Keeping Your Network Safe in a Hybrid Work Model

Before 2020 only 20% of businesses embraced a "work from anywhere" culture

Introduction

Before the Covid-19 pandemic affected just about every aspect of daily life in 2020, offices had evolved to encourage collaboration and creativity. Individual, walled-in offices were long gone, replaced by open floor plans, huddle spaces, and smart conference rooms. At that time, traditional thinking placed the office at the center of business activities, creating competition for prime office space while also feeding daily commutes.

Before 2020 only 20% of businesses embraced a "work from anywhere" culture[1]. These businesses allowed remote work by enabling employees to collaborate and communicate with workers in the office by leveraging technology; remote network access (VPN), cloud applications, mobile phones and collaboration tools to allow teams to communicate and work together.

Even with the capabilities to allow teams to collaborate, managers were still skeptical of the effectiveness of remote work. Prior to 2020, 80% of companies shunned remote work programs[2]. Citing accountability, building workplace culture and easier project collaboration, companies invested in making their physical areas more conducive to workplace collaboration rather than in tools to enable a distributed workforce.

In March 2020, however, employers were forced to flip the script and support every employee that could work from home, to work from home. The transition was tough on employees and employers alike, and more than two years later, a new normal has evolved and includes enabling employees to work and be productive wherever they happen to be.

The Future of Work

Today, the new normal has employees splitting time between their home and the office and embracing flexible work schedules. In January 2022, 59% of U.S. workers who say their jobs can mainly be done from home are doing so all or most of the time[3]. Additionally, employers realized the effectiveness of remote employees during the pandemic, enabling them to hire and retain the best talent despite their location. A growing share of workers (17%) say relocation to an area away from their workplace, either permanently or temporarily, is a major reason why they are working from home.[3]

The desire to continue to work remotely is expected to remain high. Pew Research found that 78% of workers currently working remotely would like to continue to do so[3]. This desire to work remotely even part of the time has already put pressure on employers. In May 2022, Apple received significant employee pushback when they announced a requirement to return to the office in person three days per week.[4] Apple later walked back on that requirement citing an increase in COVID-19 cases.[5]

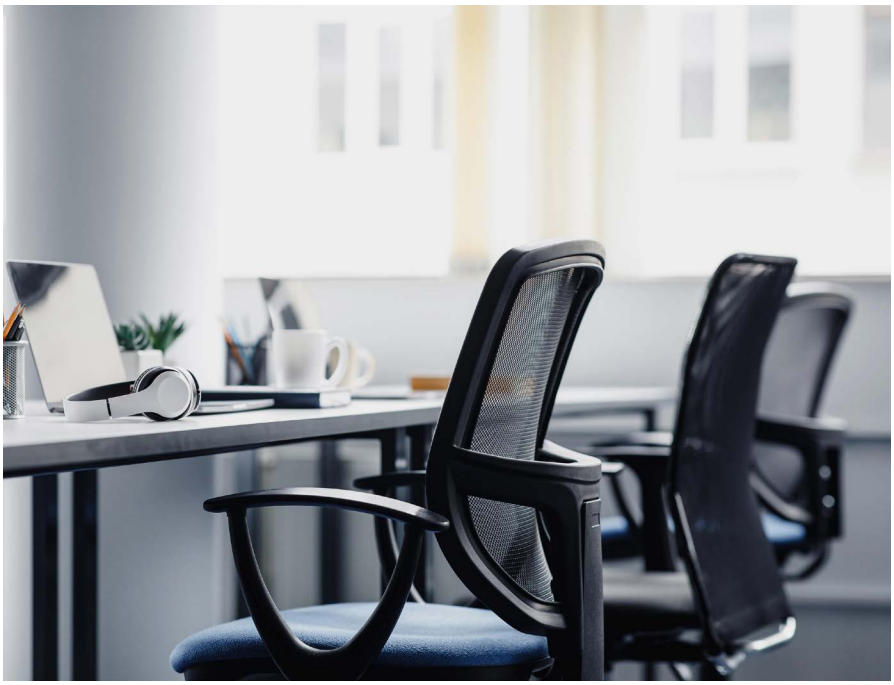
For employees that can perform some or all of their work remotely, the majority will likely have the freedom to continue to do so for the foreseeable future. Network administrators will continue to be responsible to ensure employees have access to the corporate network and the resources they need to be productive, while keeping the network and data protected from evolving cyberthreats. Embracing technology to enable employees to work productively regardless of where they are has also increased the digital attack surface for cybercriminals.

Phishing/Vishing/Smishing/Pharming attacks have increased 34% from 2020 to 2021, and have increased an incredible 1,128% from 2018 to 2021[6]

75% of IT decision makers believe that remote and hybrid scenarios will be the norm in the future[7]

Challenges of Hybrid Work

While hybrid work brings greater flexibility, it also brings new network security challenges. Cyberattacks are still on the rise. In fact, according to the FBI's 2021 Annual Internet Crime Report, Phishing/Vishing/Smishing/Pharming attacks have increased 34% from 2020 to 2021, and have increased an incredible 1,128% from 2018 to 2021[6]. There are no signs that these types of attacks are going to start declining any time soon. In addition, IT teams will need to understand the long term impacts of the hybrid model on network security as 75% of IT decision makers believe that remote and hybrid scenarios will be the norm in the future[7]. Investments made quickly to adapt to a distributed workforce in 2020 may have been enough to keep businesses running. However, now that the work from anywhere model is here to stay, more needs to be done to ensure a secure corporate network.



Companies will need to create plans and new safety protocols to keep their networks and employees safe as they transition between workplaces. While the quick shift to remote work opened the door to cyberattacks, there are also risks associated with employees moving between their home and the office. Security teams will need to be diligent to prevent them from bringing threats back to the office with them.

Most notably, employees could bring malware that is hiding in their laptops, waiting to move onto the corporate network. Employees may have also added unknown software and applications to help them while working from home. While helpful at home, they could prove dubious once on the network.

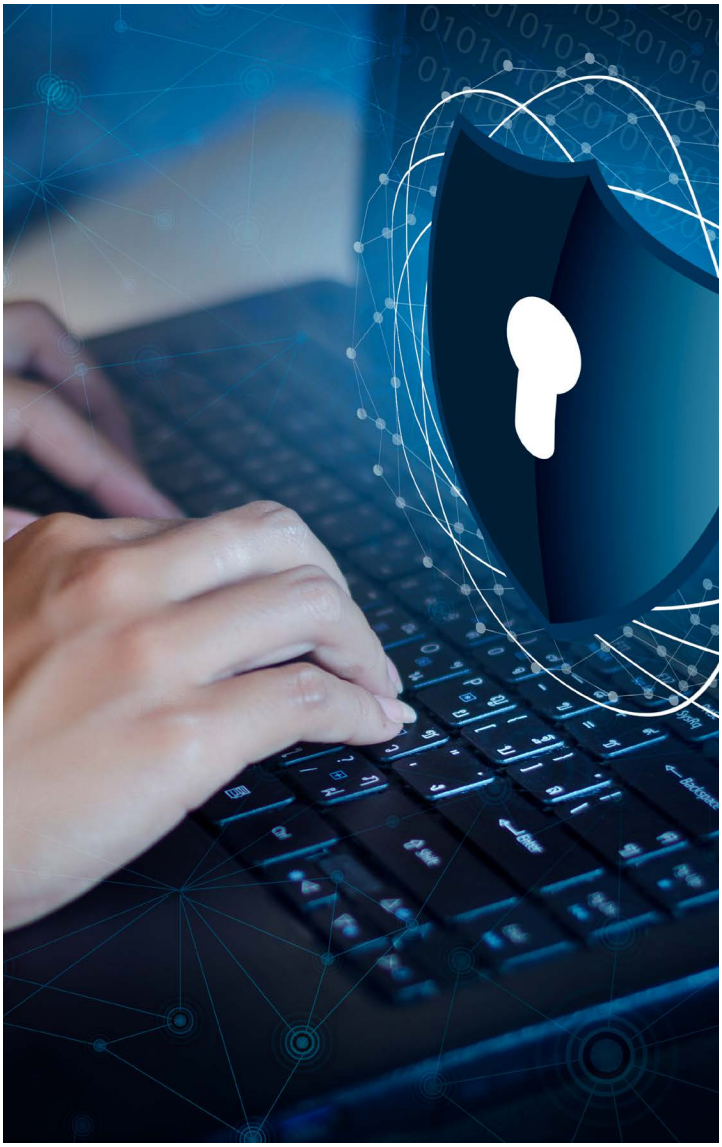
Maintaining a Secure Network

Maintaining a secure network with hybrid workers requires adopting regularly scheduled security procedures to ensure the safety of the network and devices connected. Employees that move between remote working and in the office increase the threat to the network due to connecting to home networks that are not controlled by IT, and are not as secure as the corporate network.

Business leaders and IT teams should begin by implementing the following measures:

1. **Conduct a network audit** quarterly or annually. Use the audit to confirm that all software updates or patches have been properly installed, any firewall configurations on premises or in the cloud have been done so properly, and any employee changes are correctly reflected on the current network.
2. **Continually back up all business-critical data** as well as security configurations or key infrastructure policies in place. This will ensure that there is a readily available network snapshot that can easily be restored if an employee device has been compromised. Daily automated backups are a good policy so that no more than twenty four hours worth of data is lost should there be any type of breach or system downtime.
3. **Conduct employee access reviews** of who has access to what information and whether they really need it. This is especially important as employees move between their home network and corporate network with more software, personal applications and data on their devices. It's much safer to take a zero-trust approach of denying access to everything, unless it's specifically needed, and specific access is given.
4. **Provide consistent, clear communication to employees** of protocols and steps to follow to keep their devices safe and clean from malware. Each employee should periodically update their login credentials, using strong password combinations and two-factor authentication where available. Employees should also review the standard cybersecurity policies in place, with extra attention paid to spotting phishing emails or suspicious activity.

5. **Review applications**. Companies worked hard to meet employees' needs while working from home. This included extending the use of corporate devices, such as laptops, for other personal use, such as online learning. Rules may have been relaxed in terms of web filtering and application control while employees were working at home. With a hybrid model, those leniencies should be rolled back and standard company policies regarding device usage should be enforced.
6. **Provide vendors with updated security guidelines** regarding supported and non-supported computers, laptops and devices that can access your corporate systems. Vendors who regularly access networks and corporate data systems will need to adhere to the security protocols that you have in place.
7. **Treat all returning endpoints as high risk** and scan all devices. Cybercriminals often target endpoint devices making it imperative that all endpoints are regularly scanned to ensure no malware or other latent risks are waiting to move to the network. In addition, ban USB and personal storage devices on corporate computers and systems, due to their easy corruption with malware.



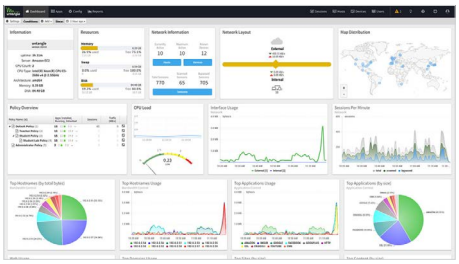
Bringing employees together, whether in the office or via technology is crucial - the camaraderie, collaboration, and culture of a business emerges when employees are able to interact with each other in person. While the future of work was shaped by the pandemic and increased acceptance of hybrid work, it is essential that network administrators continue to adopt policies and protocols for the new workplace.

Sources

1. https://www.pewresearch.org/social-trends/2020/12/09/how-the-coronavirus-outbreak-has-and-hasnt-changed-the-way-americans-work/
2. https://www.prnewswire.com/news-releases/new-study-nearly-one-third-of-workers-expect-to-work-remotely-full-time-after-the-pandemic-301081827.html
3. https://www.pewresearch.org/social-trends/2022/02/16/covid-19-pandemic-continues-to-reshape-work-in-america
4. https://www.cnet.com/news/apple-employees-criticize-return-to-work-plan-call-for-more-flexibility/
5. https://www.cnet.com/news/apple-delays-plan-to-have-employees-return-to-offices-3-days-a-week-report-says/
6. https://www.ic3.gov/Media/PDF/AnnualReport/2021_IC3Report.pdf
7. https://www.scmagazine.com/endpoint-security/organizations-look-ahead-to-2021-return-to-office-refocus-on-hybrid-security/

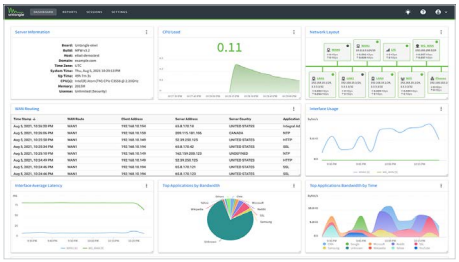
About Arista Edge Threat Management

Arista's Edge Threat Management solutions help small-to-medium businesses and distributed enterprises optimize their networks while safeguarding their data and devices. Edge Threat Management provides cloud-managed security and connectivity options that work together seamlessly to ensure protection, monitoring, and control across the entire digital attack surface from headquarters to the network edge. The award-winning products are trusted by thousands of customers and protect millions of people and their devices. We are committed to bringing open, innovative and interoperable solutions to customers through a rapidly growing ecosystem of technology, managed services, and distribution partners worldwide.



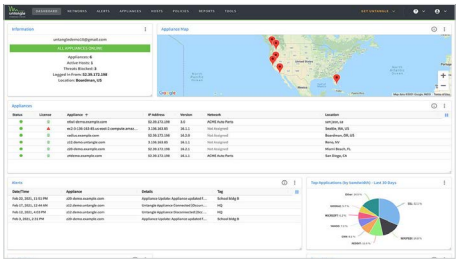
Advanced Security

- Protection, encryption, control & visibility anywhere
- NG Firewall, IPS, VPN & more
- Onboard security for small network appliances & IoT devices
- Full security processing on-premises or in the cloud



Intelligent Edge Optimization

- Secure, WAN-optimized connectivity for every location
- Seamless scalability
- Optimal predictive routing technology for first packet, dynamic path selection
- Centrally manage one or many appliances



Cloud Management at Scale

- Zero touch deployment
- Configure & push policies
- Advanced alerting & reporting
- Visibility across globally dispersed networks & endpoints

Santa Clara—Corporate Headquarters
5453 Great America Parkway,
Santa Clara, CA 95054

Phone: +1-866-233-2296
Email: edge.sales@arista.com