast, companies with 5,000-9,999 employees and those with more than 25,000 employees are anticipating a higher percentage of remote workers in the coming months.

And again, fully remote work is different from hybrid work—where workers are coming in and out of the office and potentially working from various remote locations on their days outside the office, as well as potentially using unmanaged devices to conduct work when they are out of the office. These factors introduce additional risks when combined with a return to the office.

When it comes to the remote work structure alone, a clear majority of our respondents say they are fully prepared for the cyber security implications. Fully 80 percent said they already have a remote cyber security strategy in place, and an additional 12 percent said they are working on it. (Figure 3)

A strategy is one thing, but the ability to execute on that strategy is everything. Far too often in security—

whether it concerns remote or hybrid work—operationalizing plans is a major challenge. Companies lack such essentials as the in-house security expertise necessary; and the budget to hire more internal staff, to hire outside experts, or to acquire the appropriate tooling. The IT and security professionals may lack the power to affect business decisions that would improve security posture.

Do you have a hybrid work cyber strategy in place?

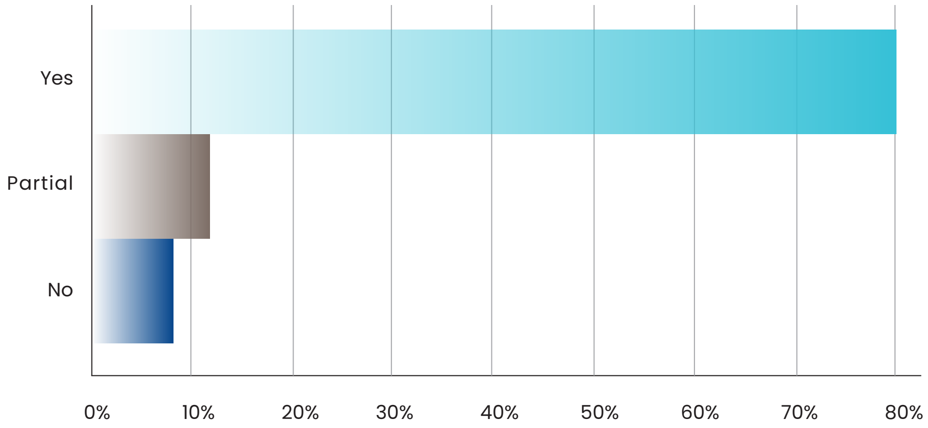
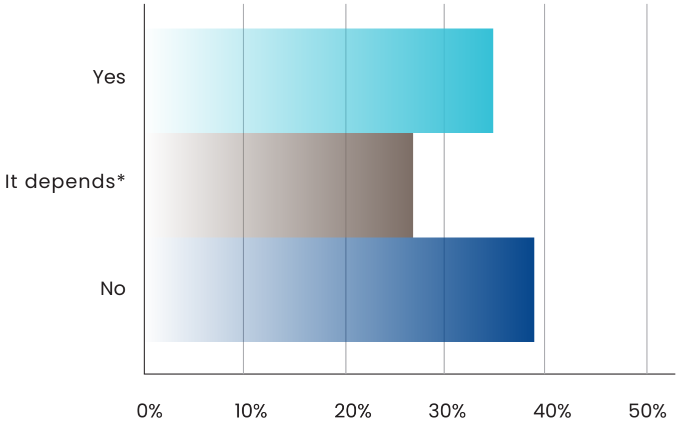


Figure 3

One area that they *are* operationalizing, when it comes to remote and hybrid work, is the management of unmanaged devices like personal laptops, phones, IoT devices, and tablets over which the security team has little to no visibility or control. This is especially true of access to SaaS applications that are now used in business settings. (Figure 4)

Are employees allowed to connect personal or unmanaged devices to corporate resources?



*It depends on the security posture of the device and/or the sensitivity of the resource

Figure 4

According to our respondents, nearly 40 percent of companies draw a line in the sand when it comes to personal and/or unmanaged devices accessing corporate resources. Thirty-four percent said employees are allowed to use non-work issued devices, and another 27 percent said employees can use personal/unmanaged devices for work purposes, depending on the security hygiene of the device. The latter, of course, relies on the company deploying and using appropriate endpoint/device management tools and access controls—not to mention the onsite (or contracted) staff to do so.

We were remiss in our survey design, though, and this potentially calls the results of this answer into question. We should have asked, *How are IT and security departments measuring when and how employees are accessing SaaS applications via unmanaged devices?* Based on our extensive work with enterprises and vendors, we know that a significant number of enterprises do not have full visibility into who or what is being accessed—and how. Especially as it relates to SaaS applications.

Getting deeper into the matter of access, the next question was: *How are you currently securing remote and hybrid worker connections?* Respondents were allowed to choose as many answers as apply. (Figure 5)

Sixty-nine percent are currently using VPNs—an outdated and nominally secure connection method—for remote connectivity.

Tied for second place, at 55.8 percent, are antivirus and firewalls/next-gen firewalls used to help secure employees' connections into corporate resources. Next is multi-factor authentication (MFA), and five points behind is encryption.

How are you currently securing remote and hybrid worker connections?

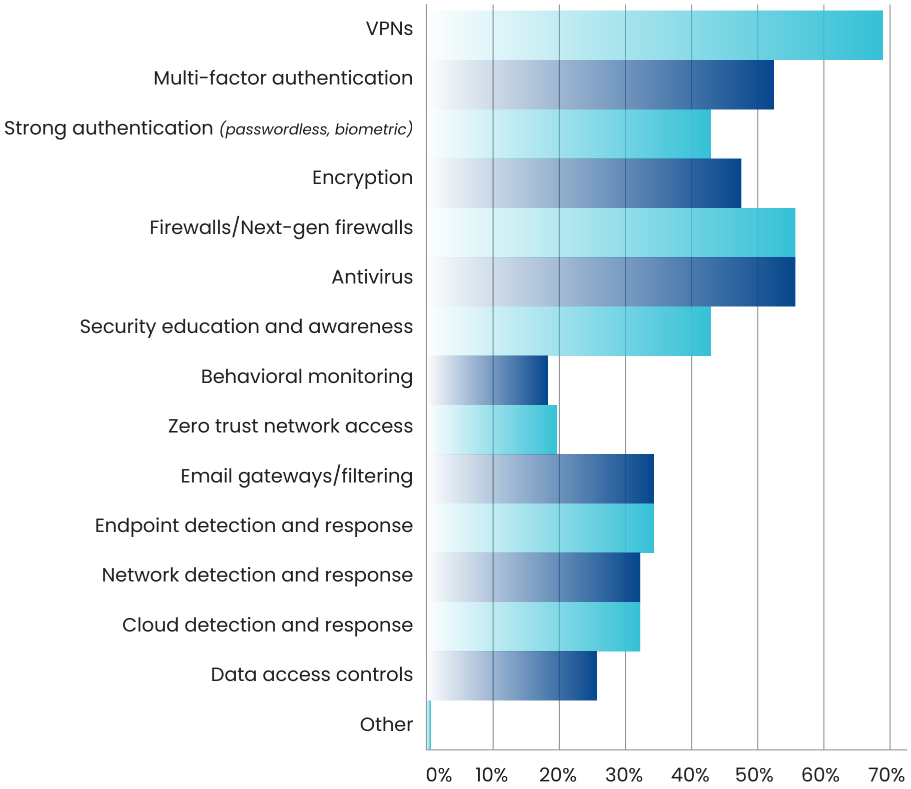


Figure 5

Interestingly, despite the buzz, zero trust network access is currently being used at less than 20 percent of companies. This finding may indicate end users' understanding that zero trust is not a product but an approach. Or it may signal that, despite all the industry hype of moving toward more secure methods of access, namely continuous verification based on context and identity, end users are not yet ready to move their systems away from a "trusted" architecture.

Which of the following will be the greatest risk to your company's hybrid work environment?

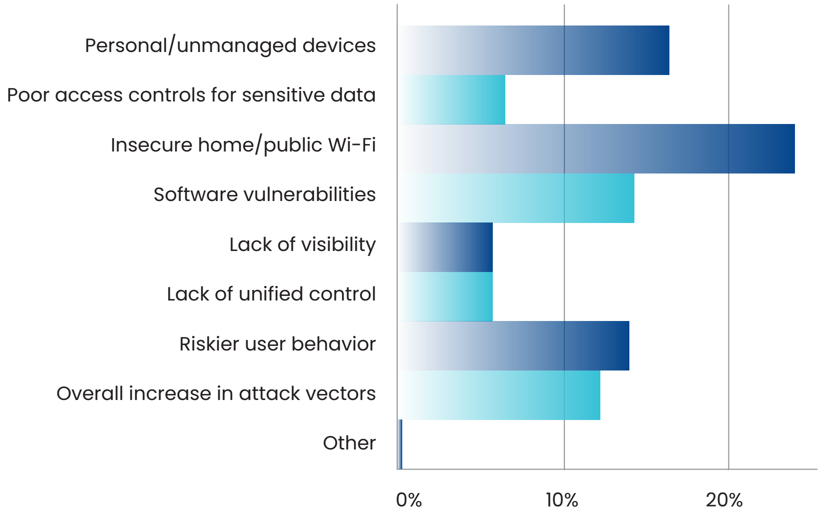


Figure 6

Regardless, the use of numerous security technologies certainly seems valuable to our survey takers. Fifty-four percent reported that their organizations saw an increase in potential attack activity as a result of remote and hybrid work. This is in light of mandated security awareness training for employees at more than 80 percent of organizations.

Looking to the future and the seeming inevitability of increased hybrid work, only 22 percent of respondents said that they do not expect the number of cyber security incidents targeted at their organization to increase as hybrid work increases.

Of the 78 percent who said attack activity will or may increase, the reasons varied. (Figure 6)

In the clear lead is concern over insecure home/public Wi-Fi, with 24 percent of the vote. With this in mind, it would be TAG Cyber's suggestion that these organizations implement zero trust access-based controls, increase use of endpoint detection and response (including built-in device hygiene assessment capabilities), and even consider behavioral monitoring (which, incidentally, was the least selected answer to the question about securing hybrid access).

Not surprisingly, respondents again expressed great concern in their answers over the use of unmanaged/personal devices. Yet, more than a third of respondents said that their organizations plan to allow the use of personal devices in the future—perhaps pressured into doing so by non-security/non-IT use cases—and nearly 50 percent said that their organizations will permit employees to manage applications from personal devices while working remotely.

Given the concern about and risks of infected personal and unmanaged devices (Figure 7), organizations must look for enhanced authentication and access options, predicated on identity (both human and machine) which conform to a zero trust approach.

When it comes to the market's opinion of methods to decrease risk in order to increase cyber security control, 59 percent of respondents said that the solution lies in security education and awareness training (respondents were allowed to choose their top 3 controls). (Figure 8)

Are you concerned about employees bringing infected devices into the office?

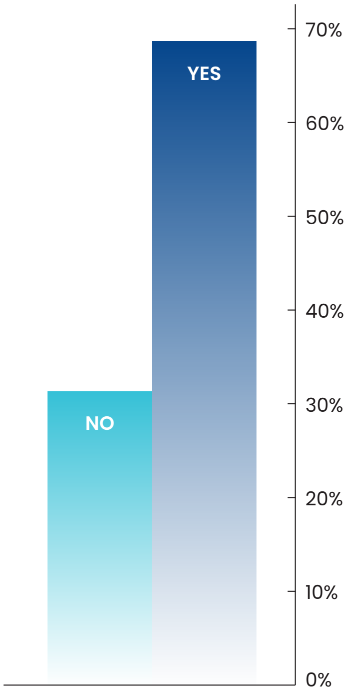


Figure 7

TAG Cyber is a proponent of ongoing education in all areas; however, cyber security must be a combination of people, process, and technology (PPT), led by security experts and not left to unsuspecting users as the first line of defense. We were thus pleased to see that email and endpoint security were ranked highly by respondents (45 percent and 41 percent, respectively), followed by strong authentication (MFA and long, unguessable passwords). Network monitoring, a tried-and-true method of identifying suspicious behavior, fell in the middle of the pack, while secure access service edge (SASE), a category gaining tremendous attention in the vendor community, fell to the bottom of organizations' choices for enhanced security control.

Which approaches do you think will have the greatest positive impact on your hybrid work cyber security posture?

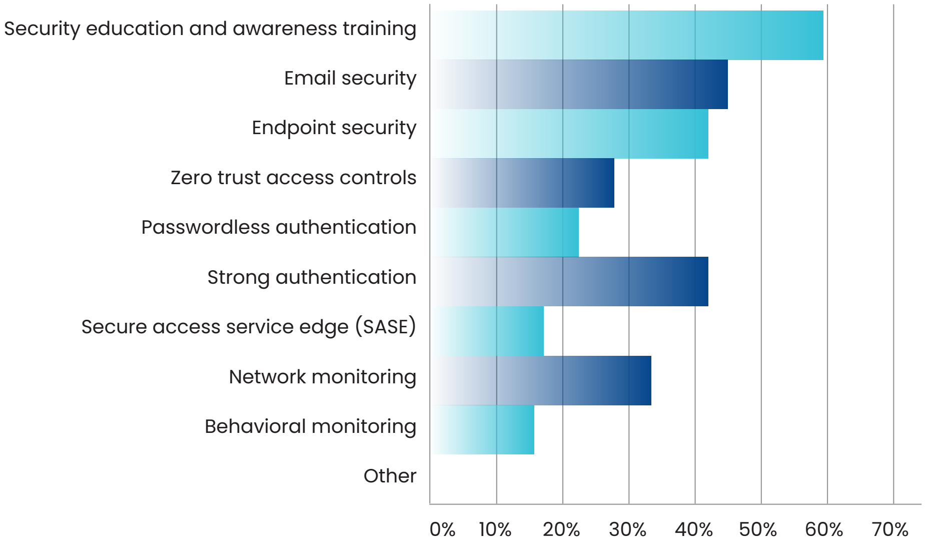


Figure 8

Though this question could have included multiple additional areas of control (TAG Cyber tracks 130+ categories of vendor products), no respondent chose them as a write-in option. With all of the choices on the market, it's a good thing that our survey takers anticipate increased cyber security budgets (72 percent) to tackle the new paradigm of hybrid work.

FIVE CYBER SECURITY TECHNOLOGIES YOU WILL NEED TO SUPPORT HYBRID WORK

EDWARD AMOROSO

As you develop your solution architecture to support work-from-home (WFH) initiatives, you will need to include these five security technologies to avoid any threat consequences.

With WFH comes new cyber protection *opportunities*. As one would expect, this shift has led to products from security vendors that can be quite *helpful*. To help enterprise buyers *find the right tools* amidst the marketing noise, we offer the following list of five security technologies that you will need to support hybrid work. (See our mirror companion piece on five security technologies *you will not need* in this context.)

Zero Trust Network Access – If ZTNA vendors had three wishes from a genie in a bottle, all three would be for WFH to continue its accelerating growth. Developed specifically to address weaknesses in virtual private networks, ZTNA supports secure access from PCs and mobiles to cloud-hosted application workloads. If you currently run a VPN (or God-help-you, a remote desktop protocol [RDP]), then it's time to check out a ZTNA vendor.

Multi-Factor Authentication (MFA) – Yes, you already know all about MFA, but please take a moment to ask yourself this: Are you still accessing a variety of different services using a password – or perhaps just a link to a site? Before you answer no, take a moment to reflect on how you authenticated to your last Zoom call. If things continue to evolve as they have, then MFA will soon become fully ubiquitous. This is good news for MFA vendors.

Endpoint Detection and Response (EDR) – There is a reason why endpoint security is considered so fundamental to zero trust: The surrounding perimeter has vanished, thus leaving your PC, mobile, or other device naked to the Internet. (And yes – this might have been true even with a perimeter, but you get the idea.) EDR solutions are therefore especially well-suited to WFH and the attendant secure access solutions for employees sitting at home in their skivvies.

Application Security – At the opposite end of the session spectrum from the endpoint sits the application. This device-to-app model allows security engineers to restrict their attention away from protecting every resource in the enterprise to the more humble and tractable goal of ensuring security during a zero-trust session. (One observation: Shouldn't the PC be called the starting point and the application called the endpoint? I'm just saying.)

Cloud Security – Just as the application must be secure for WFH, the public cloud infrastructure and associated systems must also be protected from malicious threats. For this reason, Amazon, Microsoft, Google, IBM, and VMWare are now essential components of any zero-trust architecture supporting safe and secure WFH initiatives. This obligation extends to SaaS solution providers as well.

FIVE CYBER SECURITY TECHNOLOGIES YOU WILL NOT NEED TO SUPPORT HYBRID WORK

EDWARD AMOROSO

As you develop your solution architecture to support work-from-home (WFH) initiatives, you will not need these five security technologies to avoid of threat consequences.

With WFH comes new cyber protection *pitfalls*. As one would expect, this shift has led to products from security vendors that can be quite *unnecessary*. To help enterprise buyers *avoid the wrong tools* amidst the marketing noise, we offer the following list of five security technologies that you will not need to support hybrid work. (See our mirror companion piece on five security technologies you *will need* in this context.)

Next Generation Firewalls – The invention of next generation firewalls (NG-FWs) by Nir Zuk and others represented one of the greatest achievements in modern enterprise security. Without this innovation, our industry would have languished to protect local area networks from internet attacks. But WFH initiatives are largely orthogonal to the need to install such devices. Yes, they are necessary for secure access service edge (SASE), but mostly for branch offices.

SD-WAN – Related to the SASE-orientation of NG-FWs, the use of software-defined wide area network (SD-WAN) technology is designed more for branch office replacement of multi-protocol label switching (MPLS). As such, while SD-WAN will certainly be important to the enterprise, it will not be a vital component of WFH initiatives. Secure zero trust network access solutions will be more important.

Network Access Control – Despite the presence of one after another final nails in the coffin for network access control (NAC), the capability continues to demonstrate surprising resilience in the enterprise. This is more than likely driven by the fact that so many organizations continue to operate a perimeter-based local area network. Nevertheless, NAC will not be important for WFH initiatives.

Cloud Access Security Broker – This one might surprise you because cloud seems so natively related to anything considered virtual and hybrid. But CASBs are really tuned to identify cloud and SaaS usage from the enterprise. Admittedly, the API scanning mode for CASBs might help to secure cloud interfaces, but for the most part, CASB – even in the context of SASE – is not important for WFH.

Physical Security – This might not be as obvious as you'd think. While it will certainly be less important for an enterprise team to physically protect its data centers if everything is flying out to some public cloud, a new obligation emerges for WFH. Specifically, employees must be guided to make sure the nosy neighbor doesn't peruse corporate documents while visiting the downstairs bathroom during a barbecue. This is the new WFH physical security obligation.

ARISTA

Arista Networks is an industry leader in data-driven client-to-cloud networking for large data centers, campuses, and other routing environments. The Santa Clara–based company's platforms deliver availability, agility, automation, analytics, and security through CloudVision and Arista EOS, an advanced network operating system. Its customers include global Fortune 500 companies in cloud services, finance, and other large public enterprises.

TAG CYBER
DISTINGUISHED VENDOR

REPRINTED FROM THE TAG CYBER SECURITY ANNUAL